Overview of Current Developments in Network and Information Security Technologies

ENISA/TD/ST/D(2007)0006

Executive Summary

This report provides a snapshot of recent technical developments in the area of network and information security technologies. The focus is on emerging technologies, their security implications and challenges, and bodies where those are addressed, as part of a broader effort made by ENISA, in accordance with its mandate, to maintain tracking of standardization work and other activities related to network and information security.

The report assumes the reader has some information security background. The report is meant to give insight on how to inject security issue as soon as possible in currently emerging application. It is also meant to be used as a basis for developing Position Papers aiming at a wider audience as part of the ENISA Work Program 2007

The report is structured into two parts.

Part 1 is a summary of observed developments in network and information security (NIS) technologies, gathered by ENISA by Internet research, mailing list monitoring, in particular related to standardization activities in a number of fora (Annex 1), dialogue with the security community, and participation in a few relevant fora meetings. It looks into new **developments of security tools and strategy** (Section 1). It then concentrates on a few information and communication (IC) emerging technologies and applications, examining the security challenges they face and the security solutions they require (Section 2).

Part 2 (Annex 1) contains **an inventory of fora which are active in the network and information security arena**, with a list of their **activities and relevant documents** (with particular focus on standard specifications).

Development of Security Tools and Strategy

Cryptography is one of the building blocks of security (Section 1.1). Continuous efforts in research and standardization need to be promoted in this field, to address new threats and the need for dedicated solutions for emerging technologies and scenarios, as well as to continuously improve the techniques so to be able to withstand an always-improving crypto-analysis. Open competitions for algorithm selection (such as the one undertaken by NIST for the selection of a new hash function) and promotion of collaboration among researchers (such as the EU ECRYPT network of excellence) are useful tools in this direction.

The main recent development to be noted in cryptography is in the field of ***hash functions*** (Section 1.1.1), one of the fundamental crypto components. Following the successful attacks of 2004 and 2005 on well-known and used hash functions, the security community is now looking for a better way to migrate towards stronger functions, and envisages the design of new secure hash functions. The US NIST has

published an open competition in order to design a new hash function, following the successful way the crypto algorithm AES was designed.

The need for an efficient, secure ***stream cipher*** (Section 1.1.2) has been voiced for some time now. The design for a new stream cipher sees for the time being a lot of efforts in research. Other fields where further work is needed include (Section 1.1.3 and Section 1.1.4) cryptography for high speed implementation (e.g., for real-time communications including multimedia but also process control systems' communications), lightweight and low power cryptography (e.g., for RFID and sensors), long term security, and privacy-enhancing cryptography. A need for optimized and fast protocols can also be reported.

A few new developments are important to enlighten in the field of network security. Basic infrastructure components such as ***routing*** (Section 1.2) and Domain Name System (***DNS***, Section 1.3) are in the focus of the security community's efforts since they are often pointed out as some of the weaker points of the Internet infrastructure. Often we hear about the need to re-enforce security at the end devices. However, the infrastructure is more and more a fundamental building blocks to secure, especially with the dramatic increase of ICT dependability and the dissemination of intelligent tools in the system. It turns out that this infrastructure is largely not secure today, and it is likely to be one of the next targets of attacks. The existing DNS security solution (DNSSEC) has not yet taken off, although new activities are re-launching it. However, DNS has been lately a vector of attacks and much attention is now turning to the need for a complete, working security solution for DNS embracing the DNSSEC bootstrap but also the security of the DNS infrastructure at large. Routing security is a complex technical area but in need of a rapid solution. It is now standardized in IETF, first gathering requirements and now looking at workable solutions. Best practices exist (e.g., simple filtering of unnecessary traffic), but they seem not yet extensively implemented, hence the awareness level should be raised. Furthermore, the current status of security breaches to the fundamental components of the infrastructure, such as DNS and especially routing, is not known: a systematic reporting should be encouraged.

The ***spam issue*** (Section 1.4) has already attracted a lot of attention, as it concerns users directly; however the issue is now receiving even higher attention since spam is turning into more than nuisance. E-mail spam has been lately the carrier of *phishing*, which, using social engineering, may lead to exposure of sensitive personal information and financial losses. In addition to many activities gathering best practices, some initiatives can now be observed in the field of ***e-mail authentication***, in order to implement *anti-spoofing* techniques hence reducing spam and phishing. Two emerging techniques are SenderID / Sender Policy Framework and DKIM, now under standardization in IETF.

The lack of ***Identity Management*** (Section 1.5) solutions, which provide efficiency, security, flexibility, and user-friendliness, is often pointed out as one of the issues at the base of many problems that the Internet faces today. Privacy concerns require

novel technical approaches (Privacy Enhancing Technologies, PET), but also an interdisciplinary approach to analysis, including economic and social considerations. Within the broader area of identity management and authentication, ***biometrics*** (Section 1.5.1) has recently been highlighted, mainly for its use in applications such as the e-passports. Biometric techniques require improvement as they are prone to errors and bypassing, but also lack in need of privacy and ethical guidelines.

The trend towards ***de-perimeterization*** (Section 1.6) continues. De-perimeterization is the strategy of redesigning the security perimeters, in order to promote collaboration and information sharing beyond such obsolete perimeters. The observation is that traditional approaches to network security (such as security at the perimeter) do not cope with the new business reality, characterized e.g. by high user mobility, open and shared networks due to outsourcing and partnerships, and physical dispersion. An emerging de-perimeterization practice is then ***endpoint security***, where endpoints connecting to a network are scanned for a "health check" in order to verify if their security status is aligned to the local security policies, thus allowing the network to protect itself.

Trusted Computing (Section 1.7) is an emerging technology where the device can be considered as trusted. This allows the device to become an enabler for many applications in need of a trusted platform underneath, e.g. trusted downloads (including software updates), secure communications, secure storage, reliable peripheral identifications (e.g. of added parties), access control, and endpoint security. The technology is still at its beginning and has many supporters in the industry, although it has also raised criticisms by a few security experts, warning about the possibility that Trusted Computing may take away the control from the user in favor of the owner of the Trusted Computing infrastructure.

ICT developments impacting on security

The report identifies IPv6, wireless systems, RFID, and Voice over IP as emerging technologies. Some of them are not new technologies, but they are evolving, steadily increasing in usage, although they still require experimentation. The trend that we observe is a move towards the combination of these technologies, leading to network pervasiveness (including ubiquitous computing). Another observed trend is the convergence towards the IP technology (the Next Generation Network, NGN). All of this makes that the technologies cannot be considered isolated but need to be considered and evaluated as components of services and other technologies.

IPv6 (Section 2.1) has a long design story; its adoption is still cautious but it is clear to the community that IPv6 will be needed in the long run, especially with the predicted appearance of new ways of communication such as extensive multimedia and machine-to-machine. IPv6 can also fully enable the potentials of new technologies such as 3G/B3G/4G and WiMAX. We often hear that IPv6 brings along higher security; this may happen in the long run, but in the short term IPv6 may still need experimentation also from the security point of view.

Wireless systems (Section 2.2) are gaining momentum. Hotspots are multiplying, and the offered bandwidth is increasing, making the wireless access one of the most convenient and available type of access, also suitable for new applications such as Voice over IP (VoIP) and multimedia, but also for enterprise access and access to critical infrastructure. As past experience has shown, wireless is by its own nature a link highly susceptible to security attacks. A large adoption of wireless technologies needs to be accompanied by adequate security and user awareness. On the mobile service side, the network sees the convergence towards the IP Multimedia Subsystem (IMS) and the Next Generation Network (NGN). Devices are becoming smarter and equipped with higher capabilities, once more offering new attack surface that needs to be addressed with priority, given the increasing adoption rate of mobile services. Finally, new wireless technologies are appearing, and their security implications need still to be fully assessed (for examples, RFID, wireless sensor networks, software defined radio). This will be challenging due to the criticality of the applications. Activities of deployment and dissemination fora (existing examples are the Wi-Fi Forum and the WiMAX Forum) should be promoted, as they enhance interoperability and can offer product certifications which includes security.

RFID (radio frequency identification, Section 2.3) is yet another wireless technology, but we felt it deserves a special emphasis. There is indeed increasing interest among technicians for the possible applications it may have, but also among citizens' organizations and regulators for possible invasion of privacy. Primarily intended for automated identification of objects, the RFID technology now sees a multiplication of applications where RFID is to be deployed, and it is paving the way for *ubiquitous computing*. However, security, and in particular privacy, related to the use of RFID are aspects that need urgently to be investigated and addressed, if the technology is to take off. In fact the technology is perceived controversial, and this may prevent its widespread acceptance. The most urgent action here appears to be the opening of a dialogue among the different stakeholders, including consumers, to clearly set the security (in particular, privacy) requirements.

Voice over IP (VoIP, Section 2.4) is the application growing at the fastest rate, getting common among users (see for example the popularity of Skype and similar VoIP clients), but also among enterprises, which are promoting the merging of their telephony and data networks. The use of VoIP is expected to grow further with the take-off of IMS, as well as with the spreading of access technologies such as 3G, Wi-Fi, WiMAX, and broadband. VoIP has somehow paved the way for similar, advanced interactive applications, which extend far beyond the digital transmission of voice only – ***multimedia***, which is also a strong driver for infrastructure evolution (e.g., 3G, IPv6, NGN). Although being among the fastest growing applications, VoIP and multimedia are often pointed out as applications that can expose security problems. This raises concern among many parties, given the high adoption rate of these applications. The worries increase when considering the possible dependency of critical government services on VoIP. Standardization bodies have started working to define solutions for VoIP and multimedia applications, as the report describes. These

efforts also belong to the more comprehensive work on Next Generation Network (NGN).

The ***Next Generation Network*** (NGN) is the emerging telecommunication architecture (Section 2.5). Also known as Converged Networks or Fixed Mobile Convergence (FMC), NGN is expected to introduce a substantial evolution in the communications landscape. NGN offers many advantages – transport and signaling decoupling, quality of service, distributed architecture, access independence, unified core network, to name a few – and represents the seamless evolution towards an "all-IP" network, which can fully support the new, bandwidth-demanding, feature-rich ways of communicating (e.g., multimedia). Major standardization bodies are focusing on the NGN design, e.g. ITU-T, 3GPP with the design of the IP core (the IP Multimedia Subsystem, IMS), and TISPAN designing the fixed access converged networks. Security is one of the critical components of NGN, and has been identified by ITU as an essential NGN enabler and differentiator. We summarize some of the security issues that are specific to this new architecture, gathered by observing primarily the debate in TISPAN, 3GPP IMS, and IETF.

Introduction

The existing activities in the area of network and information security (NIS) are many. This also reflects the increased attention that security has received in the recent years -- among users, more aware of security risks also thanks to press coverage, among governments, facing for example the issue of infrastructure dependability, and among industry, whose demand for business continuity requires security in place and who has to face customers' higher security demands. Security management is also gaining visibility among organizations' top management[1], implying higher commitment and new impulse in technical development. Furthermore, the migration toward the Internet Protocol (IP) technology as common base technology for communications has contributed to the emerging role that security has in the information and communications technology (ICT) landscape. In fact, the IP technology is often associated with the threats that occur in the open Internet, which has gained a very poor reputation for its security, exacerbated by media headlines that raise the users' awareness. Hence, the use of IP as common communications platform requires appropriate security solutions, and efforts are on-going in the area in order to mitigate the risk that such IP threats can extend into the next ICT generation, with broad impact on the society.

Standardization is an important process for security. Products that claim to adhere to a standard can be checked against it, thus transparency is improved as well as the interoperability of technical and procedural solutions. This drives for a strong impulse towards security standardization, although the multiplication of security activities has also brought the counter effect of fragmentation – the activities are scattered among many groups and the degree of collaboration and coordination is often not enough, nor it is easy to identify which particular activity is undertaken and where.

This study looks at different groups involved in the NIS area and at their activities.

It focuses on a series of emerging technologies[2] both from the point of view of security tools and of technology or application impacting security (Sections 1 and 2), identifying the role that these groups play in each domain. It also builds an inventory of such groups in the second part (Annex 1). The current version of the study focuses on standardization activities. The next versions will also explore some additional aspects of emerging technologies related to security, such as R&D activities as they are developing in Europe.

[1] ENISA Quarterly, June 2006, UK Information Security Breaches Survey 2006, pages 15-17.
[2] The word "*emerging*" in this report is equivalent to "under development" or "commercially spreading but not yet completely defined or at its full capacity"; it denotes something (a technology, an application, etc, but also a threat) that is expected to appear or that may be already in place but is still expected to grow further.

1. Development of security tools and strategies

1.1. Cryptographic primitives[3]

1.1.1. Hash functions

Hash functions are one of the fundamental building blocks of information security, being them used as cryptographic primitives in the majority of security functions and applications[4]. Hash functions are broadly used in authentication and integrity tools, digital signatures, encryption, and security protocols. Therefore, it is not surprising that the attacks on hash functions have been a centre of attention for the security community in the latest years. In August 2004 a number of attacks to different common hash functions (including MD5 and SHA-0) were presented, and attacks to SHA-1 (the most popular hash function today) were announced during year 2005. Message Authentication Codes (MACs) such as HMAC seem for the moment not in danger, although they are predicted to be scrutinized next[5].

The promotion of a cautious but not panicking migration from those hash functions is general advice of experts. While MD5 is now discouraged, SHA-1 can still be used although new protocols are encouraged to prefer other stronger hashes, as well as existing protocols to migrate towards stronger alternatives. One recommendation[6] is the NIST "SHA-2" family of hash functions[7] (SHA-224, SHA-256, SHA-384, and SHA-512), especially for digital signature applications.

Security communities are meanwhile encouraging research for new, stronger hash functions. NIST is involved in dedicated workshops[8] and in an open hash function competition similar to the one held for the selection of the Advanced Encryption Standard (AES) algorithm[9]. IETF is evaluating the use of hash functions within the Internet protocols, encouraging for the migration to stronger hashes and looking at how the IETF might need to change the protocols[10] (e.g., if they rely on the collision-resistance of particular hash functions). However, experts point out that it is not yet clear which stronger hash algorithm will be a good choice for the long term and that the hash migration implies interoperability issues[11]. It is therefore important for

[3] The word "primitive" designates basic mechanisms that cannot be divided and are combined to set up a cryptographic tool, e.g. algorithms.
[4] For a definition of hash function, see Menezes, van Oorschot, and Vanstone, Handbook of Applied Cryptography, CRC Press, 1997, ISBN 0-8493-8523-7, or http://www.cacr.math.uwaterloo.ca/hac/
[5] http://eprint.iacr.org/2006/187
[6] NIST, http://www.csrc.nist.gov/pki/HashWorkshop/NIST%20Statement/Burr_Apr2006.html
[7] NIST FIPS180-2, Secure Hash Standard; RFC3874, A 224-bit One-way Hash Function: SHA-224; RFC 4634, US Secure Hash Algorithms (SHA and HMAC-SHA).
[8] http://www.csrc.nist.gov/pki/HashWorkshop/index.html
[9] Selection of the Advanced Hash Standard (AHS), http://www.csrc.nist.gov/pki/HashWorkshop/timeline.html
[10] IETF draft, draft-hoffman-ike-ipsec-hash-use
[11] IETF RFC 4270, Attacks on Cryptographic Hashes in Internet Protocols, http://www.ietf.org/rfc/rfc4270.txt

protocols to have the ability to upgrade to new functions, as well as to offer communication parties the possibility to negotiate (agreement) on their preferred primitives[12].

1.1.2. Stream Cipher

Stream ciphers[13] present different features from block ciphers (which generally are the most used ciphers, e.g. AES), including speed, hardware complexity, error robustness, bandwidth, which make them more suitable for certain scenarios, such as heterogeneous (wired and wireless) environments, and for applications such as real-time applications (e.g. voice over IP and multimedia). However, stream ciphers may be easier to encounter security problems if used incorrectly[14]. A common stream cipher is RC4, which however has proven vulnerable to attacks[15] when used in certain ways (RC4 is also at the base of the Wired Equivalent Privacy algorithm, WEP, for 802.11 wireless networks, which has shown critical flaws). A few ciphers used by 3GPP also belong to the stream cipher category. It is also practice to implement stream ciphers using block ciphers in certain modes, for example AES in counter mode, which is today the emerging stream cipher for high-speed implementations.

The security community has expressed the need for new, secure, and efficient stream ciphers, and design efforts are on-going. The EU research project New European Schemes for Signatures, Integrity and Encryption (NESSIE), 2000–2003, identified a set of secure cryptographic primitives[16] but could not select any stream cipher. The EU ECRYPT project has recently undertaken the effort (the ECRYPT Stream Cipher Project, eSTREAM[17]) of evaluating candidates for the selection of new stream ciphers, which could gain widespread adoption and could be suitable for different application profiles (for software applications with high throughput requirements, and for hardware applications with restricted resources). The project is currently in its second phase and will be complete at the beginning of 2008.

[12] IETF draft, draft-hoffman-ike-ipsec-hash-use
[13] For a definition of stream cipher: Menezes, van Oorschot, and Vanstone, Handbook of Applied Cryptography, CRC Press, 1997, ISBN 0-8493-8523-7, or http://www.cacr.math.uwaterloo.ca/hac/
[14] See the Handbook of Applied Cryptography, note above.
[15] Among the others, the Fluhrer, Mantin and Shamir attack, see also http://www.wisdom.weizmann.ac.il/~itsik/RC4/rc4.html
[16] https://www.cosic.esat.kuleuven.be/nessie/ https://www.cosic.esat.kuleuven.be/nessie/deliverables/decision-final.pdf)
[17] http://www.ecrypt.eu.org/stream/

1.1.3. Algorithms for high speed applications

The emergence of high speed rate applications, such as advanced real-time applications and process control systems' communications, coupled with the increasing availability of high-bandwidth connections, have put forward the need of fast security algorithms. This need is motivated by the fact that if security has an impact on the overall performance or cost, then the risk is that security will be penalized or simply switched off.

Counter mode (CTR)[18] has emerged as the preferred encryption method for high-speed implementations, as it can be pipelined and implemented at high data rates. AES-CTR[19] has been for example adopted in IPsec (IETF RFC 3686), and in secure multimedia applications (the Secure Real time Protocol, IETF RFC 3711).

Similarly to the ciphers' case, the need for a fast hash and authentication message code (MAC) has been voiced in the last years, since the most used MAC, HMAC (RFC 2104), does not offer enough high speed authentication. Lately UMAC, designed for high performances in software, has been standardized (IETF RFC 4418), but needs yet to enter deployment phase.

A recent trend that can be observed in standardization is the promotion of cryptographic algorithms offering *combined encryption and authentication.* Security protocols often provide confidentiality and message authentication using separate algorithms and independent keys. However, the use of a single cryptographic algorithm providing both confidentiality and authentication is now accepted by the security community[20]. There are several such cryptographic algorithms standardized, and a few of them can be used when a fast hash (which is still lacking, as said above) is required, since they enable high-speed implementations in hardware. AES in Galois/Counter mode (GCM) is one example of combined cryptographic algorithm; it has been added for example to IPsec, in order to enable high-speed implementations in hardware (IETF RFC 4106).

[18] NIST SP 800-38a, Recommendation for Block Cipher Modes of Operation, Methods and Techniques http://csrc.nist.gov/publications/nistpubs/800-38a/sp800-38a.pdf
[19] http://csrc.nist.gov/CryptoToolkit/modes/workshop1/papers/lipmaa-ctr.pdf
[20] See e.g. IETF draft "Authenticated Encryption", draft-mcgrew-auth-enc.

1.1.4. Other challenges

Several issues in cryptography are still at the stage of research. ECRYPT has identified the challenges for cryptology research in Europe for the period 2007-2013 and beyond[21]. Identified challenges include "*crypto-everywhere*" (to provide security for pervasive computing), *long term security* (e.g. to protect medical and financial data), and *privacy* (e.g. cryptographic solutions for privacy in location based services, mining technologies, and e-voting). ECRYPT has also identified a need for further research in the area of *lightweight and low-power cryptography*, i.e. security algorithms and protocols for constrained environments (e.g. RFID, sensors, and satellite), and in the area of security for hostile environments such as wireless sensor networks.

The need for fast processing cryptographic algorithms discussed in the previous section is also identified at the level of *protocols*. For example, this has strongly emerged in IETF, e.g., in the real-time multimedia area, and promises to surface in other areas such as process control systems' communications, where the real-time aspect of the communication and the reaction time are critical. Low bandwidth consumption is another requirement that often accompanies the need of fast processing. Sometimes these needs are the result of requirements set by Standard Development Organizations (SDOs) such as 3GPP, for which performance is a critical component given the different constrains of their environment (e.g. bandwidth and delay). Key management in particular is a cumbersome component, as it often requires many roundtrips and heavy computation.

Fora

Work on cryptography is scattered among several bodies. NIST (with the publications of the FIPS standards) and ISO are among the bodies publishing standards for cryptographic algorithms. There are then the bodies defining the algorithms for their specific technology, for example SAGE is in charge of the design of the algorithms involved in the different ETSI works (including involvement in the design of the 2G/3G algorithms for 3GPP). IETF makes extensive use of cryptographic algorithms within its protocols, in general by referring to standards from the other SDOs and defining the use of that specific algorithm within a protocol. IETF has also a few Requests for Comments (RFCs) on algorithms.

The academia is very active in the cryptographic area. The Internet Research Task Force (IRTF) Crypto Forum Research Group (CFRG)[22] is dedicated to discuss and review new cryptographic developments for the future Internet. ECRYPT[23] is the European Network of Excellence for Cryptography. ECRYPT belongs to the EU Sixth Framework Programme (FP6) and has the mission to intensify the collaboration

[21] http://homes.esat.kuleuven.be/~preneel/ecrypt_vision.pdf
[22] http://www.irtf.org/charter?gtype=rg&group=cfrg
[23] http://www.ecrypt.eu.org/

of European researchers in information security, specifically in the field of cryptography.

Discussion

Cryptography is a critical area for network and information security, being one of its building blocks. Continuous efforts are required in order to **promote research and standardization in cryptography**. Firstly, because algorithms are continuously scrutinized and have generally a lifetime, and because attack tools continuously improve. A wise security practice is always to add stronger alternatives, or provision for such addition, and migrate to these better alternatives when needed. Secondly, because the fast pace changes in IC technologies bring new threats, and call for a continuous security assessment of the deployed systems and for a continuous effort in improving the available cryptographic tools. New applications appear, and they show the need for optimized, dedicated security solutions.

The open competition for algorithm design has shown to be highly successful, e.g. in the AES case. Similar new initiatives should be encouraged, as they are a key to lead to results that are more secure, not with local but global validity, hence contributing to raise trust. Similarly, an initiative like **ECRYPT, facilitating the collaboration of top European researchers, should continue to be promoted**, to contribute improving Europe's competitiveness.

"Just use IPsec"?
IETF has pointed out that IPsec is not the solution to all security problems, nor is a plug&play security tool. Failures to understand this would just leave users to non-interoperable IPsec implementations[24].

[24] Bellovin, Guidelines for Mandating the Use of IPsec, draft-bellovin-useipsec

1.2. Routing Security

To date, the routing infrastructure and the routing protocols remain largely unprotected and open to attacks, although without major damage: the rate of attack reporting to law enforcement on routing security is still low, but the only report of few notorious misconfiguration incidents give an indication about the impact that attacks could have. Current mitigation measures are based on basic techniques and best practices, and include route filtering (e.g., ingress and egress filtering, and implementing access control lists, RFC 2827), BGP blackhole routing (RFC 3882), passwords, and TCP authentication.

The increased dependability of ICT on interconnected networks and the Internet calls for the reliability of such infrastructures, for which routing is a fundamental component and the lack of adequate security for routing has surfaced in the last time.

Routing technologies are quite different according to the application domain. Unicast routing includes Interior Gateway Protocols (IGPs) within a domain, and Exterior Gateway Protocols (EGPs) or Inter-domain protocols, among domains. Multicast and broadcast routing protocols have emerged, as well as routing for wireless, mobile, and ad-hoc networks. All these domains present specific requirements, specific network composition assumptions and consequently, different, often changing, trust models. As a consequence, routing security is a complex technical area, where efficiency is generally the prioritized functionality, often conflicting with security. Routing protocols such as the Border Gateway Protocol (BGP) can become vulnerable to several forms of attacks (e.g. DoS, re-routing leading to traffic analysis, modifications, masquerading[25]). It is also a matter of uniform security deployment, since the problems can be mitigated only if security is implemented in all routers.

A number of activities to secure the routing infrastructure and protocols have started, led by IETF. IETF is facing the issue within its Routing Area, where the rpsec WG has collected the requirements for routing security. The recognition that inter-domain routing represents one of the areas of vulnerability in the large-scale Internet has recently motivated the start of the IETF Secure Inter-Domain Routing (sidr) WG, working at a framework to secure inter-domain routing, using as base the requirements provided by the rpsec WG. One of the issues is for example the security of the largely used BGP protocol, whose security practice (primarily RFC 2385, based on TCP MD5) does not fulfill operators' requirements, with the consequence that often authentication of the routing protocol is not used. Other problems with the TCP/MD5 option include the lack of key management (leaving unsolved a typical threat for operators, keys compromised by staff turnover) and the use of a weak cryptographic algorithm (MD5). While an initial solution was thought to be IPsec (which however is revealing to have issues in the routing scenario[26]), the trend is now the work on enhancements of TCP/MD5 (see the sidr WG).

[25] IETF RFC 4272, BGP Security Vulnerabilities Analysis.
[26] Issues discussed for example at the SAAG meeting in IETF 66th meeting, Why IPsec and BGP don't

Fora

IETF is currently addressing routing security in its Routing Area, in particular in the rpsec WG, defining the security requirements, and the sidr WG, working on the security solution for inter-domain routing. The IETF opsec WG also lists operational best practices. NANOG (North American Network Operators' Group[27]) and RIPE are involved in efforts to address routing security. NIST is working at Draft Special Publication 800-54, Border Gateway Protocol Security.

A collection of activities and presentations for BGP can be found at http://www.bgp4.as/security.

Discussion

Routing security is a complex technical area. Securing a large-scale distributed system by necessity does not allow implementing a fully secured solution but needs to focus on risk mitigation, in order to achieve the correct balance between security and effective deployment of the system (including cost, scalability, and flexibility). Nevertheless, routing security needs to be addressed with priority. In fact, with the increasing dependability of ICT on interconnected networks and the Internet, the risks posed by attacks on the routing infrastructure become significant. The security measures for routing requires a mixture of good practices, to protect the local infrastructure with appropriate measures for the routers and the routing protocols, and measures to assert the authenticity and integrity of the information carried in the routing protocols. The latter is a difficult challenge, requiring a move from security based on vague trust models to a strong assertion of authenticity.

Standardization (IETF) has started to work very actively to address the routing security space, however a stronger and more visible demand from the market it would be beneficial. For example, the current status of security breaches to the routing infrastructure is not known. A **systematic reporting of incidents should be encouraged**, in line with the ideas formulated in COM(2006)251.

play well together in real networks, http://www3.ietf.org/proceedings/06jul/slides/saag-2.pdf

[27] http://www.nanog.org/ispsecurity.html

1.3. DNS Security tools

Together with routing, the Domain Name System (DNS) represents a critical component of the Internet infrastructure. DNS has the main task of translating IP addresses into user-friendly domain names, and vice versa. The ability to corrupt DNS and its operation represents one of the most effective ways to attack the integrity of the Internet, and all the services and applications relying on it.

The original DNS infrastructure has been designed insecure. The danger that this implies has been voiced from the 90ies, yet the current DNS infrastructure continues to lack of security[28]. Being the Internet recognized as a critical infrastructure, incentives for DNS security are now put forward[29], starting from the identification of DNS threats (e.g. IETF RFC 3833 and NIST SP 800-81). Priority security services for DNS are source authentication and data integrity (to assure the authenticity of the DNS information), and availability of the DNS infrastructure. A NIST report, SP 800-81, Secure Domain Name System (DNS) Deployment Guide[30], provides an overview of DNS, threats to DNS, and guidelines for securing DNS within an enterprise.

DNS security deals with a number of different issues. One aspect is a sound implementation configuration, which includes e.g. platform security, latest patches, latest version of the software, and split DNS. Another aspect is the security of the DNS translations, which includes zone transfers among servers, notifications and updates (which may use the IETF TSIG protocol, based on shared secret), and DNS query/response (to be secured with the IETF DNSSEC).

The DNS Security Extensions (**DNSSEC**) is a protocol suite[31] defining secure DNS protocol exchanges. DNSSEC provides data origin authentication and data integrity to DNS, by digitally signing the DNS answers to the resolvers (clients) and relying on a chain of trust within the hierarchical delegation structure of DNS. DNSSEC does not represent a complete security solution for the DNS infrastructure, but solves an important issue – the authenticity and integrity of the DNS response, so that an attacker can not forge the DNS data. This property gets increasing importance, since other security protocols have started to rely on the DNS for certificate or key transport[32] and since DNS can be used as additional information to aid receiving

[28] DNS vulnerabilities are among the top ten security risks, according to the DNSSEC Deployment Initiative Newsletter, August 2006, http://www.dnssec-deployment.org/news/dnssecthismonth/

[29] For example, by the US National Strategy to Secure Cyberspace, February 2003, which cites both routing and DNS; http://www.whitehouse.gov/pcipb/

[30] http://csrc.nist.gov/publications/nistpubs/800-81/SP800-81.pdf

[31] The basic IETF specifications are RFCs 4033, 4034, and 4035. For few interesting reading of DNSSEC, see the ISP Column by ISOC, DNSSEC: The Theory (August 2006), DNSSEC: The Practice (September 2006), and DNSSEC: the Opinion (October 2006), http://www.isoc.org/pubs/isp/index.shtml

[32] Examples: RFC 4322, The Opportunistic Encryption with IPsec; RFC 4398, Storing Certificates in DNS; RFC 4255, Using DNS to Securely Publish Secure Shell (SSH) Key Fingerprints.

domains in detecting spoofing and spam (e.g. DKIM). Therefore, it is also believed by many that use of DNSSEC could as well facilitate the bootstrapping of other authenticated communication protocols[33]. There are a number of efforts encouraging the adoption of DNSSEC, including a few pilot projects[34]. In Europe, the ".se" domain (Sweden) has been the first world top level domain to adopt DNSSEC. The GEANT2 network connecting research centres in Europe and beyond also uses DNSSEC. Deployment issues[35] and promotion of large-scale deployment on a large scale remain challenges for DNSSEC.

The latest wave of attacks[36], at the beginning of 2006, has drawn the attention of the security community to the weaknesses of the DNS infrastructure. The attacks were against the root name servers and top level domain name servers and were a variant of DNS DDoS amplification attacks. The answer of the security community has been a strong campaign promoting source IP address validation (network ingress filtering), strongly supported by ICANN and RIPE.

Fora

There are several initiatives promoting the security of the Domain Name System. The Security and Stability Advisory Committee (SSAC), within ICANN (the international body responsible for the DNS management), is chartered to advice on DNS security. The RIPE forum has a Technical Security (TechSec) WG, looking at DNSSEC deployment, and has recently started an anti-spoofing task force, in order to promote the adoption of network ingress filtering (RFC 2827) to face spoofing and DNS amplification attacks. The RIPE DISI supports the development and deployment of DNSSEC.

IETF is the SDO taking care of the design of DNS security, in particular DNSSEC. The dnsext WG takes care of the maintenance of the standards and new issues, and the dnsop WG investigates operational issues.

DNSSEC information sites:
http://www.dnssec.net and http://www.dnssec-deployment.org

[33] For an interesting asset on the economic aspects of DNSSEC and its bootstrap problem, see http://weis2006.econinfosec.org/docs/46.pdf
[34] http://www.dnssec.net/projects
[35] ENISA Quarterly, October 2005, Securing the Internet's Largest Distributed Lookup Service – DNSSEC Deployment issues, page 7.
[36] See the SSAC Advisory SAC008, DNS Distributed Denial of Service (DDoS) Attacks, http://www.icann.org/committees/security/dns-ddos-advisory-31mar06.pdf.
See press articles such as http://news.com.com/DNS+servers+do+hackers+dirty+work/2100-7349_3-6053468.html.
See ENISA Quarterly June 2006, D. Piscitello, The Worrisome threat of DNS DDoS Amplification Attacks, http://www.enisa.europa.eu/doc/pdf/publications/enisa_quarterly_06_06.pdf, pages 6-7.

Discussion

The increasing dependability of ICT on interconnected networks and the Internet makes the risks of attacks to the infrastructure become significant. DNS, similar to routing, is one of the key components of such infrastructure and is largely not protected. Furthermore, we observe today that the use of DNS is expanded beyond the IP addresses-names translation, to be a base for security and robustness solutions, as seen in the case of adding keys and certificates in support of security protocols, and support for e-mail authentication in anti-spam mechanisms. This expanded role implies even higher risk for DNS to be target of attacks.

DNSSEC is emerging but slowly and with deployment issues. Also, the success of DNSSEC is conditional on a global adoption. It is important to expand experimental projects on a larger scale, and promote incremental steps in the adoption of the protocol. However, it should be also clear that DNSSEC is not the complete security solution for the DNS infrastructure, and that other security components are needed, e.g. a sound configuration of the hosting environment. These components are often the easiest to fix but are also often neglected, and they are often only matter of security best practices.

As in the case of routing, the current status of security breaches to the DNS infrastructure is not known, due to lack of breach reports. **Reporting on DNS incidents should be encouraged if not required** (see again COM (2006) 251).

1.4. Anti-spam tools

Spam (unsolicited bulk e-mails)[37] is nothing unspoken of. There are a few developments in the area that can be pointed out. They are of two kinds: first, the content of spam, and second, a few emerging mechanisms to mitigate spam.

Spam does not seem to decrease. However, the filtering capabilities of internet service providers appear to improve steadily[38]. The concern nowadays is turning at the content of spam, which has turned from being just annoying to getting harmful, as e-mails are used to carry viruses, spyware etc. targeting the infections of PCs and devices (which is also the first step to recruit zombies for escalating attacks). Lately, **phishing** has taken the stage as serious threat[39] to privacy causing financial loss for the victims. This implies that the emergency to address spam in a comprehensive way is more impelling.

There have been lately a few technical initiatives put forward in order to mitigate the problem of spam, phishing, and **spoofing** (which, by masquerading the sender identity, is often used to perpetuate spam). These mechanisms are getting increasingly adopted and tested, and are also under scrutiny by IETF. SenderID, Sender Policy Framework (SPF) and DKIM are trying to solve the issue 'who, or which domain, sent the message'. The debate on them has been long, in particular on SenderID (hence the decision of Experimental status of its specifications by IETF). The real obstacle to these mechanisms seems to be the lack of their widespread adoption, although the efforts are now increasing. Also, the community appears divided on which mechanisms to privilege (it has been observed that companies adopting one method typically also implement the other).

It should finally be noted that new forms of spam are appearing, as adaptation to other technologies. ***SPIM*** (spam over instant messaging) has been discussed for quite some time but has not proved to be a threat to the extent it was predicted. On the other hand, ***SPIT*** (spam over IP telephony) is just a hypothesis for the moment but is anticipated as an emerging threat[40]. Work to address these new forms of spam has started for example in the IETF's sipping and speermint working groups.

---

[37] "The PSG Vision for ENISA", May 2006, http://www.enisa.europa.eu/doc/pdf/news/psgvisionforenisafinaladoptedmay2006version.pdf

[38] The Messaging Anti-Abuse Working Group (MAAWG), for example, reports 80% of mails to be spam, out of an evaluation of ca. 390 millions mailboxes; E-mail Metrics Report - June 2006, http://www.maawg.org/about/FINAL_1Q2006_Metrics_Report.pdf

[39] "The PSG Vision for ENISA", May 2006, see note above.

[40] SPIT, together with the always-evolving SPAM, are for example identified as current and emerging risks by the ENISA Permanent Stakeholders Group (PSG), in "The PSG Vision for ENISA", http://www.enisa.europa.eu/doc/pdf/news/psgvisionforenisafinaladoptedmay2006version.pdf

Phishing

"Phishing is a form of online identity theft that employs both social engineering and technical subterfuge to steal consumers' personal identity data and financial account credentials. Social-engineering schemes use 'spoofed' e-mails to lead consumers to counterfeit websites designed to trick recipients into divulging financial data such as account usernames and passwords. Hijacking brand names of banks, e-retailers and credit card companies, phishers often convince recipients to respond. Technical subterfuge schemes plant crimeware onto PCs to steal credentials directly, often using key logging systems to intercept consumers online account user names and passwords, and to corrupt local and remote navigational infrastructures to misdirect consumers to counterfeit websites and to authentic websites through phisher-controlled proxies that can be used to monitor and intercept consumers' keystrokes".

Definition of phishing by the Anti-Phishing Working Group
http://www.antiphishing.org/reports/apwg_report_May2006.pdf

Sender ID and DKIM

Sender ID

Result of the merger of two proposals, the Sender Policy Framework (SPF, RFC4408) and the Microsoft's Caller ID, SenderID is published as Experimental RFC in IETF (RFC 4406). Sender ID relies on DNS (hence, it is as secure as DNS is). The receiving internet service provider or e-mail system examines the message and determines the 'purported responsible domain', i.e. the domain that purports to be the sender. It then queries the DNS to find the list (SPF record) of the authorized outbound e-mail servers published by the purported responsible domain, and checks that the address the message came from is in that list, otherwise the message may be considered spoofed.

DKIM

DomainKeys Identified Mail derives from the merging of DomainKey by Yahoo! and a Cisco proposal, and is currently under standardization by the dkim WG in IETF. DKIM is a signature-based e-mail authentication proposal, where the sending domain signs the outgoing e-mail sent by an authorized end user (the signature is added as header), and publishes the corresponding public key into a DNS record, which can be retrieved by the receiving e-mail system who can verify the signature.

Fora

IETF is discussing and developing mechanisms for e-mail authentication. The dkim WG is chartered to design the DKIM protocol, while an Experimental RFC (RFC 4406) describes the SenderID mechanism.

A session was held in the IETF meeting in Montreal in July 2006 on Web authentication enhancement (wae BOF[41]), to specifically address threats such as phishing. A discussion is on-going to evaluate the need for a new Working Group based on this BOF.

A number of initiatives exist in order to mitigate spam and phishing, including:

- The Anti-Phishing Working Group, http://www.antiphishing.org
- The Messaging Anti-Abuse Working Group (MAAWG), http://www.maawg.org
- The OECD Task Force, developing the anti-spam Toolkit
- ITU-T Study Group 17
- RIPE, with an Anti-spam Working Group and an Anti-spoofing task force
- The Contact Network of Spam Authorities (CNSA), an EU initiative that sees EU countries collaborating to combat spam in a pan-European context: http://europa.eu.int/rapid/pressReleasesAction.do?reference=IP/05/146&format=HTML&aged=0&language=en&guiLanguage=en
- The London Action Plan (LAP), promoting international spam enforcement cooperation and addressing spam related problems including phishing http://www.londonactionplan.com/

Discussion

Spam is not a new issue, and filtering techniques are improving. However, spam stays steady and it is now turning into more than just nuisance; it is getting harmful since it is often used as transport of malware and phishing attacks. Therefore, the emergency to address spam in a comprehensive way is more impelling. Attempts, such as SenderID/SPF and DKIM, are getting into deployment phase; they are not the final solution to the problem, however they represent a significant initiative by the industry to strengthen the trust in e-mail systems, especially when complemented by reputation systems.

Technology alone cannot be the final remedy. Legislation has an important role in the battle to spam, and has many challenges ahead. For example, a conflict has been identified between the ISPs obligations of delivering all the messages to the email recipient, protecting the privacy of the messages, and using spam filters that block some of the messages. Furthermore, technology needs also to be accompanied by a modified security culture. Making the Internet a trusted environment needs a

[41] http://www3.ietf.org/proceedings/06jul/minutes/wae.txt. BOF stands for Birds of a Feather, an initial meeting where people interested in a particular topic gather to discuss about it.

collaborative effort involving new technologies, research and industry, as well as legislation and user awareness.

Everyone will agree that spam has reached an unbearable level and is more than a nuisance. However, this is only half of the problem. While higher levels of spam can be countered by more sophisticated ways of filtering, the true danger lies in the mix of threats that unsolicited emails deliver to the user's inbox - viruses, worms, trojans, spyware, and phishing attacks. Consequently, there also has to be a mix of countermeasures, dealing with each threat in the most appropriate way. Some viruses can be filtered out with signature-based algorithms, fast spreading worms have to be countered with protection software that is updated automatically, the fight against trojans and spyware requires slightly different technologies and identity theft is best countered with a mix of awareness raising and software that tags such attacks.

It is this complexity that makes it difficult to judge the success - or failure - of the fight against spam. Many users successfully counter spam with a reasonable mix of filtering techniques at the client and at the server level. However, other less advanced users are not only still struggling with an increasing amount of spam, they are also more likely to become victims of identity theft. This often starts with an unsolicited email - i.e. with spam. Policy makers are struggling with this mix of threats as well, for a number of reasons.

First, legislation does not evolve as quickly as technical threats do. A more generic legislation that leaves room for covering future threats will not be able to differentiate between the various types of threats and mandate adequate countermeasures. A more specific legislation that foresees a special treatment for different threats runs the risk of being overtaken by the technological development. The fact that providers of electronic communication services range from large international corporations to tiny local outfits further complicates the matter. Also, networks are provided not only by the private sector, but also by the government, academia as well as private persons and non-governmental / not-for-profit organizations. They all have different requirements with regard to spam and related threats. Requesting policy makers to provide guidance and legislation to deal with this complexity is justified, but expectations regarding the results have to be kept realistic.

On the technical side, requiring by law "adequate countermeasures against spam and other malware" is often as good as it gets. Additional guidance must come from National Regulatory Authorities and other private and public bodies. The Article 29 Working Party on privacy has provided a good example with its opinion on how to balance filtering of emails for spam, viruses, etc. against the demand for privacy. Such guidance must be - and actually has been already - completed by initiatives to encourage and support co-operation, such as the Contact Network of Spam Authorities (CNSA), the London Action Plan (LAP), the EU SpotSpam project (driven by Germany and Poland), the French SignalSpam iniative and others.

ENISA work on Anti-Spam status and measures in Europe

ENISA has investigated the issue of spam in two 2006 reports:

- " Provider Security Measures, Part 2; Security and Anti-Spam measures of Electronic Communication Service Providers- Survey", http://www.enisa.europa.eu/doc/pdf/deliverables/enisa_security_spam.pdf
- " Provider Security Measures, Part 2; Security and Anti-Spam measures of Electronic Communication Service Providers- Status and Outlook" http://www.enisa.europa.eu/doc/pdf/deliverables/enisa_security_spam_part2.pdf

Based on targeted questionnaires as well as attendance of relevant workshops and conferences, the reports provide an overview of the current status of the spam issue in Europe and the anti-spam techniques put in place by providers, together with an outlook into trends, future, and proposals. Identified techniques in use are blacklisting/whitelisting, ingress filtering, and appearance of sender authentication techniques (Sender ID Framework and DKIM).

Transparency is one of the critical aspects identified in the reports. Reporting of security breaches, sensitive and yet discussed topic, is still too limited, with a negative impact on transparency and countermeasure promotion, hence needs to be encouraged.

1.5. Identity Management tools and procedures

The management of identities has become a critical issue in IT infrastructures. Indeed, many of the issues that Internet faces today are related to the lack of identity management solutions properly integrating user-friendliness, flexibility, efficiency, and security.

In distributed networks there are likely to be different ways of authentication and a high number of identities and service contracts per user, hence there is the need for a very flexible identity management system. Federation (including standardization efforts such as Shibboleth, Liberty Alliance, and Open SSO[42]) refers to an environment where different service actors interact to facilitate a composite service, yet with a single sign on functionality. Federation factors out trust functionalities to dedicated services and improves efficiency. Identities are managed by dedicated identity providers, which are independent from core application functionalities and core service providers. While identity management implies a whole set of technologies and infrastructure on the corporate/operator side, with related security implications, the debate is primarily focused on the user perspective. Identity management is strongly linked to the issue of trust, and privacy and protection of data are essential trust components and have a critical role for the acceptance of services.

Privacy Enhancing Technologies (PET)[43] is an area of emerging technologies; although it has been around for a number of years, it does not have yet taken off. Examples include anonymizers, anonymous credentials and P3P. The World Wide Web Consortium (W3C) released the Platform for Privacy Preferences (P3P) in 2002, providing users with the ability to define and publish their Web site's privacy policies. P3P has paved the way to a great deal of the current research on privacy languages, and W3C continues to develop their work on privacy, with workshops and a new release of P3P[44].

The PRIME project[45] is working to build a user-controlled system for identity management. PRIME's objective is to build a Privacy Enhancing architecture and prototypes which place the individual in control of his personal data, able to disclose it according to the degree of trust in the relying party and without more information than necessary being obtained (*data minimization*). However, accountability is still has to guaranteed, e.g. using revocable anonymity for certificates.

There are however more components to be considered than just privacy-enhancing technologies. The identity management landscape also involves for example

[42] https://opensso.dev.java.net/
[43] http://petworkshop.org/2006/index.html
[44] http://www.w3.org/TR/P3P11/
[45] PRIME Whitepaper, July 2005, https://www.prime-project.eu/prime_products/whitepaper/

economic considerations, and unfortunately there is still lack of research in this area. The cost of privacy breaches are often a burden for the victims, while there is a need for business to internalize these costs and hence limit the impact on society[46]. One threat that is raising concern is identity theft[47]. This threat is hitting very hard in the US[48], however the concern has also increased in Europe as well as worldwide. Identity theft combines a number of attack vectors including technical, physical and social engineering[49].

User-friendliness is a factor that is also important to bear in mind in the matter of identity management. One example of unsuccessful design is the difficulty of making decisions on enterprise privacy policies, which do not allow to easily set the rules for the user agent.

Fora

Liberty Alliance (http://www.projectliberty.org/) is a consortium addressing the technical, business, and policy challenges around identity and identity-based Web services. The consortium has also an Identity Theft Prevention WG, http://www.projectliberty.org/liberty/strategic_initiatives/id_theft.

W3C (http://www.w3.org/) developed the Platform for Privacy Preferences (P3P, http://www.w3.org/P3P/). ISO Committee SC 27 has already had Study Periods on Identity Management, and in 2006 has created Working Group 5 on Identity Management and Privacy Technologies. IFIP has WG 11.6 dedicated to Identity Management. CEN/ISSS has initiatives in the field, namely the Data Protection and Privacy Workshop (DPP) and the eAuthentication Workshop (closed).

The EU has been promoting several activities in the area of identity management, always addressing the topic in an interdisciplinary way. The PRIME Project (Privacy and Identity Management for Europe, https://www.prime-project.eu/) is a European project on privacy enhancing identity management. PRIME held a workshop to identify gaps in identity management standardization and to promote PRIME results on user-centric identity management for standardization, https://www.prime-project.eu/events/standardisation-ws/.
The FIDIS Project (The future of Identity in the Information Society, http://www.fidis.net/) and the GUIDE Project (Government User Identity for Europe, http://istrg.som.surrey.ac.uk/projects/guide/overview.html) are also involved in identity management for research, in order for Europe to develop a deeper understanding of it, hence promote the European information society and e-government.

[46] PRIME Whitepaper, see note above.
[47] "The PSG Vision for ENISA", May 2006, http://www.enisa.europa.eu/doc/pdf/news/psgvisionforenisafinaladoptedmay2006version.pdf
[48] http://idtheftcenter.org/index.shtml
[49] Liberty Alliance, Identity Theft Prevention WG, "Identity Theft Primer", http://www.projectliberty.org/liberty/strategic_initiatives/id_theft

Some interesting reading can be found in Kim Cameron's Identity Weblog, http://identityblog.com/.

Discussion

One of the most urgent works in identity management is setting the requirements for standards in the field of privacy. The issue cannot be solved only at the technical level, but requires an extensive investigation in an interdisciplinary manner. Cooperation among stakeholders is critical, and needs to include the users' perspective. **Results of dedicated EU projects such as PRIME should be promoted and brought into standardization**.

ENISA on the security level of Authentication Methods

Included in the European Commission eID roadmap, ENISA takes the initiative to find a common language between Member States – and industry - to identify the levels of security that can be met by different authentication methods. The goal is to facilitate interoperability and mutual recognition of electronic authentication schemes for the benefit of citizens and enterprises. In a Workshop held by ENISA in November 2006, experts were invited to share information on authentication methods and to discuss the different ways they are used in Europe to describe the level and appropriateness of such methods. http://www.enisa.europa.eu/pages/authentication/

1.5.1. Biometrics

Biometric techniques have been of high-profile for quite some time, especially due to their use in applications of large social impact such as e-passports[50] and national identity cards. Biometrics can be used in disparate applications, from government to business and domestic applications, including access to places, transportation, health sector, etc. Biometrics allow for identification and authentication based on "something you are", promising higher security (compared to e.g. traditional credentials that may show weaknesses, such as static passwords i.e. "something you know"). Examples of biometric techniques are: fingerprinting, face recognition, voice recognition, and iris recognition, but also novel techniques such as 3D ear recognition, hand writing, behavioral biometrics (e.g. mouse usage, gait), and DNA.

Biometric authentication may however be affected by errors, and circumventions of biometrics have proven possible, for example the false positive / false negative

[50] E.g. the EU Digital Passport Project, http://www.eudigitalpassport.com/

(FP/FN) ratio to correct authentications, which may characterize biometrics techniques. This typically poses an issue in most common authentications scenarios, and often requires the combination of biometrics with other, more traditional techniques methods.

The issue of "liveness detection"[51], for example, is under research, to assure that fingerprints are not forged (e.g. fake thumbs). IT is something that today requires the supervision of highly trained staff, hence costs. It should be noted that traditional cryptography and biometrics do not integrate perfectly, since biometrical data cannot be produced or revoked and regenerated in the same way as a cryptographic key. Cryptography for noisy data is an emerging research area[52]. Further issues include a balance between the time necessary for the matching process and the accuracy of identification, the costs, and the use of combined biometric techniques, both affecting the FP/FN ratio and the overall security level.

Privacy and accountability are pressing questions also for authentication based on biometrics (the legal basis for privacy in biometrics is the EU Directive 95/46/EC3 on Data Protection), and the issue is complicated by ethical concerns. One particular issue is around the assurance that the biometric system and data are used solely for the specific application they are intended for (threat of "*function creep*"). This issue has been identified by OECD[53] as one of the areas of concern related to privacy for biometrics, together with the risk for biometrics to become an infrastructure for surveillance, and the possible lack of transparency, i.e., the possibility that certain implementations may be used without the consent or knowledge of the user. Another privacy issue for biometrics is related to the secondary information which can be deduced, e.g. health status from iris scans, and personality from handwriting and gait recognition.

It cannot be forgotten that biometrics, like any successful identification technology, require a secure, robust infrastructure in the background. Therefore the success of the technology requires a comprehensive security solution, including the data storage, the acquisition process, and the matching process.

Fora

The EU has initiated the European Biometrics Portal (www.europeanbiometrics.info), in order to facilitate the cooperation of biometrics actors in Europe.

[51] Liveness detection checks that the biometric data comes from a live entity, physically present at the acquisition.
[52] ECRYPT, Challenges for Cryptology Research in Europe for 2007-2013 and beyond, http://homes.esat.kuleuven.be/~preneel/ecrypt_vision.pdf
[53] OECD, Biometric-based technologies, http://www.oecd.org/document/20/0,2340,en_2649_34255_35011988_1_1_1_1,00.html

Standardization work sees engaged several bodies[54], including NIST (with the CBEFF standard, Draft Special Publication 800-76-1, and the Biometrics Resource Center Website), OASIS (with e.g. the XCBF standard), the BIOAPI consortium (http://www.bioapi.org, working on standardized APIs). ISO has biometrics work in Subcommittee 17 (cards and personal identification), Subcommittee 27 (security techniques), and Subcommittee 37 (biometrics), and some work spread in other groups (e.g., ISO/TC68 on financial services, ISO/TC215 on health informatics, and ISO/IEC/JTC1 Privacy Technology Study Group).

Discussion

There are several applications possible for biometrics, which would have strong impact on European citizens. However, the technology is still evolving and its benefits are still to be completely clarified[55]: biometrics remains a young, emerging technology. There is lack of maturity in the technology and standards, and fragmentation persists. Also, there is need for a clear impact assessment on privacy and limitations.

It has to be clear that biometrics belongs to that range of technologies that encompass pure technique and extend to the social sphere. **It is important to open the dialogue with the citizens**, and explain the benefits, the limitations, and the ways to reduce fraud and improve privacy, so that the citizens can also see the benefit in giving up some degree of their privacy.

1.6. De-perimeterization and Endpoint security

De-perimeterization, i.e. the trend that phases-off security implemented only at the network boundary, is a strategy that has been around for a while[56], but that is also getting increasing acceptance. Businesses are evolving towards openness and interconnection, where networks are in trust relation with partners and third parties, and where endpoints are mobile. The concept of perimeter itself is getting harder to define and a moving target, due to the appearance of ad-hoc networks, wireless types of access, and plug&play devices including USB. This implies that it is not possible anymore to rely only on security mechanisms implemented at the borders (firewall and intrusion detection/prevention systems), but there is a need for distributed security combined with encryption, authentication, inherently secure systems and protocols, application security, etc. The identification of systems and users becomes important, and here solutions may include smartcards, biometrics techniques, and security chips

[54] For a list of relevant standards, see http://www.bromba.com/faq/biofaqe.htm#Standards
[55] European Biometrics Portal, "Biometrics in Europe", June 2006 http://www.libertysecurity.org/IMG/pdf/Trend_Report_2006.pdf#search=%22Biometrics%20in%20Europe%20unisys%22
[56] The term was coined by one of the most active promoter, the Jericho Forum (http://www.opengroup.org/tech/jericho/)

such as the Trusted Platform Module (TPM, which now popular vendors such as HP and IBM have built into laptops, see Section 1.6.1).

An emerging trend in de-perimeterization is the "***endpoint security***"[57], where endpoints (e.g., laptops, desktops, and personal computing devices such as PDAs) connecting to a network are scanned for a "health check" in order to verify if their security status is aligned to the local security policies. The security software is distributed to end-user devices but is centrally managed. The client installed in the end-user device, for example when entering the corporate, connects to the server, requests login, and reports on its security capabilities and status (operating system, personal firewall, anti-virus and anti-spyware, etc.). The server compares this information with the local policies and scans for unauthorized software before granting access, and may send updates and patches. The end-user device may then be granted or refused access, or may be quarantined.

This emerging technique is raising increased interest since endpoints are particularly exposed to threats. On one side, business is nowadays more and more relying on mobile endpoints whose disruption would have a big impact in lost productivity, and on the other, the network needs to be protected from corrupted endpoints.

Products for endpoint security have appeared, for example the Network Admission Control (NAC) by Cisco, the Network Access Protection (NAP) by Microsoft, and the Trusted Network Connect (TNC) by TCG (which is a set of open standards). However, the majority of the current solutions are proprietary and no standard has emerged. Interoperability is here a key issue, since endpoint security involves different components from different vendors. IETF has lately initiated work within the Network Endpoint Assessment (nea) WG[58], to develop standard protocols implementing endpoint security in interoperable way (e.g. with a client from one vendor able to speak with the server of another vendor).

1.6.1. Trusted Computing

Trusted Computing (TC) is a technology promoted by the Trusted Computing Group (TCG). The basic principle is the possibility to trust that the hardware and software have not been tempered with, including the idea of a "trusted bootstrap".

The TC core is the *Trusted Platform Module* (TPM), a microcontroller to be inserted in a device (e.g., PC, PDA, and other mobile devices) and able to securely store digital keys, certificates, passwords, hashes for platform configuration checking, etc. The information stored in the TPM, as well as related security processes such as signatures and key management, are in this way more secure from attacks. The technology becomes an enabler for many applications in need of a trusted platform

[57] For a source of articles, see for example http://www.endpointsecurity.org/
[58] http://www3.ietf.org/proceedings/06jul/agenda/nea.txt

underneath, e.g. trusted downloads (including software updates), secure communications, secure storage, reliable peripheral identifications (e.g. of added parties), access control, and many others. A few other TC concepts are built around TPM. The *TCG Software Specification* (TSS) is a software specification that provides a standard API for accessing the TPM functions, so to e.g. assure applications that the cryptographic keys have been generated in a more secure environment. The *Trusted Network Connect* (TNC) is an open, non-proprietary specification for enforcing security policies to endpoints connecting to a network. For example, it allows checking if the configuration of the endpoint, wishing to attach to the network, is aligned with the local network policies. TNC belongs to the emerging trend of endpoint security technologies. The *Trusted Server Specification* is the specification defining the trusted server architecture and their management, including the communication to the trusted clients. Examples of advantages of the trusted server are the higher protection of the data from unauthorized access, the assurance to meet minimum standards before being allowed to make sensitive communications, and guarantee of connecting to the intended server.

After focusing on fixed devices, TCG is also working on mobile device security, due to their increasing importance. The specification builds on the TPM concept and trust model, although it requires optimization to the mobile requirements.

Trusted Computing has raised criticisms[59] by a few security experts. While recognizing the role of secure enabler for many possible applications and its promise of security enhancing technology[60], a warning is voiced against the possibility that implementing TC would take away the control from the user in favor of the owner of the TC infrastructure. This would also effectively hinder competitiveness and product diversification. A controversial usage of TC is also in the digital right management (DRM) field, since the technology could be used as enabler for strong DRM control.

Fora

De-perimeterization is a network design strategy that can be observed in the architecture work done in the different fora. The most popular and active promoter of the concept of de-perimeterization is the Jericho Forum, belonging to the Open Group.

Trusted Computing is based on the industry standards written by the Trusted Computing Group (TGC). There are many industrial companies providing TPM products, starting from PC companies.

Discussion

De-perimeterization represents a gradual strategy to couple with the new business models, increasingly open, mobile, and interconnected, where endpoints are

[59] For example, Ross Anderson at http://www.cl.cam.ac.uk/~rja14/tcpa-faq.html, and "Trusted Computing: Promise and Risk", http://www.eff.org/Infrastructure/trusted_computing/20031001_tc.php
[60] http://www.securityfocus.com/news/11410

particularly exposed to threats, in order to establish and manage the appropriate level of trust, hence security posture. At the same time, it addresses the issue of a very high rate of internal threats, against which the perimeter is ineffective. **Risk assessment and risk management are crucial in this evolution towards a distributed security architecture** and new automated tools need to be investigated to accommodate them. Endpoint security contributes to transparency of security and usability, under the correct assumption that it is not possible to off-load security to the average user.

The Trusted Computing technology is at its beginning and needs to gain deployment experience, together with clarification of the business cases and their implications. Indeed the technology is extremely promising, and could turn out as a strong enabler for secure applications, especially in areas (such as end devices) where the user is more in charge hence where many issues may be encountered.

Virtualization

Trusted Computing can be seen as a technology belonging to the emerging industry trend of Virtualization[61]. Virtualization allows multiple virtual machines with different operating systems to run in isolation on the same physical machine. Virtualization can be used to enhance security, as it implies the concepts of separation and isolation, e.g. of processes and applications, and offers tools for authorization, monitoring, verification and recovery.

One use of virtualization is to achieve application isolation, helping administrators to control the application's stability and its integrity[62]. The attacker cannot compromise the underlying operating system, and recovery is easier because the system can revert to its original status. Virtualization can help in disaster recovery and availability, honeypot implementation, intrusion detection / prevention systems (IDS/IPS) with integrated defense and recovery, forensic analysis, monitoring implementations, etc[63].

[61] http://www.virtualization.info, and WMWare's web pages at http://www.vmware.com/virtualization/
[62] One example is the Browser by VMware, http://www.vmware.com/vmtn/appliances/directory/browserapp.html
[63] http://www.virtualization.info/2006/07/security-by-virtualization.html

2. ICT developments impacting on Security

2.1. IPv6

Background

Although the basic IETF specifications exist since 1998, the next version of the Internet Protocol, IPv6, has not yet happened beyond testbed installation and isolated implementations. The IPv6 market is evolving and promising, and IPv6 deployment is today highly promoted, e.g. via pilot projects. The shortage of IP addresses[64] offered by IPv4 is often cited as prime driving force for IPv6, since it will be unsustainable once ubiquitous networks are implemented (in particular, enabling machine-to-machine communication requires abundance of IP addresses). The emerging of the multimedia communications is another driving force for IPv6. Multimedia enriches the way of communicating, using multiple devices, multiple IP addresses e.g. for roaming, as well as push-type of services that may be hindered by NATs (which are the short-term fix to the address shortage, but which allow for smooth communication only one-way, outbound). There are many efforts in order to promote IPv6, at the standardization, industry, research, but also governmental level (e.g., support by the US Federal Government, the EU, and a few Asiatic countries such as Japan, South Korea, and China). Increasing adoption can be observed (although more at the infrastructure side than at the application development side). However there is still general cautiousness[65]. The general consensus is that IPv6 will be beneficial in the long term[66], even needed if certain applications, as predicted, take off (i.e., "push-type" services, applications that consume IP addresses, such as machine-to-machine communications, and always-on communication through a variety of devices). However, the near term benefits of IPv6 appear less clear[67].

Security Aspects

The discussion on the security advantages of IPv6 follows the same line. On the short term, IPv6 may not bring along improved security. The native support of IPsec is the

[64] For some predictions of the date of IPv4 address exhaustion, see for example the ISP Column by Geoff Huston, http://www.potaroo.net/ispcol/2005-11/numerology.html

[65] For example, IMS, enabling multimedia communications, has been designed in the original specification over IPv6 only. However, at later stage an interim solution over IPv4 has been introduced ("Early IMS" [3GPP TR 33.978]) to avoid too long delay of the system deployment.

[66] For example, the EU stated that IPv4 is considered to limit the full deployment of 3G services in the long run, COM(2001)141, The Introduction of Third Generation Mobile Communications in the European Union: State of Play and the Way Forward http://europa.eu.int/ISPO/infosoc/telecompolicy/en/com2001-141en.pdf

[67] A recent NIST-NTIA report contains an interesting technical and economic assessment of the new technology. NIST-NTIA, Technical and Economic Assessment of Internet Protocol Version 6 (IPv6), January 2006, http://www.ntia.doc.gov/ntiahome/ntiageneral/ipv6/final/IPv6final.pdf

main security advantage that IPv6 brings over IPv4, i.e. IPsec must be supported in an IPv6 implementation while it is only optional in an IPv4 implementation. However, this does not imply that it is mandatory to use IPsec in IPv6 either. Furthermore, it has been reported that some existing IPv6 implementations are rolled-out without IPsec - or with a poor IPsec implementation. Some experts point out the difficulty for attackers to perform brute force (or blind) scans [68], due to the number of IP addresses. IPv6 also brings the benefit of improved mobility, in particular with secure and easier auto-configuration of addresses and the possibility for seamless communication when moving between networks. However, security experts warn about the possibility that on the short term the transition to IPv6 may bring increased security vulnerabilities, due to the novelty of the technology and the need to experiment with it, the necessary co-existence with IPv4 (see the v6ops WG in IETF), and the fact that a wide-spread use of a technology always attracts attackers. Analysis is needed to further evaluate the security implications of the dual-stack environment (co-existence of the two versions), ICMPv6, neighbor discovery techniques, and the IPv6 address auto-configuration making use of e.g. multicast and anycast whose security is not scrutinized to the same extent as unicast security is. Other needed investigation areas are the integration of IPv6 with middleboxes such as firewalls and intrusion detection systems[69], and the development of IPv6-aware security components. One of the critical aspects of security in IPv4 is not comprehensively solved in IPv6 – key management, both in terms of credentials and infrastructure. Further areas to investigate include interaction with lawful interception, traceability, privacy.

On the long-term, IPv6 is expected to bring along security benefits. The restoration of the Internet end-to-end paradigm is one of the advantages of IPv6, including the new possibility of deploying security mechanisms in an end-to-end (e2e) fashion. This differs from the current IPv4 architecture, where deployment of middleboxes (in first place, NATs, which IPv6 promises to phase-off) not only hinder certain applications, but also often breaks, or makes difficult, the end-to-end security mechanisms and still requires strong perimeter defense. The perimeter defense approach appears instead to be corrupted by adoption of IPv6, since functions like inspection and policy enforcement may be more difficult to perform, due to the end-to-end communication (including end-to-end encryption) and tunneling. However, NATs and middleboxes in general do perform, to a certain extent, security functionalities as they are used to enforce security policies[70]; hence further research and experimentation of the possible new end-to-end security architecture is needed.

[68] IETF draft draft-ietf-v6ops-scanning-implications, IPv6 Implications for Network Scanning. It should be noted however that this effectively also prevents network administrators from using test tools.

[69] Tunneling IPv6 can raise issues with firewalls and intrusion detection systems that are not v6-aware; http://www.securityfocus.com/news/11406

[70] Work has began in the IETF v6ops WG to accommodate the perceived benefits of NATs in IPv6, IPv6 Network Architecture Protection, NAP (draft-ietf-v6ops-nap)

Middleboxes -- Hop-by-hop vs. end-to-end security

A middlebox is a network device that sits on a communication path and provides a network-assisted service. Most common examples of middleboxes are network address translators (NATs) and firewalls. The middlebox battle is long-aged in IETF: middleboxes (NATs in particular) have several implications[71], in particular they break the end-to-end (e2e) principle[72] that is at the base of the Internet. However, it is a fact that middleboxes are widespread as a mean to enforce control and security policies, and often enrich the communication (e.g. telecoms). NATs are used to solve the IP address shortage issue and for topology hiding; firewalls and detection devices for securing the network; performance enhancement proxies (PEPs, e.g. in satellite systems) for optimizing and enriching the communication. The SBC in the SIP/IMS systems performs a combination of tasks (e.g., security, policing, and protocol conversion).

The debate is part of a wider discussion on trust models: *hop-by-hop security* versus *end-to-end security*. There are several parties that feel that only the return to the e2e principle can lead to improved Internet security (this being one of the selling points of IPv6). Instead, NATs (and middleboxes in general) break end-to-end security and often do not integrate well with security protocols, since they may need to inspect the packet and/or manipulate it, to perform their tasks.

There is a general effort to harmonize middleboxes in the architecture. The IETF midcom Working Group is specifying a framework and a protocol to move application intelligence from middleboxes into external midcom agents. This has the advantage that complexity is reduced and maintenance of the middlebox is simpler.

NATs get a special attention in the discussion; they are not fully accepted by the Internet core community but their widespread usage is a fact. For example, NGN is facing the integration of access security mechanisms with the presence of a NAT/firewall at the customer premises. The NAT discussion extends much further and embraces the IPv4-IPv6 debate, since IPv6 is generally pointed out as the technology that would eventually obsolete NATs. It is however now recognized that, at least in the short/medium term of the IP version transition, NATs will be deployed[73]. The real issue is the fact that there is no standardization of NATs, which come in many variants hence are difficult to predict in behavior and make applications' life hard. The new behave Working Group in IETF is looking at NAT standardization. NAT issues with applications are addressed in many other IETF WGs, e.g. in the RAI Area for multimedia applications, for which NAT traversal is particularly difficult.

[71] RFC 2993, Architectural Implications of NAT, November 2000, and RFC 3027, Protocol Complications with the IP Network Address Translator, January 2001.
[72] RFC 1958, Architectural Principles of the Internet, June 1996, and RFC 3439, Some Internet Architectural Guidelines and Philosophy. December 2002.
[73] It is even predicted by many that NATs will continue to exist also with IPv6.

Fora

IPv6 initiatives take place in the majority of the fora, to take into consideration the differences in architecture, service, and application, once run over IPv6. IETF is the standardization body designing the IPv6 protocols.

The IPv6 Forum (http://www.ipv6forum.com/) is a world-wide consortium of Internet vendors, research and education networks, committed to the promotion of IPv6. The IPv6 Portal is source of information on IPv6, http://www.ipv6tf.org/index.php. The EU promotes several IPv6 initiatives (http://www.eu.ipv6tf.org/in/i-index.php), including within the seventh generation of pan-European research and education network GÉANT2 (http://www.geant2.net/).

Discussion

While on the long-term IPv6 is expected to bring along security benefits, on the short term it may not bring along improved security, and may even bring increased security vulnerabilities, unless appropriate risk assessment is performed. IPv6 still need experimentation from the security point of view.

Organizations are called for a careful planning and assessment before embracing IPv6, in particular concerning the involved security policies. **Further design, standardization activities and interoperability testing are needed to assess the technology and the new distributed security architecture.** Pilot projects should continue to be promoted.

2.2. Wireless Systems

Background

"Wireless technologies" is a broad categorization including many different technologies, from wireless Internet to mobile networks including mobile ad-hoc networks, and new emerging technologies such as wireless sensor networks and software defined radio. We shall comment in the following on the security implications of a few of them.

Security Aspects

In general, the mobile technologies should not be regarded as more insecure than the one of fixed technology[74]. For example, mobile networks such as GSM and, even more, 3G, have security functions (e.g. encryption, authentication) that may be lacking in fixed networks. Indeed, fixed networks often rely on some degree of physical security, and have generally a better defined perimeter where to enforce perimeter-based security. This is not applicable for wireless and mobile technologies, where the nature of the medium escapes the definition of perimeter and renders the signal easy to be intercepted and manipulated. On top of this, as observed below in the case of WLAN, available security solutions tend not to be used.

WLAN and wireless broadband

The popularity of Wireless Local Area Networks (WLAN) has rapidly expanded in the latest years, making WLAN access (e.g., hotspots) largely available to the public but also within enterprises (including critical infrastructure). The inherent security issue with the wireless technology is its openness (broadcast nature), coupled with a lack of implementation of existing security measures. It is in fact observed that the available security solutions tend not to be used. There is still, for example, a high adoption of unprotected WLAN, leading to the risk of penetration and potentially making available new platforms for launching attacks. It is reported that the number of protected wireless networks for example in the UK is increasing, but one in five is still unprotected and a further one in five is unencrypted[75]. "War driving" refers to the practice of moving in urban areas trying to locate and connect to wireless networks, using standard wireless network tools. This can result is the compromise of a company's network and leakage of sensitive information. There are warnings about rogue hotspots, to which authorized computers may connect allowing the attacker to

[74] "The PSG Vision for ENISA", May 2006, http://www.enisa.europa.eu/doc/pdf/news/psgvisionforenisafinaladoptedmay2006version.pdf
[75] ENISA Quarterly, June 2006, UK Information Security Breaches Survey 2006, pages 15-17.

eavesdrop and potentially gain access to sensitive information. Rogue hotspots are also believed to become the next platform for phishing attacks and identity theft[76].

The work on wireless security has however gained a lot of attention among the technicians and the standardization bodies. This is due primarily to discovered and exploited weaknesses in a few of the technologies, e.g. Bluetooth and WLAN. The security protocol for IEEE 802.11 (Wi-Fi), the Wired Equivalent Privacy (WEP) protocol, has proven flawed. This has initiated the work on a more secure protocol, and WEP is now replaced by the more secure Wi-Fi Protected Access (WPA) and WPA2, developed by the Wi-Fi Alliance.

Lately IEEE 802.16, known as WiMAX (Wireless Microwave Access), is emerging, as a standard for wide-range high speed broadband wireless access. The technology is promoted by the WiMAX Forum, organizing plugfests where to obtain product certification. The discovery of the security flaws of WEP has had the consequence that the WiMAX design has addressed security with priority. It has also to be considered that the security risks for WiMAX are likely to be increased compared to e.g. Wi-Fi, due to the long transmission range. This raises security and privacy issues, for example in surveillance applications, which are likely to become popular with the technology[77].

Mobile Services

Mobile phones are a kind of life accessory nowadays. The observed trend is the evolution towards smart personal devices, with open platforms, always-on and connected to the best available network (the "converged device"). On the network side, the observed trend is the migration to IP, with the proliferation of new, advanced services using the increasing bandwidth availability. The combination of those trends shows how security will play an increasing role.

The handset industry is evolving rapidly and it is anticipated that this will introduce new security risks. Mobile phones, personal digital assistants (PDAs), and smartphones continuously enhance their capabilities, and the trend for open platforms such as Symbian and Windows Mobile, makes the mobile phone not that distant from the functionalities of a PC. Mobile device malware is an emerging threat of the latest years. This, together with the migration of the networks towards the Fixed Mobile Convergence and towards the IP technology as the underlying, common platform, will make the Internet threats possible also in mobile environments[78]. This offers new attack vectors that isolated access technologies may not have otherwise introduced as a risk. The support for the dual-mode mobile handset (3G-WLAN) is now

[76] http://www.rsasecurity.com/press_release.asp?doc_id=6870&id=1034
[77] OECD, The Implications of WiMAX for Competition and Regulation, March 2006, http://www.oecd.org/dataoecd/32/7/36218739.pdf
[78] "The PSG Vision for ENISA", May 2006, http://www.enisa.europa.eu/doc/pdf/news/psgvisionforenisafinaladoptedmay2006version.pdf

standardized[79] and under testing[80], effectively allowing the same device to connect seamlessly to different access networks. SMS, MMS, uncontrolled channels such as Bluetooth[81] can be vectors for malware and spam, and the security challenges simply increase when wireless ad-hoc networks can be created. The problem of over-the-air provisioning (OTA e.g. in OMA) becomes critical, in order to securely manage the terminal. Furthermore, the mobile phone can be equipped e.g. with RFID technology and become a mobile wallet, opening to the security considerations valid for RFID. Efforts such as Trusted Computing are on-going to make the device a trusted platform and enabler for secure applications. At the same time, the network itself needs to ensure additional checking points to assist the end user and protect itself; examples of this being the session border controller (SBC) in the NGN network and the need for more extensive content screening (which does not combine with e2e security).

The evolution and enhancement of wireless technologies, offering higher bandwidth and always-on connectivity, allows for new mobile services such as advanced multimedia applications and multicast/broadcast. The security solutions for those are yet under design (e.g., multimedia security, MBMS).

Emerging wireless networks and technologies

The emerging of a few other wireless technologies can be observed, and anticipated to have security implications:

- *RFID* (see Section 2.3 hereafter)
- *Wireless sensor networks*, characterized by limited resources and a possibly highly untrustworthy environment[82]
- *Software defined radio* (SDR), an emerging technology capturing worldwide interest and investments. SDR consists of a flexible radio controlled by software running on a device. SDR essentially allows for upgrading or completely changing the features of the device by simply loading new software, for example switching between completely incompatible radio frequencies and transport techniques. SDR techniques require a proper balance between security and functionality. Security has however to be seen as an important component, especially in certain applications (such as military).

[79] The Unlicensed Mobile Access (UMA) standard has been developed, promoting Fixed Mobile Convergence. UMA allows for seamless roaming and handover between e.g. GSM/UMTS and unlicensed wireless networks such as Bluetooth and Wi-Fi. The UMA standard has been developed by the UMA Consortium (UMAC), http://www.umatechnology.org , and is now adopted by 3GPP as Generic Access Network (GAN).

[80] For example, the Nokia 2006 pilot project in Finland, http://www.nokia.com/A4136001?newsid=1066083

[81] Bluetooth is another wireless standard, IEEE 802.15.1. Examples of viruses that can spread over Bluetooth: http://www.f-secure.com/v-descs/cabir.shtml and http://www.f-secure.com/v-descs/commwarrior_a.shtml

[82] ENISA Quarterly, March 2006, Security in Wireless Sensor Networks: Status, Problems, Current Technologies and Trends, page 5.

Examples of security risks with high priority are eavesdropping, malicious radio software, fraud[83].

Fora

IEEE is a widely recognized association developing wireless standards, e.g. IEEE 802.11 for Wi-Fi, IEEE 802.15 for Bluetooth, and IEEE 802.16 for WiMAX (http://standards.ieee.org/wireless/). Reference fora include the Wi-Fi Forum for WLAN (http://wi-fi.org/) and the WiMAX Forum (http://www.wimaxforum.org). NIST is working on the publication of a Special Publication on security for WLAN (IEEE 802.11i)[84]. 3GPP is the standardization body for 3G mobile networks.

SDR is discussed in the SDR Forum, http://www.sdrforum.org/. ETSI is organizing a Workshop on SDR and Cognitive radio, http://portal.etsi.org/sdrworkshop/.

IETF supports the activities of these fora with protocol and architecture design. There are many IETF Working Groups related to wireless and mobile networks, especially in the Internet Area, e.g. the 6loWPAN (IPv6 over Low power Wireless PAN) WG and the eap (Extensible Authentication Protocol) WG. In the Security Area, the emu WG is working on EAP method update and the (now closed) mobike WG on multi-homing and mobility. OMA develops mobile services.

Discussion

For the large impact that they have on society, wireless technologies are critical areas where the security community should concentrate efforts. As past experience has shown, wireless is by its own nature a link highly susceptible to security attacks. It should be noted that the impact on society includes the direct use of such technologies done by citizens, but also the increasing practice of adopting wireless accesses within enterprises and critical infrastructures (CI). The lack of good security practices within these users makes wireless technologies easy-accessible vectors of attacks. Hence, it is important to promote efforts to assess the risks related to the single technologies, compile best practices and disseminate those to home and enterprise users, in order to increase the awareness of the risks. A clear risk assessment for emerging technologies such as SDR is important, given also the applications where they are likely to be used (military, CI and emergency, but also widely spread commercial systems). Finally, **activities of deployment and dissemination fora should be highly promoted** (e.g. the Wi-Fi Forum and the WiMAX Forum), as they enhance interoperability and can offer **product certifications where security can be included as a necessary functionality to be tested**.

[83] SDR Forum contribution, Security WG, High Level SDR Security Requirements, http://www.sdrforum.org/uploads/pub_31718206_i_0001_v0_00_high_leve_security_rqmts_01_11_06.pdf

[84] Draft SP 800-97, Guide to IEEE 802.11i: Robust Security Networks, http://csrc.nist.gov/publications/drafts/Draft-SP800-97.pdf

2.3. RFID

Background

Radio Frequency Identification (RFID) is the technology for automated identification of objects, where a small portable device, a tag, can communicate with a reader via radio signals, so that the data stored in the tag can be deployed with the involvement of a background infrastructure. The tag may be activated by the reader, including the energy needed for the tag to communicate (passive tag), or may have internal power source (active tag). There are an enormous number of applications where RFID can be deployed: inventory tracking, transport, logistic, warehouse management, supply chain management, medical applications (e.g. location of staff and patients), personal identity systems such as passports, access control, etc[85], and new markets are constantly being created. The use of RFID in mobile communications is also promising; it may be used for presence indication, to enhance location-based services, to store personal information, to allow mobile payments, etc[86]. It has been predicted that the RFID technology will bring a revolution in the industry area, and, as early implementation of pervasive (or ubiquitous) computing, it will also have a strong impact on society and individuals' life. However, there is still a lot of work (in research, standardization, and identification of business applications), required to fully develop the technology and understand all its possibilities. We concentrate hereby on security.

Security Aspects

At this point in time, it is clear that security and privacy issues will likely hinder the full deployment of the RFID technology, unless addressed in appropriate way[87]. The security concerns related to RFID are many: unauthorized disabling of the tag, spoofing, interception, unauthorized read/write of the tag, etc.[88]. For example, tags are easy to read (they are small, generally they stay switched on, and they can have a variable reading range) and it is difficult for the user to realize their misuse when it happens. The wireless nature of the communication, coupled with the decreasing size of the sensors, makes it easy to intercept and with little chance of detection[89]. This is clearly a huge concern when the RFID is carrying personal information, for example in the case of e-passport (risk of identity theft) and medical applications, but also for

[85] For more examples and their descriptions, see http://www.itu.int/ITU-T/techwatch/docs/rfid.pdf and http://www.itu.int/osg/spu/ni/ubiquitous/Papers/RFID%20background%20paper.pdf

[86] See the ITU-T Lighthouse Technical Paper, RFID Opportunities for mobile telecommunication services, May 2005, http://www.itu.int/ITU-T/techwatch/docs/rfid.pdf

[87] It was observed that the RFID design of 2005, with its features, may be still in use in 2020. Jari Juels, RSA, RFID Privacy: a technical primer for the non-technical reader, http://www.rsasecurity.com/rsalabs/staff/bios/ajuels/publications/rfid_privacy/DePaul23Feb05Draft.pdf

[88] http://www.rsasecurity.com/rsalabs/node.asp?id=2115

[89] One later attack that has gained attention concerns breach of latest generation of credit cards, announced by the RFID Consortium for Security and Privacy (RFID-CUSP), http://www.rfid-cusp.org/blog/blog-23-10-2006.html

unauthorized tracking of the user's activities. RFID may be linked to databases and credit card or royalty cards, which allows for tracking consumers. One of the most debatable areas is the implantable RFID, e.g. for animals and humans[90].

While it should be kept in mind that RFID security is not only a consumer matter, but also government and corporate (since RFID may be also used for their applications), it is at the consumers' side that the security debate is hitting at most, especially for privacy issues. Massive criticism has been voiced publicly, e.g. by consumers groups[91].

RFID malware is also anticipated as a threat. Researchers have warned[92] that RFID can be infected by viruses and malware, and are vulnerable in the same ways as other technologies, including by buffer overflow and SQL injection attacks. They also stressed the fact that the RFID technology does not only include the tag and the reader, but it is a whole infrastructure (e.g. databases) that requires a comprehensive security solution, and that the implicit trust in the integrity of the data from the RFID tag may not be a wise assumption.

A few protection mechanisms have been proposed, such as blocker tags, possibility to reduce the transmission range, kill switches to disable the tag before leaving the store, anonymous authentication that proves the membership to a group but not the single identity[93], and solutions such as wallets that block RFID transmission. However, these "ah-hoc" measures have limitations.

It is possible to prevent several of these issues, using cryptographic techniques, for example encryption (which however does not solve entirely the issue of tracking, related to privacy). However this adds costs and RFID do not implement it. Low cost will in general be prioritized over functionality in RFID. Traditional cryptographic techniques are not easily applicable here since RFID exhibit tight requirements in terms of scalability and computation cost. Lightweight, optimized crypto solutions need to be found (ECRYPT for example is working on this, within e.g. its eStream initiative, Profile 2), and key management remains one of the hardest challenges. For the time being, the applications are simple but they are expected in the future to become more complex, and the security requirements are expected to be different for each application. Tags in the future are expected to have often network capabilities (active tags); this means for example the need to study the relation to IPv6 and the

[90] E.g. VeriChip is a human-implantable RFID microchip, http://www.verichipcorp.com.
[91] See for example the opposition to the pervasive use of RFID technology voiced by the Electronic Privacy Information Centre (EPIC, http://www.epic.org/privacy/rfid/), and by the Consumers against Supermarket Privacy Invasion and Numbering (CASPIAN, http://www.nocards.org/ and http://www.spychips.com/).
[92] Is Your Cat Infected with a Computer Virus?, by the Amsterdam Free University in The Netherlands, http://www.rfidvirus.org/papers/percom.06.pdf
[93] For an extensive list, as well as a survey on the RFID security topic, see the paper "RFID Security and Privacy: A Research Survey", by Ari Juels, RSA, http://www.rsasecurity.com/rsalabs/node.asp?id=2937

integration in the converged networks landscape, towards the implementation of the ubiquitous computing.

Fora

Several leading global organizations and trade associations are involved in the standardization of the technology, although the security work is not yet developed. As pointed out by ITU-T[94], there is a broad variety of players, but lack of harmonized, globally accepted standards for RFID, especially in the area of data structure, network components, and protocols.

ISO has been working on RFID standards initiatives for long time, for example in JTC1 subcommittees 17 and 31. ANSI is also involved in RFID standardization (standards NCITS 256). ETSI TG34 developed the standard EN 302.208 and EN 300.220. EPCglobal[95] is the leading entity for the industry-driven standards for the Electronic Product Code as worldwide RFID standard. ITU investigates the technology in its Technology Watch[96] and organized a dedicated workshop at the beginning of 2006[97]. The European Commission has run a public consultation on RFID[98]. OECD has also investigated the security implications of RFID[99]. NIST is working on guidance for securing RFID with Draft Special Publication 800-98.

Discussion

It appears clear that the public perceives RFID technology as controversial. The security and privacy features (linked to the perceived trust) will impact the acceptance and the adoption of the technology. On the other hand, it is also likely that there will be a tradeoff between privacy and features that make RFID attractive, such as convenience and easy access to information. The balance between privacy and usage for this technology appears extremely delicate, but needed for the technology to take off.

It should be also clear that it is not only the specific RFID technology to be under scrutiny, but the all concept of ubiquitous computing (or pervasive computing), of which RFID are early implementations and that appear the trend of the ICT of the future. **New impulse and work should be dedicated to identify the security (including privacy) requirements, through a dialogue with the different stakeholders including consumers.** Research should also be promoted in the field of

[94] http://www.itu.int/ITU-T/techwatch/docs/rfid.pdf. The report also contains a list of fora involved in RFID standards.
[95] http://www.epcglobalinc.org/home
[96] http://www.itu.int/ITU-T/techwatch/ubiquitous.asp
[97] http://www.itu.int/ITU-T/worksem/rfid/program.html
[98] http://ec.europa.eu/information_society/policy/rfid/index_en.htm
[99] DSTI/ICCP(2005)19/FINAL, Radio-Frequency Identification (RFID): Drivers, Challenges and Public Policy Considerations, 2006, http://www.oecd.org/dataoecd/57/43/36323191.pdf, and DSTI/ICCP(2006)7, Proceedings of OECD Foresight Forum, RFID Applications and Public Policy Considerations, 2005, http://www.oecd.org/dataoecd/59/12/36069207.pdf

optimized security solutions, in particular lightweight and privacy-enabling cryptography. There should be an effort in bringing to the public the explanation of the technology and its real benefits, and making the security investigations public. In this way it would be possible to improve the public perception, increasing the trust in new, pervasive technologies. Here ENISA could play an important role, with information sharing, and collection and dissemination of best practices, but also enhancing the international collaboration to reach a common vision of ubiquitous ICT.

It is observed that the privacy discussion for RFID is quite extensive, as privacy has been clearly identified as an issue to be urgently addressed. However, the same is not yet true for other technologies which would enable ubiquitous computing, for example sensors (e.g., sensor networks) and more generally, location-based technologies. The security and privacy debates need to be extended to cover also these emerging technologies.

The standardization landscape is not structured; there is a lot of fragmentation and lack of interoperability. Security is not yet addressed to the extent it should, nor it is clear in which fora it should take place. This will likely hinder the technology and should be addressed with priority, to enable Europe's competitiveness in this important business and social area. For example, cryptographic standards for RFID are needed to allow interoperable technologies, and work on privacy is urged. Given the already extended debate, the RFID technology is one area where security and privacy can be integrated from the beginning, avoiding them to be an afterthought. Any action needs to address the different applications of the technology (as, for example, RFID applications in government may have different privacy and security implications than applications in certain business areas), and needs to consider that the technology itself will evolve very rapidly. Privacy impacts of RFID are not yet completely clear, and remain source of many controversies. **Legislation will have an important role in the investigation and affirmation of RFID privacy**, as well as in the definition of the monitoring in the development phase of RFID, so to protect its stakeholders, and ultimately the all society.

Ubiquitous computing

RFID are an example of pervasive computing technology, and are often seen as enablers of the so-called "ubiquitous computing". There are also a few other technologies and experiments that are paving the way to ubiquitous ICT, such as short-range communications (e.g. Bluetooth and Zigbee, based on the Near Field Communication, NFC, standard) and sensor networks. Wireless technologies are key enablers for ubiquitous computing.

Ubiquitous computing indicates a large number of tiny sensors, blended seamlessly in the environment and able to acquire data in order to provide context-awareness (including identification of objects and localization).

Ubiquitous computing and its pervasiveness are predicted to bring a radical change in the society[100]. However (the RFID experiment confirming this), it is predicted that one of the main challenges for ubiquitous ICT will be to achieve a balance with security, in particular privacy. The scenario of tiny radio sensors able to communicate seamlessly to each other, carry and collect data, suggests that this same data will become valuable hence more vulnerable. The location awareness that these technologies bring, is also a concern to privacy. Furthermore, the dependency on the ICT infrastructure will become much stronger, leading to high risk to infrastructure's availability.

Ubiquitous computing also urges further research and standardization in several other emerging technologies involved and their security. While security implications of RFID are highly discussed nowadays, the status of the investigation is still limited for other less mature technologies, such as sensor networks. Further research is also needed in the field of broadcast communications, and highly distributed applications. Cryptography for sensor networks has specific challenges to face, due to the hostile nature of the environment and the limitations of the technology (e.g., energy, computation, cost), which do not allow for using expensive cryptographic operations (e.g., public key based), ask for efficient key management, and requires lightweight cryptographic mechanisms.

[100] The "Internet of things", ITU, Ubiquitous Network Societies: Their Impact on the Telecommunication Industry", background paper for the ITU Workshop on Ubiquitous Societies, 2005, http://www.itu.int/osg/spu/ni/ubiquitous/Papers/UNSImpactPaper.pdf

The Grid

Yet an aspect of ubiquitous ICT and convergence, the Grid is an emerging model for distributed computing. It allows many networked computer to cooperate in a virtual architecture, deploying otherwise unused resources. This is advantageous to solve large-scale computation problems, such as research problems and weather forecast. A clear feature of the Grid is that it relies on open standards. Major forum in Grid design and standardization is the Global Grid Forum (GGF), defining the Grid architecture specification called Open Grid Services Architecture (OGSA), based on Web Services. GGF has recently merged with the Enterprise Grid Alliance (EGA, addressing Grid standards specifically at the enterprise level, http://www.gridalliance.org) to form the Open Grid Forum (OGF, http://www.ogf.org/). Lately ETSI has announced a new Technical Committee, GRID. Distributing computing of the scale of the Grid has obviously security implications, e.g. authentication, authorization, security related to resource management, data storage, and secure communications[101]. EGA has released a requirement specification for the enterprise Grid, including a list of related standards[102].

[101] http://www.princeton.edu/~jdwoskin/grid/index.html

[102] http://www.gridalliance.org/en/documents/TWGDocs/ega-grid_security_requirements-v1Approved.pdf

2.4. VoIP and Multimedia

Background

Voice over IP (VoIP) is an application carrying voice over the packet switched (IP) network, and is today a trend rapidly emerging in telecommunications[103]. VoIP is seeing a rapid commercial adoption, gaining momentum in all sectors, users, major telecommunications carriers, enterprises, and is expected to grow further with the take-off of IMS, as well as with the spread of transport technologies such as 3G, Wi-Fi, WiMAX, and broadband.

VoIP implies the merging of the telephony infrastructure and the data network, with advantage in terms of cost, flexibility, and mobility, among others. Skype is a well-known example of VoIP application, although it differentiates from other VoIP systems by operating on a peer-to-peer model and by maintaining proprietary the software. The emerging IP Multimedia Subsystem (IMS), has VoIP as one component and re-uses some of its protocols. The ITU-T H.323 umbrella recommendation, defining the protocols to provide audio-visual communication sessions in packet networks, is used for carrying VoIP and IP-based videoconferencing. The Open Mobile Alliance (OMA) has released the first version of the Push to Talk over Cellular (PoC) service, which is an open standard for Push To Talk (PTT) walkie-talkie technology and uses VoIP (IMS) to stream voice over data networks such as GPRS.

Security Aspects

The security of VoIP has been scrutinized for quite some time, since it is felt as deterrent for the full success of the technology. Stakeholders appear suspicious towards this application that relies on the IP technology and as such may be open to all the threats that are observed in Internet, and are urgently requesting analysis and standardized tools to secure it. VoIP security breaches also find strong visibility in the press[104], contributing to the pressure in demand of security solutions for VoIP. The Skype debate has generated many articles on the real security of the application, and assessments have been made[105]. Several are the bodies involved in the security

[103] Many statistics are available online. For example, the Telecommunications Industry Association (TIA) reported 4 millions residential VoIP customers (not including PC-to-PC services) in 2005, with an expectation of 18 millions by 2009.
http://www.tiaonline.org/business/media/press_releases/2006/PR06-19.cfm
There are also experts who believes that by 2006, 50% of the world's traffic will be using VoIP (reported by OECD, VoIP: Developments in the Market, January 2006, http://www.oecd.org/dataoecd/56/24/35955832.pdf).

[104] As example, http://www.networkingpipeline.com/news/188702745

[105] Berson, "Skype Security Evaluation" (http://www.anagram.com/berson/abskyeval.html); Biondi and Desclaux, "Silver Needle in the Skype" (http://www.secdev.org/conf/skype_BHEU06.handout.pdf).

analysis of VoIP. The Voice over IP Security Alliance (VOIPSA) drives the adoption of VoIP and focus on threat taxonomy and security requirement. NIST wrote the Special Publication SP 800-58, "Security considerations for VoIP systems"[106], which provides an extensive analysis of VoIP threats, the efforts in the area, and the different possible security mechanisms. The report clearly warns about the need for careful security considerations when VoIP is adopted.

The effort among standardization bodies is to secure VoIP using the security mechanisms that are used in data networks (see "Fora" below). VoIP presents a number of constrained requirements to meet users' expectations, quality of service and service attractiveness, in particular in terms of delay, jitter, packet loss, and bandwidth consumption. Even tighter requirements are present in the case of the wireless version of VoIP, VoIPoW. This implies that a number of traditional network security components, such as firewalls and intrusion detection systems, need to be specialized otherwise they would degrade the quality or would simply hinder the service. Similarly, security protocols and trust models need to keep into account the characteristics of this constrained service. For example, VoIP and in general multimedia services show relevant issues with respect to firewalls[107] and NATs[108].

One major security issue that is foreseen in VoIP is the lack of reliability of IP, worsened when the Internet is used. VoIP offers low costs and flexibility but not a reliability degree that is comparable to the traditional telephony system. This for example foments the debate on the dependency of critical government services on VoIP, and on the consequences of its vulnerabilities, a topic that sees the US in the frontline[109]. Enterprises embracing VoIP are suggested to a careful planning including a security assessment[110].

Among the different components of VoIP, signalling (or call control) and media deserve a special attention. The signalling can be based on two main alternative standard protocols, H.323 (developed by ITU-T) and the Session Initiation Protocol (SIP). SIP is the one that seems to be emerging, especially after the adoption by 3GPP as base for the IMS system. SIP security is defined in IETF at the protocol level, and by 3GPP and ETSI TISPAN at the system level by liaising with IETF and leveraging on its protocol and architecture work. One feature of SIP is its hop-by-hop nature, as it makes use of middle agents to manage the call signalling. Hence, also the protection of the signalling (needed to avoid many attacks, such as manipulation, session hijacking, and call redirection) is not end-to-end (e2e) but relies on the trust to proxies on the path. However, this trust model is not adequate when keying material intended

[106] http://csrc.nist.gov/publications/nistpubs/800-58/SP800-58-final.pdf
[107] NIST SP 800-58, chapter 7.
[108] See for example IETF draft Best Current Practices for NAT Traversal for SIP, draft-ietf-sipping-nat-scenarios-05, and NIST SP 800-58, chapter 7.
[109] See e.g. CSIA, Cyber Security for IP Telephony, https://www.csialliance.org/resources/pdfs/CSIA_VOIP_May_2005.pdf
[110] In UK half of the companies that have implemented VoIP did not evaluate the security risks. ENISA Quarterly, June 2006, UK Information Security Breaches Survey 2006, pages 15-17.

for end-to-end security of the media (e.g., voice and video) is transported within the session call setup itself (e.g., SIP), as the proxies can access it. End-to-end protection of the SIP payload is standardized (S/MIME for part of the SIP message), however it is not widely deployed.

Confidentiality of the media (e.g., voice in the case of VoIP) is felt as a needed security service, given the openness and accessibility of IP compared to traditional telephony. There are a few standards available for media protection (e.g., IPsec, SRTP, DTLS), however none of them for the moment has really emerged nor seems to clearly cover all the needs. One issue is that the architecture is quite complex and the protocols are feature-rich and perform diverse tasks, hence the security requirements are quite many and evolving. The work and standardization efforts have been accelerated lately, since there is now market pressure for a comprehensive VoIP security solution including media protection. Telecom bodies (e.g. TISPAN and 3GPP) are investigating solutions, and IETF has undertaken a larger attempt to identify needs and suitable protocols for multimedia security.

There are a multitude of other threats undermining VoIP, which are inherited from the data-type of network. Phishing over VoIP or "*vishing*"[111] is an example of emerging threat for VoIP, where phone calls are used instead of e-mails to carry phishing attacks. Vishing proves once more how adaptable attackers are: while there are many warnings on phishing by e-mail, users are not prepared for this new attack approach using calls (hence, once more, awareness of emerging threats proves to be critical). *SPIT* (spam over IP telephony) has received attention lately by the security community and is expected to become an emerging threat in short time (work to address it has started for example in the IETF sipping and speermint working groups).

The technology has yet to mature its privacy framework, and has also generated a large debate on legal issues. In particular, lawful interception solutions are under definition for TISPAN and 3GPP systems, while pure VoIP lawful interception is encountering high resistance[112].

Fora

Multimedia (including VoIP) security is addressed in many different fora.

IETF designs the security solution at the protocol level. IETF is the owner of the multimedia protocols and scatters the security work among several Working Groups,

[111] http://www.computerworld.com.au/index.php/id;914515065;relcomp;1
http://www.linuxsecurity.com/content/view/123625/65/
http://news.bbc.co.uk/2/hi/technology/5187518.stm
http://www.usatoday.com/money/industries/technology/2006-11-26-phishing-usat_x.htm?csp=34

[112] A recent paper, Security Implications of Applying the Communications Assistance to Law Enforcement Act to Voice over IP, argues about the technical difficulties of implementing VoIP wiretapping (due to the mobility and the Internet paradigm compared to PSTN), and also argues that the law would bring the destruction of US leadership in the telecom world, http://www.itaa.org/news/docs/CALEAVOIPreport.pdf

especially in the RAI Area with the design on multimedia. The msec WG specifies key management solutions and security protection for group/multicast communications. The ecrit WG addresses the issues related to public emergency calls using VoIP and Internet multimedia systems, a topic that the industry recognizes as possibly hindering the deployment of VoIP.

The telecommunication bodies are developing the multimedia systems, which have VoIP as a component and use some of the multimedia IETF protocols. 3GPP is the owner of IMS, based on the IETF SIP standard; ITU-T is the owner of H.323 and related standards (H.235 for security). ITU-T and ETSI TISPAN are working on the NGN architecture. OMA develops the Push To Talk over Cellular (PoC) service specifications. Other bodies involved in multimedia and VoIP security include NIST (SP 800-58), VOIPSA (threat taxonomy and security requirements), and CSIA.

Discussion

VoIP is an example of a fast paced technology with high potentialities, which has discovered security as a possible deterrent from its full success. VoIP is also one of the technologies whose security has been most largely brought to the attention of the public at large. This has the positive effect of increasing public awareness, however it may harm if it is limited to press releases stressing only the negative effects. While open reports of breaches should be largely promoted, these reports should also be accompanied by proper awareness campaigns, and education campaigns disseminating best practices. This practice is not followed for the time being. Indeed **user awareness and education** are of paramount importance, especially when emerging threats like phishing are exploiting new means such as VoIP.

Standardization bodies, as well as industry and academy groups, have now started working to define security solutions for VoIP and multimedia applications. Their action should be strongly encouraged.

Enterprises planning to adopt VoIP should, as in the case of adoption of any new technology and application, assess its integration in the existing infrastructure in order to identify and address possible risks. VoIP in fact promises to bring beneficial changes, but the migration towards such new, open technology requires appropriate threat and risk assessment plan. In particular, reliability of the infrastructure is, more then ever, a critical asset. Finally, adoption of VoIP for government services and critical infrastructure still requires technical work, such as to guarantee emergency service and reliability.

2.5. Next Generation Network and Network Convergence

Background

The concept of network convergence (or Next Generation Network, NGN[113]) sees the user accessing services in a seamless way over the most appropriate access network, while the core network is shared, and is access - and service -independent. The core network is packet transport based, extensively based on the Internet Protocol (IP) technology, and the different network layers (transport, control, services) use open standardized interfaces. This architecture strongly simplifies the development of applications, which do not need to take into consideration the properties of possibly different underneath transport layers. Telephony itself becomes, in this converged network scenario, only one of the services.

The convergence is built over the Session Initiation Protocol-based IP Multimedia Subsystem (SIP-based IMS) platform, which is the core of the 3rd Generation Partnership Project (3GPP) and 3GPP2 architectures and is expected to be the future IP platform for the mobile multimedia world.

We observe once more, in this network converged scenario, that the different technologies can not be considered isolated but need to be considered and evaluated as components of services and other technologies. For example, the emerging of the multimedia communications in NGN networks is a driving force for IPv6. Network pervasiveness, including wireless technologies and therefore always-available connectivity, is an enabler for network convergence.

Security Aspects

Security represents a challenge in this converged, IP-based network, and it is identified by ITU as an essential NGN enabler and differentiator. The use of the IP technology itself exposes networks to all the range of threats that are known (and yet unknown) in the Internet, due to the openness of the technology. However, the awareness of risks related to IP has the positive side effect that security is taken into a great deal of consideration in the NGN development. Operators increasingly demand clear security solutions, with the result that security standardization is active and vendors make efforts to provide security. In addition to usual security issues, such as network access authentication, network security, etc., there are a few security issues that specifically characterize the converged environment. We focus on these in the remainder of the section, on the base of discussions that were observed in the 3GPP and TISPAN relevant groups.

The converged network integrates voice, video, and data (the “Triple Play”). These applications per-se have different requirements; in particular, they may require real-time transmission, which poses a number of constraints. Furthermore, each access

[113] For the ITU definition of NGN, see http://www.itu.int/ITU-T/ngn/definition.html

network presents its peculiar characteristics (see below). The result is the need to deal with demanding applications over constrained types of access. As it is not possible to know in advance which type of access is going to be available and used, it is imperative to have a security solution that fits the different cases without penalization. For example, the cellular access appears to be heavily constrained, due to its limitation in delay and bandwidth. Signalling and media security has taken into account these new requirements, with a strong tendency to push for lightweight protocols.

The use of only few security mechanisms, protocols, and equipment would simplify the architecture and would facilitate deployment in the converged networks. For example, it is beneficial to have a user authentication mechanism that is independent of the access. Short-lived options have been adopted, both in 3GPP IMS and TISPAN, with an implicit authentication mechanism where access to the service is granted on the base of a successful access to the underlying transport network, i.e. without requiring an explicit authentication to the multimedia service. This temporary solution shows that there is still some fear that security may hinder the service. The long term vision for access authentication sees explicit authentication to the IMS core network based on the (I)SIM[114]. However, this requires an upgrade of the legacy fixed devices, whose authentication traditionally relies on physical control. Therefore, co-existence of authentication mechanisms towards the IMS core network will likely occur. There will be implicit authentication based on the access network, alternatively explicit authentication based on (I)SIM for the terminals supporting it (with a debate on the feasibility of having a software implementation of it for fixed devices, which may be more easily susceptible to attacks – it being software-based). A compromise solution uses an IMS Residential Gateway with in-built ISIM, as an authenticator bridge between the legacy-based fixed devices space and the ISIM-based IMS core network, so avoiding changes in the legacy terminals but taking advantage of the secure ISIM authentication infrastructure.

[114] The IP Multimedia Services Identity Module (ISIM) is an application running on the Universal Integrated Circuit Card (UICC) smart card in a 3G mobile in IMS. As the SIM/USIM contain the credentials for accessing GSM respectively UMTS, so ISIM contains the identifiers and credentials the user needs to authenticate to the IMS (and vice versa).

IP Multimedia Subsystem (IMS)

Within the design effort of NGN (see below "Fora"), the IP Multimedia Subsystem (IMS) set of standards have emerged. IMS is the open standardized architecture developed by 3GPP. It is an all-IP[115] system allowing multimedia conversational communication (real-time speech, video, and other types of data). IMS takes advantage of the merging of the ubiquitous access provided by the mobile networks and the flexibility offered by the IP technology in service development. Facing the emergence of always new and innovative communication services, where people interact in a myriad of different ways, different access networks and different devices, IMS is intended to be the architecture to enable multimedia communications and allow for the development and delivery of new services and applications in a quick and standardized way. IP-based services to be offered over IMS may include Voice over IP (VoIP) and Push To Talk, presence-based services, videoconferencing, gaming, content sharing, multicasting, IP television, etc.

Originally designed for mobile networks, IMS has the advantage of being access-independent and can now be coupled also with other types of access network, for example WLAN (e.g., with the 3GPP-WLAN interworking) and fixed access (with standardization in ETSI TISPAN). It can also interwork with non-IMS networks via gateways. Core of the NGN architecture, and of the so-called Fixed Mobile Convergence (FMC), IMS represents the current key development in the telecom world.

The Session Initiation Protocol (SIP)[116] is the IMS signalling standard. SIP makes use of an infrastructure of proxies (called Call Session Control Functions, CSCFs, in IMS terms) to enable endpoints to discover each other (user location), determine their willingness to communicate (user availability), agree on the session parameters (user capabilities), setup and manage the session (modification, termination, addition/removal of participants). SIP supports personal mobility, as the users maintain a single public identifier regardless of their location.

Furthermore, SIP allows for the negotiation of the peers' capabilities, for example by carrying the Session Description Protocol (SDP, IETF RFC 4566), which describes the session media content (e.g., IP addresses and ports, codec negotiation, possibly key management). The media itself consists then, in typical scenarios, of packet streams of the actual content (e.g., voice and video samples) transported by the Real-time Transport Protocol (RTP, IETF RFC 3550).

[115] The term "all-IP system" identifies a system where the services are based on IP, and where IP goes all the way to the terminal.

[116] Better said, the implementation of SIP standardized by 3GPP. In fact, SIP (and protocols related to multimedia communications) is developed by IETF, and 3GPP deploys IETF specifications adapting them to its own architecture and services.

It has to be taken into account the fact that each access technology may be subject to different threats. As a generally well accepted best practice, the security solution can be designed only after a proper threat analysis and risk assessment, which in NGN requires a separate analysis for each access network. This is clear to the Standard Development Organizations (SDOs) involved in NGN design, e.g. with 3GPP investigating the cellular access and the WLAN-interworking access, and TISPAN investigating the wireline types of access. There must be in place, in the different access networks, security mechanisms to protect against the threats of that particular access; the security measures must protect the users within the access, the access network itself, and the common core network connected to that specific access network, both from inside attacks and outside attacks.

For instance, the wireline type of access (e.g., xDSL, and especially broadband) allows for high bandwidth, therefore denial of service (DoS) attacks, and particularly distributed DoS (DDoS) attacks, are a major concern; similarly, a WLAN access poses several security issues. Other types of access, such as fixed wireless access, e.g. WiMAX, and short range wireless communication, e.g. Bluetooth, have still to be addressed.

Another tendency that can be observed is a strong improvement of security capabilities of the security network elements that protect the core elements. The IMS system uses the Session Border Controller (SBC)[117] at the points of interconnection of the core to other networks, as well as to the fixed access networks. The SBC implements a variety of functionalities in support of multimedia services, including network address translators (both for the signalling and the media), traffic shaping, protocol interworking, interception, and service level agreements (SLA) enforcement. The SBC also provides security functions, including firewall, access control, topology hiding, and DoS mitigation. The market for SBC is quite strong, however the deployment of such middleboxes has hindering security implications such as the break of end-to-end security.

The fixed types of access are then characterized by network access translators (NATs) and firewalls at the enterprise/residential side. This challenges (security) protocols in the NGN system, and for example requires TISPAN to keep this into consideration when aligning to the 3GPP IMS. Vendors often offer proprietary solutions to solve the NAT/firewall traversal, although there are also standard technologies developed within IETF (e.g., protocols such as STUN, ICE, and UDP encapsulation). Indeed NAT and firewall traversals are issues that have been investigated for many years, but are still pertinent, not completely solved, and are particularly cumbersome for multimedia applications[118].

[117] IETF draft, Requirements from SIP (Session Initiation Protocol) Session Border Control Deployments, draft-camarillo-sipping-sbc-funcs.
[118] See for example IETF draft Best Current Practices for NAT Traversal for SIP, draft-ietf-sipping-nat-scenarios-05.

Key management solutions always show to be among the trickiest security components, not only for credential handling, but, in this new, heterogeneous environment, also for their computational, bandwidth, and latency loads (e.g., see the work on MIKEY and IKEv2). Media security presents similar issues. Different security protocols can be used at the different stack layers, with IPsec being (at the network layer) a strong candidate. However, it is not completely suitable, and moving towards the application layer can better fulfill the new requirements (e.g., SRTP as application security protocol for RTP). The discussion on multimedia security is on-going in the standardization bodies. 3GPP has adopted media security for its Broadcast/Multicast Service (MBMS) architecture, based on the protocols MIKEY and SRTP, to apply access control, and has begun a work item on media security for IMS. TISPAN is also investigating the issue. While the topic has been on the table for quite some time, it is observed that the business case is not completely accepted in 3GPP and TISPAN (the protection of the media -the user plane content- is traditionally not addressed by telecom standards) and that the requirements are not fully comprehended. IETF is now undertaking the process of collecting all requirements and proposing a solution (or, more likely, a framework) for multimedia security.

Other security aspects to be addressed in NGN include spam and those related to emergency communications.

Fora

NGN, as wireline and converged architecture, is developed by the ETSI TISPAN Technical Body, and by ITU-T NGN. They leverage on other SDOs on three levels:

- System architecture: 3GPP and 3GPP2 (e.g., the IMS core, the Presence service, 3GPP-WLAN Interworking).
- Protocols: IETF, in particular the RAI Area.
- Services: primarily OMA (developing IMS services such as Push To Talk and Instant Messaging) and the Parlay Group (defining the standard APIs).

Discussion

NGN is expected to introduce a substantial evolution in the communications landscape. Security is one of the critical components of NGN, and has been identified by ITU as an essential NGN enabler and differentiator. NGN is a complex architecture and this puts many requirements on the design of the security solution.

However, the market is reacting, under customers' pressure, and there are several standardization bodies investigating the different security aspects. These bodies show high security awareness, and spend comprehensive efforts in being sure that security considerations are kept in mind and addressed in the different phases of the design of the architecture and of the functionalities. The business component is predominant here, hence there is always an effort to find a balance between security and business aspects such as time-to-market and usability. There is still the tendency to look at

security suspiciously, more as an obstacle than as an enabler. However this tendency is slowly corrected under a strong pressure of customers (including providers and users) for better security. Furthermore, the different components needed for the security solution appear to be understood and worked out, or they are on the way to be.

It has to be noted that NGN design is crossing several standardization efforts and borrows components that are designed in different bodies. This is indeed an excellent possibility to improve the collaboration among standardization bodies, which, after initially difficult periods, are now actively engaged into liaisons activities among them. This **liaison between standardization bodies activities has to be strongly encouraged, as it can help overcoming standardization fragmentation and facilitate interoperability**.

One area where improvement could be offered is the **creation of standardized checklists of baseline security requirements**, enabling customers (e.g. providers, users) to verify if a product has the necessary security functionalities, but also to allow them to input new requirements to e.g. standardization bodies, vendors, providers. Some have started to appear, e.g. in the IETF opsec WG. In this context, the use of Common Criteria Protection Profiles and Security Targets may also be worth considering.

Conclusions

Information and Communication Technology (ICT) grows at a fast pace and with it, dependability increases. Security, in this context, is raising lately a lot of attention. Efforts to provide security solutions are appearing in many disparate initiatives, and security has now gained visibility in different fora involved in the design of ICT. Lately, the migration toward the Internet Protocol (IP) technology as common base technology for communications has contributed to increase the security discussion, since the IP technology is often associated with the threats that occur in the open Internet, which has gained a very poor reputation for its security, exacerbated by media headlines.

The pressure from customers to have security solutions has increased. On the business side, also top management is realizing the cost of poor security; on the citizens' side, privacy gets a special attention, for example with respect to the use of biometrics and RFID, and new threats such as phishing bring direct financial losses; and on the legislation side, privacy and dependability need to be addressed for the common well-being. This pressure has lead to a market reaction, activating standardization bodies into developing security solutions.

Standardization is an important process for security. Products that claim to adhere to a standard can be checked against it, and transparency is improved. Open standards are preferred over security by obscurity, which hinders interoperability and has proven a failure. We see now that the market turns to standards to have security solutions. Emerging technologies and threats bring into standardization the challenge to improve the speed of response to address their security needs. Industry groups' specifications are generally faster to address needs in the short term, while formal standard development organizations (SDOs) generally requires longer time to develop specifications which however are advantageous in the long term. The good news is that security is taken seriously by many of the standardization bodies, sometimes even considered an enabler and differentiator (see for example the NGN case), not a hindrance to competitiveness. While this proliferation of initiatives is a sign that security is getting attention, on the other hand it brings *fragmentation*. This implies that it is difficult to find out what is happening and where, but also that there is danger of duplication as well as gaps, and that it is difficult to understand where the different security facets need to be addressed for complex technologies and applications (such as RFID). Furthermore, the existence of multiple security solutions, while often justified by different security requirements in different scenarios, may also have the double-edged sword effect that the market gets confused, unsure on the direction to take, and that the effect of a given security solution is limited. However, it can be noticed that lately many of the standardization bodies are engaged into efforts for closer collaboration with other SDOs, in the form of liaison activities.

In the struggle to make security an integral part of a technology design and not an 'add-on' or after-thought, it is important for security to be present in standardization. It is also the case that standardization activities are based on the consensus principle, hence they offer reliable solution, more likely to be adopted. The role of legislation here needs to seek the right balance in order not to hinder the technological development, such as in the case of anti-spam regulation and privacy laws, but can contribute largely in making sure that security is considered at early stages and through out the product lifecycle (e.g., software assurance) and in facilitating the convergence of the points of view of the different stakeholders (e.g. making sure that the user point of view is heard, for example in relation to private concerns of RFID and biometrics). In particular, legislation is an essential player when it comes to privacy, which otherwise would risk not to be taken appropriately into account. This is for example important in the case of privacy for RFID and biometrics. The work done by the European Commission in this field should be continuously supported and re-enforced.

There are security technologies available and new ones are emerging. One need of standardization bodies today is to assess the possibility to re-use existing standards also for emerging technologies and threats, versus the need to develop new ones. Existing solutions (e.g. IPsec) often are not plug&play tools but require generally tuning and optimizations to integrate into the environment and to the specific technologies and applications. A continuous new impulse is required to accommodate the new applications and scenarios. It is for example imperative to continue the research in cryptography, to address the new threats and the improvement of crypto-analysis, and to offer security solutions to the emerging technologies which bring new challenges (e.g. RFID). The exchange of experience (facilitated for example by platforms such as networks of excellence) and open design competitions (such as the one initialized by NIST for the new hash function and in the past for the cipher AES) are powerful tools for success.

The formulation of *comprehensive security requirements* remains one of the most crucial aspects to perform, in view of a successful security solution. This step becomes important noticing the increasing *complexity* of ICT, which likely implies higher complexity in the security solutions. Furthermore, many techniques encompass the technical sphere and goes into the social sphere, where consumers' trust becomes the necessary condition for an application or service to take off. This is particularly valid for privacy matters, strongly affecting for example RFID, ubiquitous computing, and biometrics. Only a dialogue with the consumers and the different stakeholders, including legislation, can allow for the identification of the correct requirements. Indeed, privacy threats are anticipated to become of most concern in the near future, and need to be address at early stages of the design of emerging technologies.

Effective risk management is required, involving appropriate mixture of people, processes, and technologies. These types of considerations apply in special way to emerging technologies, and the need to assess their security implications in timely fashion. Risk management has also a prime role when the architecture becomes highly

distributed, such as with the advent of IPv6, and with open business scenarios (where the perimeter can not be easily defined, i.e. de-perimeterisation and Trusted Computing). Appropriate risk management tools are needed to simplify the technology assessment and to identify emerging risks (i.e., identify risks that might emerge through the use of future applications). ENISA will investigate important questions such as if existing risk assessment and risk management methods are able to identify emerging risks, which could be set into scenarios, and how to plan related actions.

Greater emphasis should be given into bringing research results into the standardization channel, which would be beneficial for example in the case of identity management case. Furthermore, for security to progress, we need first to assess properly the status of security in Europe. A shared *knowledge of incidents* is too limited and should be improved, with the creation of a facilitating platform for such incident reporting. This appears to be needed in particular for the assessment of the security posture of fundamental building blocks of the ICT infrastructure such as DNS and routing.

Pilot projects, similar to the ones existing for DNSSEC and IPv6, should continue to be largely promoted. The role of *public fora* operating for the proper deployment of a given technology shows to be advantageous also from the security perspective. These bodies are active in the promotion of a technology, conduct pilot projects (hence develop the business cases), oversee its deployment, with a particular attention that deployment issues are addressed timely. They also promote the correct implementation of specifications, for example by organizing interoperability events and issuing certificates (e.g. Wi-Fi Forum and the WiMAX Forum). They make sure that the design principles are propagated to other bodies (e.g. TCG and the Jericho Group). They can also promote the security solution in a more comprehensive way and facilitate security awareness among different target groups.

One observation permeates many of the fields that this report has looked into: *best practices* are fundamental for security to happen, many exist, yet very often they are not used. This lack of implementation of best practices unfortunately is a recurrent theme that crosses all the users' groups, from the ordinary citizen as service consumer, to - often - network administrators (as the example of infrastructure protection, routing and DNS, shows e.g. with the lack of appropriate filtering). The need for extensive promotion of best practices remains urgent more than ever. *Checklists for baseline security protection* could also be a useful tool for standardization to consider.

There are a few additional aspects that can accompany this overview of security developments.

The *economics of information security* is an emerging science and could play an important role in enabling security. This field requires incentives. It is not enough to address NIS from the technology point of view, but the business drivers behind it need

to be investigated, in order to bootstrap security at a broader level and from the very beginning. Indeed, business drivers are an essential base for standardization, and are needed for security to bloom there.

Complexity of standards is a topic that never phases-off. This is a problem that surfaces especially in the field of security, which often introduces complexity and has to find a balance with cost, functionality, and time-to-market. In particular, as for example voiced by the IETF community, security solutions often add complexity for the user. The usability problem often results in that the user turns off the security features or uses them improperly (e.g. the web certificate case, which verification is more a nuisance to the user, resulting often in a blind, automatic acceptance of the certificate). Indeed *usability* is a facet that is not enough taken into proper consideration by many of the security solutions. Usability requirements should be appropriately identified and given as input to standardization.

The business attitude identifying security as an 'add-on', often in tension with functionality and richness in features of products, is still existing, and the priority of addressing security requirements is generally not high. However, this trend is slowly changing, although needs incentives to speed up. Top managements are starting to see the value of security, thanks to their higher awareness of the risks that their business can encounter when exposed (brand damage, lost of competitiveness, copyright breach, etc.) but also thanks to increasing attention paid to security by customers. This is what is called "*culture of security*", which needs to span all the hierarchy, from users to top management, triggering a positive demand chain. ENISA is largely engaged in fostering this culture of security.

Generally, tackling a security issue is more than only technical matter (see e.g. the threats of identity theft and spam). It requires an approach that includes a mixture of legislation, best practices, technology, processes, culture, and behavior. ENISA is working to build up the platform for such information sharing.

Next Version of the Report

This report is kept open by ENISA to continuously collect NIS developments and expand the NIS Security Activities and Standards Inventory. The report will be expanded to cover also NIS research activities. Future versions of the report will be in web format, to provide for the possibility of dynamic and easy updating and information triggering.

The Network and Information Steering Group (NISSG) has performed a parallel work[119] to the ENISA study, providing an overview of existing NIS standards and

[119] Network and Information Security Report - ICTSB/NISSG, in support of the Communication form the Commission to the Council, the European Parliament, the European Economic and Social Committee and the Committee of the Regions: A strategy for a Secure Information Society – "Dialogue, partnership and empowerment". To be soon released.

recommendations for SDOs' actions. Collaboration among NISSG and ENISA will bring their work in closer relation.

Topics that ENISA expects to cover in the next version of the report include:

- Security for Multicast and Broadcast communications
- Emergency Communications
- Emerging Services, including for example Web services, Presence, Location-based services
- Peer-to-peer communications
- Accreditation and Certification, taking the input from the ENISA Workshop in November 2006.
- Long-Term Archive Services

Annex 1
Activities in Network and Information Security
Inventory of Fora

Objective of the Inventory

This Inventory of Fora is intended to provide a snapshot of the different bodies that are involved in network and information security activities. The technical work in network and information security is very lively, and it increasing in the latest years, yet it is fragmented into many separated efforts and disseminated among different bodies. This inventory is intended to facilitate a first step for ENISA, and its stakeholders, to gain an overview of the different activities going on in the security community. The scope is quite broad, and the nature of involved bodies is heterogeneous, including standardization bodies, industry consortium, academy, public sector, and combinations of them. For each body, relevant security activities are pointed out, and relevant specifications/reports are referenced.

The Inventory is part of a broader effort made by ENISA, in accordance to its mandate, to maintain tracking of standardization work and other activities related to network and information security. The Inventory is considered by ENISA an on-going effort, to be continuously updated and expanded.

Structure of the Inventory

The identified Fora are grouped into the following categories:

1. **European Standardization**
   - ICT Standard Board (ICTSB)
   - The European Telecommunications Standards Institute (ETSI)
   - European Committee for Electrotechnical Standardization (CENELEC)
   - European Committee for Standardization (CEN)
2. **International Standardization**
   - The Internet Engineering Task Force (IETF)
   - International Telecommunication Union (ITU)
   - National Institute of Standards and Technology (NIST)
   - International Organization for Standardization (ISO) and the International Electrotechnical Commission (IEC)
   - American National Standards Institute (ANSI)
3. **Industry Association**
   - Voice over IP Security Alliance (VOIPSA)
   - Cyber Security Industry Alliance (CSIA)
   - Open Mobile Alliance (OMA)
   - Trusted Computing Group (TCG)
   - VPN Consortium (VPNC)
   - The Information Systems Security Association (ISSA)
4. **European Institutions**
   - Joint Research Center (JRC)
   - The European Network and Information Security Agency (ENISA)
5. **International Institutions**
   - Organization for Economic Co-operation and Development (OECD)
   - International Federation for Information Processing (IFIP)
   - Organization for the Advancement of Structured Information Standards (OASIS)
6. **Other Fora relevant to NIS**
   - The Internet Corporation for Assigned Names and Numbers (ICANN)
   - RIPE
   - The Open Group

European Standardization

The European Standard Development Organizations (SDOs) are the European Committee for Standardization (*CEN*), the European Committee for Electrotechnical Standardization (*CENELEC*), and the European Telecommunications Standards Institute (*ETSI*).

A description of the standardization work within Europe to achieve the targets of the European Commission's eEurope Action Plan can be found at http://www.e-europestandards.org/. It covers primarily CEN, CENELEC, and ETSI, but also other standardization bodies such as the World Wide Web Consortium (W3C). It also collects the activities based on the eEurope 2005 Action Lines (e-government, e-learning, e-health, e-business, secure Information infrastructure, Smart Cards, Broadband).

ICT Standard Board (ICTSB)

http://www.ictsb.org/

ICTSB is a collaborative group of organizations supporting ICT standardization by making proposals and recommendations. ICTSB membership includes for example the European Standard Development Organizations (CEN, CENELUC, and ETSI).

The European Electronic Signature Standardization Initiative (EESSI)

http://www.ictsb.org/EESSI_home.htm

ICTSB was involved in the area of electronic signatures in the period 1999-2004, with the **EESSI** Working Group. The mandate for EESSI was to coordinate the standardization activities that were developed to support the EU Directive 1999/93/EC[120] on electronic signature. Such standardization activities take place within CEN (CEN/ISSS), e.g. with the *E-Sign Workshop* (closed in 2003), and within ETSI (ETSI ESI). The coordination task has been taken over by NISSG (see below).

The Network and Information Steering Group (NISSG)

NISSG was formed in 2004 with the mission to ensure the implementation of the NIS standardization requirements identified in a Special Report [NISSG1]. The second version of the report is currently being drafted.

Further work engaging ICTSB includes e-commerce, data privacy, network services, localization services, identification cards.

[120] http://www.ictsb.org/EESSI/Documents/e-sign-directive.pdf

[NISSG1]	ETSI SR 002 298, Response from CEN and ETSI to the "Communication from the Commission to the Council, the European Parliament, the European Economic and Social Committee and the Committee of the Regions: Network and Information Security: Proposal for a European Policy Approach"

The European Telecommunications Standards Institute (ETSI)

http://www.etsi.org/

ETSI is a non-profit organization, responsible for ICT standardization within Europe. ETSI covers many technology areas, e.g. telecommunications, broadcasting, information, communication, and related areas such as intelligent transportation and medical electronics. Thanks to its broad and differentiated membership, directly involved in the standards design, ETSI succeeds in producing standards which are closely aligned with the market needs and widely accepted (notable examples being GSM and UMTS).

ETSI is organized into *Technical Committees* (TCs) and *Partnership Projects* (PPs, where external bodies cooperate), of which a few, operating in the NIS area, are described below. ETSI uses also *Specialist Task Forces* (STFs), groups of experts working on a specific task with a given timescale, working under the guidance of a TC or PP, typically taking care of urgent issues.

The security work in ETSI is described in a Whitepaper, "Security for ICT – the Work of ETSI", January 2006, http://www.etsi.org/etsi_radar/whitepaper/home.htm[121].

> Note: the websites of the TCs/PPs described in the following can be reached via the ETSI Portal, http://portal.etsi.org/Portal_Common/home.asp

[121] See also ENISA Quarterly, December 2005, Security for ICT and the work of the European standards organizations, page 8.

TISPAN

ETSI Technical Committee Telecommunications and Internet converged Services and Protocols for Advanced Networking
http://www.etsi.org/tispan/

Keywords: *Next Generation Network*

TISPAN deals with the convergence of fixed and mobile networks and the migration from switched circuit networks to packet based networks. Core focus is on the *Next Generation Networks (NGN)*, the new network model based on convergence and access-independency, strongly IP oriented. This new type of communication, seamless through any access (cellular, WLAN, broadband, etc.), introduces challenging security requirements, which are address in the TISPAN work.

The TISPAN converged network is based on the IP Multimedia Subsystem (IMS), "owned" by 3GPP. Therefore, TISPAN works in close collaboration with 3GPP, to reuse the security mechanisms developed in the 3GPP IMS, at the same time taking into consideration the new security requirements coming from the fixed access. The joint goal is the design of a converged IMS-centric core network for both wireless and wireline networks, all-IP based.

ETSI NGN Release 1 specifications were published in December 2005, and work on Release 2 is on-going.

TISPAN WG7 is in charge of the security work for TISPAN. The *security requirements* for the NGN Release 1 have been identified [TISPAN1]. TISPAN is working on guidance for proper standard design. In particular, guidance is provided to write the ETSI standards so to facilitate the assessment of Common Criteria (ISO/IEC 15408) [TISPAN2]-[TISPAN6]. A security framework provides an overview of NGN security which is release-independent [TISPAN7]. The NGN Release 1 comprises the security solution for that specific release, including a threat and risk analysis [TISPAN8], [TISPAN9], and related countermeasures [TISPAN10], [TISPAN11]. NGN Release 1 security architecture is specified in [TISPAN12]. The lawful interception solution for NGN1 is specified in [TISPAN13].

The TISPAN WG7 gets the support of the **Specialist Task Force STF 292** ('TISPAN security: Standards development in support of the eEurope secure and trusted network environment'). STF 292 is working on a threat analysis for TISPAN, related countermeasures, and definition of Common Criteria Protection Profiles for NGN.

[TISPAN1]	TS 187 001, Requirements - NGN Release 1
[TISPAN2]	EG 202 387, Security Design Guide; Method for application of Common Criteria to ETSI deliverables
	Gives guidance to standards developers in preparing standards in a format that can be assessed by evaluators using the Common Criteria.
[TISPAN3]	ES 202 382, Security Design Guide; Method and proforma for defining Protection Profiles
	Gives guidance on the preparation of Protection Profiles (PP) based upon ETSI standards. Common Criteria (CC) evaluation involves the preparation of a PP, an "implementation-independent set of IT security requirements for a category of equipment intended to meet common consumer needs for IT security", and standards defining requirements are closed to PP.
[TISPAN4]	ES 202 383, Security Design Guide; Method and proforma for defining Security Targets
	Provides guidance on the preparation of Security Targets (ST) based upon ETSI standards.
[TISPAN5]	TR 102 420, Review of activity on security
	Presents the results of a case study looking at a security analysis of ENUM.
[TISPAN6]	DTS/TISPAN-07008-Tech, Protocol Framework Definition; Protection Profile
	Definition of Protection Profiles (as defined by Common Criteria) in TISPAN.
[TISPAN7]	DTS/TISPAN-07015-NGN, Framework and Requirements - Release Independent
[TISPAN8]	TR 187 002 TISPAN; Threat and Risk Analysis - NGN Release 1, Security Threat and Risk for NGN release 1
[TISPAN9]	TS 102 165-1, Protocol Framework Definition; Methods and Protocols for Security; Part 1: Threat Analysis
[TISPAN10]	TS 102 165-2, Protocol Framework Definition; Methods and Protocols for Security; Part 2: Counter Measures
[TISPAN11]	DEG/TISPAN-07004-Tech, Design Guide; Application of security countermeasures to service capabilities.
[TISPAN12]	TS 187 003 TISPAN; Security Architecture - NGN Release 1, Security architecture NGN R1
[TISPAN13]	DTS/TISPAN-07013-Tech, NGN Lawful Interception, Lawful Interception
	Defining the lawful interception solution for NGN
[TISPAN14]	TR 102 419; Security analysis of IPv6 application in telecommunications standards
	An analysis of the security solution in IPv6 and a few notes on its applicability to NGN.

SAGE

ETSI Security Algorithms Group of Experts

Keywords: *Cryptographic algorithms*

The Security Experts Group provides the ETSI expertise in the matter of cryptography (algorithms and protocols), with the specific mandate of addressing fraud and guarantee user data privacy. SAGE has developed algorithms for e.g. GSM, GPRS, UMTS, DECT, TETRA. Some of the work of SAGE is not publicly available but can be distributed under license, typically to telecommunication entities, with ETSI acting as Custodian for these documents.

TETRA Algorithms

A multi-part Technical Report (TR) covers the management of the TETRA standard encryption, authentication and key management algorithms. There are four standardized TETRA encryption algorithms (TEA1, TEA2, TEA3, TEA4), and one standardized TETRA authentication and key management algorithm (TAA1) [SAGE1]-[SAGE8].

Audio and Visual Systems Algorithms

[SAGE9]-[SAGE12].

GPRS Algorithms

SAGE work also includes the design of the GPRS algorithms [SAGE13]-[SAGE16], the GSM/EDGE algorithms, and the Milenage algorithm set, an example for the 3GPP algorithm suite.

[SAGE1]	MI/SAGE-00010-2, Standard Trans European Trunked RAdio (TETRA) air interface encryption algorithm TEA1 and TEA2
[SAGE2]	TR 101 053-1, Security Algorithms Group of Experts (SAGE); Rules for the management of the TETRA standard encryption algorithms; Part 1: TEA1
[SAGE3]	TR 101 053-2, Security Algorithms Group of Experts (SAGE); Rules for the management of the TETRA standard encryption algorithms; Part 2: TEA2
[SAGE4]	MI/SAGE-00017-2, Security Algorithms Group of Experts (SAGE); TEA3 and TEA4 Security Algorithms
[SAGE5]	TR 101 053-3, Security Algorithms Group of Experts (SAGE); Rules for the management of the TETRA standard encryption algorithms; Part 3: TEA3
[SAGE6]	TR 101 053-4, Security Algorithms Group of Experts (SAGE); Rules for the management of the TETRA standard encryption algorithms; Part 4: TEA4
[SAGE7]	TR 101 052, Security Algorithms Group of Experts (SAGE); Rules for the management of the TETRA standard authentication and key management algorithm set TAA1
[SAGE8]	MI/SAGE-00011-2, Standard Trans European Trunked RAdio (TETRA) set of air interface authentication and key management algorithms TAA1
[SAGE9]	TCTR 001, Security Algorithms Group of Experts (SAGE); Requirements specification for an encryption algorithm for use in audio visual systems

[SAGE10]	TCTR 003, Security Algorithms Group of Experts (SAGE); European Encryption Algorithm for the use in audiovisual systems
[SAGE11]	Universal Personal Telecommunications (UPT) Algorithms:
[SAGE12]	TCRTR 031, Security Algorithms Group of Experts (SAGE); Universal Personal Telecommunication (UPT) authentication; Rules for the management of the USA-4
[SAGE13]	TR 101 375, Security Algorithms Group of Experts (SAGE); Report on the specification, evaluation and usage of the GSM GPRS Encryption Algorithm (GEA)
[SAGE14]	MI/SAGE-00015-2, Security Algorithms Group of Experts (SAGE); GPRS encryption algorithm
[SAGE15]	MI/SAGE-00019-2, Design of a Standard GSM GPRS Encryption algorithm 2 (GEA2)
[SAGE16]	TR 101 740, Security algorithms Group of Experts (SAGE); Rules of the management of the standard GSM GPRS Encryption Algorithm 2 (GEA2)

ESI

Electronic Signatures and Infrastructures

Keywords: *E-signatures, Certificates*

ESI was formed in support of EU Directive 1999/93/EC; the specifications produced by ESI are the most referenced as for qualified (i.e., legally binding) signatures.

The ETSI standard TS 101 733 [ESI1] defines a format (CAdES) for electronic signatures based on Cryptographic Message Syntax (RFC 3369) and using the Abstract Syntax Notation 1 (ASN.1). The ETSI standard TS 101 903 [ESI2] defines a format for electronic signatures based on XML, XAdES. These formats remain valid over long periods and are compliant with the European Directive. Profiles of these two electronic signature formats for business needs are developed respectively in [ESI1b] and [ESI2b].

[ESI7] defines a profile for Qualified Certificates, i.e. certificates complying with Annex I and II of the EU Directive 1999/93/EC. [ESI7] is based on the technical definitions in IETF RFC 3739. [ESI9] further profiles the ITU-T Recommendation X.509 / ISO/IEC 9594-8, for Qualified Certificates issued to natural persons, in compliance also with IETF RFC 3280.

The algorithms (hash function, symmetric key schemes for secure channel), and related parameters, necessary for the security and the interoperability of electronic signatures under the EU Directive, are defined in the “algo paper” [ESI11] [ESI11b].

TS 102 042 [ESI3] specifies the policy requirements for certification authorities in the matter of issuing and managing certificates. These certificates may be used in support of any asymmetric mechanisms requiring certification (e.g., signatures, encryption,

key management). TS 101733 [ESI4] [ESI4b] narrows the scope down to qualified certificates.

Certificates may contain attributes, so that e.g. authorization is granted on the base of a role. [ESI5] specifies the policy requirements on the operation and management practices of the authorities issuing Attribute Certificates used in support of qualified electronic signatures.

Time stamping is a requirement for non-repudiation. [ESI6] defines policy requirements on the operation and management practices of Time-stamping Authorities, primarily in support of qualified electronic signatures but also more generically, for any application that needs to prove that certain data existed before a particular time. [ESI8] adopts the IETF Time Stamp Protocol (RFC3161) and profiles it.

To enhance the confidence on certificates and services related to electronic signatures, the Trust-service Status List (TSL) is defined [ESI10]. A TSL is a (signed) set of information that enables to determine if the operation of a trust service is (or was, at a given time) approved by any recognized scheme. The TSL is not intended to replace the certificate chain validation, however is intended to provide useful information before trusting the certificate or service. TSLes can, for example, be used within a closed community such as the EU among the Member States, for example to attest that the creation rules were different but belonging to the same framework.

ESI is currently working on Storage of Digital Accounting Documents (SODA): policy requirements and management to produce and reliably store fiscal documents such as electronic invoices [ESI12], and a framework with best practices to comply with policy requirements to issue SODA [ESI12b].

ETSI is also constantly working on harmonizing its specifications with international standards and activities (e.g., W3C, IETF, OASIS, ISO, ANSI, CEN), for example in the field of formats (TS 101 733 and TS 101 903) [ESI13] and policy requirements for certification authorities (TS 101 456 and TS 102 042) [ESI4, ESI3].

[ESI1]	TS 101 733, CMS Advanced Electronic Signatures (CAdES)
[ESI1b]	TS 102 734, Profiling for Electronic Signatures based on ETSI TS 101 733
[ESI2]	TS 101 903 Ver. 1.1.1, XML Advanced Electronic Signatures (XAdES)
[ESI2b]	TS 102 904, Profiling for Electronic Signatures based on ETSI TS 101 903
[ESI3]	TS 102 042, Policy requirements for certification authorities issuing public key certificates
[ESI4]	TS 101 456, Policy requirements for certification authorities issuing qualified certificates
[ESI4b]	TR 102 437, Guidance on TS 101 456
[ESI5]	TS 102 158, Policy requirements for Certification Service Providers issuing attribute certificates usable with Qualified certificates
[ESI6]	TS 102 023, Policy requirements for time-stamping authorities.

[ESI7]	TS 101 862, Qualified Certificate profile
[ESI8]	TS 101 861, Time stamping profile
[ESI9]	TS 102 280, X.509 V.3 Certificate Profile for Certificates Issued to Natural Persons
[ESI10]	TS 102 231, Provision of harmonized Trust-service status information
[ESI11]	TS 102 176-1, Algorithms and Parameters for Secure Electronic Signatures; Part 1: Hash functions and asymmetric algorithms
[ESI11b]	TS 102 176-2, Algorithms and Parameters for Secure Electronic Signatures; Part 2: Secure channel protocols and algorithms for signature creation devices
[ESI12]	Ref. DTS/ESI-000047, Policy requirements for issuance and Storage of Digital Accounting Documents (SODA)
[ESI12b]	Ref. DTR/ESI-000046, Best practices Framework to implement the Policy requirements for issuance and Storage of Digital Accounting Documents (SODA)
[ESI13]	TR 102 047, International Harmonization of Electronic Signature Formats
[ESI13b]	TR 102 040, International Harmonization of Policy Requirements for CAs issuing Certificates.

TETRA

ETSI Terrestrial Trunked Radio

Keywords: *Emergency services, Military services*

The Terrestrial Trunked Radio (TETRA) TC takes care of the design of the digital radio communication infrastructure of Professional Mobile Radio (PMR), e.g. emergency services, government, military, transportation, utility and industrial organizations, and Public Access Mobile Radio (PAMR) operators.

TETRA security is designed within TETRA WG 6. A goal for the TC is to take care of users' requirements, hence a few documents collects the security requirements [TETRA1], [TETRA2]. TETRA security comprises protection mechanisms for the air interface: mutual authentication, encryption, anonymity. [TETRA3] and [TETRA4] describe the security architecture; the cryptographic algorithms are designed by SAGE. Given the sensitivity of communication for PMR and PAMR, end-to-end encryption is also envisioned (the algorithms can be chosen by the users: IDEA is provided as example) [TETRA5]. [TETRA6] and [TETRA7] take care of Emergency and Lawful Interception.

Currently, work is done for identifying the security requirements for TETRA Release 2 [TETRA8]. To ensure interoperability between the Subscriber Identity Module (SIM) and the mobile equipment, [TETRA9]-[TETRA11] specify the interface between them, during the network operation phase of TETRA, and the related internal organization of the SIM.

[TETRA1]	TR 102 021-7, User Requirement Specification TETRA Release 2; Part 7: Security
[TETRA2]	TR 102 021-6, User Requirement Specification TETRA Release 2; Part 6: Subscriber Identity Module (SIM)
[TETRA3]	EN 300 396-6, Direct Mode Operation (DMO); Part 6: Security
[TETRA4]	EN 300 392-7, Voice plus Data (V+D); Part 7: Security
[TETRA5]	ES 202 109, Security; Synchronization mechanism for end-to-end encryption
[TETRA6]	TBR 035, Emergency access
[TETRA7]	EN 301 040, Security; Lawful Interception (LI) interface
[TETRA8]	DTR/TETRA-06139, Security; Security requirements analysis for TETRA-2
[TETRA9]	EN 300 812, Security aspects; Subscriber Identity Module to Mobile Equipment (SIM-ME) interface
[TETRA10]	ES 200 812-1, Subscriber Identity Module to Mobile Equipment (SIM-ME) interface; Part 1: Physical and logical characteristics
[TETRA11]	ES 200 812-2, Subscriber Identity Module to Mobile Equipment (SIM-ME) interface; Part 2: Characteristics of the TSIM application

3GPP

The 3rd Generation Partnership Project
http://www.3gpp.org/

Keywords: *2G / 3G security, IMS, LI, Multicast / broadcast security, Cryptography, Fraud prevention.*

The 3rd Generation Partnership Project (3GPP) is in charge of the specification of the 3rd Generation (3G) Mobile System, which is based on the GSM system. 3GPP also takes care of the maintenance of the GSM specifications and the development of the new radio accesses (such as GPRS and EDGE). Established in December 1998, 3GPP puts together relevant telecommunications standards bodies ("Organizational Partners"), including ETSI and ATIS.

The GSM and 3G systems specify their security architecture, with particular effort to prevent fraud. Protection of the communication over the air-link and a very successful key management based on symmetric key are key components of the solution. Threats are addressed in a dynamic way, following the evolution of the technologies, architecture, services, user needs, and emerging security trends. [3GPP1] provides an overview of security services implemented in GSM.

TSG SA WG 3 Security (Technical Specification Groups, Services and System Aspects, Working Group 3 Security) is responsible for the security of the 3GPP system. The work of WG 3 includes the security threat analysis for the system (including the new threats introduced by IP-based services), security requirements, and design of the security solution.

http://www.3gpp.org/TB/SA/SA3/SA3.htm

Security solution for the 3G mobile telecommunication system

[3GPP2] and [3GPP3] provide the threat analysis and identification of 3G security requirements; [3GPP4] defines the security architecture for the 3G mobile telecommunication system, while the integration of the 3G security architecture into the 3G system architecture is investigated in [3GPP5].

3G Core Network protection

The protection of the 3G core network ("NDS/IP", Network Domain Security) is provided using IPsec as security communication protocol, and (manual key) IKE as its key management protocol (so called "Za and Zb interfaces") [3GPP6].

NDS/IP is extended through a scalable authentication framework, providing entity authentication for the nodes that are using NDS/IP (e.g. introducing PKI and automated IKE) [3GPP7], [3GPP8].

NDS work for protecting Signalling System No. 7 (SS7) signalling is also taken care of, with MAPsec in Release 5 and 6, and TCAPsec in Release 7 [3GPP9], [3GPP10]. Lawful interception solution for 3G networks

A series of specifications define the lawful interception solution for 3G networks, including requirements, architecture, and specification of the handover interface (the interface towards the lawful enforcement agencies) [3GPP11]-[3GPP13].

3GPP IP Multimedia subsystem (IMS)

3GPP specifies the architecture of the IP Multimedia subsystem (IMS) for the 3G mobile telecommunication system, supporting applications such as video, audio and multimedia conferences, based on the IETF Session Initiation Protocol (SIP) as the signalling protocol and IP as underlying transport technology. The security specification for IMS is TS 33.203 ("3GPP IMS") [3GPP14], dealing with IMS authentication, SIP signalling protection, etc.

IMS is also defined in the context of fixed access (see ETSI TISPAN NGN R1 and R2). TR 33.802 [3GPP15] investigates the security requirements and solutions for fixed broadband access to IMS, so to extend TS 33.203 to this access.

It is understood that "early" implementations of IMS will exist without being fully compliant with TS 33.203. For example, 3GPP IMS requires IPv6, but IMS implementations based on IPv4 are expected. As for the security solution of 3GPP IMS, a problem is anticipated in the potential lack of support of the USIM/ISIM interface at the client side (especially in 2G-only devices) as well as support of IPsec in all clients. TR 33.978 [3GPP16] takes these 'early implementation' requirements and provides simple security mechanisms, based on the existing security of the underlying networks.

The Presence Service

Multimedia services such as IMS take advantage of the Presence service, which enables a user to publish and spread his presence information, maintaining the control of the access to such information. TR 33.941 [3GPP17] defines the security architecture, trust model and requirements for the presence service.

Authentication Framework

Generic Authentication Architecture (GAA) has been designed as an authentication framework to address the need of mutual authentication for a number of applications between the client (UE) and an application server, for example a presence server (possibly via an authentication proxy), a PKI portal for requesting a digital certificate, or a content server. The framework and components for GAA are described in TR 33.919 [3GPP18]. The Generic Bootstrapping Architecture (GBA) is part of GAA [3GPP19], [3GPP20]. Based on the 3GPP authentication mechanism (3GPP Authentication and Key Agreement Protocol, AKA), GBA has been defined to enable the security for applications and to establish shared keys. Alternatively, GAA specifies the use of authentication methods that rely on public key method and digital certificates, described in TS 33.221 [3GPP21].

GAA can be used for accessing services over HTTP in a secure manner (using TLS) [3GPP22]. An application residing on a UICC[122] may use the mechanism defined in TS 33.222 to secure the communication with a Network Application Function (NAF). The "HTTPS connection between a UICC and a NAF" [3GPP23] is a candidate for early implementation in release 7 specifications.

[3GPP24] investigates a possible interworking between the 3GPP GAA, the Liberty Alliance Identity Federation Framework (ID-FF), and the Identity Web Services Framework (ID-WSF).

3GPP-WLAN interworking

[3GPP25] describes the security solution for the interworking of WLAN networks with 3GPP networks. It defines a few possible trust models that are possible when coupling the 3G and WLAN domains, and defines the mechanisms for access security.

The Broadcast/Multicast Service (MBMS)

The security architecture for the 3GPP system network bearer service Multimedia Broadcast/Multicast Service (MBMS) is defined in TS 33.246 [3GPP26]. It makes use of GBA (see above) and of the IETF MIKEY key management protocol.

Future GERAN security

3GPP is currently working on future GERAN[123] Access Network Security [3GPP27]. The work comprises a threat and risk analysis of GERAN and UTRAN[124] accesses, in

[122] Universal Integrated Circuit card, where applications such as SIM/ISIM reside.
[123] GSM EDGE Radio Access Network

order to identify what is needed to address new threat scenarios that were not considered at the time the cellular security solutions were first designed. The discovery of the A5/2 cipher vulnerability has been a driver of the activity. The work also includes a threat analysis related to the re-use (transfer) of a security context between GSM and UMTS, as well as other access networks.

Algorithm design

The design of the 3GPP algorithms for confidentiality and integrity protection is also covered by SA3, in cooperation with ETSI SAGE. Of the nine algorithms needed in 3G, the two algorithms for cipher and integrity protection of the 3GPP radio interface (f8 and f9) are standardized [3GPP28] - [3GPP32]. Among other algorithms not fully specified, an example set is provided for authentication and key generation functions, the Milenage Algorithm Set [3GPP33] - [3GPP37]. The specifications in the 55 series define the algorithms for GSM only (GSM/EDGE) [3GPP48]-[3GPP50]; the GSM Milenage set is also defined based on the above UMTS Milenage set [3GPP38].

New work has began for developing new security algorithms for the UMTS radio interface, UEA2 and UIA2, based on the SNOW algorithm instead than Kasumi [3GPP39] - [3GPP43].

Fraud prevention

Fraud (i.e., a user making use of the service without paying) is one of the critical threats concerning operators. FIGS (Fraud Information Gathering System) is a method that address this threat [3GPP44]-[3GPP47]. It allows the transfer of relevant information on the user activity from the visited network to the home network, so that potential fraud may be detected.

[3GPP1]	TS 43.020 Security-related network functions
[3GPP2]	3GPP TS 21.133; 3G Security; Security Threats and Requirements".
[3GPP3]	3GPP TS 33.120; 3G Security; Security Principles and Objectives".
[3GPP4]	TS 33.102 3G security; Security architecture
[3GPP5]	TS 33.103 3G security; Integration guidelines
[3GPP6]	TS 33.210 3G security; Network Domain Security (NDS); IP network layer security
[3GPP7]	TS 33.310 Network domain security; Authentication framework (NDS/AF)
[3GPP8]	TR 33.810 3G Security; Network Domain Security / Authentication Framework (NDS/AF); Feasibility Study to support NDS/IP evolution
[3GPP9]	TS 33.200 3G Security; Network Domain Security (NDS); Mobile Application Part (MAP) application layer security
[3GPP10]	TS 33.204 Network Domain Security (NDS); TCAP user security
[3GPP11]	TS 33.106 Lawful interception requirements
[3GPP12]	TS 33.107 3G security; Lawful interception architecture and functions
[3GPP13]	TS 33.108 3G security; Handover interface for Lawful Interception (LI)
[3GPP14]	TS 33.203 3G security; Access security for IP-based services
[3GPP15]	TR 33.802 Feasibility study on IMS security extensions

[124] UMTS Terrestrial Radio Access Network

[3GPP16]	TR 33.978 Security aspects of early IP Multimedia Subsystem (IMS)
[3GPP17]	TS 33.141 Presence service; Security
[3GPP18]	TR 33.919 Generic Authentication Architecture (GAA); System description
[3GPP19]	TS 33.220 Generic Authentication Architecture (GAA); Generic bootstrapping architecture
[3GPP20]	TR 33.920 SIM card based Generic Bootstrapping Architecture (GBA); Early Implementation Feature
[3GPP21]	TS 33.221 Generic Authentication Architecture (GAA); Support for subscriber certificates
[3GPP22]	TS 33.222 Generic Authentication Architecture (GAA); Access to network application functions using Hypertext Transfer Protocol over Transport Layer Security (HTTPS)
[3GPP23]	TR 33.918 Generic Authentication Architecture (GAA); Early implementation of Hypertext Transfer Protocol over Transport Layer Security (HTTPS) connection between a Universal Integrated Circuit Card (UICC) and a Network Application Function (NAF)
[3GPP24]	TS 33.980, Liberty Alliance and 3GPP security interworking; Interworking of Liberty Alliance Identity Federation Framework (ID-FF), Identity Web Services Framework (ID-WSF) and Generic Authentication Architecture (GAA)
[3GPP25]	TS 33.234 3G security; Wireless Local Area Network (WLAN) interworking security
[3GPP26]	TS 33.246 3G Security; Security of Multimedia Broadcast/Multicast Service (MBMS)
[3GPP27]	TR 33.801 Access security review
[3GPP28]	TS 33.105 Cryptographic algorithm requirements
[3GPP29]	3GPP TS 35.201; Specification of the 3GPP Confidentiality and Integrity Algorithms; Document 1: f8 and f9 Specification".
[3GPP30]	3GPP TS 35.202; Specification of the 3GPP Confidentiality and Integrity Algorithms; Document 2: KASUMI Specification".
[3GPP31]	3GPP TS 35.203; Specification of the 3GPP Confidentiality and Integrity Algorithms; Document 3: Implementors' Test Data".
[3GPP32]	3GPP TS 35.204; Specification of the 3GPP Confidentiality and Integrity Algorithms; Document 4: Design Conformance Test Data".
[3GPP33]	3GPP TS 35.205; Specification of the MILENAGE Algorithm Set: An example algorithm set for the 3GPP authentication and key generation functions f1, f1*, f2, f3, f4, f5 and f5*; Document 1: General".
[3GPP34]	3GPP TS 35.206; Specification of the MILENAGE Algorithm Set: An example algorithm set for the 3GPP authentication and key generation functions f1, f1*, f2, f3, f4, f5 and f5*; Document 2: Algorithm Specification".
[3GPP35]	3GPP TS 35.207; Specification of the MILENAGE Algorithm Set: An example algorithm set for the 3GPP authentication and key generation functions f1, f1*, f2, f3, f4, f5 and f5*; Document 3: Implementors' Test Data"
[3GPP36]	3GPP TS 35.208; Specification of the MILENAGE Algorithm Set: An example algorithm set for the 3GPP authentication and key generation functions f1, f1*, f2, f3, f4, f5 and f5*; Document 4: Design Conformance Test Data".

[3GPP37]	TR 35.909; Specification of the MILENAGE algorithm set: an example algorithm set for the 3GPP authentication and key generation functions f1, f1*, f2, f3, f4, f5 and f5*; Document 5: Summary and results of design and evaluation
[3GPP38]	TS 55.205; Specification of the GSM-MILENAGE algorithms: An example algorithm set for the GSM Authentication and Key Generation Functions A3 and A8
[3GPP39]	TS 35.215; Specification of the 3GPP Confidentiality and Integrity Algorithms UEA2 & UIA2; Document 1: UEA2 and UIA2 specifications
[3GPP40]	TS 35.216; Specification of the 3GPP Confidentiality and Integrity Algorithms UEA2 & UIA2; Document 2: SNOW 3G specification
[3GPP41]	TS 35.217; Specification of the 3GPP Confidentiality and Integrity Algorithms UEA2 & UIA2; Document 3: Implementors' test data
[3GPP42]	TS 35.218; Specification of the 3GPP Confidentiality and Integrity Algorithms UEA2 & UIA2; Document 4: Design conformance test data
[3GPP43]	TR 35.919; Specification of the 3GPP Confidentiality and Integrity Algorithms UEA2 & UIA2; Document 5: Design and evaluation report
[3GPP44]	TR 41.031; Fraud Information Gathering System (FIGS); Service requirements; Stage 0
[3GPP45]	TS 22 031; Fraud Information Gathering System (FIGS); Service description; Stage 1
[3GPP46]	TS 23 031; Fraud Information Gathering System (FIGS); Service description; Stage 2
[3GPP47]	TR 41 031; Fraud Information Gathering System (FIGS); Service requirements; Stage 0
[3GPP48]	TS 55.216; Specification of the A5/3 encryption algorithms for GSM and EDGE, and the GEA3 encryption algorithm for GPRS; Document 1: A5/3 and GEA3 specification
[3GPP49]	TS 55.218; Specification of the A5/3 encryption algorithms for GSM and EDGE, and the GEA3 encryption algorithm for GPRS; Document 3: Design and conformance test data
[3GPP50]	TS 55.226; Specification of the A5/4 encryption algorithms for GSM and ECSD, and the GEA4 encryption algorithm for GPRS; Document 1: A5/4 and GEA4 specification

EMTEL

ETSI Special Committee on Emergency Telecommunications
Also: http://www.emtel.etsi.org/home.htm

Keywords: *Emergency telecommunications*

EMTEL focuses on solutions for emergency telecommunication, public protection, and preparedness. EMTEL works closed to other ETSI groups, e.g. TETRA, TISPAN, 3GPP and MESA, to define requirements and, in particular, define the location identification in the different services.

Two Special Reports have been published, one on requirements for the emergency call service [EMTEL1] , and one on regulatory principles in the area of Emergency Communications [EMTEL2].

A set of documents identifies the requirements for emergency communication between organizations and citizens [EMTEL3]- [EMTEL5]. [EMTEL7] collects requirements for building robust and reliable networks to guarantee emergency communications. [EMTEL6] contains a study on the applicability of SMS and Cell Broadcast Service (CBS) in emergency handling. A study investigates the applicability of Voice over IP (VoIP) for emergency communication, motivated by the fact that VoIP is gaining momentum [EMTEL8].

[EMTEL1]	SR 002 180, Requirements for communication of citizens with authorities/ organizations in case of distress (emergency call handling)
[EMTEL2]	SR 002 299, Collection of European Regulatory principles
[EMTEL3]	TS 102 181, Requirements for communication between authorities/organizations during emergencies
[EMTEL4]	TR 102 182, Requirements for communications from authorities/organizations to the citizens during emergencies
[EMTEL5]	TR 102 410, Requirements for communications between citizens during emergencies
[EMTEL6]	TR 102 444, Suitability of SMS and CBS for Emergency Messaging
[EMTEL7]	TR 102 445, Requirements for Emergency Communications Network Resiliency and Preparedness
[EMTEL8]	TR 102 476, Emergency calls and VoIP: standardization activities and possible short and long term solutions

MESA Project

Mobility for Emergency and Safety Applications (ETSI-TIA Project)
Also: http://www.projectmesa.org

Keywords: *Emergency telecommunications*

MESA is a Partnership Project involving ETSI and TIA (North America Telecommunications Industry Association), nowadays with wide international coverage. MESA works on defining an advanced digital mobile broadband system that could allow for emergency communications, embracing applications in need of highly reliable and high capacity networks, such as telemedicine, fire-fighting, mobile robotics and peacekeeping operations.

MESA system requirements and glossary are documented in [MESA1]-[MESA3]. Attention is paid to the users' requirements and relevant scenarios, in order to derive the appropriate system technical requirements [MESA4]. The system overview for MESA describes the different network configurations, components, and linking between different technologies and systems that could be used by MESA services [MESA5]. Current work includes the definition of an emergency data exchange standard, based on a Markup Language (XML) [MESA6], and the inventory and evaluation of emerging technologies that could be used as base for the MESA system [MESA7].

[MESA1]	TS 170 001, Service Specification Group - Services and Applications; Statement of Requirements (SoR)
[MESA2]	TR 170 003, Service Specification Group - Services and Applications; Basic requirements
[MESA3]	TR 170 002, Service Specification Group - Services and Applications; Definitions, symbols and abbreviations
[MESA4]	TS xxx, Technical Specification Group - System; Identification and derivation of the System Technical Requirements from the SoR (Ref. DTS/MESA-SYS0070014v311)
[MESA5]	TR 170 012, Technical Specification Group - System; System Overview
[MESA6]	TS xxx, Service Specification Group - Services and Applications; MayDayML - Emergency Data Exchange Language (Ref: DTS/MESA-SA0070004v311)
[MESA7]	TR xxx, Technical Specification Group - System; Technologies with potential applicability to Project MESA (Ref. DTR/MESA-SYS0070008v311)

AT TC

Technical Committee Access and Terminals

Keywords: *IPCablecom security,Home Area Networks*

The AT TC focuses on terminal standardization. AT TC is involved in the work around the definition of telecom services over cable TV networks. This includes the lawful intercept service, and security architecture ("IPCablecom security", specified in [AT1]). Another area of work is the Home Area Networks and the support of Next Generation Services to end devices within the home [AT2], including security and copyright (e.g., Digital Rights Management and Privacy) [AT3].

[AT1]	TS 101 909-11, Digital Broadband Cable Access to the Public Telecommunications Network; IP Multimedia Time Critical Services; Part 11: Security
[AT2]	TR 102 160-1, AT NGN@Home, Access and Terminals (AT); Home Area Networks and the support of Next Generation Services; Part 1: General aspects, Home networking: Part 1 General
[AT3]	TR 102 160-6, AT NGN@Home, Access and Terminals (AT); Home Area Networks and the support of Next Generation Services; Part 6: Security and Privacy issues, Home networking : Part 6 Security and Copyright

SES TC

Satellite Earth Stations & Systems

Keywords: *Satellite communications, Multicast/ broadcast security.*

The SES TC is in charge of specifying satellite communications in its different aspects.

[SES1] provides a threat analysis for the Broadband Satellite Multimedia (BSM) system with a survey of security protocols and key management protocols applicable to the BSM architecture, which in turn is defined in [SES2] and [SES3], based on interworking with IP. Satellite security faces a few interesting security issues, for example the use of Performance Enhancing Proxy (PEP) - which by nature challenge end-to-end security - and secure, scalable multicast. SES TC produced (2001) the security specifications for the GMR (Geostationary Earth Orbit Mobile Radio) system, used for mobile satellite services using geostationary satellites. GMR is based on standard GSM and supports access to GSM core networks, and derives its security from GSM security [SES4]-[SES6].

[SES1]	TR 102 287, Broadband Satellite Multimedia (BSM); IP Interworking over satellite; Security aspects
[SES2]	TS 102 465, Broadband Satellite Multimedia (BSM); General Security Architecture
[SES3]	TS 102 466, Details and Download Satellite Earth Stations and Systems (SES); Broadband Satellite Multimedia (BSM); Multicast Security Architecture
[SES4]	TS 101 376-3-9, GEO-Mobile Radio Interface Specifications; Part 3: Network specifications; Sub-part 9: Security related Network Functions; GMR-1 03.020
[SES5]	TS 101 377-2-3, GEO-Mobile Radio Interface Specifications; Part 2: Service specifications; Sub-part 3: Security Aspects; GMR-2 02.00
[SES6]	TS 101 377-3-10, GEO-Mobile Radio Interface Specifications; Part 3: Network specifications; Sub-part 10: Security related Network Functions; GMR-2 03.020

Other security related areas

Keywords: *Smart card, RFID, GRID, Digital wireless, Broadcast, Lawful Interception*

SCP TC

Smart Card Platform

The SCP TC is in charge of the maintenance and evolution of the ETSI successful specifications on smart cards, e.g. the SIM (Subscriber Identity Module) card in GSM and the USIM (Universal SIM, ETSI TS 131 102) card in UMTS. SCP works on developing an Integrated Circuit (IC) Card platform for mobile telecommunication systems which can work for multiple applications. E-commerce is an area of interest for SCP.

RFID TC

ETSI in engaged in standardization of Radio Frequency Identification (RFID) within ERM TG34, the Task Group of the Electromagnetic Compatibility and Radio Spectrum Matters Technical Committee. The specifications (ETSI EN 302 208-1 and ETSI EN 302 208-2) are not directly investigating security issues.

GRID TC

ETSI has announced its new involvement in GRID work in 2006, with the creation of a new TC. Security matters related to GRID are to be addressed.

DECT TC

DECT is a digital wireless technology for cordless telephones, and wireless telephone lines to the home. DECT security builds on the security of the GSM system. The DECT security solution is defined in [DECT1].

[DECT1]	EN 300 175-7, Common Interface (CI); Part 7: Security features

Broadcast TC

The Broadcast TC is a joint European Broadcasting Union (EBU) /CENELEC/ETSI Technical Committee. It deals with the broadcast technologies to e.g. pay-per-view and subscription-based channel distribution. [BR1] defines the security solution for Digital Video Broadcasting

[BR1]	EN 301 790, Digital Video Broadcasting (DVB); Interaction channel for satellite distribution systems

LI TC

The Lawful Interception (LI) TC standardizes lawful intercept solutions, and has produced specifications that are widely adopted by European countries. One of the main focuses is the specification of the LI handover interface, between the Operator/Provider and the Lawful Enforcement Agency, LEA [LI1] - [LI3]. The specifications cover GSM, GPRS, ISDN, PSTN and partially TETRA, and are expanding to cover other technologies and accesses, e.g. IMS [LI2], WLAN [LI7], TISPAN.

[LI 4] adds to them the specification of the handover interface for IP-based networks. Service-details (i.e., description of the interception information, and when Intercept Related information, IRI, and Content of Communication, CC, are sent, and with which information) for two specific services over IP, e-mail and Internet access, are respectively in [LI5] and [LI6], and for IMS in [LI8].

An LI solution is defined for an Access Provider that has access to layer 2 session information and that is not required to have layer 3 information [LI9]. The document defined for example IRI based on application of DHCP and RADIUS.

A new item is the analysis of a LI architecture and handover interface specification to serve the Data Retention law [LI10].

LI work is also carried out in other TCs, for example GSM, TETRA, 3GPP, TISPAN.

LI1]	ES 201 158, Requirements for network functions
[LI2]	ES 201 671, Handover interface for the lawful interception of telecommunications traffic

[LI3]	TS 101 671, Handover interface for the lawful interception of telecommunications traffic
[LI4]	TS 102 232, Handover specification for IP delivery
[LI5]	TS 102 233, Service specific details for E-mail services
[LI6]	TS 102 234, Service-specific details for internet access services
[LI7]	TRxxx, Ref. DTR/LI-00014, Lawful Interception of WLAN Internet Access
[LI8]	TSxxx, Ref. DTS/LI-00024, Lawful Interception, Service-specific details for IP Multimedia Services
[LI9]	TS 102 815, Service-specific details for Layer 2 Lawful Interception
[LI10]	TR xxx, Ref. DTR/LI-00020, Stored data handover architecture

European Committee for Electrotechnical Standardization (CENELEC)

http://www.cenelec.org/

CENELEC is a non-profit technical organization working to produce standards requested by the market and in support of European legislation, with the aim of developing the European Internal Market.

A few of the work items within CENELEC have relation to security. CENELEC is linked to the eEurope initiative, e.g. with activity within e-Accessibility and Smart House. TC 206 (Consumer equipment for entertainment and information and related sub-systems) deals with standards for digital video broadcasting, which includes security mechanisms such as encryption.

European Committee for Standardization (CEN)

http://www.cenorm.be

Keywords: *E-business, E-commerce, E-invoicing, Data protection, Privacy, Smart cards, E-government, E-signatures, E-ID, Biometrics, E-health, DRM.*

CEN produces European Standards in several fields, e.g. safety, environment, network interoperability, ICT.

CEN/ISSS

Information Society Standardization System
http://www.cenorm.be/cenorm/businessdomains/businessdomains/isss/about_isss/index.asp
CEN/ISSS is dedicated to ICT standardization.

CEN/ISSS Workshops
CEN runs *Workshops*, bridging industrial consortia with the European standardization in a specific area of interest. The Workshop's output are CEN Workshop Agreements

(*CWAs*), which are open, consensus-based specifications. The list of CEN/ISSS active Workshops can be found at http://www.cenorm.be/CENORM/businessdomains/businessdomains/isss/about_isss/workshops+list.asp

Work is done in the area of e-business and e-commerce, e.g. within the **eInvoicing Workshop**, **eCataloguing/Classification Workshop**, and the eBES Workshop. The **e-business Board for European Standardization (eBES)** is involved in an effort of facilitating the spread use of the ebXML[125], the OASIS suite of specifications for business over Internet. The **e-Business Interoperability Forum** (**eBIF**) focus on investigation of interoperability issues concerning electronic business, particularly related to standardization.

The **Data Protection and Privacy Workshop (DPP)**, 2003-2007, supports the implementation of the Data Protection Directive and relevant national legislations. The CWAs already published are listed below. http://www.cenorm.be/cenorm/businessdomains/businessdomains/isss/cwa/dppcwa.asp

CWA	***TITLE***
15262:2005	Inventory of Data Protection Auditing Practices
15263:2005	Analysis of Privacy Protection Technologies, Privacy- Enhancing Technologies (PET), Privacy Management Systems (PMS) and Identity Management systems (IMS), the Drivers thereof and the need for standardization
15292:2005	Standard form contract to assist compliance with obligations imposed by article 17 of the Data Protection Directive 95/46/EC (and implementation guide)
15499-01:2006	Personal Data Protection Audit Framework (EU Directive EC 95/46) Part I: Baseline Framework - The protection of Personal Data in the EU
15499-02:2006	Personal Data Protection Audit Framework (EU Directive EC 95/46) Part II: Checklists, questionnaires and templates for users of the framework - The protection of Personal Data in the EU

The **eAuthentication Workshop** (*closed*, 2003-2005) made contributions in the area of smart cards and eGovernment applications. The CWAs are also accompanied by a strategic vision document, "Towards an electronic ID for the European Citizen", containing the state of the art developments, threats, and opportunities in the area of electronic identification in EU. http://europa.eu.int/idabc/servlets/Doc?id=19132

CWA	***TITLE***
15264-1	Architecture for a European interoperable eID system within a smart card infrastructure.
15264-2	Best Practice Manual for card scheme operators exploiting a multi-application card scheme incorporating interoperable IAS services

[125] http://www.ebxml.org/

15264-3	User Requirements for a European interoperable eID system within a smart card infrastructure.

CEN is involved in the area of *Electronic Signatures*; the work was initiated in support of the European Directive 1999/93/EC on a Community framework for electronic signatures. In 1999 ICTSB created the European Electronic Signature Standardization Initiative (**EESSI**), in order to coordinate the standardization activities in support of the EU Directive in CEN (the E-Sign Workshop, see below) and ETSI ESI. NISSG takes now care of the coordination task that was of EESSI. Electronic signatures were the topic for the **E-sign Workshop**, closed in 2003. Several CWAs were then developed, see list below and http://www.unI.polito.it/WS_Esign/. A few of those CWAs are maintained by CEN/ISSS, ETSI ESI, and CEN/TC 224. **CEN/TC 224** (Personal identification, electronic signature and cards and their related systems and operations) is in particular working in the area of smart cards. The Commission Decision of 14 July 2003 (on the publication of reference numbers of generally recognized standards for electronic signature products in accordance with Directive 1999/93/EC of the European Parliament and of the Council) lists CWA 14169 and CWA 14167-1/2 as generally recognized standards for electronic signature.

CWA	***TITLE***
14169	Secure Signature-Creation Devices "EAL 4+"
14170	Security requirements for signature creation applications
14171	Procedures for electronic signature verification
14167-1	Security Requirements for Trustworthy Systems Managing Certificates for Electronic Signatures - Part 1: System Security Requirements
14167-2	Security Requirements for Trustworthy Systems Managing Certificates for Electronic Signatures - Part 2: Cryptographic module for CSP Signing Operations with Backup - Protection Profile
14167-3	Security Requirements for Trustworthy Systems Managing Certificates for Electronic Signatures - Part 3: Cryptographic module for CSP key generation services - Protection profile (CMCKG-PP)
14167-4	Security Requirements for Trustworthy Systems Managing Certificates for Electronic Signatures - Part 4: Cryptographic module for CSP signing operations - Protection profile - CMCSO PP
14890-1:2004	Application Interface for smart cards used as Secure Signature Creation Devices - Part 1 - Basic requirements
14355:2004	Guidelines for the implementation of Secure Signature-Creation Devices.
14365:2003	Guide on the use of Electronic Signatures.
CWA 14890-2:2004	Application Interface for smart cards used as Secure Signature Creation Devices - Part 2: Additional Services.
14172-1:2001	EESSI Conformity Assessment Guidance - Part:1: General.
14172-2:2001	EESSI Conformity Assessment Guidance - Part 2: Certification Authority services and processes.
14172-3:2001	EESSI Conformity Assessment Guidance - Part 3: Trustworthy systems managing certificates for electronic signatures.
14172-	EESSI Conformity Assessment Guidance - Part 4: Signature Creation

4:2001	Applications and Procedures for Electronic Signature Verification.
14172-5:2001	EESSI Conformity Assessment Guidance - Part 5: Secure signature creation devices.
14167-2:2002	Security Requirements for Trustworthy Systems Managing Certificates for Electronic Signatures - Part 2: Cryptographic Module for CSP Signing Operations - Protection Profile (MCSO-PP).
14172-6	EESSI Conformity Assessment Guidance - Part 6: Signature-creation devices supporting signatures other than qualified, Version: 1.
14172-7	EESSI Conformity Assessment Guidance - Part 7: Cryptographic modules used by Certification Service Providers for signing operations and key generation services, Version: 1.
14172-8	EESSI Conformity Assessment Guidance - Part 8: Time-stamping Authority services and processes, Version: 1.

CEN/ISSS Focus Groups
http://www.cenorm.be/cenorm/businessdomains/businessdomains/isss/index.asp?pClose=2

A CEN/ISSS *Focus Group* deals with a specific standardization topic and produces reports, overviews, and recommendations, effectively functioning as a pre-standardization body. CEN/ISSS Focus Groups related to NIS include:

- **Biometrics Focus Group**
  Work on biometric, although the group is not a standardizing group since there is not yet requirement for any dedicated European work. The Forum collaborates with the European Biometrics Forum and the ISO/IEC JTC1 SC37.
- **eGovernment Focus Group**
  Work to determine the role that standards eGovernment[126], for the interoperability of public administration at the pan-european, national, regional, and local levels.
- **eHealth Focus Group** (closed), connected to the long-term **CEN TC 251**, Health Informatics.
- **eBusiness Focus Group** (**eBIZ**) (closed), which produced a report and a Roadmap on key e-business standards
  http://www.cenorm.be/cenorm/businessdomains/businessdomains/isss/activity/ebusiness_fg.asp

	CEN/ISSS eBusiness Standards Focus Group, CEN/ISSS report and recommendations on key eBusiness standards issues 2003-2005, July 2003.
	CEN/ISSS eBusiness Standards Focus Group, CEN/ISSS Roadmap for addressing key eBusiness standards issues 2003-2005, August 2003.

[126] "eGovernment" is defined as "the use of ICT in public administrations combined with organisational change and new skills, in order to improve public services and democratic processes, and strengthen support to public policies" [European Commission Communication COM(2003) 567 final, "The Role of eGovernment for Europe's Future", Brussels, 26.9.2003].

- **e-Invoicing Focus Group** (closed), leading to the eInvoicing Workshop **Digital Rights Management Focus Group** (DRM) (closed), which produced in 2003 a report covering DRM inventory, description of DRM technologies, and recommendations.

	CEN/ISSS, Digital Rights Management, Final Report, September 2003

The **CEN BT/WG 161 'Protection and Security of the Citizen'** is in charge of monitoring of standardization activities, and need for new ones, related to e.g. critical infrastructure (energy supply, building and civil engineering works) and emergency services.
http://www.cenorm.be/cenorm/businessdomains/businessdomains/security+and+defence/security/btwg161.asp

COPRAS

http://www.w3.org/2004/copras/

COPRAS is a three-year project launched in March 2004, supported by the ICTSB and funded by IST, with the European SDOs (CEN, CENELEC, ETSI), and the two industry groups the World Wide Web Consortium (W3C) and the Open Group. Its objective is to improve the interface between research and standards.

International Standardization

The Internet Engineering Task Force (IETF)

http://www.ietf.org/

"Rough consensus and running code"
the IETF credo

Keywords: *Internet protocols and architecture*

IETF is an international community working for the development of the Internet architecture. IETF follows the open principle that anyone can contribute to the definition of the Internet. Its large, worldwide membership includes vendors, operators, academies, network designers, and individuals, with a strong influence of industry R&D. IETF is the prime source for Internet architecture and protocols, and its importance is nowadays even greater due to the tendency towards network convergence and all-IP architectures. Other relevant standardization bodies, including 3GPP and ETSI, base part of their specifications on IETF protocols and architectures.

IETF is organized into *Working Groups* (WGs), each related to a specific technical matter. A WG runs for a given period of time, needed to fulfill its mandate to produce the specifications that define the problem(s) and the related solution(s). The list of active WG can be found at http://www.ietf.org/html.charters/wg-dir.html.WGs are gathered under *Areas*, each Area dealing with a particular topic. Current (2006) Areas are: Applications, General, Internet, Operations and Management, Real-time Applications and Infrastructure, Routing, *Security*, Transport. Most of the standardization work is handled via e-mails. IETF meetings take place three times per year and are a major event for members of the Internet community to meet and discuss (an IETF meeting has an average of 1500 attendees and represents a milestone for discussion and progression of standards). The IETF Journal (http://www.isoc.org/tools/blogs/ietfjournal/index.php) summarizes the discussions in each IETF meeting.

IETF's specifications undergo a standardization process[127] to advance their status. Initial documents are in the status of *Internet Drafts* (IDs). An ID is generally an individual submission, and can advance its status remaining individual submission or becoming a WG item in case it deals with a subject that is relevant for a WG and can be included in its charter. In order to advance in the standardization status, the ID undergoes a review by the all Internet community and ultimately by the experts within IETF. If an ID advances in the review process, it reaches the status of *Request for*

[127] The IETF Internet Standard Process is specified in RFC 2026, and is well described for example in the Spring 2006 issue of the IETF Journal, "The Evolution of an Internet Standard", page 26, http://www.isoc.org/tools/blogs/ietfjournal/?cat=8

Comment (RFC), stable enough to allow for product implementations. An RFC may reach the *Internet Standard* status (label STDxxx), or become a best practice (label BCPxxx), while RFCs not following the standard track are published as Experimental or Informational RFCs.

The process is supervised by the Area Directors, who form the **IESG** (Internet Engineering Steering Group). The **IAB** (Internet Architectural Board) provides architectural guidance, and the **IANA** (Internet Assigned Numbers Authority) is the centralized body for the assignment of unique parameter values for Internet protocols. The **ISOC** (Internet Society) is the professional membership society addressing issues related to the future of the Internet, and is the organization home for IETF and IAB. The ISOC web page (http://www.isoc.org) offers interesting articles about Internet, including security related topics.

The role of security in IETF
http://sec.ietf.org/

Network and information security has deep roots in IETF (see RFC 3365). Security matters in IETF are supervised by the *Security Area*, which is made of two Directors, assisted by the *Security Area Directorate*, which comprises security experts committed in supporting the security work within the IETF. Further security advices are provided by the SAAG, the *Security Area Advisory Group*, open to anyone with interest and competence in security.

IETF has Working Groups dedicated to specific security issues (see table below). However security is embedded in all IETF standards and WGs. In fact, it is mandatory for each document to include a "Security Considerations" section, which is checked during the evaluation process. Remarkably, the awareness of the criticality of security has enormously increased within the Internet community in the latest years, and the IESG demands particular attention to have comprehensive, well documented security considerations. This is primarily a consequence of unpleasant past experiences in IETF, where security was overlooked in the design phase of a technology, whose development was delayed due to the insufficient security solution (e.g. Mobile IPv6). The IESG has realized that it has sometimes happened that, in the past, security has not been kept into appropriate consideration from the beginning, and that designers have too often adopted the philosophy "IPsec solves it all", often wrong or at least not acceptable without providing guidance on how to use IPsec with the given technology. Furthermore, security is one of those cross-topics that touch all WGs, and requires not only security expertise, but also deep knowledge of the technology it applies to[128]. Such mixed expertise is difficult to find. The IESG is trying to alleviate this problem via the Security Directorate Review Process (http://sec.ietf.org/instructions.html).

[128] In the SAAG meeting in IETF 66th, 2006, it was said that 35% of the discussion in the IESG review is security related.

WG	WG Name	Focus	Examples of relevant security Standards	Active/ Closed
Security Area				
ipsec	IP Security Protocol	Overall security design for IP Security	IPsec (ESP, AH), IKEv1/v2, HMAC	C
mobike	IKEv2 Mobility and Multihoming	Develop IKEv2 with extensions for handling multihoming, mobility and roaming.	MOBIKE	C
btns	Better-Than-Nothing Security	Develop extensions to the IPsec architecture to support creation of unauthenticated security associations.		A
pki4ipsec	Profiling Use of PKI in IPSEC	Work to favor the deployment of IPsec based on certificates		A
emu	EAP Method Update	EAP methods for other SDOs		A
krb-wg	Kerberos WG	Interoperability of Kerberos systems.	Kerberos v5	A
kink	Kerberized Internet Negotiation of Keys	Key management using Kerberos	Kink	C
sasl	Simple Authentication and Security Layer	Standardization for authentication protocols.	SASL	A
msec	Multicast Security	Standardization for secure group communication.	GDOI, GSAKMP, MIKEY, TESLA	A
dkim	Domain Keys Identified Mail	E-mail security (e.g. anti-spam)		A
smime	S/MIME Mail Security	S/MIME standardization.	S/MIME, CMS	A
openpgp	An Open Specification for Pretty Good Privacy	Further standardization of PGP.	OpenPGP	A
isms	Integrated Security Model for SNMP	SNMP security		A
tls	Transport Layer Security	TLS standardization work.	TLS	A
kitten	GSS-API Next Generation	Extensions to the The Generic Security Services API		
secsh	Secure Shell	Update SSH.	SSH	C
idwg	Intrusion Detection Exchange Format	Requirements and specifications for Intrusion Detection Systems	IDMEF (draft)	C
inch	Extended Incident Handling	Exchange of incidence information with other parties.		C
syslog	Security Issues in Network Event Logging	System for logging system events.	Syslog (draft)	A
ltans	Long-Term Archive and Notary Services	Secure usage of archive and notary services		A

pkix	Public-Key Infrastructure (X.509)	PKI Standardization.	X.509 support, CMP, CRMF, OCSP	A
nea	Network Endpoint Assessment	Check the security posture of endpoint devices before granting access to the network		A
hokey	Handover Keying	Handover and re-authentication, based on EAP		A
ipseckey	IPSEC KEYing	Storing IPsec keys in DNS.		C
ipsp	IP Security Policy	Policies for providing IPsec solutions		C
keyprov	Provisioning of Symmetric Keys	Protocols to provision symmetric keys		A
Other Areas				
IPv6	IPv6 Internet Area	Standardizing the next generation of Internet.		
ieprep	Internet Emergency Preparedness	Support emergency management and recovery operations		A
hip	Host Identity Protocol	New architecture and protocol separating the end-point identifier and locator roles of IP addresses, with also focus on security	HIP (draft)	A
midcom	Middlebox Communication	Develop an architecture for communicating requests between applications and middleboxes (e.g. firewalls, NATs), including security aspects.	STUN	A
behave	Behavior Engineering for Hindrance Avoidance	Definition of best common practices for NAT technologies, in order to not penalize applications.	STUN	A
aaa radext dime	Operations and Management Area Authentication, Authorization and Accounting RADIUS EXTensions Diameter Maintenance and Extensions	Developing requirements for authorization, authentication, and accounting (AAA) for network access. Work on the AAA protocols.	Diameter, Radius, NAI,	C (aaa) A
mipshop	The Mobility for IP: Performance, Signaling and Handoff Optimization	Work on e.g. authentication optimization in handoff, AAA, CGA		A
opsec	Operational Security for IP Network	Best Practices for operation security for ISPs and enterprises.		A
pana	Protocol for carrying Authentication for	IP-based network authentication protocols	PANA (draft)	A

	Network Access			
rpsec sidr	Routing Security Requirements Secure Inter-Domain Routing	Routing security		A
geopriv	Geographic Location/Privacy	Privacy of location based information.		A
RAI Area	Real-time Applications and Infrastructure Area.	Work around multimedia security, disseminated in several WGs, e.g. sipping, avt, mmusic.	SRTP, ICE (draft)	A
xmldsig	XML Digital Signatures	Development of XML compliant syntax for signatures.		C

The following chapters provide a walk-through of a few WGs' activities. We want to stress once more that the security work in IETF is done in almost all WGs and specifications; hence the following summary of security activities in IETF is not exhaustive.

> Note: in the following text, references to RFCs and drafts are listed. Given an RFC number, the document can be retrieved by inserting the number itself in the search field at http://www.ietf.org/rfc.html.The notation "draft-…." denotes a work-in-progress draft, whose latest version can be retrieved by visiting the I-D search tool at https://datatracker.ietf.org/public/idindex.cgi and by inserting the keyword "draft-…", as provided, in the filename field.

IETF Security WGs

A short description of a few security WGs follows; covered areas include:

- extensions to IPsec or work related to IPsec (the mobike WG on multihoming and mobility for IKEv2, the btns WG on unauthenticated IPsec, the pki4ipsec WG certificates-based IPsec)
- key management protocols and authentication (the emu WG on EAP, the Kerberos work in the krb-wg WG and in the kink WG, the sasl WG)
- multicast security (the msec WG)
- mail security and spam (the dkim WG, the smime WG, the openpgp WG)
- network management (the isms WG on a security for SNMP)
- security protocols related (the tls WG, the kitten WG on GSS-API, the secsh WG on SSH)
- network security related (the idwg WG on intrusion detection exchange, the inch WG on incident language, the syslog WG on Syslog)
- certificates (the pkix WG)
- applications (the ltans WG on long-time archive).

IP Security Protocol (IPsec) WG

http://www.ietf.org/html.charters/OLD/ipsec-charter.html

[concluded]

The IP Security WG was closed, but its relevance is still remarkable since the WG has designed the IPsec protocol suite (ESP and AH), and its key management protocol, IKE. Late 2005, the IPsec WG concluded the effort of designing the new version of those protocols, for ESP and AH (new base specifications are RFCs 4301 to 4303), and IKEv2 (RFC 4306).

IKEv2 Mobility and Multihoming (mobike) WG

http://www.ietf.org/html.charters/OLD/mobike-charter.html

[concluded in April 2006]

The Internet Key Exchange version 2 (IKEv2), which is the key management for IPsec, requires extensions to handle multiple IP addresses per host (*multihoming*) and change of IP address due to mobility (*mobility and roaming*). In these cases, the desire is not to renegotiate all the security associations. Typical scenarios of interest are the Virtual Private Network (VPN) roamer who changes address and keeps the connection with the VPN gateway, and a multihomed host that can switch the connection among multiple network interfaces (e.g. WLAN and GPRS). Protocols such as the Stream Control Transmission Protocol (SCTP, RFC 2960) also use multihoming as feature imbedded in the protocol.

RFC 4261	Design of the MOBIKE Protocol
	It documents background, discussions, and design choices of RFC 4555, the MOBIKE protocol.
RFC 4555	IKEv2 Mobility and Multihoming Protocol (MOBIKE)
	The specification of the MOBIKE protocol.

Better-Than-Nothing Security (btns) WG

http://www.ietf.org/html.charters/btns-charter.html

The IPsec protocol suite requires network layer authentication (via IKE) using pre-existing credentials, such as pre-shared keys, certificates signed by a Certificate Authority (CA) or other authentication infrastructure (e.g. Kerberos). This is perceived as hindering the deployment of IPsec. The btns WG works on an extension of IPsec and IKE that allows for *relaxed authentication*, where the peers can share "*unauthenticated Security Associations (SAs)*" without possessing credentials that can be validated , for example self-signed certificates or standalone public keys (currently, the focus is on bare RSA keys and self-signed certificates transported by IKE). The offered protection is against passive attacks, but not against active attacks.
Unauthenticated SAs can then be cryptographically bound to applications, which in turn perform their own authentication ("*channel binding*").

The WG is currently working on a few IDs:

draft-ietf-btns-prob-and-applic	Problem and Applicability Statement for Better Than Nothing Security (BTNS)
	Analysis of the central idea of the btns WG, the threats addressed and the threats uncovered with respect to normal IPsec. Two btns types are presented: *(1) standalone btns, and (2)channel bound btns, where the authentication is done in a later step by higher*

	layers in the stack
draft-ietf-btns-core	Better-Than-Nothing-Security: An Unauthenticated Mode of IPsec
	It specifies how to use IKE (v1 and v2) to setup unauthenticated SAs for IPsec, by defining appropriate extensions to the Peer Authorization Database (PAD) and the Security Policy Database (SPD).
draft-ietf-btns-connection-latching	IPsec Channels: Connection Latching
	On channel binding to IPsec, which protects applications against accidental reconfiguration of IPsec that might expose live packet flows to unintended peers, as might happen with btns.
draft-ietf-btns-ipsec-apireq	Requirements for an IPsec API
	Applications protocols do not have visibility of the use of IPsec underneath. The draft collects requirements for a host IPsec implementation in order to allow applications to observe and influence how IPsec protects their communications.

Profiling Use of PKI in IPSEC (pki4ipsec) WG

http://www.ietf.org/html.charters/pki4ipsec-charter.html

IETF has observed a low deployment of IPsec based on certificates, although standardization exists. The pkix WG works to promote it, by developing an X.509 certificate profiling for IPsec, and working on related issues such as enrolment and certificate lifecycle.

draft-ietf-pki4ipsec-mgmt-profile-rqts	Requirements for an IPsec Certificate Management Profile
	Requirements for transactions to handle Public Key Certificate (PKC) lifecycle transactions between IPsec VPNs using IKEv1-v2 and PKI. It will serve as base for the design of a management protocol for enterprise scale IPsec VPN deployments.
draft-ietf-pki4ipsec-ikecert-profile	The Internet IP Security PKI Profile of IKEv1/ISAKMP, IKEv2, and PKIX

EAP Method Update (emu) WG

http://www.ietf.org/html.charters/emu-charter.html

The Extensible Authentication Protocol (EAP, RFC 3748) is an access authentication framework used in different access networks (e.g. 802.11 and 801.16, 3G) and different protocols (e.g., PPP, PANA). EAP as such is the encapsulating protocol; different authentication methods can be carried within EAP. This also implies that EAP is largely used in different contexts, being a framework, but this has brought issues such as too many extensions (there are over 40 profiles, and many not documented as RFC), and purposes other than the original ones. A few features are also missing in the framework, e.g. application key derivation and support for certain types of access.

The emu WG is working out a small set of EAP methods needed by other standardization bodies, e.g. TLS-based EAP with shared secret and password based methods. Interoperability will also be promoted, after interoperability issues were reported.

Kerberos WG (krb-wg) WG

http://www.ietf.org/html.charters/krb-wg-charter.html

Kerberos is widely used authentication protocol, however problems of interoperability have been reported. The WG strives to overcome such problems, specifying the new version of Kerberos (now version 5, RFC 4120), and takes care of the extension work for the protocol.

Kerberized Internet Negotiation of Keys (kink) WG

http://www.ietf.org/html.charters/OLD/kink-charter.html

[concluded in April 2006]

The kink WG has designed a centralized key management protocol for IPsec, based on Kerberos. As alternative to IKE (v1), the kink protocol strives for low computational cost, low latency, and a small footprint.

Simple Authentication and Security Layer (sasl) WG

http://www.ietf.org/html.charters/sasl-charter.html

SASL is the framework for authentication and data security that decouples authentication mechanisms from application protocols, allowing for different authentication mechanisms. The sasl WG focuses on the design of the new version of SASL, RFC2222bis. Protocols currently using SASL include BEEP, IMAP, LDAP, POP, and SMTP.

Multicast Security (msec) WG

http://www.ietf.org/html.charters/msec-charter.html

The msec WG standardizes protocols for Internet group and multicast communication, including one-to-many and many-to-many multicast applications. Given the different requirements of the many possible applications, msec is working at a Framework which defines the security architecture and the building blocks:

RFC 4046	Multicast Security (MSEC) Group Key Management Architecture
	Definition of the reference MSEC architecture, including terminology and concepts. The architecture provides the necessary guidelines and framework to develop key management protocols tailored to different scenarios.
RFC 3740	The Multicast Security Architecture
	Overview and rationale of the multicast security architecture for large multicast groups.

Different key management protocols are then defined to be used in specific scenarios:

RFC 3547	The Group Domain of Interpretation
	GDOI offers key distribution from one source to a group and manages group security associations used by IPsec (and potentially other data security protocols), largely borrowing from the ISAKMP and IKEv1 key management protocols. Update of GDOI is on-going, draft-ietf-msec-gdoi-update.
RFC 4535	GSAKMP: Group Secure Association Group Management Protocol
	GSAKMP provides a security framework for creating and managing cryptographic groups on a network, including dissemination of group policy
draft-ietf-msec-gkdp	GKDP: Group Key Distribution Protocol
	Largely based on IKEv2 (therefore lighter that GDOI which is based on IKEv1)
RFC 3830	MIKEY: Multimedia Internet KEYing
	MIKEY is a lightweight group key management, particularly suitable for heterogeneous environment (mix of wired and wireless networks). It performs key management for the Secure RTP (RFC 3711), although MIKEY can be defined to support other data security protocols. MIKEY can be piggybacked (RFC4567) into session establishment protocols, such as SIP and RTSP, to reduce setup time.

More work has been generated around the base MIKEY protocol:

draft-ietf-msec-mikey-applicability	On the applicability of various MIKEY modes and extensions
	An overview of the different extensions of the MIKEY protocol.
RFC 4650	HMAC-authenticated Diffie-Hellman for MIKEY
	An addition MIKEY mode, intended to be lightweight and point-to-point, using a Diffie-Hellman key agreement protocol, authenticated by a keyed hash message authentication code.
draft-ietf-msec-mikey-ecc	ECC Algorithms For MIKEY
	MIKEY support for elliptic-curve cryptography (ECC).
RFC 4738	MIKEY-RSA-R: An additional mode of key distribution in MIKEY
	An addition MIKEY mode, the RSA-R mode, which allows for a public-key mode in scenarios where the MIKEY Initiator does not know the other party's public key or identifier.
RFC 4563	The Key ID Information Type for the General Extension Payload in Multimedia Internet KEYing (MIKEY)
	A 3GPP-specific extension payload for the MBMS architecture, where MIKEY is used as key management protocol.

The msec WG is also working on source origin authentication (SOA) for group scenarios, by designing the Timed Efficient Stream Loss-tolerant Authentication Protocol (TESLA). TESLA is an efficient protocol with low communication and computation overhead, providing source authentication in multicast scenarios. TESLA is based on loose time synchronization between the sender and the receivers, can scale to large numbers of receivers, and tolerates packet loss. .

RFC 4082	Timed Efficient Stream Loss-Tolerant Authentication (TESLA): Multicast Source Authentication Transform Introduction
	Delayed authentication that provides source authentications in groups (where integrity using the group key does not provide SOA, since a group key can only prove that the message was sent by a member within the group but can not prove which one), without using the standard but cumbersome approach of digital signatures.

RFC 4383	The Use of Timed Efficient Stream Loss-Tolerant Authentication (TESLA) in the Secure Real-time Transport Protocol (SRTP)
	It adds source authentication, using TESLA, to the Secure RTP (RFC 3711)
RFC 4442	Bootstrapping Timed Efficient Stream Loss-Tolerant Authentication (TESLA)
	Defines how the MIKEY protocol (RFC 3830) can carry the parameters needed by SRTP to apply TESLA (i.e. makes MIKEY a key management solution for RFC 4383).
RFC 4359	The Use of RSA/SHA-1 Signatures within Encapsulating Security Payload (ESP) and Authentication Header (AH)
	SOA for multicast IPsec using the standard approach (digital signatures).

Other relevant work:

RFC 4534	Group Security Policy Token v1
	Within the Multicast Group Security Architecture (RFC3740), the Policy Token is defined to enforce security parameters for the group. The Token is signed by the group owner and used for authorization purposes.
draft-ietf-msec-ipsec-extensions	Multicast Extensions to the Security Architecture for the Internet Protocol
	It adds multicast to IPsec, whose RFC 4301 (or "2401bis") describes supports only unicast packets and manually configured IP multicast packets
draft-ietf-msec-ipsec-composite-group	Multicast IP Security Composite Cryptographic Groups
	While the basic multicast IPsec architecture (draft-ietf-msec-ipsec-extensions) assumes homogeneous cryptographic capabilities and security policies for the group, this draft accommodates large-scale cryptographic groups which may contain a heterogeneous endpoint population ("composite cryptographic group" IP security architecture capability).

Domain Keys Identified Mail (dkim) WG
http://www.ietf.org/html.charters/dkim-charter.html

The dkim WG has begun anti-spam standardization work. Based on ideas of Yahoo! and Cisco, and with the collaboration of several industry players, dkim is defining a mechanism that allows a domain to sign e-mail messages, so that receiving domains can more easily detect spoofed messages, hence spam. The basic principle is that the sending domain signs the outgoing e-mail sent by an authorized end-user (the signature is added as header), and publishes the corresponding public key into a DNS record. The receiving e-mail system can verify the signature, by retrieving the public key published by the sender domain in the received e-mail. Local policies are then applied according to the verification result.

The dkim mechanism has several advantages, such as transparency to existing e-mail architecture, scalability, and possibility of implementation that is independent of clients. It does not require trusted third parties, such as certificates authorities and related signing infrastructure, since the public key is provided directly by the signer, e.g. by publishing it in the DNS. Reputation schemes are out of scope for the WG. However they are a useful tool to complement authentication schemes in the effort of combating spam (it is well understood that dkim alone is not the comprehensive answer to spam; much more is needed, not least a different security culture and user behavior).

The dkim framework is under experimentation in the Internet. Reference implementations are available from Yahoo! and Sendmail, http://antispam.yahoo.com/domainkeys.

RFC 4686	Analysis of Threats Motivating DomainKeys Identified Mail (DKIM)
	Threat analysis for dkim
draft-ietf-dkim-base	DomainKeys Identified Mail (DKIM) Signatures
	Design of the dkim framework
draft-ietf-dkim-overview	DomainKeys Identified Mail (DKIM) Service Overview
	Overview of DomainKeys Identified Mail and how it relates to other IETF message signature technologies, implementation and migration considerations, potential applications and future extensions.
draft-ietf-dkim-ssp-requirements	Requirements for a DKIM Signing Practices Protocol
	Requirement draft for the mechanism that would allow an administrator to publish statements about their e-mail accountability practices.

Note: there are other proposals in IETF on the same line as dkim, to combat spam. One is SenderID (RFC 4406), supported by Microsoft. Currently, SenderID and DomainKeys are the two most experimented alternatives.

S/MIME Mail Security (smime) WG

http://www.ietf.org/html.charters/smime-charter.html

The smime WG works on specifying security for the MIME format (popular for mail, but can be used with other transport mechanisms such as HTTP). The specifications for S/MIME version 3.1 (RFC 3850 and RFC 3851) have been completed.

The Cryptographic Message Syntax (CMS, RFC 3852) is used as the key cryptographic component of S/MIME. The WG specifies the cryptographic algorithms to be used with CMS.

This WG also hosts work on electronic signatures. "CMS Advanced Electronic Signatures (CAdES)" (draft-ietf-smime-cades-01.txt) is equivalent to the ETSI TS 101 733.

The WG has produced many RFCs and has a few IDs work in progress, see http://www.ietf.org/html.charters/smime-charter.html

Central RFCs for S/MIME 3.1:

- S/MIME Version 3.1 Message Specification (RFC 3851)
- S/MIME Version 3.1 Certificate Handling (RFC 3850)
- Cryptographic Message Syntax (CMS) (RFC 3852)

An Open Specification for Pretty Good Privacy (openpgp) WG

http://www.ietf.org/html.charters/openpgp-charter.html

Work on the popular PGP, used to digitally sign and encrypt e.g. e-mails and files in storage.

RFC 2440	OpenPGP Message Format
	Specification of the OpenPGP format.
draft-ietf-openpgp-rfc2440bis	OpenPGP Message Format
	Revision of RFC 2440
RFC 3156	MIME Security with OpenPGP
	Use of OpenPGP to secure the Multipurpose Internet Mail Extensions (MIME) security content types (RFC 1847)

Integrated Security Model for SNMP (isms) WG

http://www.ietf.org/html.charters/isms-charter.html

Version 3 of the Simple Network Management Protocol (SNMPv3) adds security to the previous versions of the protocol, largely used for network management. The currently defined security model is the User Security Model (USM) [RFC3414]. USM avoids existing security infrastructures, typically using a separate user and key management infrastructure, so to function also when the third party authentication is not available. However USM has seen limited deployment so far, among the reasons also the lack of integration with deployed authentication infrastructures. Therefore, the ism WG has started to work on the definition of a new SNMPv3 security model, which could use widely deployed user and key management systems, e.g. SSH together with the AAA infrastructure. This work has been welcome by the community as it is felt important.

draft-ietf-isms-secshell	Secure Shell Security Model for SNMP
	Defines how SNMP can be used within a Secure Shell (SSH) session, making use of any of the SSH user authentication methods [RFC 4252], including integration with several deployed infrastructure such as AAA servers using the RADIUS protocol [RFC2865].
draft-ietf-isms-tmsm	Transport Mapping Security Model (TMSM) for the Simple Network Management Protocol
	TMSM is a model, as an extension of the RFC3411 architecture, allowing security to be provided by an external protocol (e.g. TLS or SSH) connected to the SNMP engine through an SNMP transport-mapping.
draft-ietf-isms-transport-security-model	Transport Security Model for SNMP
	A Transport Security Model for SMTP, for use with secure transport models [draft-ietf-isms-tmsm].

Transport Layer Security (tls) WG

http://www.ietf.org/html.charters/pkix-charter.html

The tls WG is dedicated to the design of transport layer security, starting from SSL 3.0 to the different versions of TLS, v1.0 and v1.1, and v1.2 (main goal in the updated charter). Main achievements are also the TLS extensions, e.g. adding new crypto suites and wireless adaptations.

A few relevant specifications are listed in the following.

RFC 2246	The TLS Protocol Version 1.0
	The TLS v1.0 specification
RFC 4346	The TLS Protocol Version 1.1
	The TLS v1.1 specification
RFC 4366	Transport Layer Security (TLS) Extensions
	The TLS extensions (e.g. MAC truncation, negotiation of the use of client certificate URLs, etc.) are designed to enable TLS to effectively operate in new environments like wireless networks.
RFC 2818	HTTP Over TLS
	Pre-Shared Key Ciphersuites for Transport Layer Security (TLS) (RFC 4279) The support of pre-shared key authentication method for TLS is added to the existing public key certificates and Kerberos methods. Useful in performance-constrained environments (e.g. cellular)

Secure Shell (secsh) WG

http://ietf.org/html.charters/OLD/secsh-charter.html

[concluded in October 2006]

Further work on Secure Shell (SSH), a protocol widely used to secure remote logins. The core specifications are RFCs 4250-4256.

Kitten (GSS-API Next Generation) (kitten) WG

http://www.ietf.org/html.charters/kitten-charter.html

Work on further development of the Generic Security Services API (RFC 2743, RFC 2744), which defines an API for applications to set up security contexts for message protection.

Intrusion Detection Exchange Format (idwg) WG

http://ietf.org/html.charters/OLD/idwg-charter.html

[concluded in 2006]

The idwg WG is defining data formats and exchange protocol for sharing information between intrusion detection systems and related management systems. This issue is of greater importance, given that many different intrusion detection system (IDS) products are in use and they need often to communicate to a central manager, which in turn needs facilitated ways for correlation.

draft-ietf-idwg-requirements	Intrusion Detection Message Exchange Requirements
	Requirement draft
draft-ietf-idwg-idmef-xml	The Intrusion Detection Message Exchange Format
	Defines the message exchange format
draft-ietf-idwg-beep-idxp	The Intrusion Detection Exchange Protocol (IDXP)
	An application-level protocol for exchanging data between intrusion detection entities

Extended Incident Handling (inch) WG

http://ietf.org/html.charters/OLD/inch-charter.html

[concluded]

The inch WG is defining a data format for exchanging information about security incidents. The issue is to standardize the communication between CERTs/CSIRTs and any involved parties.

draft-ietf-inch-requirements	Requirements for the Format for Incident Information Exchange (FINE)
	Requirement draft
draft-ietf-inch-iodef	The Incident Object Description Exchange Format Data Model and XML Implementation
	Defines the Incident Object Description Exchange Format (IODEF) as data representation to exchange CSIRTs information. It also includes an implementation of the data model in the Extensible Markup Language (XML).
draft-ietf-inch-rid	Incident Handling: Real-time Inter-network Defense
	Network Providers need to act promptly in communicating and tracing security incidents. Tracing may be a challenging task, due to the nature of the

	attacks (e.g. DDoS), and has also to face the issue of establishing a cooperation among different network providers. The Real-time Inter-network Defense (RID) is intended to build such communications for tracing. RID is an extension of IODEF.
draft-ietf-inch-phishingextns	Extension to IODEF-Document Class for Phishing, Fraud, and Other Non-Network Layer Reports
	Extension of the INCH format (originally designed for network-layer incidents such as DoS attacks and compromised computers, but easily extendible) to report phishing and fraud incidents

The ENISA Inventory of CERT activities in Europe
http://www.enisa.europa.eu/doc/pdf/deliverables/enisa_cert.pdf

There exist a few other standardization activities in support of CERTs/CSIRTs cooperation. A list can be found in the ENISA Report "**ENISA Inventory of CERT activities in Europe**". The Inventory provides an overview on the actual situation concerning CERT matters in Europe. It provides a list of response teams and similar facilities by country, but also contains a catalogue of cooperation activities, support activities, and standardization activities related to them.

Security Issues in Network Event Logging (syslog) WG
http://www.ietf.org/html.charters/syslog-charter.html

The syslog WG is working to define the specifications for SYSLOG, a widely used protocol for logging, which however has not yet been standardized.

draft-ietf-syslog-protocol	The SYSLOG protocol
	Specification of the Syslog Protocol
draft-ietf-syslog-transport-tls	TLS Transport Mapping for SYSLOG
	How to protect Syslog messages using TLS

Public-Key Infrastructure (X.509) (pkix) WG

http://www.ietf.org/html.charters/pkix-charter.html

The long-living pkix WG works on standards for X.509-based Public Key Infrastructure (PKI). Main tasks are advancing the existing standard into the standardization process, profiling of the ITU-T standards, and updating the specifications as protocols (such as LDAP3) evolve. Protocols related to certificate management are also hosted here, e.g. the Certificate Management Protocol (CMP) and the Online Certificate Status Protocol (OCSP). A few pkix standards are listed below; more standards are available on the WG's web page.

RFC 2560	X.509 Internet Public Key Infrastructure Online Certificate Status Protocol - OCSP
	Specifies a protocol to determine the current status of a digital certificate without requiring Certificate Revocation Lists (CRLs).
RFC 3029	Internet X.509 Public Key Infrastructure Data Validation and Certification Server Protocols
	Describes a general Data Validation and Certification Server (DVCS), a Trusted Third Party used for example to assert the validity of signed documents, public key certificates, and the possession or existence of data.
RFC 3161	Internet X.509 Public Key Infrastructure Time Stamp Protocols (TSP)
	Describes the format of request/response to a Time Stamping Authority (TSA) and defines security-relevant requirements for TSA operations.
RFC 3280 draft-ietf-pkix-rfc3280bis	Internet X.509 Public Key Infrastructure Certificate and CRL Profile
	Profiles the X.509 v3 certificate and X.509 v2 Certificate *Revocation List (CRL) for use in the Internet, defining the relation with the ISO/IEC/ITU-T standards.*
RFC 3281	An Internet Attribute Certificate Profile for Authorization
	Defines a profile for the use of X.509 Attribute Certificates in Internet Protocols.
RFC 3739	Internet X.509 Public Key Infrastructure: Qualified Certificates Profile
	A certificate profile, based on RFC 3280, for identity certificates issued to natural persons. A Qualified Certificate is a certificate that is qualified within a defined legal framework.
RFC 4210	Internet X.509 Public Key Infrastructure Certificate

	Management Protocols
	The Certificate Management Protocol (CMP) provides on-line interactions between PKI components, including an exchange between a Certification Authority (CA) and a client system.
RFC 4211	Internet X.509 Public Key Infrastructure Certificate Request Message Format (CRMF)
	The Certificate Request Message Format (CRMF) is used to convey a request for a certificate to a Certification Authority (CA), possibly via a Registration Authority (RA), for the purposes of X.509 certificate production. The request will typically include a public key and the associated registration information.
RFC 4386	Internet X.509 Public Key Infrastructure Repository Locator Service
	The PKI repository locator service, using DNS, enables certificate-using systems to locate PKI repositories.
	Server-based Certificate Validation Protocol (SCVP)
draft-ietf-pkix-scvp	*SCVP allows a client to delegate certificate path construction and certificate path validation to a server.*

Long-Term Archive and Notary Services (ltans) WG

http://www.ietf.org/html.charters/ltans-charter.html

The ltans WG works on aspects related to long-term archive, e.g. long-term non-repudiation of digitally signed data. In these scenarios, users need to prove the existence of data at a specific time, generally far away in the past, and its integrity since then. Then, pure cryptography is not enough, but needs to be accompanied by standards mechanisms to handle issues such as certificate expiration, and change of format.

draft-ietf-ltans-reqs	Long-Term Archive Service Requirements
	Requirements draft.
draft-ietf-ltans-ers	Evidence Record Syntax (ERS)
	Specifies the syntax and processing of an Evidence Record, designed for long-term non-repudiation of existence of data (e.g. of digitally signed data).
draft-ietf-ltans-ltap	Long-term Archive Protocol (LTAP)
	Describes the long-term archive service (LTA), a service operated as a trusted third party to securely archive electronic documents, and how clients can interact with such a service.
draft-ietf-ltans-ers-scvp	Using SCVP to Convey Long-term Evidence Records

	Describes the use of the Simple Certificate Validation Protocol (SCVP), supporting the development and validation of certification paths well after the expiration of the certificates in the path, together with the Evidence Record Syntax (ERS, draft-ietf-ltans-ers).

Other IETF WGs with security work

Security has deep roots in IETF. Every document is required to have security considerations, therefore NIS activities are spread through the different WGs. A few relevant WGs where relevant NIS work is done, outside of the dedicated Security Area, are listed below.

Geographic Location/Privacy (geopriv) WG

http://www.ietf.org/html.charters/geopriv-charter.html

The WG looks at the security issues (in particular privacy), related to the acquisition and transmission of geographic location information. This type of service is growing in importance, due to the increase number of resources available on the Internet and of location-aware applications. The work focuses on security requirement identification, and the enhancement of a selected transmission format in order to fulfill such requirements. One goal of the WG is a specification that could become mandatory-to-implement for IETF location-aware protocols.

The WG is also working at an API for an application to manage link-based location information, such as the one from a 3G wireless link.

The WG states in the charter that the development of technology to support regulatory requirements is out of scope, although the output will be a framework that might be used for such technology defined in other bodies.

Host Identity Protocol (hip) WG

http://www.ietf.org/html.charters/hip-charter.html

The Host Identity Protocol (HIP) has been one of the protocols that have attracted most of the interest among the IETF community the latest years.

The HIP proposal introduces a new namespace (in addition to IP addresses and DNS), with the intent of filling a few gaps between IP and DNS namespaces, i.e. dynamic readdressing, anonymity, and authentication. Security is a key feature of the HIP protocol and its underlying architecture. Normally an IP address has a double role of "locator" (routing) and "identifier" (endpoint identifier); HIP separates these roles. The HIP architecture adds a new layer between the IP and the transport layers, hence

decoupling the layers and splitting the dual roles of IP addresses. It introduces a new Host Identity (HI) name space, based on public keys. A public/private key pair is used as Host Identifier (the public key, which may be self-generated), to which higher layer protocols are bound instead of an IP address. This allows enhancing security (e.g. resistance to DoS and secure establishment of communication, e.g. via IPsec) and mobility (e.g., enable continuity of communications across IP address changes).

The HIP standardization is now in the phase when the base specifications are written and approved or under final evaluation. The protocol will get an Experimental RFC status, to first allow the implementers' community to experiment with it and evaluate the protocol and its functionalities. While the IETF hip WG focuses on the short-term design of the framework and its specification, the research work around HIP is taking place in the Internet Research Task Force (IRTF) HIP Research Group. One of the central issues under investigation there, is the impact of a wide-scale adoption of the separation of the identifier and locator roles of IP addresses (http://www.irtf.org/charter?gtype=rg&group=hip).

RFC 4423	Host Identity Protocol Architecture
	A background document, describing the reasons that motivated the design of the HIP protocol.
draft-ietf-hip-base	Host Identity Protocol
	Specifies the details of protocol. It is intended to be an Experimental RFC.
draft-ietf-hip-dns	Host Identity Protocol (HIP) Domain Name System (DNS) Extensions
	Specifies a new DNS resource record (RR) to be used with HIP, to allow a HIP node to store in the DNS its Host Identity (i.e., the public component of the node public-private key pair), Host Identity Tag (HIT, a truncated hash of its public key), and the Domain Names of its rendezvous servers. (Host Identifiers have a concise representations -- 128-bit Host Identity Tags (HITs) and 32-bit Local Scope Identifiers (LSIs), used to represent host identities in IPv6/v4-sized address structures, respectively, allowing most legacy applications to work unmodified on top of HIP).
draft-ietf-hip-rvs	Host Identity Protocol (HIP) Rendezvous Extension
	HIP nodes make use of rendezvous servers in order to improve reachability and operation when HIP nodes are multi-homed or mobile.
draft-ietf-hip-esp	Using ESP transport format with HIP
	Use of IPsec ESP with HIP.
draft-ietf-hip-mm	End-Host Mobility and Multihoming with the Host Identity Protocol
	Mobility and multihoming extensions HIP. For example, the document includes a parameter

	("LOCATOR") that allows a HIP host to notify peers about alternate addresses at which it may be reached, or change the primary locator (mobility of HIP host).
draft-ietf-hip-registration	Host Identity Protocol (HIP) Registration Extensions
	Registration mechanism for HIP hosts to register with services, such as HIP rendezvous servers [I-D ietf-hip-rvs] or a middlebox [RFC3234].

Operational Security Capabilities for IP Network Infrastructure (opsec)

http://www.ietf.org/html.charters/opsec-charter.html

The goal of the opsec WG is to analyze and offer best common practices on how to securely manage and operate networks. The specifications aim at providing a support in order for vendors and network operators to exchange requirements for secure networks. The focus for the moment is on ISPs and enterprise networks only, while wireless devices, Small Office/Home Office (SOHO) devices, security devices (e.g. firewalls and IDS) and hosts are explicitly out-of-scope for the time being.

The opsec WG conveys very useful guidance gained during operational experience, based on a very broad information gathering exercise among operators and manufactures. The opsec capability drafts have started to be used as reference material for security checklists in real-life environments, e.g. for baseline security checklists among network operators and vendors.

draft-ietf-opsec-framework	Framework for Operational Security Capabilities for IP Network Infrastructure
	Sets the framework for the WG work, e.g. threat model, scope, definitions, etc. The framework introduces the list of capabilities documents to be produced, which will cover each: Packet Filtering, Event Logging, In-Band and Out-of-Band Management, Configuration and Management Interfaces, AAA, and Documentation and Assurance.
draft-ietf-opsec-efforts	Security Best Practices Efforts and Documents
	Overview of Standards Developing Organizations developing standards to improve the robustness of the Internet.
draft-ietf-opsec-current-practices	Operational Security Current Practices
	A survey of current practices used in large ISPs to secure layer 2 and layer 3 infrastructure devices.
draft-ietf-opsec-filter-caps	Filtering and Rate limiting Capabilities for IP Network Infrastructure

	List of filtering and rate limiting capabilities needed in the network to secure the infrastructure (as support to the practices in draft-ietf-opsec-current-practices).
draft-ietf-opsec-infrastructure-security	Service Provider Infrastructure Security
	Best current practices for implementing Service Provider network infrastructure protection for network elements, complementing the filtering policies of RFC 2267 and RFC 3704.
draft-ietf-opsec-nmasc	Network Management Access Security Capabilities
	Secure network management using either the in-band network or an out-of-band network. Each access method is evaluated in terms of its security capabilities.
draft-ietf-opsec-misc-cap	Miscellaneous Capabilities for IP Network Infrastructure
	Covers additional miscellaneous capabilities which do not fit into the categories specified in draft-ietf-opsec-framework

Routing Security

The **Routing Protocol Security Requirements (rpsec) WG** addresses the security requirements for routing (RFC 4593). The WG focuses on routing-to-routing protocols for unicast and multicast systems (it does not include host-to-router protocols such as the Internet Group Management Protocol (IGMP), and in particular on Border Gateway Protocol (BGP) security (draft-ietf-rpsec-bgpsecrec) and the Open Shortest Path First (OSPF) (draft-ietf-rpsec-ospf-vuln) requirements. http://www.ietf.org/html.charters/rpsec-charter.html

Using the requirements identified by the rpsec WG, the new **Secure Inter-Domain Routing (sidr) WG** has started working on an extensible architecture for an inter-domain routing security, identified as one of the problems for the security of the Internet environment. One of the work topic is the description of usage of certification objects to support the distribution of authorization and authentication information for routing, under the assumption of different underlying trust characteristics. http://www.ietf.org/html.charters/sidr-charter.html

In the IETF 66th meeting (July 2006), a few individual submissions where presented as proposals for routing authentication:

draft-bellovin-keyroll2385	Key Change Strategies for TCP-MD5
	The TCP-MD5 option (RFC2385) is the most commonly used to secure BGP sessions between routers, however it has the issue of key management, as

	changing the long-term key is difficult in terms of synchronization. The draft proposes a short-term mechanism, based on a list of valid keys and associated (conceptual) timestamps.
draft-touch-tcpm-tcp-simple-auth	The TCP Simple Authentication Option
	Intended to replace the TCP MD5 Signature option (RFC 2385), the draft specifies the use of stronger HMAC-based hashes, assuming an out-of-band mechanism (manual or via a separate protocol) for key management.
draft-bonica-tcp-auth	Authentication for TCP-based Routing and Management Protocols
	Enhancement of the TCP MD5 Signature option (RFC 2385) to improve the security of TCP-based protocols, e.g. BGP; it uses algorithms stronger than MD5.
draft-weis-tcp-auth-auto-ks	Automated key selection extension for the TCP Authentication Option
	An automated key selection extension for the TCP authentication option (I-D bonica-tcp-auth).

Other relevant security work on routing is also done in other WGs, for example in the **IS-IS for IP Internets (isis) WG**[129] (http://www.ietf.org/html.charters/isis-charter.html) and in the **Inter-Domain Routing (idr) WG** (http://www.ietf.org/html.charters/idr-charter.html). The idr WG hosted for example the design of the BGP protocol itself and the identification of BGP vulnerabilities (RFC 4272).

DNS Security related Working Groups

dnsext WG: http://www.ietf.org/html.charters/dnsext-charter.html
dnsop WG: http://www.ietf.org/html.charters/dnsop-charter.html

The security solution for the DNS service, DNSSEC, which was initiated within the dnssec WG, closed in 1999, is maintained and developed by the DNS Extension (dnsext) WG, while operational issues are investigated in the Domain Name System Operations, dnsop, WG. The core DNSSEC standards are listed in the table below.

RFC 3833	Threat Analysis of the Domain Name System (DNS)
	Documents some of the known threats to the DNS, and use of DNSSEC to address them.
RFC 4033	DNS Security Introduction and Requirements
	Introduces the DNSSEC extensions, their capabilities

[129] IS-IS is an Interior Gateway Protocol (IGP) protocol, i.e. is intended for use within an administrative domain or network.

	and limitations.
RFC 4034	Resource Records for the DNS Security Extensions
	Defines the DNSSEC collection of resource records, their purpose and format.
RFC 4035	Protocol Modifications for the DNS Security Extensions
	Describes the DNSSEC protocol modifications
RFC 2845	Secret Key Transaction Authentication for DNS (TSIG)
	TSIG allows for transaction level authentication using shared secrets and one way hashing, e.g. to authenticate dynamic updates or responses. No assumptions are made on the key management (i.e., out-of-band mechanisms are expected).
RFC 2930	Secret Key Establishment for DNS (TKEY RR)
	Specifies a TKEY resource record to be used for establishing shared secret keys for TSIG.

The dnsext has published several other standards related to DNS security, see the list at the dnsext WG page. Current work-in-progress is also listed on the dnsext WG page. In particular, the WG is working on the issue of zone enumeration (DNSSEC Hashed Authenticated Denial of Existence, draft-ietf-dnsext-nsec3), introduced by the basic set of RFCs. The issue is that DNSSEC requires the enumeration, hence exposure, of a zone content (e.g. the enumeration of the employees in an organization).

In the dnsop WG, operational aspects and practices for DNSSEC are collected in RFC 4641, DNSSEC Operational Practices.

Middlebox Communications (midcom) WG

http://www.ietf.org/html.charters/midcom-charter.html

A middlebox is a device in the network providing transport policy enforcement. Examples are firewalls, NATs and IPv4/v6 translators, signature management for intrusion detection systems, and multimedia buffer management. Middleboxes may be required to make policy decisions, hence applications need to be able to communicate their needs to the middlebox. This has also the advantage to remove application logic from the middlebox, which often cause bottleneck. The midcom WG is developing such framework, focusing on firewalls and NATs as middleboxes.

RFC 3304	Middlebox Communications (MIDCOM) Protocol Requirements
	midcom requirements
RFC 3303	Middlebox Communication Architecture and framework

	Defines the midcom architecture and framework, in which trusted third parties can be delegated to assist the middleboxes which can remain application agnostic.
RFC 3489	STUN - Simple Traversal of UDP Through Network Address Translators
	STUN is a lightweight client-server protocol allowing applications to discover the presence and types of NATs and firewalls, as well as to determine the allocated IP addresses.
RFC 3989	MIDCOM Protocol Semantics
	Specifies semantics for a MIDCOM protocol.
RFC 4097	Middlebox Communications (MIDCOM) Protocol Evaluation
	Evaluation of MIDCOM candidates: SNMP, RSIP, Megaco, Diameter, and COPS.

Behavior Engineering for Hindrance Avoidance (behave) WG

http://www.ietf.org/html.charters/behave-charter.html

IETF asserts the e2e principle (RFC 1958). The debate on network address translators (NATs) in IETF has long history and NATs have always found a very hard opposition, however it is acknowledged that NATs are a reality and that will survive lengthily in the Internet. Nevertheless, they cause problems with many applications. One of the reasons is that there is no well-defined behavior of a NAT: there are many different types of NATs, treating the traffic in different ways, and none is standard. The behave WG is working at the definition of best common practices for NAT technologies, in order to not penalize applications.

draft-ietf-behave-rfc3489bis draft-ietf-behave-turn	Simple Traversal Underneath Network Address Translators (NAT) (STUN). Obtaining Relay Addresses from Simple Traversal of UDP Through NAT (STUN)
	Work on RFC3489bis and extensions, allowing the traversal of UDP packets.
draft-ietf-behave-nat-udp draft-ietf-behave-tcp draft-ietf-behave-nat-icmp	NAT Behavioral Requirements for Unicast UDP NAT Behavioral Requirements for TCP NAT Behavioral Requirements for ICMP protocol
	Basic terminology for describing different types of NAT behavior when handling Unicast UDP (resp. TCP), and a set of requirements that would allow many

	applications such as multimedia communications, on-line gaming (resp. peer-to-peer and on-line games), to work consistently. The development of NATs following these requirements will greatly increase the likelihood for those applications to work. Also for ICMP.
draft-ietf-behave-p2p-state	*State of Peer-to-Peer (P2P) Communication Across NATs*
	Inventory of existing methods used by P2P applications to traverse NATs.

Other work of the WG includes all the IPsec/IKE crypto suites specifications, and IPsec NAT Traversal (UDP Encapsulation of IPsec, RFC3948, and Negotiation of NAT traversal in IKE, RFC 3947). The IPsec community is now engaged in the different active WGs, to apply the IPsec suite to the other technologies and domains, as well as in the deployment efforts (such as VPNC). The interoperability efforts report still issues to be solved, e.g. failures for message fragmentations and certificate issues.

Real-time Applications and Infrastructure (RAI) Area on Multimedia Security

Several WGs are involved in the design of security solutions for multimedia applications.

Audio/Video Transport (AVT) WG

http://www.ietf.org/html.charters/avt-charter.html

The avt WG hosts the work around the Real time Transport Protocol (RTP, RFC 3550), and has worked on RTP security by defining the Secure RTP.

RFC 3711	The Secure Real-time Transport Protocol
	SRTP is one of the candidate protocols for securing the media in VoIP/IMS scenarios. SRTP is an application security protocol, designed for providing confidentiality, message authentication, and replay protection to RTP/RTCP. It is particularly designed for heterogeneous (wired and wireless) environments.
draft-ietf-avt-srtp-big-aes	The use of AES-192 and AES-256 in Secure RTP
	SRTP is, as good practice requires, extendible to new algorithms. This draft adds the use of AES 192 and AES 256 within SRTP, for the encryption (Counter Mode) and the Key Derivation Function.

Multiparty Multimedia Session Control (mmusic) WG
http://www.ietf.org/html.charters/mmusic-charter.html

The mmusic WG has developed well-known session control protocols: the Real Time Streaming Protocol (RTSP, RFC 2326), the Session Description Protocol (SDP, RFC 4566), the initial version of the Session Initiation Protocol (SIP, now brought into the sip WG with RFC 3261 and others), and SAP (Session Announcement Protocol, RFC 2974). The RFCs also define the security solution for these protocols.

Another security work undertaken by the WG is related to the key management for media security that can be piggybacked into the session control protocol.

draft-ietf-mmusic-securityprecondition	Security Preconditions for Session Description Protocol (SDP) Media Streams
	SDP preconditions (RFCs 3312 and 4032) used to freeze a session setup or modification, until successful negotiation of the security for the media stream.
RFC 4567	Key Management Extensions for Session Description Protocol (SDP) and Real Time Streaming Protocol (RTSP)
	Piggybacking a key management protocol into the session control protocol (SIP/SDP and RTSP). The usage with the MIKEY key management protocol is specified.
RFC4568	Session Description Protocol Security Descriptions for Media Streams
	Alternative way to piggyback key material and key attributes (not a key management) within SDP, for the protection of unicast media streams. The support for the SRTP media protocol is defined
RFC4572	Connection-Oriented Media Transport over the Transport Layer Security (TLS) Protocol in the Session Description Protocol (SDP)
	SDP used to establish secure connection-oriented media transport sessions over TLS.

NAT traversal is an issue for multimedia

draft-ietf-mmusic-ice draft-ietf-mmusic-ice-tcp	Interactive Connectivity Establishment (ICE): A Methodology for Network Address Translator (NAT) Traversal for Offer/Answer Protocols
	ICE, based on STUN (draft-ietf-behave-rfc3489bis, see the behave WG), is a protocol for NAT traversal of multimedia session signaling protocols based on the offer/answer model (such as SIP).

Session Initiation Protocol (SIP) and Session Initiation Proposal Investigation (sipping) WGs

sip WG: http://www.ietf.org/html.charters/sip-charter.html
sipping WG: http://www.ietf.org/html.charters/sipping-charter.html

The SIP WG maintains and develops the work on the Session Initiation Protocol (SIP), which is the signaling protocol at the base of NGN network and of the IMS system.

RFC 3261 RFC 3853	SIP: Session Initiation Protocol S/MIME AES Requirement for SIP
	RFC 3261 is the main RFC for SIP. It defines the basic security of the protocol (e.g. use of http digest, security SIP headers fields, S/MIME for e2e security). RFC 3853 updates RFC 3261, by adding the support for AES (in addition to 3DES) for S/MIME.
draft-ietf-sip-e2m-sec	End-to-middle Security in SIP
	Defines the use of S/MIME so that a client can protect the SIP messages up to an intermediary that is trusted (and that needs to inspect the SIP message to provide some service).
RFC 4474	Enhancements for Authenticated Identity Management in the Session Initiation Protocol (SIP)
	Defines a mechanism for securely identifying originators of SIP messages, by adding two new SIP header fields, Identity (for conveying a signature), and Identity-Info (for conveying a reference to the certificate of the signer).
RFC 3310	Hypertext Transfer Protocol (HTTP) Digest Authentication Using Authentication and Key Agreement (AKA)
	Specifies AKA-based one-time password generation mechanism for HTTP Digest access authentication. (AKA is the key management in UMTS networks, a challenge-response mechanism based on symmetric cryptography). This RFC is used e.g. in 3GPP IMS specifications.
RFC 3329	Security Mechanism Agreement for the Session Initiation Protocol (SIP) Sessions
	Defines the negotiation of the security mechanisms used between a SIP user agent and its next-hop SIP entity. This RFC is used e.g. in 3GPP IMS specifications.
RFC 3325	Private Extensions to the Session Initiation Protocol (SIP) for Asserted Identity within Trusted Networks

	Defines private SIP extensions to enable a network of trusted SIP servers to assert the identity of authenticated users. It is a valid scheme only inside an administrative domain, not between different trust domains.
RFC 3323	A Privacy Mechanism for the Session Initiation Protocol (SIP)
	Privacy considerations for SIP.
draft-ietf-sip-certs	Certificate Management Service for The Session Initiation Protocol (SIP)
	Defines how a SIP client can discover the certificate of other users, and how the client can store and retrieve its certificate and private keys via the Credential Service.

The sipping WG is supporting the SIP WG by investigating the use of SIP in applications related to telephony and multimedia, and by developing requirements for SIP extensions (which will then be referred to the SIP WG). The sipping WG is also investigating issues related to SIP that are in need of standardization, e.g. session border controller (SBC, draft-camarillo-sipping-sbc-funcs) requirements, IPv4/v6 considerations, and service requirements such as inclusion of real-time text conversation (ToIP) and support for hearing/speech impaired users.

draft-ietf-sipping-nat-scenarios	Best Current Practices for NAT Traversal for SIP
	Best practices for the SIP NAT traversal, which is a complex issue for multimedia
draft-ietf-sipping-spam	The Session Initiation Protocol (SIP) and Spam
	Addresses the threat of spam for SIP, highlighting the differences from the e-mail spam and the different solutions that have been discussed within the IETF community.
RFC 3702	Authentication, Authorization, and Accounting Requirements for the Session Initiation Protocol (SIP)
	AAA requirements for SIP.
RFC 4189	Requirements for End-to-Middle Security for the Session Initiation Protocol (SIP)
	Requirements for the end-to-middle security solution standardized in the SIP WG (draft-ietf-sip-e2m-sec).
draft-camarillo-sipping-sbc-funcs	Requirements from SIP (Session Initiation Protocol) Session Border Control Deployments
	Functionalities' description (including security) of the SIP intermediaries called Session Border Controllers (SBCs).

RTP Security

The discussion on real-time (primarily RTP) security has been going on in IETF for a few years and got particular attention in the 2006 IETF meetings (IETF64-65). There are multiple security mechanisms available but not comprehensive solution that can fulfill all the scenarios, two of the reasons being the complexity of the real-time applications and systems (e.g. the SIP architecture), and the changing nature of the requirements.

The security solution has to cover two main aspects, the signaling security (e.g., SIP), and the media security (i.e., of RTP, both the key management and the media security protocol). These components are linked since there are solutions that piggyback the media key management into the signalling. Furthermore, the signalling (SIP in particular) is very feature-rich and poses several requirements on the media security protocol (e.g. forking, redirection, early media). As such, real-time security is a cross-issue involving several IETF Working Groups where the work is spread, e.g. avt WG with RTP security, sip and sipping WGs for the signaling, mmusic WG for the piggyback of the key management into the signaling, and key management WGs such as msec WG and IPsec WG. It has also direct impact on other SDOs which are currently investigating media security, e.g. 3GPP, ETSI TISPAN, and ITU-T.

There are different media security protocols that may be used for RTP security, for example IPsec at the network layer, the Datagram Transport Layer Security (DTLS, RFC 4347) at the transport layer, SRTP at the application layer. For the time being, none of them has emerged as preferred standard, because they indeed fulfill different requirements and because the business case for media security has still to mature.

The key management for the media protocol is the most debated issue. There are two different approaches to it, key management piggybacked into the signalling ("SIP path" keying) or key management in-band with the media ("media path" keying).

IETF65 hosted a BOF[130] on this topic, trying to set the SIP requirements for the media keying. Work is now continuing in order to select the most appropriate security mechanisms.

[130] Birds of a Feather, an initial meeting (held during an IETF meeting) where people interested in a particular topic gather to discuss about it.

Session PEERing for Multimedia INTerconnect (speermint) WG

http://www.ietf.org/html.charters/speermint-charter.html

This new WG has begun work on architectures to identify, signal, and route delay-sensitive (real-time) communication sessions, based on SIP. The peering concept includes important security considerations, e.g. trust establishment, security, and attack resistance, considerations that will be investigated by the speermint WG. Work on Spam over IP Telephony (SPIT) has also been included in the WG's charter.

SIP for Instant Messaging and Presence Leveraging Extensions (simple) WG

http://www.ietf.org/html.charters/simple-charter.html

The simple WG investigates the applicability of SIP within the instant messaging and presence (IMP) services. This includes for example an architecture for instant messaging and presence based on a traditional buddy-list. There are security aspects here too to be considered, in particular related to privacy (e.g. who can modify and/or read the presence information).

Emergency Context Resolution with Internet Technologies (ecrit) WG

http://www.ietf.org/html.charters/ecrit-charter.html

Emergency call handling in the context of Internet is challenging, e.g. with regards to location of the call originator and call routing management. The ecrit WG solely concentrate on these issues in the case of any Internet user, e.g. VoIP user (not e.g. government or military, which pose different requirements, for example in security).

draft-ietf-ecrit-security-threats	Security Threats and Requirements for Emergency Call Marking and Mapping
	This document identifies the security threats associated with the marking of signaling messages to indicate that they are related to an emergency, and with the mapping for emergency routing.
draft-ietf-ecrit-phonebcp	Best Current Practice for Communications Services in support of Emergency Calling
	Best current practice on how devices and services should use IETF standards to reliably make emergency calls.

Internet Emergency Preparedness (ieprep) WG

http://www.ietf.org/html.charters/ieprep-charter.html

Work on best common practices documents for the support of recovery operations in telecommunications networks, e.g. in case of natural hazards and catastrophes, or terrorist attacks (Emergency Preparedness), using existing Internet protocols.

Authentication, Authorization and Accounting (aaa) WG

http://www.ietf.org/html.charters/OLD/aaa-charter.html

[concluded in 2007]

Further development of the AAA infrastructure for access networks. The WG primarily focus on the Diameter (RFC 3588) protocol as AAA protocol (trying to maintain compatibility with the other AAA protocol, RADIUS).

Sieve Mail Filtering Language (sieve) WG

http://www.ietf.org/html.charters/sieve-charter.html

The sieve WG is defining the new specifications for the SIEVE mail filtering language (RFC 3028) and its extensions.

IPv6-related Working Groups

IETF is the standardization forum hosting the design of the next generation of IP, IPv6.

IP Version 6 (ipv6) WG

http://www.ietf.org/html.charters/ipv6-charter.html

The ipv6 WG is the WG in change of the maintenance of the main IPv6 specifications, defining the next generation of the IP technology (RFC 2460). The WG is also taking care of the IPv6 main security aspects, among those the following:

- ICMPv6, with the need to update RFC2463
- address auto-configuration, draft-ietf-ipv6-rfc2462bis updating RFC 2462
- neighbour discovery, draft-ietf-ipv6-2461bis updating RFC 2461
- privacy extensions for address auto-configuration, draft-ietf-ipv6-privacy-addrs-v2 updating RFC 3041

Mobility for IPv6 (mip6) WG

http://www.ietf.org/html.charters/mip6-charter.html

Mobile IPv6 (MIPv6, RFC 3775 and 3776) is a protocol that allows a node to remain reachable while moving around IPv6 networks. Each mobile node has associated a *home address*, which remains the same, and a *care-of address*, which provides information of the mobile node's current location. The mobile node is then reachable via the home address or directly to the care-of address.

Security is a critical component of the protocol, given the need to secure the signalling, and indeed security has been one of the most discussed issues in the MIPv6 design process. See for example RFC 3776, "Using IPsec to Protect Mobile IPv6 Signaling between Mobile Nodes and Home Agents".

The WG is also looking at the security implications in home agent discovery and change of the home address, at a bootstrap mechanism for setting up security associations between the mobile node and the home agent (RFC 4640, draft-ietf-mip6-bootstrapping-split, draft-ietf-mip6-bootstrapping-integrated-dhc), and at the interaction with firewalls (RFC 4487). Route optimization in particular requires security mechanisms (RFC 4225) for trusting and updating the binding information (e.g. return-routability, RFC 3775, or pre-shared key, RFC 4449).

IPv6 Operations (v6ops) WG

http://www.ietf.org/html.charters/v6ops-charter.html

The v6ops WG is chartered to develop guidelines for the operation of a shared IPv4/IPv6 Internet, with focus on immediate deployment issues. The following topics belong to the security effort:

- IPv6 Transition/Co-existence Security Considerations (draft-ietf-v6ops-security-overview)
- Security analysis when the tunneling mechanism is used for v4-v6 co-exist ("IPv6-in-IPv4", RFC4213)
    - Security Considerations for 6to4 (RFC 3964)
    - Using IPsec to Secure IPv6-in-IPv4 Tunnels (draft-ietf-v6ops-ipsec-tunnels)
- ICMPv6, with Recommendations for Filtering ICMPv6 Messages in Firewalls (draft-ietf-v6ops-icmpv6-filtering-recs)
- IPv6 and port scanning, draft-ietf-v6ops-scanning-implications
- IPv6 Network Architecture Protection, NAP (draft-ietf-v6ops-nap) *NATs are largely deployed and have some perceived benefits, including security benefits. NAP is the collection of techniques that can achieve the same benefits of NATs and retain the boundary inside-outside the private network.*

International Telecommunication Union (ITU)

http://www.itu.int

Keywords: *ITU Security Architecture, Certificates (X.509), PKI, H.235, Biometrics, Spam, Network security, NGN, VoIP security, Security management, Identity Management.*

ITU is an international organization for the development of the telecom technology, involving governments and private sector. ITU is divided into tree sectors:

- Radio-communication Sector (***ITU-R***), for the management of the radio spectrum
- Telecommunication Standardization Sector (***ITU-T***), for international standards for networks and services
- Telecommunication Development Sector (***ITU-D***), for the promotion of the access to information and ICT by developing countries.

ITU-T is in charge of producing standards (*Recommendations*) for telecommunications (excluding radio), and is the sector most involved in NIS work, e.g. with the X Series Recommendations. ITU-T has published many Recommendations in the NIS field. The X.800 Series comprises a set of documents describing the (broadly referenced) ***ITU Security Architecture*** (Rec. X.800, X.801-802), and a framework covering authentication, access control, non-repudiation, confidentiality, integrity, security audit and alarms (Rec. X.810-816). X.805 defines the security architecture for end-to-end communication systems.

X.509 is one of the most recognized security standard published by ITU. X.509 (also ISO/IEC 9594-8) belongs to the X.500 series of standards covering electronic directory services, although is today widely used outside of X.500. X.509 is an ITU recommendation for electronic authentication over public networks; it specifies a standard format for public-key certificates and is the reference for the Public Key Infrastructure (PKI).

ITU-T has also developed the security solution for applications and services. Examples are the security solution for Voice over IP (***VoIP***) based on ***H.323*** (Recommendation X.235) or IPCablecom, and fax transmission.

ITU has started work on IPTV, i.e. a digital television service delivered on IP over a broadband connection, towards the offering of triple-play (video, voice, and data). Security is part of the work, with the intent to reuse existing work.
http://www.itu.int/ITU-T/IPTV/index.phtml

Other Recommendations by ITU-T cover Network Management Security (e.g., M.3010), Availability (G.8080, G.806), guidelines for Security Incident Handling (E.409).

The second edition of the security manual "Security in telecommunications and information technology - An overview of issues and the deployment of existing ITU-T Recommendations for secure telecommunications", October 2004, lists the most recognized ITU-T Recommendations in the NIS area, including their content. The document also provides highlights on the major security work efforts taking place in ITU-T Study Groups, for the study period concluded in 2004. http://www.itu.int/itudoc/itu-t/86435.html

The ITU-T flyer on security lists some NIS topics of interest for ITU and related ITU Recommendations, http://www.itu.int/itudoc/gs/promo/tsb/86261.pdf.

The ITU's ICT Security Standards Roadmap
http://www.itu.int/ITU-T/studygroups/com17/ict/index.html
The Roadmap is a (work-in-progress) collection of NIS standards from key Standards Development Organizations (SDOs). It offers information about the key standard development bodies, their activities, and available or under development standards. The Roadmap will also contain an investigation about possible needs in NIS standardizations.

The Roadmap comprises four parts:

1. ICT Standards Development Organizations and Their Work
   defines the Roadmap scope and provides an overview of major SDOs playing a role in the NIS area:
   - *formal SDOs, e.g. ITU-T, ISO/IEC*
   - *other international standards bodies and forums, e.g. IETF, OASIS, 3GPP, 3GPP2*
   - *regional SDOs, e.g. ATIS, ETSI, RAISS*
2. ICT security standards and guidance documents
   a collection of NIS standards, divided by topic
3. Security Standards under development
   a collection of NIS standards under development
4. Future needs and proposed new security standards

ITU-T Study Group 17

Lead Study Group on telecommunication security and Lead Study Group on languages and description techniques

ITU-T Study Group 17 is the Study Group in charge of security and of its coordination across all Study Groups. Two of its Working Parties are related to security, Working Party 1/17 Open Systems Technology, and Working Party 2/17 Telecommunication Security, http://www.itu.int/ITU-T/studygroups/com17/index.asp.

SG17 works on issues directly related to security (identified by Questions), listed at http://www.itu.int/ITU-T/studygroups/com17/questions.html. A summary of activities is also available in the ITU Security Roadmap, see above.

Examples of Questions:

- Directory Services, Directory Systems, and Public-key/Attribute Certificates (Question 2/17)
  Further work on certificates in the X.500 Series
- Security Architecture and Framework (Question 5/17)
  The ITU security architecture is described in the Series X.800, which have to be maintained and enhanced. The work also covers the study of new types of networks and services and their security architecture, e.g. security solution for NGN and IP-based networks and for emerging technologies.
- Cyber Security (Question 2/17)
  Focus on processes for distribution, sharing and disclosure of vulnerability information, standard procedure for incident handling, strategy for protection of critical network infrastructure. It implies collaboration with international standardization.
  http://www.itu.int/osg/spu/cybersecurity/index.phtml
- Security Management (Question 7/17)
  Starting from Recommendation X.1051, new areas of Security Management need to be explored, in particular, risks management and incident management, including response procedure.
- Telebiometrics (Question 8/17)
  Starting from Recommendation X.1081, standardization of biometric techniques, in collaboration with ISO/IEC.
- Secure Communication Services (Question 9/17)
  Provide comprehensive security solutions for mobile telecommunications, secure communication services, and secure web services. Recommendations X.1121 and X.1122, for example, are dedicated to mobile communications.
- Countering spam by technical means (Question 17/17)
  Investigation on spam, use of new telecommunication network technologies as spam means (e.g. SMS, VoIP, instant messaging), technical mechanisms to counter spam.
  Related work on spam: http://www.itu.int/osg/spu/spam/

Focus Group on Identity Management

http://www.itu.int/ITU-T/studygroups/com17/fgidm/index.html

A new Focus Group has been created in 2007, under the parentage of Study Group 17, dealing with the harmonization in the matter of identity management.

Focus Group on Security Baseline for Network Operators

http://www.itu.int/ITU-T/studygroups/com17/sbno/index.html

Starting 2006, the Focus Group will define security baseline for network operators to assess their network security. This will focus on available security standards and their appropriate use. Further objective is to identify recommendations and standards for the evaluation of operators' network and information security.

The ITU-T Technology Watch

http://www.itu.int/ITU-T/techwatch/index.phtml

The Technology Watch focuses on emerging technologies and market trends, in order to identify topics for standardization work. Current topics: RFID, ubiquitous networks, grid computing, NGN.

Security in other Study Groups

SG 17 is dedicated to security, however there is security work also spread in other Study Groups. A summary is available in the ITU Security Standards Roadmap as well as at http://www.itu.int/ITU-T/worksem/security/200510/sgI_sec.pdf

- SG4, Telecommunication Management
  SG4 focuses on the management of telecommunication services and networks, including NGN. The security work going on in SG4 includes security alarm reporting, security audit, security for management networks.
- SG9, Integrated broadband cable networks and television and sound transmission
  SG9 focuses on integrated broadband cable and television networks, and deals with e.g. broadband services security, VoIP services security (IPCablecom), secure home networking services (e.g. firewall, NAT), security for interactive television services.
- SG11, Signalling requirements and protocols
  SG 11 is in charge of signalling and protocols, including for NGN, and Intelligent Networks. The security requirements are strong.
- SG 12: Performance and quality of service
  Interaction between quality of service and security.
- SG 13, Next Generation Networks
  Security is a central feature in NGN (NGN Security, Question 15). The work includes threat analysis, identification of security requirements, design of the NGN security solution. SG 13 has taken the NGN Focus Group's security reports as input, and works closely with the security SG 17.

NGN Global Standards Initiative (NGN-GSI)

http://www.itu.int/ITU-T/ngn/index.phtml

The NGN work in ITU-T has been carried out by Study Group 13 (publishing Recommendations Y.2001 and Y.2011), and then by the Focus Group on NGN. As the hype of NGN has grown, the NGN-GSI has been established, encompassing different Study Groups (e.g. including SG 17 on security). A tool for NGN standard is available online:
http://www.itu.int/ITU-T/newslog/NGN+Standards+Tracking+Tool+Online.aspx

- SG 15, Optical and other transport networks
  Security questions for SG 15 include security management, call connection operations and secure routing in automatically switched optical networks.
- SG 16: Multimedia services, systems and terminals
  Advanced multimedia applications (e.g., VoIP, conferencing), especially IP-based, present a set of security requirements. The SG deals with security issues such as NAT/ firewall traversal for the H.300 Series, multimedia security in NGN, disaster relief.
- SG 19, Mobile Telecommunications Networks
  SG 19 is working on services, network, and architecture for beyond IMT-2000 and the NGN. This includes e.g. solutions for global roaming and seamless mobility. Many are the security aspects involved in these activities, e.g. threat analysis, cryptographic protection, security architecture, lawful interception.

National Institute of Standards and Technology (NIST)

http://www.nist.gov

Keywords: *FIPS, Cryptographic algorithms, Security protocols, VoIP, Federal security, Security guidelines, Forensics, Biometrics, Security incident handling.*

NIST is a non-regulatory federal agency within the U.S. Commerce Department's Technology Administration. It deals with technical innovation in a number of fields, including NIS.

NIST's centre of NIS expertise is the Computer Security Division, whose activities comprise awareness raising; security guidance development; NIS standards, metrics, tests and validation programs. NIST is involved in a vast range of NIS activities and offers a rich web site. NIST is also host of the **National Vulnerability Database** (NVD) (http://nvd.nist.gov/), where mainly researchers (and now also vendors) can post known vulnerabilities in CVE naming standard[131].

NIST publications are highly recognized. NIST's Federal Information Processing Standards (**FIPS**) are standards developed by the U.S. Federal government to be used by all non-military government agencies and by government contractors. FIPS standards may be modified versions of standards used in the wider community such as ANSI, IEEE, ISO, IETF. Well-known FIPS are in the field of cryptographic algorithms [NIST1]-[NIST4]. A complete list of FIPS can be found at http://csrc.nist.gov/publications/fips/index.html.

NIST provides also support to the Federal Information Security Management Act (*FISMA*), 2002, http://csrc.nist.gov/sec-cert/

The NIST **Special Publications (800 series)** analyze security topics of general interest, e.g. security of emerging technologies [NIST5], and provide recommendations and guidance on a number of practices [NIST6]-[NIST19]. A complete list of NIST 800 Series can be found at http://csrc.nist.gov/publications/nistpubs/index.html.

NIST has also relevant work on Biometrics, e.g. with the CBEFF standard (Common Biometric Exchange File Format) [NIST20]. The **Biometrics Resource Center Website** is dedicated to the topic, http://www.itl.nist.gov/div893/biometrics/.

Among the many activities, NIST is also planning for an open competition on the selection of a new hash function, after the 2005 attacks to a few existing hash functions. http://www.csrc.nist.gov/pki/HashWorkshop/timeline.html

[131] Common Vulnerabilities and Exposures, it standardizes the names of publicly known vulnerabilities and security exposures. http://cve.mitre.org/

[NIST1]	FIPS PUB 180-2: Secure Hash Standard
	Specifies the SHA family of secure hash algorithms (SHA-1, SHA-256, SHA-384, SHA-512), with the addition of SHA-224 and discussion on truncation.
[NIST2]	FIPS 186-2 January 2000, Digital Signature Standard (DSS)
	Specifies the DSS algorithm suite for digital signatures.
[NIST3]	FIPS 197 November 2001, Advanced Encryption Standard
	Specifies the symmetric block cipher Rijndael.
[NIST4]	FIPS 198 March 2002, The Keyed-Hash Message Authentication Code (HMAC)
	The HMAC specification, generalization of IETF RFC 2104 and ANSI X9.71.
[NIST5]	SP 800-58 Security Considerations for Voice Over IP Systems, January 2005
[NIST6]	SP 800-90, Recommendation for Random Number Generation Using Deterministic Random Bit Generators
[NIST7]	SP 800-57, Recommendation on Key Management, August 2005
[NIST8]	SP 800-56A Recommendation for Pair-Wise Key Establishment Schemes Using Discrete Logarithm Cryptography
[NIST9]	SP 800-81, Secure Domain Name System (DNS) Deployment Guide, May 2006
	Provides technical details and implementation guidance to assist federal agencies in the deployment of DNS security measures
[NIST10]	SP 800-77 Guide to IPsec VPNs, December 2005
[NIST11]	SP 800-70, The NIST Security Configuration Checklists Program May 2005
[NIST12]	SP 800-63, Electronic Authentication Guideline: Recommendations of the National Institute of Standards and Technology, September 2004)
[NIST13]	SP 800-67, Recommendation for the Triple Data Encryption Algorithm (TDEA) Block Cipher, May 2004
	Specification of the Triple DES (or Triple DEA) algorithm (originally specified in ANSI X9.52).
[NIST14]	SP 800-86, Guide to Integrating Forensic Techniques into Incident Response.
[NIST15]	SP 800-83, Guide to Malware Incident Prevention and Handling November 2005
[NIST16]	SP 800-76 Biometric Data Specification for Personal Identity Verification, February 2006
[NIST17]	SP 800-61 Computer Security Incident Handling Guide, January 2004
[NIST18]	SP 800-12 An Introduction to Computer Security: The NIST Handbook, October 1995
[NIST19]	SP 800-100 Information Security Handbook: A Guide for Managers, October 2006
[NIST20]	NISTIR 6529, Common Biometric Exchange File Format (CBEFF), January 2001

International Organization for Standardization (ISO) and the International Electrotechnical Commission (IEC)

Keywords: *Cryptographic algorithms, Security functions, Security management, Biometrics, Network security, Incident management, Security assurance.*

ISO is the world's largest developer of standards. ISO is organized into Committees, each dedicated to a particular field of standardization. The Joint Technical Committee of ISO and IEC (JTC 1) deals with IT standardization.

JTC 1

Joint Technical Committee of ISO and IEC (Information technology)
http://www.iso.org/iso/en/stdsdevelopment/tc/tclist/TechnicalCommitteeDetailPage.TechnicalCommitteeDetail?COMMID=1

JTC 1/SC 27: Subcommittee SC 27 IT Security techniques

http://www.iso.org/iso/en/stdsdevelopment/tc/tclist/TechnicalCommitteeDetailPage.TechnicalCommitteeDetail?COMMID=143

JTC 1/SC 27, IT Security techniques, is divided into Working Groups:

- WG 1 Requirements, security services and guidelines
  Work on requirements, development of standard security services based on the mechanisms designed by WG2, security guidelines
- WG 2 Security techniques and mechanisms
  Work on security techniques and mechanisms, e.g. encryption, integrity, key management etc.
- WG 3 Security evaluation criteria
  Standards for IT Security evaluation and certification
- WG 4: Security controls and services
  Covers the development and maintenance of standards and guidelines addressing services and applications supporting the implementation of control objectives and controls as defined in ISO/IEC 27001
- WG 5: Identity management and privacy technologies
  Addresses security aspects of identity management, biometrics, the protection of personal data.

ISO/IEC Standards

A number of the ISO/IEC standards are emerging as international standards, for example ISO/IEC 9798 for entity authentication techniques, ISO/IEC 9594-8 (also published and known as ITU-T Recommendation X.509), and the ISO 27000 Family. The list of Standards published by JTC 1/SC 27 can be found at http://www.iso.org/iso/en/stdsdevelopment/tc/tclist/TechnicalCommitteeStandardsListPage.TechnicalCommitteeStandardsList?COMMID=143.

The following is a (non-exhaustive) list grouped by topic.

General	
ISO/IEC 19790:2006	Security requirements for cryptographic modules
ISO/IEC TR 14516:2002	Guidelines for the use and management of Trusted Third Party services
Hash-functions	
ISO/IEC 10118-1:2000	Hash-functions -- Part 2: Hash-functions using an n-bit block cipher
ISO/IEC 10118-2:2000	Hash-functions -- Part 2: Hash-functions using an n-bit block cipher
ISO/IEC 10118-3:2004	Hash-functions -- Part 3: Dedicated hash-functions
ISO/IEC 10118-3:2004/ Amd 1:2006	Dedicated Hash-Function 8 (SHA-224)
ISO/IEC 10118-4:1998	Hash-functions -- Part 4: Hash-functions using modular arithmetic
MACs	
ISO/IEC 9797-1:1999	Message Authentication Codes (MACs) -- Part 1: Mechanisms using a block cipher
ISO/IEC 9797-2:2002	Authentication Codes (MACs) -- Part 2: Mechanisms using a dedicated hash-function
Entity authentication	
ISO/IEC 9798-1:1997	Entity authentication -- Part 1: General
ISO/IEC 9798-2:1999 ISO/IEC 9798-2:1999/ Cor 1:2004	Message Authentication Codes (MACs) -- Part 2: Mechanisms using a dedicated hash-function
ISO/IEC 9798-3:1998	Entity authentication -- Part 3: Mechanisms using digital signature techniques
ISO/IEC 9798-4:1999	Entity authentication -- Part 4: Mechanisms using a cryptographic check function
ISO/IEC 9798-5:2004	Entity authentication -- Part 5: Mechanisms using zero-knowledge techniques
ISO/IEC 9798-6:2005	Entity authentication -- Part 6: Mechanisms using manual data transfer
Digital signature	
ISO/IEC 9796-2:2002	Digital signature schemes giving message recovery -- Part 2: Integer factorization based mechanisms
ISO/IEC 9796-3:2000	Digital signature schemes giving message recovery -- Part 3: Discrete logarithm based mechanisms
ISO/IEC 14888-1:1998	Digital signatures with appendix -- Part 1: General
ISO/IEC 14888-2:1999	Digital signatures with appendix -- Part 2: Identity-based mechanisms
ISO/IEC 14888-3:1998	Digital signatures with appendix -- Part 3: Certificate-based mechanisms
ISO/IEC 15945:2002	Specification of TTP services to support the application of digital signatures
Non-repudiation	
ISO/IEC 13888-1:2004	Non-repudiation -- Part 1: General
ISO/IEC 13888-2:1998	Non-repudiation -- Part 2: Mechanisms using symmetric

	techniques
ISO/IEC 13888-3:1997	Non-repudiation -- Part 3: Mechanisms using asymmetric techniques
Encryption	
ISO/IEC 18033-1:2005	Encryption algorithms -- Part 1: General
ISO/IEC 18033-2:2006	Encryption algorithms -- Part 2: Asymmetric ciphers
ISO/IEC 18033-3:2005	Encryption algorithms -- Part 3: Block ciphers
ISO/IEC 18033-4:2005	Encryption algorithms -- Part 4: Stream ciphers
ISO/IEC 10116:2006	Modes of operation for an n-bit block cipher
Key management	
ISO/IEC 11770-1:1996	Key management -- Part 1: Framework
ISO/IEC 11770-2:1996 ISO/IEC 11770-2:1996/ Cor 1:2005	Information technology – Security techniques -- Key management -- Part 2: Mechanisms using symmetric techniques
ISO/IEC 11770-3:1999	Key management -- Part 3: Mechanisms using asymmetric techniques
ISO/IEC 11770-4:2006	Key management -- Part 4: Mechanisms based on weak secrets
Security management	
ISO/IEC 13335-1:2004	Management of Information and communications technology security -- Part 1: Concepts and models for Information and communications technology security management
ISO/IEC TR 13335-3: 1998	Information technology -- Guidelines for the management of IT Security -- Part 3: Techniques for the management of IT Security
ISO/IEC TR 13335-4: 2000	Guidelines for the management of IT Security -- Part 4: Selection of safeguards
ISO/IEC TR 13335-5: 2001	Guidelines for the management of IT Security -- Part 5: Management guidance on network security
ISO/IEC 27001:2005	Information security management systems -- Requirements
Elliptic curves	
ISO/IEC 15946-1:2002	Cryptographic techniques based on elliptic curves -- Part 1: General
ISO/IEC 15946-2:2002	Cryptographic techniques based on elliptic curves -- Part 2: Digital signatures
ISO/IEC 15946-3:2002	Cryptographic techniques based on elliptic curves -- Part 3: Key establishment
ISO/IEC 15946-4:2004	Cryptographic techniques based on elliptic curves -- Part 4: Digital signatures giving message recovery
Time-stamping	
ISO/IEC 18014-1:2002	Time-stamping services -- Part 1: Framework
ISO/IEC 18014-2:2002	Time-stamping services -- Part 2: Mechanisms producing independent tokens
ISO/IEC 18014-3:2004	Time-stamping services -- Part 3: Mechanisms producing linked tokens
Random generator	
ISO/IEC 18031:2005	Random bit generation
ISO/IEC 18032:2005	Prime number generation
Access Control	
ISO/IEC 15816:2002	Security Information objects for access control

Network security	
ISO/IEC 18028-2:2006	IT network security -- Part 2: Network security architecture
ISO/IEC 18028-3:2005	IT network security -- Part 3: Securing communications between networks using security gateways
ISO/IEC 18028-4:2005	IT network security -- Part 4: Securing remote access
Incident Management	
ISO/IEC TR 18044:2004	Information security incident management
Evaluation criteria for IT security and IT security assurance	
ISO/IEC 15408-1:2005	Evaluation criteria for IT security -- Part 1: Introduction and general model
ISO/IEC 15408-2:2005	Evaluation criteria for IT security -- Part 2: Security functional requirements
ISO/IEC 15408-3:2005	Evaluation criteria for IT security -- Part 3: Security assurance requirements
ISO/IEC TR 15443-1:2005	A framework for IT security assurance -- Part 1: Overview and framework
ISO/IEC TR 15443-2:2005	A framework for IT security assurance -- Part 2: Assurance methods
ISO/IEC TR 15446:2004	Guide for the production of Protection Profiles and Security Targets
ISO/IEC 17799:2005	Code of practice for Information security management
ISO/IEC 18045:2005	Methodology for IT security evaluation
ISO/IEC 15292:2001	Protection Profile registration procedures
ISO/IEC 21827:2002	Capability Maturity Model (SSE-CMM®)
PKI	
ISO/IEC 9594-8:1998	Information technology -- Open Systems Interconnection -- The Directory: Authentication framework
	By ISO/IEC JTC 1/SC 6, Telecommunications and information exchange between systems

Drafts and new work items under the direct responsibility of JTC 1/SC 27 include intrusion detection systems, identity management, and biometrics.
http://www.iso.org/iso/en/CatalogueListPage.CatalogueList?COMMID=143&scopelist=PROGRAMME
In particular, a family of Standards for Information Security Management System (ISMS) is under development, the ***27000 Family***:

- 27001, ISMS requirements, published
- 27002, will incorporate (April 2007) the new edition of ISO/IEC 17799
- 27003, ISMS implementation guidelines, work in progress
- 27004, ISMS measurements, work in progress
- 27005, ISMS risk management, work in progress.

JTC 1/SC 37 Biometrics

http://www.iso.org/iso/en/stdsdevelopment/tc/tclist/TechnicalCommitteeDetailPage.TechnicalCommitteeDetail?COMMID=5537

The Biometrics SC is organized into 6 WGs, respectively dealing with vocabulary, technical interfaces, data interchange formats, functional architecture and related profiles, testing and reporting, cross-jurisdictional and societal aspects.
Drafts and new work items under the direct responsibility of JTC 1/SC 37:
http://www.iso.org/iso/en/CatalogueListPage.CatalogueList?COMMID=5537&scopelist=PROGRAMME

American National Standards Institute (ANSI)

http://www.ansi.org

Keywords: *Homeland security, Emergency communications, Biometrics, Identity management*.

ANSI is a private, non-profit organization that manages the U.S. voluntary standardization and conformity assessment system.

The ANSI's **Homeland Security Standards Panel** (**ANSI-HSSP**) is active in the NIS area, with the mandate to identify existing consensus standards useful for homeland security, and to assist the Department of Homeland Security (DHS) to accelerate the development of standards where needed. Work includes biometrics (e.g. the X9.84 standard), emergency communications and emergency preparedness, cyber security.

ANSI has planned the establishment of the **Identity Theft Prevention and Identity Management Standards Panel**, dedicated to the harmonization of voluntary consensus standards on identity theft prevention.

ANSI X9

http://www.x9.org

Accredited by ANSI but operated by the American Bankers Association, Committee X9 develops standards for the financial industry. It comprises a few subcommittees, e.g. the X9F-Data & Information Security.

Industry Associations

Voice over IP Security Alliance (VOIPSA)

http://www.voipsa.org

Keywords: *VoIP security*

Voice over IP (VOIP), also known as IP telephony, is an emerging application which brings the promise of a change of the telecommunication landscape. However, one of the open issues with VoIP is its security, primarily due to the use of the IP technology. VOIPSA drives the adoption of VoIP by promoting the current state of VoIP security research, VoIP security education and awareness, and free VoIP testing methodologies and tools.

VOIPSA has two active working groups:

- Threat Taxonomy WG, which defines security threats to VoIP deployments, services, and end users.
  http://www.voipsa.org/Activities/taxonomy.php
- Security Requirements WG, which defines security requirements for e.g. the VoIP building blocks, supporting security components (such as session border controller, firewall), architecture and network design (such as NAT, VPN, port security), network management, and endpoint access and authentication.
  http://www.voipsa.org/Activities/securityrequirements.php

Cyber Security Industry Alliance (CSIA)

http://www.csialliance.org

Keywords: *Certification, E-voting, VoIP*

CSIA is a group working towards the improvement of cyber security. Current CSIA committees are:

- *Public Policy*, working to develop and implement initiatives to advance the public policy agenda of the CSIA
- *Standards*, working to evaluate and improve standards, validation, certification and testing processes
- *Education and Alliances*, working with academia and federal and state authorities to focus on education issues
- *Awareness*, working with media, academia, private and public sectors to build awareness.

Relevant security work in 2005 has been for example in the area of Health Care, Certification (seeking to improve the certification process for Common Criteria), secure e-voting, VoIP whitepaper, https://www.csialliance.org/resources/pdfs/CSIA_VOIP_May_2005.pdf),

Open Mobile Alliance (OMA)

http://www.openmobilealliance.org/

Keywords: *Mobile services security, Trust, Smart cards, Wireless security, Certificates, POC, OTA*

OMA develops mobile service enablers to facilitate mobile data services and their wide adoption. Companies participating in OMA are representatives of mobile operators, device and network suppliers, information technology companies, and content providers. OMA works on specifications in support of interoperable end-to-end mobile services, developing market-driven service enabler architectures and open enabler interfaces independent of the underlying wireless networks and platforms. Founded by consolidating the efforts of the Open Mobile Architecture initiative and the WAP Forum, OMA also integrates initiatives such as the Wireless Village and the Mobile Wireless Internet Forum (MWIF).

OMA has a dedicated Security Group, which functions as security expertise centre for OMA and its other Working Groups and which specifies protocols for secure communication between mobile clients and servers (at transport layer and the application layer), security and trust services (e.g. authentication, confidentiality, and integrity) for mobile clients and servers, and interactions with entities (e.g. secure hardware tokens) to assure appropriate security. In particular, the Smart Card Technology Subgroup (SEC SCT) focuses on hardware tokens (e.g. smart cards) technology.

OMA specifically takes care of the development and maintenance of several specifications and enablers, for example: the Wireless Transport Layer Security (WTLS), the Wireless Profile of Transport Layer Security (“TLS Prof”), the Wireless Identity Module (WIM), the WMLScript Crypto Library (“Crypto API”, and extensions), the Wireless Public Key Infrastructure (WPKI), the Wireless Certificate Profile (“CertProf”), the Online Certificate Status Protocol (“OCSP”), the SmartCard Web Server enabler.

Current work items are on Application Layer Security Common Functions, Smart Card Web Server, Mobile Profile of Online Certificate Status Protocol (OCSP), On-Board Key Generation and Key Enrolment.

OMA specifications can be found at:
http://www.openmobilealliance.org/tech/publicmaterial.html

It has to be noted the security work going on in the different OMA Working Group, for example the security architecture of one of the emerging services, Push To Talk over Cellular (PoC), and of the enablers and architecture for Presence http://www.openmobilealliance.org/tech/wg _committees/workinggroups.html.

Trusted Computing Group (TCG)

https://www.trustedcomputinggroup.org/home

Keywords: *Trusted computing, Trusted platform, Endpoint security*

TCG was formed in 2003 to develop and support open industry standards for trusted computing across multiple platform types, e.g. PCs, servers, PDA's, and digital phones. These platforms are increasingly spreading and have a tendency towards 'openness' (e.g., Symbian for mobile devices), hence the issue of how to integrate trust in them plays an important role in the NIS landscape. One distinguishing idea of TCG is the incorporation of "roots of trust" into computer platforms.

TCG is organized into several Work Groups:

- The *TPM Work Group* works on the Trusted Platform Module (TPM) specification. https://www.trustedcomputinggroup.org/specs/TPM/
- The *Infrastructure Work Group* works to adopt and integrate TCG platform specifications into Internet and enterprise infrastructure technologies. For example, it works on standard ways to exchange information in order to allow trust decisions. The Trusted Network Connect Sub Group has worked on an open architecture and standards for endpoint integrity. https://www.trustedcomputinggroup.org/specs/IWG/
- The *PC Client Work Group* focuses on security and privacy requirements for PC clients that use TCG components. https://www.trustedcomputinggroup.org/specs/PCClient/
- The *Software Stack Work Group* works on standard APIs for Application vendors to make use of the TPM (regardless of the hardware, Operating System, or environment), https://www.trustedcomputinggroup.org/specs/TSS/
- The *Mobile Phone Work Group* works to promote the adoption of TCG concepts for mobile devices. The specification is under development, https://www.trustedcomputinggroup.org/groups/mobile
- The *Server Work Group* looks at the adoption of TCG technology in servers. https://www.trustedcomputinggroup.org/specs/Server/
- The *Storage System Work Group* will build upon existing TCG technologies and concepts, and produce standards for security services in storage systems. The specification is under development, https://www.trustedcomputinggroup.org/groups/storage/
- The *Trusted Network Connect Work Group* has recently published the specification of TNC, an open architecture and set of standards for endpoint

integrity (it enables the check of the endpoint configuration and security posture before allowing it to connect to the network).
https://www.trustedcomputinggroup.org/groups/network/

VPN Consortium (VPNC)

http://www.vpnc.org/

Keywords: *IPsec VPN*

VPNC is the international trade association for manufacturers in the VPN market. VPNC does not define standards, but supports IETF standards in the area of VPN technology, focusing in particular in interoperability tests.

The Information Systems Security Association (ISSA)

http://www.issa.org/

Keywords: *Security practices*

ISSA is the largest international, not-for-profit association for security professionals, targeting primarily small businesses, global enterprises and government organizations. ISSA facilitates global information systems security by interaction, education and information resources to its members. It works primarily through its chapters spread all over the world, promoting training and information sharing among its members.

ISSA, ASIS and ISACA have formed an Association Alliance to address Enterprise Security Risks,
http://www.issa.org/PDF/pressroom/ISSAAlliancePressReleaseFeb.17.05.pdf

The Generally Accepted Information Security Principles (GAISP) collects information security principles, based on standards and well established security practices. http://www.issa.org/gaisp/gaisp.html

European Institutions

Joint Research Center (JRC)

http://www.jrc.cec.eu.int/

Keywords: *Identity management, Privacy, E-government, Forensics, Biometrics, Critical infrastructure*

JRC is a Directorate General (DG) of the European Commission supporting Community policies and a reference centre for science and technology for the Community. Two Institutes are relevant for NIS in JRC: the Institute of the Protection and Security of the Citizen (IPSC), and the Institute for Prospective Technological Studies (IPTS).

Institute of the Protection and Security of the Citizen (IPSC)

http://ipsc.jrc.cec.eu.int/

IPSC's mission is to protect the citizen though research-based support to the EU policies. Cybersecurity and fight against fraud are among the main application areas.
Within the JRC's multi-annual work programme 2003-2006 (supporting for example the EU FP6), IPSC hosted the Unit 'Sensors, radar technologies and cybersecurity (SERAC)' and its "*Reference Systems for Cybersecurity (RSC)*" Institutional Action (http://cybersecurity.jrc.it/), whose activities included:

- *Digital identity management and privacy*, focusing on:
  - Privacy evaluation: a collaboration between JRC and W3C brought to recommendations to be integrated in the P3P (Privacy Preferences Project in W3C), http://p3p.jrc.it/
  - Identity theft
  - Partnership in the EU funded project PRIME in the area of digital identity management and privacy.
- *Trustworthy eGovernment and consumer protection information systems.*
  The JRC develops the software reference implementation of the European network for cross-border complaint handling and dispute resolution, called *EEJNET* (www.eejnet.org). The JRC is studying (testbed) the security of Internet voting systems against severe attacks.
- *Digital evidence systems for combating cybercrime.*
  The JRC is involved in international initiatives aimed at better characterizing cybercrime, e.g. gathering of reliable digital evidence. A main project was the EU-funded Cyber Tools On-Line Search for Evidence (*CTOSE project)*, ended in 2004, which developed tools for the identification and secure gathering of verifiable digital evidence of illicit online activities (http://www.ctose.org/).

- *Information infrastructure interdependencies and risks*.
  Work in the area of ICT dependability. Critical infrastructure will be a focus area.
- *E-Health*

The Institute for Prospective Technological Studies (IPTS)

http://www.jrc.es/home/index2.cfm

IPTS monitors and analyses science and technology developments, their socio-economic impacts, and their implications for future policy development. The IPTS' Information and Communications Technologies (ICTs) unit embraces two actions related to NIS:

- Foresight on Information Society Technologies in Europe (FISTE), http://fiste.jrc.es/
- Privacy and Identity in the Information Society (PRIDIS), http://cybersecurity.jrc.es/

Focus areas for IPTS include:

- Future of Identity, including privacy, identity theft, and Identity Management Systems study
- Socio-economic aspects of security at large, e.g. security for e-payment schemes and location based services
- Security and privacy for ambient intelligence, http://swami.jrc.es/pages/index.htm
- Biometrics and its impact on society http://cybersecurity.jrc.es/pages/ProjectlibestudyBiometrics.htm

European Network and Information Security Agency (ENISA)

http://www.enisa.europa.eu/

Keywords: *NIS, Awareness raising, CERT coordination, Security policies, Risk Management, Emerging threats, Best Practices*

ENISA is the EU Agency dedicated to network and information security. The Agency's activities consist of giving advice and recommendations, data analysis, as well as supporting awareness raising and cooperation among the EU bodies and Member States. Activities of the Agency include the following:

- Computer Emergency Response Team (CERT) coordination, with an inventory of CERT activities in Europe (http://www.enisa.europa.eu/doc/pdf/deliverables/enisa_cert.pdf), practices for CERT's set up, and work to facilitate cooperation among CERTs
- Information security awareness raising activities, with collection of best practices for different target groups
- Risk management, with the generation of an inventory of methods and their analysis

- Security policies, with collection of best practices, as well as studies and surveys, such as a study on security and countermeasures against spam, (http://www.enisa.europa.eu/doc/pdf/deliverables/enisa_security_spam.pdf and http://www.enisa.europa.eu/doc/pdf/deliverables/enisa_security_spam_part2.pdf).
- NIS standardization and activities tracking.

ENISA deliverables and publications can be found at http://www.enisa.europa.eu/pages/05_01.htm.
The ENISA Work Programme 2006 can be found at http://www.enisa.europa.eu/doc/pdf/management_board/decisions/work_programme_2006.pdf.

International Institutions

Organization for Economic Co-operation and Development (OECD)

http://www.oecd.org/

Keywords: *Security and Privacy, Anti-spam toolkit*

The OECD is an international forum, grouping a large number of countries, addressing the economic, social and governance challenges of globalization and the exploitation of its opportunities. By addressing emerging issues and policies, OECD has an important role in making policies, and is well known for its individual country surveys and reviews.

OECD's work in NIS is relevant, and has the goal to build confidence and security in the use of ICT. Two works are specifically dedicated to the NIS thematic, the work on security and privacy, and the work on anti-spam.

OECD Working Party on Information Security and Privacy

www.oecd.org/sti/security-privacy

To build confidence and security in the use of ICTs, infrastructure and services must be reliable, transactions secure and private, and personal data protected. The OECD Working Party on Information Security and Privacy promotes a global, coordinated approach to policy making in these areas, to help build trust online.

OECD Spam Task Force

www.oecd-antispam.org

The OECD Spam Task Force addresses the problem of spam, strongly promoting international cooperation. The Task Force is developing the anti-spam Toolkit (www.oecd.org/sti/spam/toolkit), which includes a guide to best practices for ISPs and is intended to help governments, regulators, and industry in their anti-spam policies.
The Task Force publishes a number of reports on the website (http://www.oecd.org/department/0,2688,en_2649_22555297_1_1_1_1_1,00.html).

International Federation for Information Processing (IFIP)

http://www.ifip.org/

Keywords: *Database security, Identity management, Law and security, Security, Education, Forensic*

IFIP is an international umbrella organization, with a large country presence, promoting the development and exploitation of Information Technology in favor of people's benefit.

IFIP is organized into Technical Committees, of which **Technical Committee 11** (TC11) works on Security and Protection in Information Processing Systems. TC11 is structured in Working Groups (http://www.ifip.tu-graz.ac.at/TC11/WG/index.htm):

- WG 11.1: Information Security Management
  Focus on methods and tools needed by top management to achieve robust information security within the organization. The activity covers many different aspects, from managerial to technical, and includes e.g. research on ways to identify vulnerabilities, methods to measure the security level of the company, standards.
- WG 11.2: Small System Security
  Focus on security techniques for end users and small organizations, to have the responsibility for secure systems distributed to the end users. The WG also embraces work on intelligent tokens and smart cards.
- WG 11.3: Data and Application Security (database security)
  Focus on enhancing the security of database systems.
- WG 11.4: Network & Distributed Systems Security
  Focus on network aspects of information systems security.
- WG 11.5: Systems Integrity and Control
  Focus on research and use of standards (including standard evaluation criteria) to ensure the integrity and control of information systems.
- WG 11.6: Identity Management
  Focus on technical, political, social and legal issues concerning identity management, including biometrics and national identity management.
- WG 9.6/11.7: Information Technology Misuse and the Law
  Focus on information security in relation to IT misuse (in its different perceptions) and law, including implications between the law and new technologies.
- WG 11.8: Information Security Education
  Promotion of information security education and training at the university level and in government and industry.
- WG 11.9: Digital Forensics
- WG 11.10: Critical Infrastructure Protection

IFIP is known through its books and annual conferences. The list of IFIP publications (books) for WG 11 can be found at http://www.ifip.org/publications/books.htm

Organization for the Advancement of Structured Information Standards (OASIS)

http://www.oasis-open.org

Keywords: *Web services security*

OASIS (Organization for the Advancement of Structured Information Standards) is an international consortium involved in the development of web services and e-business standards. OASIS has a number of security Technical Committees, http://www.oasis-open.org/committees/tc_cat.php?cat=security.

- OASIS Application Vulnerability Description Language (AVDL) TC
  developing a uniform way of describing application security vulnerabilities, using XML definitions. AVDL v1.0 (Oasis standard) was released in May 2004 and focus on HTTP.
- OASIS Digital Signature Services (DSS)
  Developing techniques to support digital signatures, e.g. including the definition of a web interface for requesting a web service to produce/verify digital signatures. This has the advantage to avoid implementing the function within user applications.
- OASIS eXtensible Access Control Markup Language (XACML)
  Developing a flexible language for access control, the eXtensible Access Control Markup Language (XACML, Oasis standard), particularly designed to support large-scale environments with distributed resources and federated policy administration.
- OASIS Provisioning Services
  Working on an XML framework for managing the provisioning and allocation of identity information and system resources within and between organizations. The Service Provisioning Markup Language (SPML) 1.0 (Oasis standard) relates to e.g. federated identity standards such as Liberty Alliance.
- OASIS Public Key Infrastructure (PKI) TC
  Addressing the issues of PKI deployment and usage.
- OASIS Security Joint Committee
  For the coordination of the security activities within OASIS
- OASIS Security Services (SAML)
  Developing the Oasis standard SAML (Security Assertion Markup Language), an XML-based framework for communicating user authentication and attribute information. SAML is used to exchange security information between entities, e.g. between a security system (such as an authentication authority) and an application that trusts the security system, or between two partner companies. Practical usage of SAML is for example for Web Single Sign On (SSO), attribute-based authorization, and securing web services (SAML

assertions can be for example carried in SOAP, e.g. in Liberty Alliance). SAML v2.0 is considered a critical step towards full convergence for federated identity standards.

- OASIS Web Application Security (WAS)
  Creating an open data format to describe Web application security vulnerabilities, providing guidance for initial threat and risk ratings
- OASIS Web Services Secure Exchange (WS-SX)
  Working on the definition of extensions to OASIS Web Services Security (see TC below) to enable trusted SOAP message exchanges involving multiple message exchanges, and the definition of security policies that govern the formats and tokens of such messages.
- OASIS Web Services Security (WSS)
  Further working on Web Services security foundations, e.g. security functions such as integrity and confidentiality in messages implementing higher-level Web services applications.
- OASIS XML Common Biometric Format (XCBF)
  defining a common set of XML encodings for the formats defined in the Common Biometric Exchange File Format (CBEFF, NIST specification http://www.itl.nist.gov/div893/biometrics/*).*

OASIS has also other work relevant to security. One example is the development of specifications in the area of e-commerce, e.g. with the ebXML standards. http://www.oasis-open.org/committees/tc_cat.php?cat=ec

Other Fora relevant to NIS

The Internet Corporation for Assigned Names and Numbers (ICANN)

http://www.icann.org

Keywords: *Internet security, DNS security*

ICANN is the international body responsible for the management the Internet Domain Name System (DNS).

The **Security and Stability Advisory Committee (SSAC)** is chartered to advice on the security and integrity of the Internet's naming and address allocation systems. This includes threat assessment and risk analysis, development of a security framework, and communication towards relevant bodies such as IETF. SSAC reports, including recommendations and best practices, can be found at http://www.icann.org/committees/security/ssac-documents.htm :

- Alternative TLD Name Systems and Roots: Conflict, Control and Consequences (March 2006)
- DNS Distributed Denial of Service (DDoS) Attacks (March 2006)
  Recommendations for ISPs and TLD name server operators to mitigate amplification attacks based on DNS.
- Domain Name Hijacking Report (July 2005)
- Redirection in the COM and NET Domains (July 2004)
- DNS Infrastructure Recommendation (November 2003)
- Securing The Edge (October 2002)
- WHOIS Recommendation (December 2002)
- ICANN DNS Security Update (4 January 2002)
- DNS Security Reading List (November 2001)

Réseaux IP Européens (RIPE)

http://www.ripe.net/

Keywords: *Anti-spam, Anti-spoofing, Internet security, DNS security*

RIPE is a collaborative forum with the objective of ensuring the administrative and technical coordination for a pan-European IP network. As such, RIPE is involved in several security issues across the different Working Groups (WGs) and task forces, of which some examples are reported in the following.

Anti-spam Working Group

Developing a “code of conduct” for ISPs, in order to build synergies to address the problem of spam, and making a recommendation on the feasibility of a "Centre for European Network Abuse Resolution (CENAR)".

Technical Security (TechSec) WG

TechSec has the mandate to discuss technical issues that can help improving the security of the Internet infrastructure. The WG is currently focused on DNSSEC deployment.

Anti-spoofing task force

http://www.ripe.net/ripe/tf/anti-spoofing/

Promoting the adoption of Network Ingress filtering (RFC 2827). The task force has been set up to face a new wave of spoofing and DNS amplification attacks (causing an amplifier host to send traffic to the spoofed address) that was observed at the beginning of 2006.

Deployment of Internet Security Infrastructures (DISI)

DISI supports the RIPE community in the deployment of security technologies, and currently focuses on DNSSEC deployment.

The Open Group

http://www.opengroup.org

"Making Standards work"

Keywords: D*e-perimeterization, Identity management, Messaging security, Anti-spam, Safety embedded system security*

Consortium promoting ICT open standards and global interoperability, the Open Group works through Forums, a few of which are dedicated to security activities:

- **The Jericho Forum**
  http://www.opengroup.org/jericho/
  One of the most active promoters of the *de-perimeterization* approach, the Jericho Forum is dedicated to the development of open standards for secure and boundary-less information flows across organizations.
- **Identity Management Forum**
  http://www.opengroup.org/tech/idm/
- **Messaging Forum**
  http://www.opengroup.org/messaging/
  Work on secure messaging and spam countermeasures.
- **The Real-time and Embedded Systems Forum**
  http://www.opengroup.org/rtforum/
  Work on security requirements for real-time and embedded systems, and issues with the use of Commercial-off-the-shelf (COTS) devices in safety systems.

Next version of the Inventory

Fora to be covered in the next version of the inventory may include:

- **W3C**
- **3GPP2** TSG-S WG4 (Security)
- The **RAISS** Forum (Regional Asia Information Security Standards) http://www.itsc.org.sg/standards_news/raiss.html
- **ATIS**, Alliance for Telecommunications Industry Solution, US based body for the development and promotion of IT standards.
- **IEEE.** For example the IEEE P1363 Standard Specifications for Public-Key Cryptography. http://grouper.ieee.org/groups/1363/, and security for wireless technology.
- The **Parlay Group**, for standardized APIs, http://www.parlay.org.
- PCI Security Standards Council

- Fora related to NIS research activities

Related Inventories

- The ITU's ICT Security Standards Roadmap,
  http://www.itu.int/ITU-T/studygroups/com17/ict/index.html
  Security standardization inventory by ITU (bodies and standards)

- eEurope
  http://www.e-europestandards.org/
  Standardization work within Europe to achieve the targets of the European Commission's eEurope Action Plan.

- NISSG Reports
  - ETSI SR 002 298 (2004 version)
  - New version (on-going)

  Report on standardization issues which are relevant to European SDOs.

- ETSI Security Whitepaper, "Security for ICT – the Work of ETSI", January 2006
  http://www.etsi.org/etsi_radar/whitepaper/home.htm
  Overview of ETSI activities in the NIS area.

- IETF I-D in the Operational Security Working Group (opsec) Working Group, "Security Best Practices Efforts and Documents", draft-ietf-opsec-efforts.
  Collection of the SDOs involved in the definition of security practices, primarily focusing on the availability of Internet.

- http://www.consortiuminfo.org/

ANNEX 2: Glossaries, Acronyms, and Abbreviations

Existing Security Glossaries

The ITU-T online SANCHO provides a list of terms, definitions, and acronyms. http://www.itu.int/sancho/

IETF RFC2828, Internet Security Glossary
http://www.ietf.org/rfc/rfc2828.txt?number=2828

IETF RFC2828bis, draft-shirey-secgloss-v2

SANS Glossary
http://www.sans.org/resources/glossary.php

IT Security Glossary
http://www.itsecurity.com/dictionary/

Microsoft Glossary
http://www.microsoft.com/security/glossary.mspx

RSA Glossary
http://www.rsasecurity.com/glossary/

Other Glossaries are listed at
http://www.alphadictionary.com/directory/Specialty_Dictionaries/Security/

Acronyms and Abbreviations

Note: Acronyms of fora/bodies are in a separate list below.

2G	2nd Generation
3G	3rd Generation
AES	Advanced Encryption Standard
AKA	UMTS Authentication and Key Agreement
API	Application Programming Interface
B3G	Beyond 3G
BGP	Border Gateway Protocol
BOF	Birds of a Feather (IETF)
CBEFF	Common Biometric Exchange File Format
CERT	Computer Emergency Response Team
CI	Critical Infrastructure
CMP	Certificate Management Protocol
CSCF	Call Session Control Function
CTR	Counter Mode
DDoS	Distributed Denial of Service
DH	Diffie Hellman
DKIM	DomainKeys Identified Mail
DNS	Domain Name System
DNSSEC	Domain Name System Security Extensions
DOA	Data Origin Authentication
DoS	Denial of Service
DRM	Digital Rights Management
DTLS	Datagram TLS
E2e	End-to-end
EAP	Extensible Authentication Protocol
EGP	Exterior Gateway Protocol
EPC	Electronic Product Code
ESP	Encapsulating Security Payload
FIPS	Federal Information Processing Standards (NIST)
FMC	Fixed/Mobile Convergence
FP	(EU) Framework Project
GBA	3GPP Generic Bootstrapping Architecture
GDOI	Group Domain of Interpretation
GPRS	General Packet Radio Service
GCM	Galois/Counter Mode
GSAKMP	Group Secure Association Key Management Protocol
GSM	Global System for Mobile Communications
HMAC	Keyed-Hash Message Authentication Code
HTTP	Hypertext Transfer Protocol
ICE	Interactive Connectivity Establishment
ICMP	Internet Control Message Protocol

IC	Information and Communication
ICT	Information and Communication Technology
ID	Internet Draft (IETF)
IDS	Intrusion detection System
IGMP	Internet Group Management Protocol
IKE	Internet Key Exchange
IMS	IP Multimedia Subsystem
IP	Internet Protocol
IPTV	Internet Protocol Television
IPsec	IP Security Protocol
IPTV	IP Television
IPv4/v6	Internet Protocol version 4 / version 6
IPS	Intrusion Protection (Prevention) System
IGP	Interior Gateway Protocol
ISIM	IP Multimedia Services Identity Module
ISP	Internet Service Provider
MAC	Message Authentication Code
MBMS	Multimedia Broadcast/Multicast Service
MIKEY	Multimedia Internet KEYing
MIME	Multi-Purpose Internet Mail Extensions
MMS	Multimedia Messaging Service
NGN	Next Generation Network
NIS	Network and Information System
NAT	Network Address Translation
NFC	Near Field Communication
OCSP	Online Certificate Status Protocol
OS	Operating System
OSPF	Open Shortest Path First
OTA	Over-the-Air (programming/provisioning)
P3P	Platform for Privacy Preferences
PDA	Personal digital assistant
PEP	Performance Enhancement Proxies
PET	Privacy Enhancing Technologies
PoC	Push-to-talk over Cellular
PRF	Pseudo-random Function
PKI	Public-Key Infrastructure
PSTN	Public Switched Telephone Network
PTT	Push To Talk
QoS	Quality of Service
R&D	Research and Development
RFC	Request For Comments (IETF)
RFID	Radio Frequency Identification
RTCP	Real-time Transport Control Protocol
RTP	Real-time Transport Protocol
SA	Security Association
SASL	Simple Authentication and Security Layer

SBC	Session Border Controller
SDP	Session Description Protocol
SIM	Subscriber Identity Module
SIP	Session Initiation Protocol
SLA	Service Level Agreement
S/MIME	Secure MIME
SMS	Short Message Service
SP	Special Publication (NIST)
SPF	Sender Policy Framework
SPIM	Spam over Instant Messaging
SPIT	Spam over IP Telephony
SRTCP	Secure Real-time Transport Control Protocol
SRTP	Secure Real-time Transport Protocol
SSO	Single Sign On
TC	Trusted Computing
TCP	Transmission Control Protocol
TESLA	Timed Efficient Stream loss-tolerant Authentication
TLS	Transport Layer Security Protocol
TNC	Trusted Network Connect (TCG)
TPM	Trusted Platform Module (TCG)
TSIG	Transaction Signature (DNS)
UDP	User Datagram Protocol
UICC	Universal Integrated Circuit Card
UMAC	Universal Message Authentication Cose
UMTS	Universal Mobile Telecommunications Service
VoIP	Voice over IP
VoIPoW	Voice over IP over Wireless
VPN	Virtual Private Network
WEP	Wired Equivalent Privacy
WG	Working Group
WLAN	Wireless Local Area Network
WPA	Wi-Fi Protected Access
WTLS	Wireless TLS
XCBF	XML Common Biometric Format

Fora/Bodies

3GPP	3rd Generation Partnership Project
3GPP2	3rd Generation Partnership Project 2
ANSI	American National Standards Institute
CASPIAN	Consumers against Supermarket Privacy Invasion and Numbering
CEN	European Committee for Standardization
CNSA	Contact Network of Spam Authorities
CSIA	Cyber Security Industry Alliance
ETSI	The European Telecommunications Standards Institute
EC	European Commission

ENISA	European Network and Information Security Agency
EPIC	Electronic Privacy Information Center
EU	European Union
FIDIS	Future of Identity in the Information Society
GUIDE	Government User Identity for Europe
ICANN	Internet Corporation for Assigned Names and Numbers
IEC	International Electrotechnical Commission
IEEE	Institute of Electrical and Electronics Engineers
IETF	Internet Engineering Task Force
IRTF	Internet Engineering Task Force
ISO	International Organization for Standardization
ISOC	Internet Society
ISSS	Information Society Standardization System
ITU	International Telecommunication Union
ITU-T	International Telecommunication Union-Telecommunication
LAP	London Action Plan
MAAWG	Messaging Anti-Abuse Working Group
NANOG	North American Network Operators' Group
NIST	National Institute of Standards and Technology
NTIA	National Telecommunications and Information Administration
OASIS	Organization for the Advancement of Structured Information Standards
OECD	Organisation for Economic Co-operation and Development
OMA	Open Mobile Alliance
PRIME	Privacy and Identity Management for Europe
RAI	Real-time Applications and Infrastructure Area (IETF)
RIPE	Réseaux IP Européens
SAAC	Security and Stability Advisory Committee (ICANN)
SAAG	Security Area Advisory Group (IETF)
SAGE	Security Algorithms Group of Experts (ETSI)
SDO	Standard Development Organizations
TCG	Trusted Computing Group
TIA	Telecommunications Industry Association
TISPAN	Telecommunications and Internet converged Services and Protocols for Advanced Networking (ETSI)
VOIPSA	Voice over IP Security Alliance
W3C	World Wide Web Consortium
WG	Working Group