How Safe is Your Firewall: On the Security of Intranets

A.B. Ruighaver,
A. Ahmad

Department of Information Systems,
University of Melbourne
Parkville 3052, Australia
Email: tobias@dis.unimelb.edu.au

This paper contains a general evaluation of Intranet security and has been written for a non-technical IS audience. It has been published in the Proceedings of the 7th Australasian Conference on Information Systems, December 1996, Hobart, Australia, pp. 601 – 608.

How Safe is Your Firewall: On the Security of Intranets

A.B. Ruighaver,
A. Ahmad

Department of Information Systems,
University of Melbourne
Parkville 3052, Australia
Email: tobias@dis.unimelb.edu.au

Abstract

"An Intranet is an Internet behind a firewall" is a popular description of the use of Internet technology for corporate information systems. A closer examination of the issues involved, shows that the role of the firewall in the security of your Intranet is minimal. As the major advantages of this powerful new technology will also make your Intranet a preferred target for hackers, it will be necessary to improve the security of the Intranet servers themselves. As we believe that adequate confidentiality of your business-critical information can not yet be achieved, it will be safer to restrict the use of Intranets to the many non-security-sensitive applications in your organisation.

INTRODUCTION

The explosive growth of the World Wide Web (WWW) in the past few years has made it feasible to utilise this simple but powerful technology for the development of corporate information systems as well. Although Intranets certainly have become fashionable as a cheap electronic publishing system, for the distribution of newsletters, phone lists, and online manuals, it is by no means clear that this technology should also be your first choice for more business-critical information systems.

The essence of an Intranet is the leverage of Internet technology such as WWW servers and browsers to improve information exchange within the organisation. However, the improved availability of your valuable information and the lack of controls on its further distribution may make it easy for other interested parties to get access as well. To keep its sensitive information from leaking, an Intranet is normally deployed behind a firewall (Taylor 1996), which has lead to the popular definition of the Intranet as "an Internet behind a firewall".

This paper evaluates the security of Intranets from an Information Systems point of view. The first section discusses the security issues of Intranets in general, aimed to narrow down the focus of our investigation. We will then evaluate the usefulness of the firewall strategy, followed by a section on covert channels where we will look at some of the alternatives available to an outside agent trying to move information from inside the firewall to the outside world. In the final section we will examine the consequences of all these security issues with the aim of demonstrating how insecure your Intranet might be.

GENERAL SECURITY ISSUES IN INTRANETS

From a security point of view, we first have to make a distinction between the risk an Intranet poses to your internal network, including all your computer systems, and the security of the Intranet itself. When we consider the general opinion that Intranets are reasonably secure, we agree that the use of Intranets does not greatly increase the risk of intrusions in your computer systems if you have already been using Internet protocols and WWW browsers within your organisation. A complete disconnection from the Internet is no longer a feasible option, and we assume that you have already considered the obvious risks of employees downloading software or the risks of browsers using Java.

Java applets in particular are not always what they seem to be. A number of hostile applets have already been identified, and exploitation of bugs in your browser's implementation of Java may enable a hacker to connect to machines behind your firewall. Disabling Java at the browser may not be an adequate solution. A single user enabling Java again will put your entire network at risk. Blocking Java at your firewall is a better solution and will also allow the use of Java for internal Web pages.

Even though Intranets, on their own, may not put your internal network at risk, we do **not** agree, however, that any business-critical information on your Intranets is secure. In evaluating the security of your Intranet, you have to consider the following three issues:

- The availability of services provided by your Intranet.

When the availability of your Intranet is critical, you should not rely on a single WWW server. Even with several duplicate servers, the Intranet will be vulnerable to *denial of service* attacks, i.e. attacks through the network or other means aimed at bringing down your systems or your internal network. If, for example, you discover a virus on your network, you may have to bring it down until you have eradicated the virus on each computer connected to the network. This will also make your Intranet unavailable, and can sometimes last for more than a day. Distribution of your information on a CD-ROM to all critical users (in HTML form) might offer a safe alternative.

- The integrity of your Intranet.

A recent example of an intrusion at the U.S. Department of Justice, with hackers changing the name to the Department of Injustice and putting up pornographic pictures, has shown how vulnerable public WWW servers can be. Intranets, in general, will be more than just information providers and will therefore be more vulnerable. Intranets are expected to be used for information input as well, and work-flow based applications in particular may become a favourite target of hackers. As the popularity of phone phreaking has shown in the past, any opportunity to get services or products without paying will eventually be exploited by the unscrupulous hacker community. Hence, any unauthorised change to the information on your Intranet will pose unacceptable risks to your business organisation. It is crucial that you prevent and detect such changes, as well as minimise the damage such changes may do to your organisation.

- The confidentiality of your Intranet.

Keeping your valuable information secure from unauthorised access is likely to be your most difficult problem. The more people are allowed to access your Intranet from inside the organisation, the larger the risk of unauthorised access from outside the organisation. In the section of covert channels we will discuss how easy it is to move data from inside your firewall to the outside world. If you allow access to your Intranet through your firewall (most likely using encryption techniques) it may become even more difficult to detect unauthorised access by advanced hackers.

ON THE USE OF FIREWALL TECHNOLOGY

A firewall is a security system placed between your internal network and the rest of the world, commonly known as the Internet. There is plenty of information on the technical aspects of firewalls (Cheswick 1994, Ranum 1993), but good information on the management of firewalls, e.g. should I put my WWW server inside or outside my firewall, is surprisingly hard to find.

In its most simple form a firewall is simply a screening router. Any network traffic from the Internet is directed to this router, which screens each packet according to a specified security policy and forwards it to the intended internal recipient. Similarly, outgoing traffic will also be screened and forwarded. The security achieved with such simple firewalls is limited, but a simple firewall is better than no firewall.

More advanced firewalls make use of application-oriented security filters, called proxies, to augment the capabilities of the screening router. The system running these proxies is an obvious target for any hacker and needs to be protected accordingly. This highly secure system is therefore often called a *bastion*. The bastion host is situated inside the screening router and has full access to the internal network. To limit the damage a compromised bastion host can inflict, a second screening router can be used to separate the bastion from the internal network. The resulting perimeter network with one or more bastion hosts offers the most expensive and most secure firewall configuration.

As an example of how a firewall improves security, we will look at a proxy server for general WWW Internet access from within your organisation.

The communication between a WWW browser and your WWW server normally takes place using the standard TCP/IP protocol (Santifaller 1991). This protocol is used for many other network services as well. To distinguish between the different network traffic streams each packet has source and destination addresses as well as the identifiers, or port numbers, of the services on both the source and destination host that are supposed to use this data. The usual port number for WWW is 80, but other port numbers may be used as well.

For the firewall, your Intranet is just another TCP/IP service to block. The easiest solution is to block traffic on port 80 for all internal systems except to the bastion host. To enable clients within the firewall to access outside Internet servers they need to use the WWW proxy server on the bastion host. The proxy server should block all incoming WWW requests allowing only outgoing WWW requests and filters the returned WWW data before transferring it to the client. The security policy for this proxy server is, in general, concerned with transferring data from the outside world to the internal network and has little influence on the security of the Intranet. We will therefore not further discuss this policy in this paper.

With the firewall blocking all traffic on the port number you have chosen to use for your Intranet, the security of the Intranet now depends on the general security of the internal network and on the security of the Intranet server. In this section we will first concentrate on the security of the internal network. We will discuss the security of the server in a later section.

Intrusions on any of the internal computer systems may enable snooping of the internal network and, as a result, will also endanger the Intranet. Your first line of defence, therefore is to prevent such intrusions. This is the real job of the firewall. To prevent intrusions, a real firewall will need to support advanced access and authentication mechanisms based on one-time passwords and encryption, but most of all it will need constant monitoring by a competent system administrator.

Looking at the flood of possible attack strategies a firewall has to thwart (Arnold 1993), it will quickly become evident that there is no such thing as a secure firewall. Although the use of a firewall is mandatory, on its own it will generally not keep your company's network completely safe from intruders. To illustrate this, we'll examine the analogy of building security. In our current society, you can no longer leave your front door unlocked, but a door with a simple lock is sufficient to keep many unwanted visitors away. These so called door-knockers just look for easy access by checking the backdoor and the windows.

For a more professional burglar, who has probably selected your building based on externally available intelligence, a simple lock is not a problem at all. And when you put in a security door with heavy locks, a professional burglar may decide to go in through the roof or the walls or even the floor. As security becomes more important, it becomes more difficult to tell which weakness in your perimeter defence will be exploited and you'll have no choice but to resort to internal security measures as well. Having an expensive perimeter defence and no internal security will result in a waste of your resources (Avolio).

The situation becomes even more problematic when you are responsible for protecting the information resources stored in your building. How will you know whether someone has been able to access the files in any of the locked file cabinets. As long as there are no files missing you will probably assume everything is in order. A hidden camera, however, might give you some surprising new insights.

Hence, a firewall is only the lock on your front door. If you don't have anyone checking who is using the front door to get in, you will just keep out the door-knockers. The success of a firewall on preventing more serious breaches of security depends solely on the skills of your firewall administrator and on the availability of internal security and monitoring services. Without internal security, intruders will just find a way around your firewall. As several recent intrusions have shown, one employee using a modem is sufficient to endanger your whole security. Even one of your system administrators, who likes to be able to use remote administration tools from home, may have offered an opportunity to get around your firewall.

COVERT CHANNELS

As we will show now, it is not necessary for an outside party to break in to your network to get access to your Intranet. As long as the Internet itself is not secure, it will be simple to insert some code behind the firewall that allows information to be collected and transferred to the outside world. The continuing threat of viruses shows how difficult it is to prevent such attacks. And getting the data out, using a *covert channel,* is even more difficult to prevent.

A covert channel is any mechanism that can be used to communicate between two parties through secured boundaries of data. Even in systems that are considered to be secure leaking information is relatively easy, as shown by a simple illustration of this problem using a scenario proposed by Lampson (1973):

Assume the existence of a client process, requiring work to be done by a server process, and a collaborator process which intends to spy on the data exchange between the client and server with the help of the not-so-loyal server. The “confinement problem” as stated by Lampson aims to design a system which prevents the server from leaking information. Examples of subtle techniques available for the communication between the server and the collaborator include binary communication where intervals of high page faults represent a 1 and relatively few page faults represent a 0. Other binary communication channels can be implemented by having frequent versus infrequent disk accesses, or periodic surges in overall network traffic, and so on. The conclusion of this exercise was that the server can not be prevented from passing information to the collaborator.

Figure 1: Setting up a covert channel

Similar techniques can be used to transfer data through a firewall. In figure 1, all the data from the Internet is passing via the firewall before proceeding to computers C1, C2.. and so on. Renegade, outside the firewall, has been given the task of stealing confidential data from the Intranet. Assuming that the firewall is heavily guarded and monitored it would seem that the theft of data would be near impossible. Though it would appear that strict censorship of outgoing data by the firewall would prevent leakage of confidential information, any system able to monitor (part) of the traffic from the firewall to the Internet, such as Renegade, can be used to receive data from Collaborator. A simple surge in traffic caused by Collaborator at regular intervals can form a pattern that can be construed by Renegade as a message. This message will not be censored by the firewall and will in fact be nearly impossible to detect.

Of course, most covert channels do not have to go to such lengths to get past the firewall.

Any network service allowed through the firewall can be used to tunnel through, and the use of encryption can make the monitoring of those channels almost impossible. The availability of WWW services through the firewall can easily be used to transfer short messages, such as stolen passwords or the Internet address and port number of each Intranet server. Just encode the information and post it to one of the many WWW sites that allow you to leave information.

A more advanced covert channel can include the readily available code for a simple WWW proxy server, making the whole Intranet visible to the outside world. To make the tracing of access to the stolen Intranet information impractical, it can even announce itself on one of the many search engines pretending to be a legitimate WWW server.

HOW SECURE IS YOUR INTRANET ?

In the section on general security issues, we discussed the three main areas of interest for Intranets: Availability, Integrity and Confidentiality.

The availability of information systems is a security issue that will not change significantly when you move from legacy information systems to the new Intranet technology. The main difference is the increased dependency on the internal network, but adequate planning may make the impact of a network breakdown less critical. Most denial of service attacks will still involve some kind of intrusion and the firewall will therefore be your first line of defence.

The integrity of your information becomes a slightly bigger problem with an Intranet, especially when interactive applications of Intranet technology have been introduced. Adequate authentication of users, when they provide data to the Intranet server is a must. It should be noted that simple password based access control, as available on most WWW servers, does not provide adequate security. When used in operating systems such as Unix and NT to control access to computer systems, guessing or stealing of passwords has become the most common source of intrusions.

Of course, direct attacks on the computer system that runs the Intranet will also endanger the integrity of your Intranet. The firewall will again guard against intrusions on the Intranet servers from the outside world, but additional security measures on the servers to detect and protect against direct unauthorised changes of the files or database used in the Intranet will also be necessary.

Keeping your information confidential will be your biggest security problem on an Intranet. Traditionally, a hacker will try to break in to your system, i.e. become a user, because most of the valuable information on a normal computer system can only be accessed when you are logged in on the system itself. A favourite target of hackers has always been the personal mail of other users as it contains a wealth of sensitive information and may also contain data, such as passwords, that allow the attacker to move to other systems. With the use of interactive WWW technology, much of that information will move from each user’s personal mail folder to the much more accessible Intranet.

With the use of WWW technology for the exchange of information, it is also no longer necessary for a hacker to run programs on the system that contains your valuable information, to be able to retrieve it. Simple WWW tools such as webcrawlers and other WWW agents, can easily be modified to allow the hacker to retrieve data from all your Intranets using a single compromised machine behind your firewall. The hacker no longer needs to know the specific operating system you are using on each system because the same Intranet technology is available on all of them. Neither does the hacker need to study your legacy application to get access to its information. A standard user friendly interface allows a single intelligent agent program to select and access your valuable information and post it to a public noticeboard outside your organisation. Once tested, this agent can be used again and again, without modification, for any organisation a hacker would like to penetrate.

The only way to prevent these attacks from happening is to make your Intranet server a bastion as well. Use of advanced user authentication tools and encryption of network traffic, as already supported by advanced firewalls, needs to be implemented in the Intranet as well. All the bugs in your server software that may endanger its security will have to be patched. More importantly, it will be necessary to use a competent system administrator to monitor both your Intranet computer system as well as the access patterns of each user on the Intranet server.

While it is possible to reduce the users on your firewall bastion to the absolute minimum (which allows the real-time monitoring of its security status), your Intranet may involve thousands of users. This makes monitoring the security of your Intranet bastion without advanced intrusion detection tools almost impossible.

Even for normal system security, the current state-of-the-art in intrusion detection (Lunt 1993) is not strong, as evident from the few sites that actually have an intrusion detection system running. Most of the current research prototypes examine the full audit logs of a computer system to detect whether one of a series of predefined intrusions has taken place. If an intrusion does not belong to those the prototype knows about, it will not be detected.

Current intrusion detection systems also cannot warn you when the intrusion is just starting. They can not prevent the intrusion, they only warn you after the fact that an intrusion has occurred.

The Computer Forensic and System Security Group at the University of Melbourne is one of the few research groups involved in the development of real-time intrusion detection systems. Our intrusion detection system is based on neural networks capable of fingerprinting a user’s behaviour (Tan 1995). Any anomalous behaviour of the user will be detected and can be evaluated to take direct and appropriate action. As our system does not require full auditing until an malicious user has been identified, the system overhead will be minimal. A prototype for intrusion detection in Unix based systems has been successfully completed, while work on a version for NT is in progress.

We are currently extending this research to real-time monitoring of Intranet servers. Without such a tool, capable of detecting anomalies in the access patterns of your Intranet users, you may never know whether your information is being accessed illegally. Until then you will have to rely on after-the-fact statistical analysis of audit trails to find only the most obvious information thefts, those by a greedy hacker.

Until now most intrusions in computer systems have taken place by stealth. As the increasing use of multimedia has lead to the use of higher speed links to connect your organisation to the outside world we also expect the occurrence of the equivalent of *smash and grab* raids. As WWW servers are built for performance, it will not be difficult to retrieve most of their information before you notice that something is wrong. A simple attack on your firewall to compromise your screening router may be sufficient to open up your Intranet to the outside world. Only a real-time monitoring of your firewall, capable of forcing an automatic shutdown of your Intranet server, may prevent the transfer of all of your valuable information.

CONCLUSION

Intranets are still a relatively new phenomenon and reports on security-related incidents are still rare. Of course, that does not mean that there have been no incidents, as the majority of system intrusions are not reported or simply not noticed. We expect the number of Intranet intrusions to soar in the next few years. The major advantages of Intranets, such as platform independence and standard protocols, will also make Intranets a favourite target for hackers and other unwanted guests.

Firewalls alone will not offer adequate protection of your valuable data and neither will the use of advanced encryption techniques for your network traffic or for your user authentication. Real-time monitoring of your Intranet users is essential to detect unauthorised access and to abort it before too much of your valuable information has been transferred to the outside world.

There are many applications of Intranets where security is not an issue. However, until your Intranet vendor can demonstrate a track record on the security of his Intranet servers, we advise against using Intranets for security-sensitive applications. Even with a properly configured Intranet server and firewall there will be no guarantees, especially when the confidentiality of your valuable information is at stake.

REFERENCES

Arnold, N (1993) *UNIX Security: A Practical Tutorial*, McGraw-Hill Inc.

Avolio, F. Firewalls are not enough, *Data Security Letter*, number 50,
URL http://www.tis.com/docs/NetSec/Firewalls/FirewallsNotEnough.html

Cheswick, William R. and Bellovin, Steven M (1994) *Firewalls and Internet Security,* Addison Wesley, 1994.

Lampson, B.W. (1973) A Note on the Confinement Problem, *Communications of the ACM*, Vol 10, pp 513-615, October.

Lunt, T.F. (1993) A Survey of Intrusion Detection Techniques, *Computers & Security*, Vol 12., No. 4.

Ranum, M.J. (1993) Thinking about firewalls, In *Proceedings of the Second International Conference on Systems and Network Security and Management.*

Santifaller, M. (1991) *TCP/IP and NFS, Internetworking in a UNIX Environment*, Addison Wesley.

Tan, K (1995) An application of Neural Networks To Unix System Security, *In Proceedings of the IEEE International Conference On Neural Networks*, November 1995

Taylor, D (1996) Inside the firewall, *Infoworld*, Vol 18, No. 14., April 3.