Intranet Security Threats from Organizational Point of View

Jorma Kajava
University of Oulu, Department of Information Processing
Science, Linnanmaa, FIN-90014 OULU UNIVERSITY, FINLAND,
E-mail: jorma.kajava@oulu.fi

Timo Remes
Sonera Corporation, FIN-00051 Sonera, Box 120, FINLAND,
E-mail: timo.remes@sonera.com

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.

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.

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) [9]. Intranets are based on Internet technology, i.e. technologies that all together generate the Internet [2]. 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 [4]. In yet another sense, Intranets could be viewed as private networks based on WWW servers [5].

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.

3. 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).

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.
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.

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.

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.

4. 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

4.1 Threats based on technology

The following list of technology-based threats is presented without further discussion.

- 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

4.2 Threats based on human activities

Hacking comprises the most serious threat for the modern society in the next decade. 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 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 enable 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).

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.

4.3 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.
5. 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 [6] 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.

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 [7], 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.

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.

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.

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 [1]. Remote access must also be carefully regulated to ensure security.

6. 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.
7. References


http://www.process.com/Intranets/wp2.htp


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