Intranet Security from Organizational Point of View

Jorma Kajava [a] & Timo Remes [b]

jorma.kajava@oulu.fi and timo.remes@sonera.com

[a] Oulu University, Department of Information Processing Science, Linnanmaa, FIN-90014 OULU UNIVERSITY, FINLAND

[b] Sonera Corporation, FIN-00051 Sonera, Box 120, FINLAND

Abstract

This paper discusses the three dimensions of information security: confidentiality, integrity and availability. The key to understanding Intranet security involves recognizing the crucial differences between Intranets and the Internet and the various co-operation possibilities that virtual networks offer. The specific security threats of Intranets can be found in communications, software, data and operations security. In this paper, we shall put forward some ideas concerning protection against such threats.

Keywords: Information security, Intranet security, hacking, inside threats

1. Introduction

Although the difference between Intranets and the Internet is not great in terms of technology, the transmission of information is completely different from the organizational point of view. In this presentation, we shall concentrate on the differences and similarities between Intranets and the Internet. We also discuss information security threats surrounding Intranets and methods of protection against these threats. We have tried to make the presentation independent of the business area, so no references will be made to particular organizations or trademarks.

The use of Intranets as internal information transmission channels within organizations serves to emphasize the importance of their secure realization. Information security threats between Intranets and other networks and information systems are rather similar. The technology used in Intranets and the way that technology is used comprises a new threat source. Information security solutions in Intranets are based both on experiences gained from the Internet and on new solutions designed particularly for Intranets. Special areas of interest within Intranet security are communications, software, data and operations security. By researching these four areas, we hope to find usage differences in information security solutions between Intranets and the Internet.

Proceedings of IRIS 23. Laboratorium for Interaction Technology, University of Trollhättan Uddevalla, 2000.
L. Svensson, U. Snis, C. Sørensen, H. Fägerlind, T. Lindroth, M. Magnusson, C. Östlund (eds.)

Information security seeks to protect data and information, systems and services under both normal and exceptional conditions. Such protection creates data and information confidentiality, integrity and availability.

2. Intranets versus the Internet

The technologies of the Internet and Intranets are quite similar, but the way in which the technologies are exploited, are different. We could define the Internet as a computer network, which is based on smaller independent networks owned by single organizations. These small networks are connected by means of routers and fixed communications connections to the global Internet.

The Internet was originally only a communication channel for scientists, researchers and specialists. Then, the introduction of browser software and the graphical user interface simplified data and information search. The uncomplicated use of browsers and the explosive increase of information available on the net attracted new groups of people.

Intranets have been defined as internal communication systems of organizations based on the standards of the Internet and the World Wide Web (WWW) (Telleen, 1996). Intranets are based on Internet technology, i.e. technologies that all together generate the Internet (Hinrichs, 1997). For example, Internet routers and their communication connections constitute a part of this technology. Intranets could also be defined as the use of Internet technology in organizational networks (Levitt, 1996). In yet another sense, Intranets could be viewed as private networks based on WWW servers (Pal, 1996).

By combining all these definitions, Intranets could be regarded as internal information systems owned by single organizations employing Internet technology. And like the Internet, Intranets may also be global. Communications between the various sites of an organization are transmitted via its computer network or via the Internet.

As a conclusion, we offer the following definition:

An Intranet is an internal computer system based on Internet technology and owned by a single organization. Outsiders have strongly restricted access to the Intranet. The communication networks of the Intranet are based on local networks at the different sites of the organization and the interconnecting networks between them. Communication between the remote sites of the organization is carried out via the Internet, the network of the organization or a hired network supplied by a network operator. The user interface consists of WWW browsers, enabling the transmission of text, voice and image files.

Although this definition does not include a reference to the technical background of Intranets, a measure of technical knowledge is necessary for understanding and detecting threats posed by the technology.

2.1. Differences between Intranets and the Internet

Intranets employ the same software tools and protocols than the Internet. In other words, they are technologically similar. The differences between Intranets and the Internet can be found in network usage, user groups and information contents. Intranets are internal systems of particular

organizations that barr outsider access. The Internet, on the other hand, is a public system, open to everybody. Intranets are only used by single organizations as internal communication channels and provide a working environment for application programmes.

There is no direct contact from Intranets to the Internet. The same user interface can be used in transmission both in Intranets and the Internet, but all telecommunications between them must always be directed through a gateway with a strong control mechanism. Thus, there can never be unrestricted access from the Internet to Intranets or vice versa.

What makes Intranets particularly attractive targets for external and internal attacks is the internal information of the organization. The use of Intranets as internal information systems emphasizes the importance of threats against Intranets from within organizations. It goes without saying that the connection to other networks outside an organization must be designed very carefully during the Intranet construction process. However, the same careful design and construction work is necessary even when implementing connections to other networks within the organization. A potential attacker working inside the organization should not find it any easier to gain access to confidential information. Most networks are protected against external attacks, while failing to address insider attacks adequately. Such internal attacks tend to be underestimated, although are can be extremely harmful to the organization.

2.2. The advantages of using Intranets

The main idea of Intranets is the same as that of the Internet, i.e. to facilitate the flow of information. Intranets enable users to keep in touch with physically remote sites of their organizations by using the Internet or other communication networks, which simplifies the transmission of information between the different sites. When using the Internet, the information security threats posed by the Internet to the organization must be borne in mind at all times. For example, the Internet service could be shut down for a while constituting a severe threat for the availability of information.

One significant advantage of using Intranets in comparison with other solutions based on corresponding network systems is the hardware independence of the Internet technology. Internet technology has successfully solved the problem of incompatible hardware and software and permits organizations to connect all their computers, operating systems and databases to a single independent system (Cortese, 1996). There is, however, an unresolved compatibility problem in browser technology.

Another major advantage of Intranets in comparison with other corresponding technologies is the simplicity and versatility of the Intranet user interface and the ease with which voice and images can be transmitted. The WWW-based user interface is easy to learn and use. By clicking on hyperlinks it is easy to move from one document to another and to fetch files to workstations. The technology also allows the real time transmission of voice and images.

Intranets also enable one user interface to contain functions belonging to a number of different applications. Reports, announcements, notices, memorandums, phone and address books could all be accessed by a single browser. In addition, the maintenance and use of databases can also be carried out via the Intranet.

Moreover, Intranets make it is possible to distribute real time information to all employees, provided that every information producer puts their documents immediately on a proper platform. The use of electronic platforms decreases the distribution of paper documents, as everyone can read and print only such documents as s/he deems important. The distribution

of information over an Intranet makes it easier for everybody to follow important news.

The transfer of multienvironment applications to a single Intranet-based system significantly facilitates the use and maintenance of the system. As every Intranet application is based on the same principles of use, users are no longer required to learn the characteristic details of every system. Also maintenance personnel has to deal with one working environment instead of several disparate systems.

2.3. Intranets and organizational personnel

The way an organizational Intranet is used has great effect on how the personnel perceives the system. Thus, the following arrangements in the personnel policy must be carefully considered:

- How to organize the technical maintenance of the Intranet
- How to produce information from systems
- How to publish information on the Intranet
- How to use the Intranet.

As far as the ease of use in information maintenance is concerned, the optimum situation would include that all information producers on the Intranet would transfer their documents to the right place in the system and delete them when they become obsolete. This would enable maintenance personnel to concentrate their efforts on the technical administration of the Intranet. However, the free presentation of documents on Intranets is not a good option from the point of view of information security. Lack of content control could result in the publication of incorrect information either intentionally or unintentionally. This, in turn, could have an adverse effect on the organization, for example, in making decisions concerning the development of new products.

The lines of responsibility for the logical design of the system must be defined. Those in charge should make administrative decisions concerning the Intranet and make plans for dividing the activities of the Intranet to accommodate different user groups.

Intranet users comprise the fourth group of people involved. Users do not produce new materials, they only use the information produced by others.

2.4. Short technical review

There are a lot of open questions concerning Intranet security and further research is an absolute necessity. It is very difficult to discuss security without reference to technical solutions. However, this presentation is limited to a consideration of the technical structure (Figure 1) and hardware of Intranets (Figure 2). A more thorough technical review has been presented earlier in (Remes, 1997).

From the technical point of view, Intranets are systems using physical network From the technical point of view, Intranets are systems using physical network components. The basic components are the same in every organization:

- Server computers
- Workstations
- Network cables
- Physical interfaces to networks
- Network and transportation protocols
- TCP/IP services

Internet technology and all its components are based on the TCP/IP protocol. Therefore, a basic understanding of TCP/IP and WWW protocols and other relevant technologies is a prerequisite for recognizing and understanding Intranet security threats.

Figure 1 presents current services offered by means of TCP/IP and WWW protocols along with other potentially usable services, hardware and interfaces on Intranets.

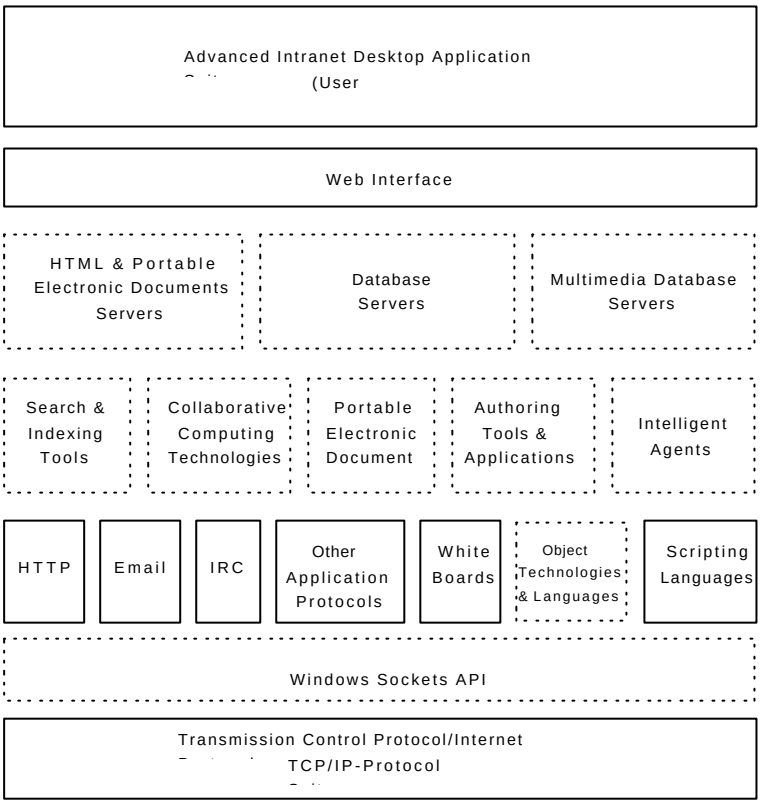

Figure 1. Intranet building blocks (Hummingbird, 1996)

The realization of an Intranet is always organization-dependent. There is no one correct way to realize an Intranet. The simplest Intranet solution consists of a server computer and a number of workstations connected to it by means of a network. The server houses Intranet software and the documents presented. Browser software allows the viewing of these documents from the workstations.

As far as hardware is concerned, Intranets are in many senses identical to traditional local area networks (LANs), the only difference is that Intranets include a server.

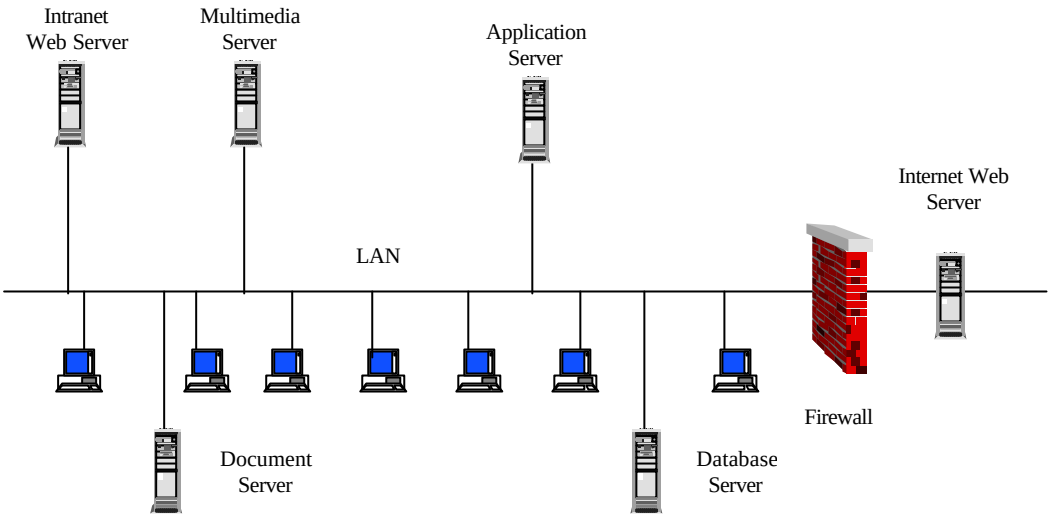

Figure 2. Intranet hardware (Remes, 1997)

From the point of view of information networks, Intranets are virtual networks based on real network architecture. A virtual network is a logical information network connecting limited groups of users by means of real networks.

From the organizational point of view, Intranets are private networks within a single organization. Moreover, they only reserve a small part of the organization's network for their own use.

In Figure 3, the thicker lines represent the virtual network connecting the different sites A, B and C of an organization. The thinner lines, in turn, depict the rest of the organization's communications network.

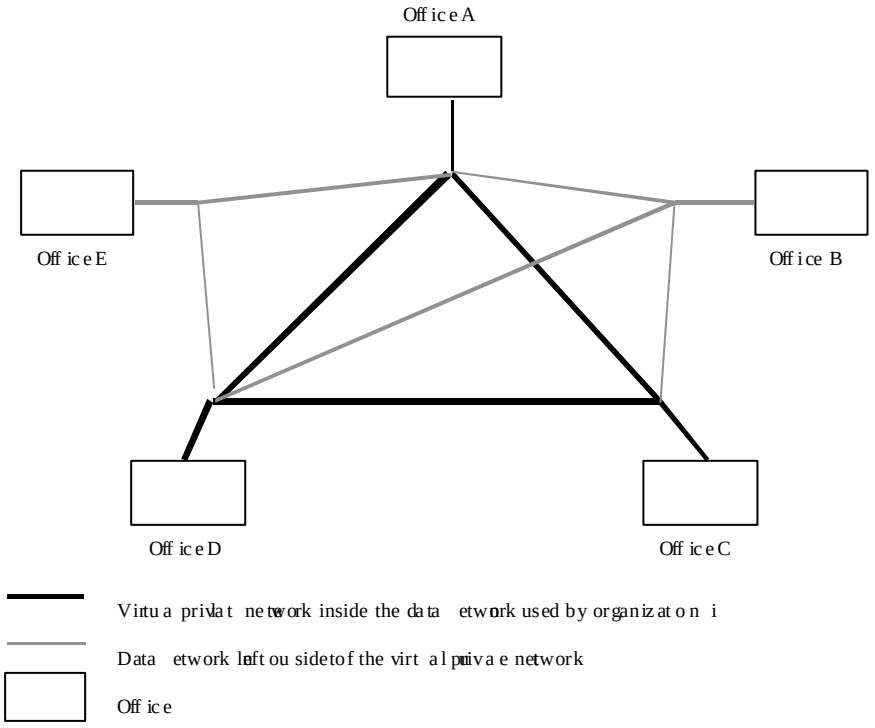

Figure 3. Virtual private network (Remes, 1997)

In terms of available application programs, the work environment offered by Intranets increasingly resembles that of the Window desktop. A growing number of applications are capable of exploiting the advantages provided by Intranets, thereby blurring the distinction between Intranet applications and workgroup tools. In addition to their communication facilitation function, Intranets are capable of offering a wide variety of services including decision support systems, applications supporting group work, expert tools, database management tools, corporate telephone directories and orientation applications for new employees. The possibilities are practically limitless.

3. Information Security Threats in Intranets

The use of Intranets as internal information channels emphasizes the importance of information security. Assets held on internal Intranets may increase the interest of potential misusers. Hence, protecting Intranets and the data and information transmitted via them against various threats endangering the confidentiality, integrity and availability of information is an extremely important consideration..

There are several ways of classifying information security threats. In this research, we use the following classification:

- Threats based on technology
- WWW technology
- Software
- Software code under process
- Telecommunications
- Viruses
- Threats based on human activities
- Natural phenomena

3.1. Threats based on technology

The following list of technology-based threats is presented without further discussion. An in-depth analysis of these threats can be found in Remes (1997).

- Threats based on WWW technology
- New features in browser software
- Browser software test versions
- Server software
- CGI scripts
- Cookies
- Threats based on Unix and TCP/IP tools
- Difficulties in firewall management
- Use of cryptographic software
- Hacker tools
- Other software based threats
- Intranet application software

- Java language
- ActiveX
- Threats based on communications
- Threats based on viruses

3.2. Threats based on human activities

Hacking comprises the most serious threat for the modern society in the next millennium. All other types of harm may be derived to hacking. Thus, hackers may be behind virus attacks, software piracy, theft, information misuse and sabotage.

Hackers exploit human illiteracy and weaknesses in computer systems to gain access to these systems. Hackers may study the system they attack, damage it or steal information held on it (Simonds, 1996) causing harm to the owner of the system. Even if a hacker does not cause any damage, there will be expenses for the owners as they have to study whether any damage has occurred or not.

Using the Internet as a part of an Intranet poses a serious threat, because the Internet is inherently nonsecure. As a result, users must be very careful particularly in encrypting their communications. Imitation (spoofing), reply (rapid fire), alteration of message contents (superzapping), prevention of service availability and active and passive wiretapping are among the most malicious threats. Wiretapping, for example, could lead to a situation where strategic knowledge regarding an organization gets in the hands of outsiders, if communication encryption is not implemented by means of strong encryption methods.

Hacker tools, although developed for the Internet, are also usable on Intranets. They can be software or hardware based or a combination of both. Their authorized use includes finding and correcting information security weaknesses on Intranets. However, they also anable insiders to hack such communication systems and access information which they are not authorized to access. Hacker tools can be divided into six categories:

- Tools for finding attack objects (searching telephone numbers and network addresses)
- Password tools (stealing and opening passwords)
- Communication tools (following, disturbing and misleading communications)
- Security hole tools (searching and “defining” security holes)
- Damage and teasing tools (viruses, worms and chain letters)
- Other tools (based on well-known information security holes of systems and combination tools) (Miettinen, 1995).

Threats caused by people, employees in particular, can be much more serious on Intranets than on the Internet. Personnel invariably constitutes the most severe information security threat. Intranets have made it easier for employees to access information, but they have also made it easier to misuse this information.

Dishonesty among personnel is always an information security threat. After all, it is easier for corporate personnel to gain access to sensitive information than outsiders. Authorized users may be tempted to misuse vital information. Even unauthorized members of staff may access sensitive information, if, for example, they know the weaknesses of the system.

Also carelessness and negligence among personnel may result in sensitive information landing in the hands of unauthorized persons. Papers left lying on a table are easy to read and copy. Printing a document into a wrong address may also have an undesirable outcome.

A low level of knowledge concerning security among personnel is a clear vulnerability.

This is partly a result of the current employment situation in which it might in some cases be a problem finding educated personnel to recruit. Shortcomings in training and education combined with the use of uneducated personnel in the realization and maintenance of Intranets may seriously undermine the security of the information held on Intranets.

The use of outsiders in the construction and maintenance of Intranets could also be detrimental to information confidentiality. Therefore, security concerns are of utmost importance in designing outsourcing and in drawing outsourcing contracts.

3.3. Threats based on natural phenomena

Natural phenomena have always been and always will be a difficult to estimate source of information security threats. Although such threats may feel unimportant, they must nevertheless be registered. Attention should be paid at least to the following eventualities: floods, thunderstorms, frost in the ground and earthquakes. They all have the capacity to bring down Intranets.

4. Protection Methods

In an attempt to provide protection against Intranet security threats a number of governments have adopted the model of the Canadian Mounted Police (1980) based on eight security levels. The most important levels in Intranets are those of communications, software, data and operations security. These are the areas in which Intranet security solutions differ most from their Internet counterparts.

4.1. Communications protection

Communications security is very important, particularly when the Internet is employed as a communication channel between the different sites of an organization. The same solutions are applicable for isolating Intranets from external networks than in protecting internal networks. Intranets may be protected against external hacking and other information security threats by firewall hardware. Firewalls are used to control traffic in communication networks (Siyan & Hare, 1995), and they do it by examining the communication passing through them and by imposing certain restrictions on it. Such communications as fail to follow the restrictions are filtered out. Firewalls use one or more of the following basic technologies:

- Router-and-server-based packet filtering
- Server-based communications filtering
- Server-based communication transmission for every single application software (Bernstein et al, 1996).

The various parts of an Intranet can be isolated with firewalls thus increasing information security against internal misuse. Such firewalls also prevent external intruders from moving on the Intranet.

An organization's network addresses can be encrypted for outsiders using address translation. In address translation, all data packages have an identical network address when they leave the network of the organization. Address translation disables outsiders from making

decisions based on real network addresses and the number of addresses within the organization (Bernstein et al, 1996).

Encryption precludes external parties from examining the contents of messages in networks and information in systems. Encryption is realized by means of encryption methods based on encrypting algorithms. The most common methods are DES, IDEA and RSA. One popular method on the Internet is SSL, which is used in WWW contacts. In Intranet communications, encryption works with application software that uses some encryption algorithm. It is of paramount importance that the encryption software fulfils the requirements of the organization and is applicable to the intended application area. The strength of the encryption is particularly important, if the organization uses the Internet as a communication channel.

Another method of protecting communication on the Internet is known as tunnelling. In this method, the data area of a communication packet contains another communication packet in its entirety. To enhance the degree of protection, a tunnelling communication contact may also be encrypted.

4.2. Software protection

Development is faster within software security than in any other area of Intranet security. The application software used on Intranets constitutes the most salient difference between Intranets and the Internet. In practice, Internet software security equals browser and server software security and security of software for producing WWW applications. Also Intranet software security is based on application programmes in browsers. This fact has far-reaching consequences, because many Intranet applications are tailor-made for one single organization.

It is essential to establish the trustworthiness of CGI scripts in Intranet applications. If possible, scripts readily available on the Internet should not be used at all. Erroneous software code may unintentionally open a trap door for intruders. The following considerations should be attended to in Intranet applications involving CGI operations:

- CGI scripts must be compiled, not interpreted
- The application software must always check the correctness of user inputs, before allowing the inputs to operate
- The minimum requirement involves that the right formulation and length of content of every input is controlled
- No assumptions should be made with compiled scripts. (Pabrai & Gurbani, 1996).

All critical Intranet applications must require user identification. Together with password controls, user identification provides protection against unauthorized use of applications. From the organizational point of view, the right to use critical applications could be enhanced by one-time passwords.

Audit trails record exceptional incidents and other security releted events in the use of Intranet applications. Audit trails should be produced and stored for an agreed period of time to assist in eventual investigations and to monitor access control by recording, for example, all dates and times for logon and logoff.

Virus protection is an important aspect of Intranet security. Intranets make it is easy to transfer documents and files between the different sites of organizations. Moreover, e-mail attachments can also be used as a vehicle for transferring computer viruses and infecting new computer systems and networks.

4.3. Data protection

Appropriate data protection decreases the probability of internal information security threats. Personnel should have guidelines concerning all materials that can be published on a corporate Intranet. A simple, yet effective way of providing a security classification on an Intranet is to divide all corporate data into data that can be published and data that cannot be published on the Intranet. When publishing confidential data on the Intranet, the limitations of user rights are an essential consideration. There must also be clear guidelines about the deletion of data on the Intranet. In addition, all data published on the Intranet must be backed up using appropriate back-up media. Finally, user rights for every Intranet directory and file must also be carefully defined.

4.4. Operations protection

Intranet operations security consists of activities which advance security without influencing practices. Thus, security threats posed by corporate personnel should be prevented in a simple and efficient manner without compromising the efficiency of the system as perceived by the users. The right to use the different parts of an Intranet and the right to access each data directory must be defined for every employee in accordance with to his/her tasks (Code of Practice 1993). Remote access must also be carefully regulated to ensure security.

The design and implementation of effective user rights management is in many ways a demanding process, but a successful solution significantly decreases information security threats posed by corporate personnel.

5. Conclusion

Intranets have gained in popularity during the past few years. Unfortunately, also the number of security problems has increased. From the organizational point of view, these problems call for particular Intranet solutions. Intranets started out as private communication channels, but their use has been extended to include DSS, CSCW, expert systems, database maintenance tools, corporate telephone directories and user guidelines.

Intranet security solutions are similar to those of the Internet. However, as the usage area of Intranets differs from that of the Internet, it is important to re-examine well-known security threats on the Internet and try to find ways of protecting Intranets against these threats. Intranets make organizations more vulnerable to internal threats.

All parts of information security must be considered in protecting Intranets against security threats, but there are areas of Intranet security that require particular attention. The areas of special interest are communications, software, data and operations security. The differences in these areas between Intranets and the Internet necessitate different information security solutions for the two.

6. References

Bernstein, T., Bhimani, A. B., Schults, E. & Siegel, C. A. Internet security for business. John Wiley & Sons Inc. 1996.

A Code of Practice for Information Security Management. Department of Trade and Industry. GBIS. PD 0003, England, 1993..

Cortese, A. Here comes the Intranet. Business Week. February 26, 1996.

Hinrichs, R. J. Intranets: What´s The Bottom Line? Prentice Hall, 1997.

Hummingbird Communications Ltd The Intranet: Implementation of Internet And Web Technologies In Organizational Information Systems, 1996. http://www.hummingbird.com/whites/Intranet.html.

Levitt, L. Intranets: Internet Technologies Deployed Behind the Firewall for Corporate Productivity, 1996. http://www.process.com/Intranets/wp2.htp

Miettinen, J. E.. Internet Hackers Basic Tools. Hetky Ry. Helsinki 1995.

Pabrai, U. & Gurbani, V. Distributed Protocols and Security: Securing Protocols and Applications. The McGraw-Hill Companies Inc, 1996.

Pal, A., Ring, K. & Downes, V. Intranets for Business Applications; User and Supplier Opportunities. Ovum Ltd, 1996.

Remes, T. Intranetin tietoturvauhkat ja niiltä suojautuminen. University of Oulu, Department of Information Processing Science, Oulu, 1997.

Simonds, F. Network Security, Data and Voice Communications. McGraw-Hill Companies, Inc, 1996.

Siyan, S. & Hare, C. Internet Firewalls and Network Security. Indianapolis, USA: New Riders Publishing, 1995.

Telleen, S. T. The Intranet Architecture: Managing information in the new paradigm. Sunnyvale, California. Amdahl Corporation, 1996..

http://www.amdahl.com/doc.products/bsg/intra/infra.html