# Internet Telephony - Security Issues in Skype™

Samuel Korpi
Helsinki University of Technology
Samuel.Korpi@hut.fi

## Abstract

Skype™ and other "Internet telephony" services are becoming more and more attractive alternatives to the Plain Old Telephone System (POTS), now that Internet connections providing the necessary bandwidth are available at affordable prices almost everywhere. Understandably, cheap or even free phone calls are very attractive.

In addition to the apparent cost advantages, Internet telephony can offer a lot of extra services which would not be feasible in POTS. Video telephony is one such service. Another example is the integration of other Internet applications with telephony, like Instant Messaging (IM) and file sharing, for example.

So, what is the catch? In this paper, we try to answer that question. The focus is on the services traditionally provided by POTS and especially on the security issues. Additional services, like the video telephony mentioned above, are not discussed. Skype™ (using peer-to-peer architecture) is compared to more centralized Voice over IP (VoIP) services that use Session Initiation Protocol (SIP). Skype™, as well as many other VoIP services, provides ways to connect to the traditional telephone network, also known as the Public Switched Telephone Network (PSTN). How does the bridging of these two networks affect security, is one point to consider.

KEYWORDS: Skype, VoIP, Internet telephony, security

## 1 Introduction

The paper is structured as follows: This first section introduces the Voice over IP (VoIP) technology in general. Also, different VoIP service architectures, centralized and decentralized (peer-to-peer), are discussed shortly. Skype™, as an example of a peer-to-peer (P2P) VoIP solution, is introduced in Sec. 1.4.

In the second section we discuss how different security aspects affect VoIP in general. A detailed analysis of the Skype security is given in the third section.

Finally, some legal issues concerning Skype™ and VoIP in general are covered in Sec. 4, followed by conclusions in Sec. 5.

### 1.1 VoIP in general

The idea in VoIP is to encapsulate voice transmissions into Internet Protocol (IP) packets. These packets are then sent over packet-switched IP network(s).

The two main benefits of VoIP are cost advantages and improved network utilization. No separate infrastructure has to be provided for VoIP, it can utilize whatever broadband Internet connection is available. Also, PSTN dedicates a 64 Kbps line for each connection, even though not all of that is required all the time (pauses in the speach, etc.). In VoIP, the voice data is digitized and compressed and the necessary bandwidth is dynamically allocated.

VoIP dates from the 1970s, but until recently it had not achieved much of a market share [1]. A major problem was latency (i.e. the delay in the transmission) [2]. Nowadays, ADSL and other fast Internet connections have slowly made VoIP a real alternative to POTS.

VoIP uses the User Datagram Protocol (UDP) [2]. Unlike Transmission Control Protocol (TCP) segments, UDP datagarams are always delivered according to the best-effort philosophy (i.e. there is no guarantee that the packets will ever reach their destination). There is no acknowledgement of missing packets. The decision to use UDP is intentional, as acknowledgments and retransmissed packets create overhead. And, after all, in real-time voice transmissions (e.g. phone conversions) there is no use in retransmitting lost packets – the damage is already done.

A phone call includes two phases: establishing the connection (signaling) and the actual conversation (data). In POTS these form two separate planes. In VoIP the separation is only logical, as both signaling and data flows are IP traffic. [3]

The separation of the signaling and data planes shows in the application-layer protocols – different functionality requires different protocols.

The International Telecommunication Union (ITU) has produced an ITU-T Recommendation H.323 [12] to provide a standardized agreement on which protocols to use. A competing solution from the Internet Engineering Task Force (IETF) is called the Media Gateway Control Protocol (MGCP) [14]. MGCP, like H.323, relies on other protocols to actually get the job done [2].

Lately, IETF and ITU-T have been working together towards a common standard, the Gateway Control Protocol [15, 13]. It was originally called Megaco by IETF and H.248 by ITU-T, but in later versions the name changed to the Gateway Control Protocol.

### 1.2 Centralized VoIP services

Some operators, including Ipon Communications [23] in Finland and Wengo [24] in France, provide centralized VoIP services. These rely on the use of a client-server architecture.

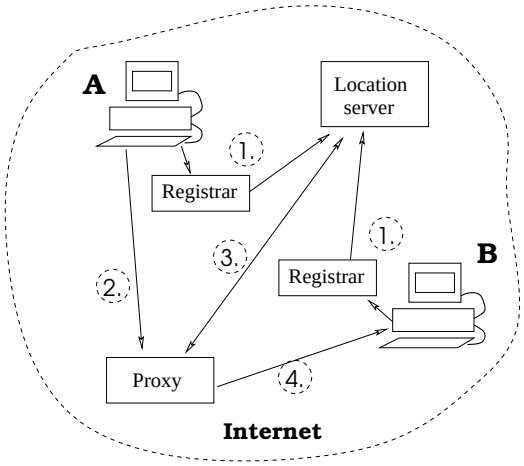


Figure 1: An example of a VoIP call establishment using SIP. The numbers depict the order in which connections are made. *First A and B register themselves with a local registrar service which in turn stores the information in the location server. Call from A to B is established through a proxy, which first enquires the location of B from the location server and after that connects with B. The actual data transfer is not shown here.*

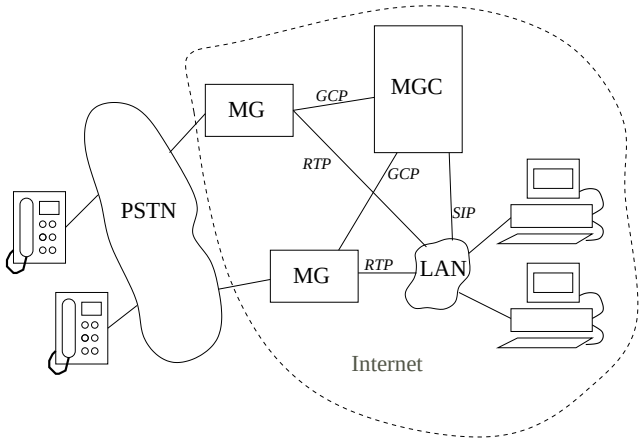


Figure 2: A general VoIP architecture using the Gateway Control Protocol and SIP.

As the service providers often do not give out detailed information about their service architecture, we will use as an example a hypothetical architecture using the Gateway Control Protocol and SIP. Fig. 1 shows a simple scenario of a VoIP call establishment between two VoIP clients using SIP.

As shown in Fig. 2, the operator may also provide gateweying functionality to PSTN. New elements include a Media Gateway Controller (MGC) and two Media Gateways (MG) which handle the routing of data between the circuit-switched PSTN and the packet-switched Internet. In this kind of a scenario, the operator usually associates a phone number with the user's account. Incoming calls from the PSTN would be transferred to the user if the client is correctly registered. Otherwise, a recorded message could be played for the caller.

For the actual data transfer, Real-time Transport Protocol (RTP) is often used, as shown in Fig. 2.

Both figures have been adapted from [7]. In Fig. 2 the newer Gateway Control Protocol has been used instead of Megaco/H.248. Changes in the protocols do not show as they do not affect the general architecture.

## 1.3 Decentralized VoIP services

Decentralized VoIP services rely on a P2P architecture, where the difference between a client and a server is blurred (i.e. every client, or peer, can dynamically act as either a client or a server). P2P architecture is familiar from many filesharing networks such as Kazaa [22].

One big advantage of P2P architectures is their scalability. Each new client adds computing power and further distributes the user information databases etc.

One example of a decentralized VoIP service is Skype™ [21], which is covered in the next section. There is also research being done to bring the advantages of P2P to SIP-based VoIP solutions [19].

## 1.4 Skype™

Skype™ is a popular Internet telephoning service using VoIP technologies in a peer-to-peer manner. The main application for it is voice communications between two (or more) Skype clients. Connection to PSTN is also provided at a charge.

The implementation of Skype™ (e.g. the client applications, the protocols and the architecture) is mostly proprietary (i.e. closed from the public) [10]. Furthermore, Skype uses end-to-end encryption for secure communications. All this makes it quite difficult to analyze the inner workings of Skype.

Each computer running the Skype client software is called a node or a peer. We use the term *node* in this article. Most nodes are just simple *client nodes*, but each node has the potential to become a *super node* in the Skype P2P network. A super node acts as an intermediary between Skype connections where either one of the client nodes is behind a NAT (Network Address Translation) firewall. [4, 5]

More on the subject of Skype super nodes and firewall traversal can be found in Sec. 3.3 and 3.2.

According to Baset and Shulzrinne [4] logging on to the Skype network is done through a central login server. However, in their research they used Skype version 0.97.0.6, which is now obsolete. Laalak Nassiri, in her research, used a newer version 1.3.0.60 and found out that there are at least three different login servers [17], but still the login servers are not part of the actual Skype P2P network. An updated analysis by Baset and Shulzrinne [5], with Skype version 1.4.0.84 (for Windows), claims that the number of login servers is two.

Our own tests, using Skype version 2.0.0.81, seem to indicate that there are actually different types of logins. Detailed information about the test environment can be found in table 1.

First scenario with automatic login is discussed in Sec. 1.4.1. Another scenario, where the user manually enters the login information (i.e. username and password), is

| OS | Microsoft Windows XP Home Edition SP 2 |
|---|---|
| Skype™ | Version 2.0.0.81 |
| Ethereal | Version 0.10.14<br>Running with WinPcap version 3.1 |
| Network | Private, NAT |
| Firewall (Hardware) | **Outbound**: allow ALL<br>**Inbound**: allow HTTP (TCP:80),<br>SIP (TCP+UDP:5060),<br>RTP (UDP:5004-5014) |

Table 1: The details of our test environment.

presented in Sec. 1.4.2.

For a thorough analysis, a lot more testing should be done in different environments (e.g. with different firewall settings). Unfortunately, we did not have the resources nor the time to do that. So, within the scope of this paper, we rely on the couple of our own tests and the research done by others.

Skype™ provides connection to PSTN through the SkypeIn and SkypeOut services. Skype has made agreements at least with COLT [26], iBasis [27], Level 3 [28] and Teleglobe [29] to provide the necessary "call termination" service [18]. In other words, the voice traffic bound for PSTN is directed to one of these partners which handle the transfer process to PSTN. Because of the circuit-switched nature of PSTN, the gateway points add some structure to the Skype network.

#### 1.4.1 Automatic login

Here is what happens during a normal Skype login using our test environment. The user account has been created earlier and the user has been logged on the network before, after which the Skype client program has been restarted. Furthermore, the "Sign me in when Skype starts" option has been enabled.

1. The client selects, seemingly randomly, a host from its host cache, which is stored in a file called `shared.xml`. If the host cache is empty, a host is apparently selected from an internal list hard coded into the Skype executable. Baset and Schulzrinne [5] refer to these as the *bootstrap super nodes*.

2. The client sends the selected host an UDP packet and waits for an answer. After receiving an answer the client sends another UDP packet, probably checking for authentication capabilities or something like that.

3. Depending on the answer, the client either initiates a TCP connection or tries another host, the address for which it apparently got in the answer, as the host is not necessarily listed in the client's host cache.

4. Once a TCP connection is opened, the user authentication apparently takes place. In this authentication process, user credentials stored in a file called `config.xml` are used instead of a username/password pair. This can be concluded through the fact that if the credentials hash has been modified, an error occurs and the program asks for username and password, thus changing the scenario to a manual login (see Sec. 1.4.2). Keep in mind, though, that all this is only an assumption, as the TCP stream seems to be garbled (i.e. encrypted or uses some proprietary encoding).

5. The TCP connection stays open for as long as the Skype client is open. A lot of UDP traffic takes place in the meantime to various addresses, this is probably part of the normal P2P traffic updating the host cache and transferring Skype user data (who is online etc.) back and forth.

6. Another TCP connection is also observed, this one a normal HTTP connection to 212.72.49.131 (ui.skype.com) and the apparent reason is checking for software updates.

#### 1.4.2 Manual login

If the "Sign me in when Skype starts" option has not been enabled, Skype asks for username and password before logging on to the network.

As a difference to the automatic login presented in the previous section, three TCP connections can be observed. One with the super node and one with the ui.skype.com server, as with the automatic login. The third TCP connection is initiated with a server not necessarily listed in the host cache. This seems to be the login server, which handles username/password pairs.

During the connection with the login server, a credentials hash is created which will later be stored in the `config.xml` to allow automatic login directly with a super node. If the "Sign me in when Skype starts" is not enabled, no hash is stored.

## 2 Security Issues in VoIP

Here we will cover the different security aspects and how they affect VoIP in general. Each aspect is dicussed in turn, roughly following the list provided in the ITU-T Recommendation X.805 [11]. Further analysis of security in Skype™ is provided in Sec. 3.

When analyzing the security issues in VoIP, the fact that VoIP runs on a network architecture radically different from PSTN must be taken into account. Compared to the circuit-switched PSTN, in packet-switched IP networks the intelligence is moved from the network itself to the end-points. [6]

### 2.1 Access Control

*"Ensure that only authorized personnel or devices are allowed to access end-user data that is transiting a network element or communications link"* [11].

Here it is assumed that we know who is authorized to access the data. Authentication (see Sec. 2.2), takes care of confirming the authority.

In traditional telephone networks access control is physical. Each connection is supplied with a separate line. The

only way to listen to a connection is to physically tap the line, or to access the exchange points of the network. [9]

VoIP uses the Internet. The voice packets are mixed with other traffic. Thus, no separate lines, making physical access control virtually impossible. This is where encryption comes into play. Only the authorized personnel or devices know the encryption keys thus providing access control.

VoIP protocols like SIP and H.323 do not implicitly include encryption. Additions has been made to the original standards to allow for secure connections.

Skype, on the other hand, encrypts all connections thus providing access control for data in transit.

## 2.2 Authentication

*"Verify the identity of the person or device attempting to access end-user data that is transiting a network element or communications link"* [11].

In PSTN, a phone number is associated with a physical location. This, together with the knowledge of a separate line to each location, is all the authentication needed. If somebody uses a phone in a certain location, it is assumed that he or she has the right to do that. In other words, it is the location, not the user, that is authenticated. Some services, like voice-mail, might employ additional authentication methods, like PIN codes, for example.

In mobile networks there can be no specific location-number association, so the number is associated instead with a SIM card. This is also a type of physical authentication. Further association with the owner of the phone is attained via a PIN code. Of course, after the owner has input the correct code, anyone can use the phone and thus be authenticated.

Username/password authentication is by far the most common authentication method used in different types of Internet services, VoIP among them.

## 2.3 Non-repudiation

*"Provide a record identifying each individual or device that accessed end-user data that is transiting a network element or communications link ... and the action that was performed"* [11].

In PSTN and mobile networks it is the job of the phone companies to keep records of connections.

In centralized VoIP solutions the service provider has the possibility to log the activities in the network as the service provider controls the servers used to establish connections.

In P2P solutions, like Skype, it can be hard to track the actual route of data, as there are no central servers involved in the actual communications.

## 2.4 Confidentiality

*"Protect the end-user data that is transiting a network element or communications link ... against unauthorized access or viewing"* [11].

This goes hand-in-hand with Access Control (see Sec. 2.1). So, the means to ensure confidentiality are more or less the same as the means for controlling access.

In VoIP, encryption offers not only access control but confidentiality as well.

## 2.5 Communication Security

*"Ensure end-user data that is transiting a network element or communications link is not diverted or intercepted as it flows between endpoints without authorized access (e.g., legal wiretaps)"* [11].

This security dimension overlaps with Access Control (see Sec. 2.1) and Confidentiality (see Sec. 2.4).

An example might be a man-in-the-middle attack, where a third-party sits in between two communication partners intercepting all communications without being noticed. A simple version of the attack involves only eavesdropping, but a more sophisticated one could even forge some data to lure one of the communication partners into giving out some sensitive information (see Sec. 2.6).

In Internet scenarios, end-to-end encryption should effectively prevent these kind of attacks.

## 2.6 Integrity

*"Protect end-user data that is transiting a network element or communications link ... against unauthorized modification, deletion, creation, and replication"* [11].

Breaking the integrity of a voice transmission is not easy, at least to do it unnoticed, according to Sicker and Lookabough [9]. Humans are fairly good in voice recognition an alterations are fairly easily noticed.

Encryption, when done correctly, helps to protect integrity. Though it might not be enough. Encrypted data can be replicated just as easily as unencrypted data. The attacker, however, has no idea of what he or she actually has unless the encryption can be cracked, making it difficult to take advantage of the replicated data. And, using session keys (i.e. keys that are generated new for each connection), the replicated data cannot even be sent to the receiver at a later time as the key used to encrypt the data would already be obsolete.

## 2.7 Availability

*The user should be able to use the service at any given point in time with acceptable probability.*.

The availability of POTS is amazing 99,999% [2]. People are accustomed to the idea that when you pick up the phone, it works, and you can call the person you want. Often even during a power outage, as the telephone lines provide the necessary electricity.

Internet connection is a pure data connection. You need power for various devices in order to make a VoIP call. Power outage is bound to cut your Internet connection also, or if not that, then your computer. UPS (Uninterruptible Power Source) can help, but only during short outages. Especially in the country side, the power can be out for hours and most UPS devices run out of power within half an hour. So, VoIP is not suitable for a complete telephone replacement in regions where long power outages are to be expected.

### 2.8 Privacy and Anonymity

**Privacy:** *"Ensure that the network-based application does not provide information pertaining to the end user's use of the application to unauthorized personnel or devices."* [11].

**Anonymity:** *your actions can neither be traced back to you (untraceability) nor linked to you in any way (unlinkability).*

When Access Control (Sec. 2.1), Authentication (Sec. 2.2), Confidentiality (Sec. 2.4) and Communication Security (Sec. 2.5) are handled, you can be reasonably sure that your connection is also private.

Anonymity is another matter. In PSTN, your phone number is used as a caller ID and transferred to the receiver along with the signaling data. This effectively identifies you to any recipient. Clients requiring anonymity can request their number to be private (i.e. empty caller ID).

In the Internet, connections might seem inherently anonymous. However, every packet leaves a trace when it passes through the network, and a skilled person can find out quite a lot from these traces. A certain amount of anonymity can be achieved through the usage of services that mask the traffic you generate. Full anonymity cannot be guaranteed even by using such services, as is demonstrated in [8].

## 3 Analysis of the Skype Security

In this section, we will analyze the security in Skype™ and relate to the different security aspects introduced in Sec. 2.

### 3.1 User Authentication

As discussed in Sec. 1.4, Skype uses different levels of authentication.

Originally, there was one central login server handling the user authentication [4]. On a purely security perspective this is good, as keeping the login data at one location makes it easy to control. On the other hand, it effectively reduces the advantages of P2P, as the login server can become a bottleneck making expanding the network difficult, if not impossible.

In the second phase, Skype increased the amount of login servers [4, 17]. How this is done, exactly, is unknown. Are the login servers just mirrors of each others, or is there some kind of division of the user information? Also, how is the load balanced between the login servers?

The third phase, and the current situation, has reduced the need for the login servers. The login process is only required the first time the user logs onto the network by manually giving the username/password pair. This pair is validated at the login server, and a credentials hash is created for the user. In subsequent automatic logins (default method in Skype) the client registers directly with a super node using the credentials given by the login server. In this case no direct communication between the client and the login server was observed. Whether or not a super node does some checking with the login server in this case is unknown. In any case, the load of the login servers is reduced.

One alternative solution would be to integrate the whole login process in the P2P network. The main concern with this solution is how the user information should be divided between peers and how can we make sure that the user information is secure (i.e. that the owner of a random peer cannot browse through the user information stored in that peer).

### 3.2 Blocking Skype

Skype™ is known for its firewall traversal capabilities [10]. From a user's point of view this is usually a good thing, as it makes modifications to the firewall unnecessary and assures the functionality of Skype™ virtually everywhere.

Skype uses random TCP and UDP ports when possible. As a last resort it can also utilize the well-known ports 80 (HTTP) and 443 (HTTPS) which usually are open for outbound traffic to allow the normal web usage.

Enterprises are not as thrilled about this charasteristic of Skype. It makes it harder, though not impossible, to effectively block Skype alltogether [10].

As mentioned in Sec. 1.4, Skype does use central login servers for the actual username/password matching. Because of this, it could be concluded that blocking all connections to these servers would block Skype also. However, as shown in Sec. 1.4.1, the automatic login process does not directly involve the login servers. Furthermore, it seems that Skype is able to route the login through a super node, if direct connection with the login server is not possible [5].

### 3.3 Super Nodes in the Skype Network

Super nodes in the Skype network act as intermediaries between connections where at least one of the communication partners is behind a NAT firewall [5].

This means that a lot of data passes a super node that is not meant for it. Care has to be taken that this super node cannot act as a middle-man in these connections (e.g. by listening into the conversation). In Skype, this is handled through an end-to-end encryption. [10]

### 3.4 Skype Voicemail

Securing Voicemail and other services that hold data on the behalf of a client is especially tricky in a P2P network. The situation is similar to the one of authentication - do we use a separate central service to handle the storage, or do we try to employ the P2P network itself. [20]

Skype offers Voicemail as a separate service for a charge. No technical specification on how the service actually works is available, but within the information on the Skype web site there is a phrase *"Voicemails that are not listened to are stored on our servers for 60 days before they are deleted"*, which seems to indicate a centralized solution.

### 3.5 Skype Call Termination (PSTN)

Skype has outsourced the PSTN call termination to several telecom companies (see Sec. 1.4). This is probably the only viable alternative for a company which does not own the necessary infrastructure for routing the calls between circuit-switched PSTN and packet-switched Internet.

However, outsourcing can also become a security risk. In order for the calls to transfer from the Skype network to the

PSTN they have to be first decrypted, which means that there is a point where the call could be intercepted.

### 3.6 Caller ID in SkypeOut

In PSTN, users are authenticated via physical location, in mobile networks via the SIM card. These both methods link the phone number (the caller ID) to a certain person with a fair amount of certainty. Someone else might, of course, be on the phone than the actual owner.

SkypeOut service can be used to call to any phone number in PSTN. The question is, what is the caller ID for such a Skype user? If the user also has bought the SkypeIn service, a logical choice would be the number the user is linked with through the SkypeIn service. For users that only use SkypeOut, it is not this easy. No definite information concerning the decision Skype has made could be found. However, a conversation in a Skype forum indicated that the caller ID is fixed for all Skype users. This is a simple solution which takes care of the possible security issues (e.g. identity forging). However, it also makes it impossible for the receiver to know the identity of the caller before answering.

## 4 Legal Issues

People want to communicate securely. At times this means complete privacy, some times even anonymity. On the other hand, legislation has its own demands, which may not always go hand-in-hand with what the user wants. This section describes some situations, where the need for security can cause conflicts with the legislation.

The real issue with Skype™ and other VoIP services is whether they are considered *voice telephony* in the same sense as POTS. That is, whether the same rules and regulations should apply both to the traditional fixed telephone networks and to the VoIP services.

In 2003, the Finnish Communications Regulatory Authority (FICORA) made a decision concerning TeliaSonera's VoIP service, called Puhekaista. It was decided that the Puhekaista service is in fact comparable with a publicly available telephone service [16].

This decision, if adopted to apply to VoIP services in general, creates new requirements which have to be met. One of these involves the way in which emergency calls can be handled in a VoIP environment (see Sec. 4.1).

### 4.1 Emergency calls

If VoIP services really are to become a viable substitute to PSTN, a sufficient implementation for providing emergency call functionality is essential.

One issue here is that VoIP service are not localized the same way as fixed telephone network subscriptions. You can hook your laptop on to the Internet anywhere in the world and use your Skype™ account regardless of the geographical location. And still, for emergency calls to be effective, they should always be routed to the nearest emergency centre.

Notice, that according to the current Terms of Service (Jan 2006), Skype™ does not support emergency calls.

Some VoIP service providers, among them Vonage [25], have come up with a solution, which requires the user to manually register the location when changing from place to place. This works, assuming that the user remembers to update the location information and does so correctly. The software could remind the user that the location should be checked after a change in the IP address, for example. This, however, could lead to false alarms with dynamically assigned IPs, which in turn could frustrate the user and lead to mistakes in the location data.

### 4.2 Should Skype be banned?

This is a question many enterprises, organizations, and even governments are faced with.

Educational organizations, especially universities, have high-speed Internet connections, and a large base of public IP addresses. Thus, if Skype is running on an university computer, for example, it becomes an ideal candidate of becoming a super node in the Skype network (see Sec. 1.4).

Section 4.1 of the Skype End User License Agreement (EULA) states: *"You hereby acknowledge that the Skype Software may utilize the processor and bandwidth of the computer (or other applicable device) You are utilizing, for the limited purpose of facilitating the communication between Skype Software users"*.

This may be in violation of the organization's own computer usage policies and thus should be banned. If this is the case, the next question is how to effectively implement the ban. Blocking Skype alltogether is one possibility. This is covered in more detail in Sec. 3.2.

## 5 Conclusions

Is Skype secure? Unfortunately, this question does not have a simple *yes* or *no* answer. It all depends on what is considered secure and how much faith can be put on the proprietary implementation of Skype.

When considering the security of Skype, it should be remembered that there are no such thing as perfect security in digital communications over the Internet. The fact is that no matter how good security measures are used, sooner or later someone comes up with a way to crack them. Fortunately, when the security measures are well-planned and tested, the cracking usually comes a lot later. Well-known encryption methods, when used correctly, provide reasonable guarantees that by the time the information can be read by a third-party, the data will already be obsolete.

On the other hand, people are even now widely using completely insecure communications with little or no thought to it. Take a look at emails, for example. They are transferred unencrypted, and provide no implicit way of guaranteeing the identity of the sender. PGP (Pretty Good Privacy) addresses these problems, but it is rarely used.

Sensitive information, like credit card numbers, should never be transferred over the Internet unencrypted. Even though Skype uses end-to-end encryption, it is still wise to be a little careful with sensitive information.

The most important thing is to know the possible threats and plan accordingly the use of a service like Skype. As

email is commonly accepted to meet a lot of communication needs, so has Skype or any other VoIP service a lot of potential. Keeping the risks in mind, Skype can also be used as a reasonably secure communication method.

Skype's shortcoming, in the long run, might turn out to be the reluctance to give out details of the implementation and architecture of the service. Standards by ITU and IETF are maturing fast to provide a good basis for many new VoIP services with the added advantage of interoperability. Currently, you have to be a Skype user yourself to contact another Skype user, with the exception of the SkypeOut/SkypeIn services. As more and more standards-based services emerge Skype has to rethink its philosophy if it plans to maintain its market share.

# References


[1] Schulzrinne, H. Converging on Internet telephony *IEEE Internet Computing*, Volume 3 Issue 3. IEEE, May/June 1999.

[2] Varshney, U., Snow, A., McGivern, M., and Howard, C. Voice over IP. *Communications of the ACM*, Volume 45 Issue 1. ACM Press, January 2002

[3] Ackermann R., Schumacher, M., Roedig, U., and Steinmetz, R. Vulnerabilities and Security Limitations of current IP Telephony Systems. *Proceedings of the Conference on Communications and Multimedia Security* (CMS 2001). `ftp://ftp.kom.e-technik.tu-darmstadt.de/pub/papers/ASRS01-1-paper.pdf`

[4] Baset, S. A. and Schulzrinne, H. An Analysis of the Skype Peer-to-Peer Internet Telephony Protocol. Columbia University Technical Report CUCS-039-04. 2004. `http://www1.cs.columbia.edu/~salman/publications/cucs-039-04.pdf`

[5] Baset, S. A. and Schulzrinne, H. An Analysis of the Skype Peer-to-Peer Internet Telephony Protocol. To appear in IEEE Infocom 2006. `http://www1.cs.columbia.edu/~salman/publications/skype1_4.pdf`

[6] Posegga, J. and Seedorf, J. Voice over IP: Unsafe at any Bandwidth? Eurescom Summit 2005 – Ubiquitous Services and Applications, Heidelberg, 27.-29.4.2005, S. 305-314. `http://www.informatik.uni-hamburg.de/SVS/papers/Eurescom_VoIP-unsafe.pdf`

[7] Kuhn, D. R., Walsh, T. J., and Fries, S. Security Considerations for Voice Over IP Systems. *Recommendations of the National Institute of Standards and Technology*. SP 800-58. `http://csrc.nist.gov/publications/nistpubs/800-58/SP800-58-final.pdf`

[8] Wang, X., Chen, S., and Jajodia, S. Privacy and anonymity: Tracking anonymous peer-to-peer VoIP calls on the internet. *Proceedings of the 12th ACM conference on Computer and communications security* (CCS '05). ACM Press, November 2005.

[9] Sicker, D. C. and Lookabaugh, T. Queue Focus: Voice Over IP: VoIP Security: Not an Afterthought. *Queue*, Volume 2 Issue 6. ACM Press, September 2004.

[10] Lazar, I. Debunking the Hype About Skype. Burton Group. 2006.

[11] ITU-T Recommendation X.805. Security architecture for systems providing end-to-end communications. International Telecommunication Union. 2003.

[12] ITU-T Recommendation H.323. Packet-based multimedia communications systems. International Telecommunication Union. 2003.

[13] ITU-T Recommendation H.248.1. Gateway control protocol: Version 3. International Telecommunication Union. 2005.

[14] RFC 3435. Media Gateway Control Protocol (MGCP) Version 1.0. The Internet Society. 2003. `http://www.ietf.org/rfc/rfc3435.txt`

[15] RFC 3525. Gateway Control Protocol Version 1. The Internet Society. 2003. `http://www.ietf.org/rfc/rfc3525.txt`

[16] Decision of the Finnish Communications Regulatory Authority on Compliance with Law of the Sonera Puhekaista Service. Finnish Communications Regulatory Authority. 2003. `http://www.ficora.fi/englanti/document/Sonera Puhekaista.pdf`

[17] Nassiri, L. Sicherheitsanalyse des Peer-to-Peer Netzwerkes SKYPE, Studienarbeit. Universität Hamburg, Fachbereich Informatik. 2005.

[18] Skype Signs 4 Carrier Agreements for SkypeOut with COLT, iBasis, Level 3, Teleglobe to Provide Global Call Termination. `http://www.skype.com/company/news/2004/4carriers.html`

[19] Singh, K. and Schulzrinne, H. Peer-to-Peer Internet Telephony using SIP. *Proceedings of the International workshop on Network and Operating systems support for digital audio and video* (NOSSDAV '05). ACM Press.

[20] Cao, F., Bryan, D. A., and Lowekamp, B. B. Providing Secure Services in Peer-to-Peer Communications Networks with Central Security Servers *Proceedings of the Advanced International Conference on Telecommunications and International Conference on Internet and Web Applications and Services* (AICT/ICIW 2006). IEEE.

[21] Skype. `http://www.skype.com/`

[22] Kazaa. `http://www.kazaa.com/`

[23] Ipon Communications. http://www.ipon.fi/

[24] Wengo. http://www.wengo.com/

[25] Vonage. http://www.vonage.com/

[26] COLT. http://www.colt.net/

[27] iBasis. http://www.ibasis.net/

[28] Level 3. http://www.level3.com/

[29] Teleglobe. http://www.teleglobe.net/