



**Institut für Telematik**

unter Betreuung der  
**Fraunhofer Management GmbH**



 **Preprint 00-03**

**Techniques for Securing  
Networks against  
Criminal Attacks\***

Ernst-Georg Haffner  
Thomas Engel  
Christoph Meinel

\*Reprint of:

Proceedings of the „International Conference on Internet Computing“, CSREA, IC00, Las Vegas, Nevada, 2000

Institut für Telematik e.V., Bahnhofstr. 30-32, D-54292 Trier, Telefon +49 (0)651-97551 0

Die Verarbeitung oder Vervielfältigung der Inhalte/Daten in jedweder Form ist ausschließlich mit schriftlicher Zustimmung des Instituts für Telematik gestattet. Die Wiedergabe von Inhalten ist nur bei Nennung der Quelle erlaubt. © 2000 Institut für Telematik e.V.



Authors	Ernst-Georg Haffner Thomas Engel Christoph Meinel
Copyright	© 2000 Institut für Telematik e.V., Trier
Trademarks	All terms that are mentioned in this paper that are known to be trademarks or service marks have been appropriately capitalised. Use of a term in this paper should not be regarded as affecting the validity of any trademark and service mark. The product or brand names are trademarks of their respective owners.
Printing	06/2000
Document status	Version 2.1 (11.8.2000)
	Printed in Germany All rights reserved
	The documentation was accomplished through the Institut für Telematik. The information contained in this document represents the current view of the authors on the issues discussed as of the date of publication. Because the mentioned enterprises must respond to changing market conditions, the results of this paper should not be interpreted to be a commitment on the part of the authors. Any information presented after the date of publication are subject to change. The right to copy this documentation is limited by copyright law. Making unauthorised copies, adaptations or compilation works without permission of the authors or institutions mentioned above is prohibited and constitutes a punishable violation of the law.

The main Internet security problems nowadays can be reduced to three major fields: Hackers have software programs that scan automatically networks for security weaknesses, more and more PC's are connected directly to the Internet without using security mechanisms and E-Commerce paradigms require high quality consumer access that contradicts security objectives.

As we will show in this preprint, several means of defense can help to prevent hackers from successfully compromising a network. We will present classes of technical and organizational solutions to avoid criminal attacks. One central aspect will be the use and the integration of the Lock-Keeper™ Principle as part of modern security architectures.

## **Techniques for Securing Networks against Criminal Attacks**

Ernst-Georg Haffner  
Thomas Engel  
Christoph Meinel

### **Introduction**

Due to the breath-taking growth of the Internet, especially of the WWW, not only the chances but also the security risks are more dangerous than ever before. More and more computer systems are connected to the net of nets to improve electronic communication, business-to-business applications, E-Commerce and information retrieval. The manifold possibilities and conveniences of the connection with the Internet lead tacitly to an increasing dependency of being online, not only for commercial activities but also for the private way of life.

- There are three main reasons for reconsidering security aspects when connecting the Internet:
- Finding security holes and weaknesses of networks can be automated so that criminal attacks require not too much special knowledge of protocols, of company's internals or of general programming abilities.
- The Internet community is growing very fast and even private households have flat rates from the ISP's and are connected directly to the Internet without any further security mechanisms (like Firewalls).
- The WWW becomes a market place and many people believe in the possibilities and advantages of E-Commerce. Security considerations are counter-productive: they restrict consumer accesses, they decrease user perceived latencies and they reduce - apparently and at short notice - the gain of commercial activities.

The aim of this paper is to show techniques to overcome the problems above. Especially, we will describe the *Lock-Keeper*™ as an adequate tool for high security requirements. Therefore, we will present the major technical solutions to secure networks from hacker attacks at first. Then, we will compare the classical Firewall mechanisms to the new evolved Lock-Keeper™ principle. In the next section, the main organizational mechanisms to prevent attacks from the outside world are described. A short summary closes the preprint.

### **Technical Devices to Repel Criminal Attacks**

In general, the securest way to avoid attacks from the Internet is to have no data exchange with the net of nets at all. In this section, we will show two principle ideas to secure a networks against attacks while providing data exchange and electronic communication.

The classical, high quality solutions are the Firewalls, and we will compare them to the high security mechanisms of the *Lock-Keeper*™, a security concept designed and implemented by the Institute of Telematics.

**Firewalls.** Firewalls act mostly as packet filters. They analyze the source and target IP<sup>1</sup>-addresses of all packets, check their TCP<sup>2</sup>-port number and reject the packets if they are not allowed to pass.

Figure 1 shows the principle mode of operation of Firewalls (symbolic description).

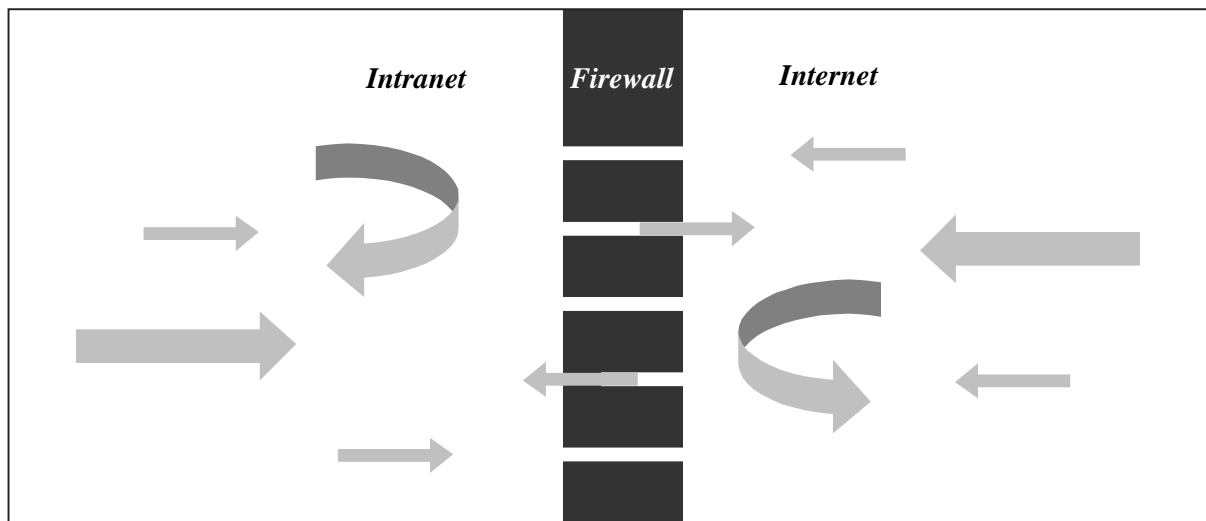


Figure 1: Mode of Operation of Firewalls

The critical aspect of these Firewalls is the meaning of their rules. Every attacker from the outside world can penetrate a Firewall if he can only pretend to be someone else who is allowed to pass. That is not too simple, but there are many possibilities to deceive this system (see [1] or [2] for an overview).

Additionally, there exist nowadays special software programs to find holes in the Firewall configuration. Most of those attacks use certain lacks in the TCP. For instance:

- TCP sequence number attack
  - Tunneling
  - Message encapsulating
  - Tiny fragment attack
  - Overlapping fragment attack
- (more details can be found in [3] and [4]).

A main problem of the Firewall is caused by the time: all packets must be filtered *online* and the decision if they are allowed to pass must happen immediately. A second problem arises from the decision criteria: as stated earlier, everyone who is able to fake his/her identity can compromise the Firewall. The advantage of the Firewall is the providing of high quality communication with several services (e.g. browsing in the Internet/HTTP, email traffic/SMTP, file transfer/FTP; references for service/program based securities are [5] and [6]).

Certainly, if there are tools to find security holes in Firewalls automatically, these tools can also be used to check and verify configuration changes of those Firewalls.

**Lock-Keeper™ Architectures.** The *Lock-Keeper™* provides data exchange between two networks, for instance the Internet and a company's Intranet, based on the idea of a lock with temporary connections. At first, a connection between the Internet and the Lock-Keeper™ is established and data is exchanged. Then this connection is cut and a connection between the Lock-Keeper™ and the Intranet is established (and vice versa). With this mechanism, data exchange happens without a permanent connection between Internet and Intranet at any time.

Figure 2 demonstrates the basic idea of the Lock-Keeper™ architecture.

<sup>1</sup> Internet Protocol

<sup>2</sup> Transmission Control Protocol

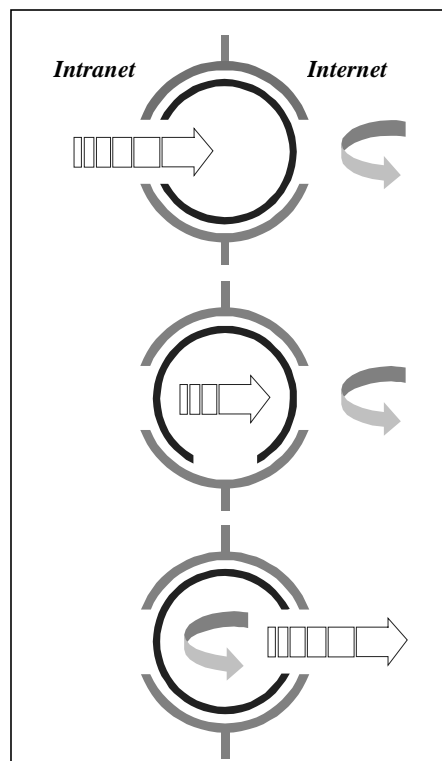


Figure 2: Idea of the Lock-Keeper™ Architecture

The main principle of the Lock-Keeper™ is that it must be *physically impossible* that both connections are established at the same time.

The advantage of the Lock-Keeper™ consists of the additional security feature: there is no possibility to compromise the integrity of the inner network (the Intranet) while attacking from the outside world (the Internet) during data exchange even though the identity could have been faked. The reason for this security enhancement must be paid by the decreased quality of service: online file transfer and email-exchange is possible, while online browsing through the Lock-Keeper™ produces too much latency.

**Common Difficulties of Firewalls and Lock-Keepers™ in Avoiding Beastware.** All kinds of *offline-attacks* or denial-of-service problems must be defended by virus scanners and mail analyzing tools independently of using a Firewall or a Lock-Keeper™ technology.

Unfortunately, *Trojan Horses* [7] - these are programs that must not be executed because they do things that the user not want to do - can hardly be found by "pattern scanning" [8]. A very strict security policy does not allow to transfer any kind of executables (or macro-programs) from one network to the other.

**Related Work .** The approach to separate physically network components has a long history. Woodward [9] and Denning [10] use the term "Security Guard" (SG) as a (hardware) link between a "low" (un-trusted) and a "high" (trusted) computer. The SG grants a "one way traffic" between two systems and a kind of "Human Review" is the central part of this structure.

Furthermore, security mechanisms that work as "Application-Level gateways" describe a class of Firewalls, which are not all-purpose gateways for a network, but provide entrance to only some defined programs. From that standpoint the Lock-Keeper™ is an Application-Level gateway. But the term does not describe how to realize such a system. Moreover, though it is clear what types of services are provided by the Lock-Keeper™, there are many possibilities - secure and insecure ones - to select the right applications to build a good Application-Level gateway.

### Organizational Strategies to avoid criminal attacks

**Knowledge Transfer.** Perhaps the most important condition for successful repelling of criminal attacks is fundamental security knowledge of system administrators and users. Administrators must not bypass the principles of their own security policy even if some circumstances tempt to do so. The security mechanisms

should not allow - with small effort - to be penetrated even from the internal network. Surveys show that the majority of all attacks come from the inside ([11], [12]). Ideally, the security mechanisms are based on hardware modules that can not be easily overridden.

The qualification and knowledge of a system administrator is the most important requirement for configuring a Firewall correctly. Often, very good products open temporarily or permanently network weaknesses due to false configuration of the administrator.

It must be inhibited that users with PC workplaces that are part of the internal network have any other possibilities to exchange electronic data without passing the Firewall and the analyzing tools (e.g. mail analyzers and virus scanners). Also, CD-ROM or diskette drives should not be available directly at the user workstations. Additionally, even the system administrators must not use modems or ISDN-devices to connect directly to the Internet.

**User Behavior.** It is most important that security considerations are understood and applied by the users who must obey them. A famous example is the password written as a tiny notice and posted beneath the screen or the keyboard. In this case, the security idea is lead "ad absurdum". Also, if personal identification numbers (PINs) are written on the credit card, their security value vanishes.

Computer users should not be afraid of using their systems due to security considerations, but some essential rules described in the according security policies have to be obeyed.

Additionally, employees who take care of security considerations can help to find weaknesses in the security policy of the company and thus improve the workflow. Certainly, the security policies of the companies have to support appropriate user behavior. For instance, if every employee has to choose a new password to login every month, it is no wonder when most of these people write down their passwords or try to find rules to generate another word every month. But then they reduce the security of the password mechanism to the security of that single rule. This might be - perhaps - more insecure than using just one password a whole year!

## Summary

Security issues become more and more important due to the growth of the Internet. Even though attackers have software tools that scan networks and find their weaknesses automatically, there are many possibilities to prevent criminals from damaging the internal systems. One solution is the use of security mechanisms like Firewalls and, for high security requirements, Lock-Keeper<sup>TM</sup>. The other is an organizational strategy to distribute the knowledge of security principles to avoid successful attacks.

## References

- [1] William R. Cheswick, Steven M. Bellovin: *Firewalls and Internet Security*, Addison-Wesley, 5<sup>th</sup> printing April, 1995
- [2] Douglas E. Comer: *Internetworking with TCP/IP: Principles, Protocols and Architecture*, Vol. 1, Prentice-Hall, second edition, 1991
- [3] G. Paul Ziemba et al.: *Request for Comments: 1858*, Security Considerations – IP Fragment Filtering, October 1996
- [4] Greg Bossert et al.: *Request for Comments: 2084*, Considerations for Web Transaction Security, January 1997
- [5] B. Costales, E. Allmann: *sendmail*, O'Reilley and Associates, 2<sup>nd</sup> edition, 1997
- [6] David A. Curry: *UNIX System Security: A Guide for Users and System Administrators*, Addison-Wesley, 1992
- [7] P. A. Karger: *Limiting the Potential Damage of Discretionary Trojan Horses*, Proceedings of the 1987 Symposium on Security and Privacy, IEEE Computer Society, 1987, 32-37
- [8] F. Cohen: *Computer Viruses: Theory and Experiments*, proceedings of the 7<sup>th</sup> National Computer Security Conference, Gaithersburg 1984, 240-263
- [9] J. P. L. Woodward: *Applications for Multilevel Secure Operating Systems*, proceedings of the NCC 48, 1979, 319-328



- [10] D. E. Denning: *Cryptographic Checksums for Multilevel Database Security*, Proceedings of the 1984 Symposium on Security and Privacy, Silver Spring 1984, 52-61
- [11] Morrie Gasser: *Building a secure Computer System*, Van Nostrand Reinhold, 1988
- [12] Kare Presttun: *Security in Distributed Data Systems, Secure Information, Secure Communication*, Springer-Verlag, 1994, 251-259