IT-SERVICES

Institut für Telematik

unter Betreuung der
**Fraunhofer-Gesellschaft**

Security Solutions

**Lock-Keeper™**
**Security Architecture**

# Lock-Keeper™

German Patent No. 198 38 253.7-31

IT-Services s.à.r.l, 25C, boulevard Royal, L-2449 Luxembourg, Telefon +352 46 13 3 13 - 01, Fax +352 46 13 3 13 - 09, http://www.it-services.lu/

**The**

# *Lock-Keeper™*

**Architecture**

| | | |
|---|---|---|
| Authors | | Dr. Ernst-Georg Haffner<br>Dr. Thomas Engel<br>Prof. Dr. sc. Christoph Meinel<br>Gerhard Müllenheim<br>Michael Noll<br>Thomas Wagner |
| Copyright | | © 2001<br>IT-Services, Luxembourg |
| 60<br>Trademarks | | 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 | | 10/2001 |
| Document status | | Version 1.1 |
| | | Printed in Luxembourg<br>All rights reserved |
| | | The documentation was accomplished through IT-Services sàrl.<br>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 is subject to change.<br>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.<br>All Graphics are created and copyrighted by IT-Services. |

## Contents

Addendum:

### Integrating Lock-Keeper™ - the gatekeeper technology into modern security architectures

Dr. Ernst-Georg Haffner
Dr. Thomas Engel
Prof. Dr. sc. Christoph Meinel
Gerhard Müllenheim
Michael Noll
Thomas Wagner

The threats originating from the Internet are ever-increasing and far from being "under control". Modern security is designed to protect the vast range of business communication facilities from external as well as internal intruders –so-called "hackers". To this effect, various defensive mechanisms have been developed to protect company data and systems from unauthorized access. To achieve this, a multitude of security levels is assigned to the applications and utilized. These security levels define the authorized activities. The lowest security levels permit all protocols, while higher security requirements restrict potential applications. These are usually verified by *Firewalls*. At the upper end of the security scale, communicating networks are physically separated. The authorized protocols are restricted accordingly. This review introduces an option for highly secure data exchange - the *Lock-Keeper™ Architecture*[1] and explains how it can be integrated into complex security structures.

## 1. Introduction

Computers are increasingly networked via the Internet on a global basis. This results in ever-expanding possibilities for data-transfer for a wide spectrum of purposes and goes hand in hand with ever more demanding business computer communications requirements. Today, it is virtually impossible for any company to operate without having access to the gigantic data volume stored on the Internet. Even the internal – often encoded - data-exchange between the subsidiaries of large corporations is frequently handled via the network of net works.

Consequently, data format quality expectations are getting increasingly stringent. While modern media does improve the usability of the information they carry, they also require broadband transfer channels.

Today's multitude of information exchange options does, however, go hand in hand with increased risks. The Internet connections of institutions, government offices and businesses via open lines create dangerous opportunities for attacks. Consequently, security policies are being drawn up to safeguard the integrity of company-owned data, verify the authenticity of communications partners and to guarantee wire-tapping and manipulation security during data exchange.  Depending on the safety needs of the respective user, these documents stipulate different electronic data interchange and employee rules and regulations. In large corporations, however, the same security requirements cannot be applied to all departments. Instead, the security policies of these organizations assign different security levels to different areas. The policy has to define, case-by-case, what communication goals are to be attained under which security measures. To this effect, difficult and crucial decisions and often compromises must be made.

In most cases, firewalls are the tools utilized to attain these electronic information exchange security infrastructure objectives. These systems work a bit like a filter: They are set up to allow access by authorized and authenticated users[2] via permitted protocols only. In this review we will also introduce the Lock-Keeper™ - a gatekeeper system – and the security options it provides. This product was developed by the Institut für Telematik (Institute for Telematics). It guarantees higher levels of security and completely prevents specific intruder attacks by physically separating the communicating networks. We will also show what areas

[1] The patent proceedings for the Lock-Keeper™-Architecture have been filed under patent number 198 38 253.7-31.

[2] In most cases, the verification of the source computer system is also accepted in lieu of user authenticity.

of security architectures are suitable for performing an adequate analysis of incoming and outgoing data.

We will initially discuss the potential attack vulnerabilities of business networks in the following sections of this review. Moreover, we will take a look at the basic security policy issues (section: "Data Network Attacks"). In a later section we will evaluate various approaches to the defense against such attacks that result in the creation of complex security architectures (section: "Defenses Against Attacks"). The focus of this analysis will be on the performance of Lock-Keeper™. A synopsis and a preview of future activities conclude the review.

## 2. Data Network Attacks

### Attack Classification

To adequately rate and evaluate data network attack prevention technologies, we will first take a look at the most important aspects of modern security concepts.

To this effect we are differentiating between internal (inner network, "IN") and external (outer network, "ON") computer networks. The IN contains all types of confidential company, government office or institutional information that must be protected. The ON is a network or a consolidation of networks designed for data exchange with communications partners. The Internet is a prime example of such a network. Company-owned Intranets or LANs are INs. Network structures can, however, be more complex than that. Larger companies and corporations can also model their data-exchange via INs and ONs.

One of the security aspects in this context – and not the only one by far – focuses on how the data exchange between IN and ON can be protected against possible external attacks (from the ON). Nonetheless, users are well-advised to remember that as a matter of fact most attacks actually come from the INs [1].

Possible data exchange risks: Non-verifiable sender and recipient authenticity, third party wire-tapping and manipulations and unauthorized intrusions into the IN while data is interchanged between the networks. The transferred data as such can also pose dangers for the computer network. "Viruses", "Worms" and other so-called "Beastware" ([7], [8], [9]) threaten the IN.

Given these complex and extensive threats, companies should initially compile a security policy [2] that must address the most important security issues. As stipulated in the introduction, the highest electronic data transfer security risk goes hand in hand with the highest quality of service (QoS). Users enthusiastically embrace options that give them access to all types of programs and protocols, while these scenarios give security experts grave headaches. Typical modern Internet protocols and applications, such as http, ftp, telnet, rlogin [3], smtp and sendmail [4] pose enormous risks as well[3].

### The Importance of Security Policies

To compile a specific security policy that provides a foundation for defenses against internal and external attacks, potential attacks must classified. It is also essential to define what defense mechanisms can adequately handle the needs of the relevant company or departments.

Computer network attacks can generally be divided into two different categories:

[3] For information on general Unix security risks see [5].

An online attack is a very dangerous type of attack. The intruder accesses the internal network systems via the net interactively, which allows him to copy sensitive data and obtain passwords via a direct channel.

Most PCs offer administrators certain services (such as *telnet* or *ftp*) that allow Internet interactions. While the administrator will enjoy the fact that he or she can easily log into other Internet-linked PCs from his or her PC, this service also allows potential hackers to disguise themselves as administrators and manipulate the system.

Attackers primarily utilize so-called session-loggers to obtain third party passwords or get an idea of a person's profile by monitoring the target's social environment. This usually allows them to "guess" the password after just a few attempts. Another scenario frequently exploited by hackers is what experts refer to as "security holes" or "security bugs" in applications or operating systems. More complex program codes also increase the potential for back doors and security holes. At the time new software is released the "holes" in the software are generally not known since it is impossible to anticipate all of the potential vulnerabilities of new software.

A few comments on the offline attack mechanisms produced by small program fragments that are "sneaked" into the system where they act independently reproduce themselves and send data out or render the system operational. Computer viruses, (Internet) worms or Trojan horses – referred to as beastware – are examples of such independent programs or executable code fragments. In the past few years, new viruses and virus mutations have surfaced again and again. Over time, they have become more intelligent and more devastating.

In the interim, a series of tools and analysis tools that are capable of identifying and eliminating known beastware have been developed (virus scanners, mail analyzers etc.,) but it is important to remember that nonetheless the security risks for any executable code remain.

From an informative theoretical point of view the fact that a program is principally incapable of determining what actions a certain type of software can execute creates a virtually irresolvable problem. And this does not just apply to automatic beastware analysis: How do we expect a human administrator to evaluate all of the effects of a program, utilizing a multitude of entry values (if, for example, an endless volume of tests is required)?

Consequently, the concerns of corporate security experts who do not allow the introduction of unknown external software into the company-owned network and impose very stringent measures to prevent various compilation, adaptation or decoding processes from changing simple ASCII text into a piece of independent software, are absolutely justified. Within the framework of clearly defined security policies all users can usually be convinced of the necessity of such restrictions, especially in high security areas.

Table 1 below provides a brief overview of potential attack classes and shows if the attack is an online attack during which the intruder accesses the IN systems interactively via the net (also refer to [2]).

This classification shows that there are numerous ways to attack an IN. In mere numbers, offline attacks via beastware are now the most widely spread types of attacks, whereas online attacks are considered the most dangerous since they potentially threaten the overall integrity of internal networks.

| Class | Description of the Source | On-line |
|---|---|---|
| Password Theft | Passwords are located in clear text files or obtained from the IP level by listening in. Dictionary attacks guess passwords systematically. | ✓ |
| Social Engineering | Passwords are consciously or unconsciously transferred during human interaction (e.g., via phone). | ✓ |
| Bugs and Backdoors | Software performs erroneously, conscious deviation from program specification by the programmer or new backdoors created by viruses and worms. | ✓ |
| Authenticity Error | Programs show log in screen in the IN and send passwords to the ON. | ✓ |
| Protocol Level Error | Security gaps in the TCP protocol, such as TCP sequence number attacks; tunneling; message encapsulating; „tiny fragment attacks; overlapping fragment attacks [6]. | ✓ |
| Offline Attack (primarily denial-of-service) | Worms, Trojan horses and viruses (beastware) have the capability to hamper the IN's functionality or even destroy it. IN data may also be transferred to the ON. | -- |

Table 1: Potential Network Computer Attack Classification

### Psychological Factors

Interestingly enough in addition to technical relevance, psychological factors also play an important role when security measures are being implemented. The feeling of "security" is not a mere enhancement or a side effect in today's information and communication-driven workplaces. A system that convinces from a security-technical point of view can confuse the people concerned if the relevant security policy reveals gaps and pending issues. The clarity and comprehensiveness of the security concept stipulated in the security policy plays a central role in this context.

## 3. Defense Against Attacks

### Firewalls

As indicated earlier, firewalls have established themselves as crucial tools in providing network security in recent years. A firewall consists of a collection of components between two networks with the following attributes:

- Data interchange between both networks must pass through the firewall in either direction.
- Only authorized data interchanges that comply with the applicable security policy are permitted to pass through the firewall.
- The firewall as such cannot be attacked (see [2])

### Principle and Functionality

Almost all firewalls are based on the package filtering principle. They analyze TCP/IP[4]-packages by verifying the sender and the recipient through the IP address, the monitor the TCP port to ensure that the selected service is also authorized for use. There are, however, various methods that allow others to bypass the analytical mechanisms of a firewall.  Manufacturers try to eliminate errors and close security gaps in the construction of a firewall as quickly as possible. In addition to the actual firewall, the operating system it is based upon, for example, also provides opportunities to attack and compromise the system.

Moreover, a conceptual weakness of the firewall can enable unauthorized parties to access the IN from the ON despite firewall protection. The root of the problem is in this security measure's basic functionality: A firewall must differentiate between authorized and unauthorized requests. It must authorize the former and deny the latter. During highly criminal attacks, the unauthorized attacker usually falsifies the access information to obtain authorized access and is therefore in a position to pass the firewall unhindered. In other words, the functional principle of this system poses an inherent security risk.

[4] **T**ransmission **C**ontrol **P**rotocol/**I**nternet **P**rotocol

# 4. The Lock-Keeper™ Architecture

## The Idea

Many companies, such as for example banks, have such enormous security requirements that standard IT security measures are no longer sufficient. In these cases the Lock-Keeper™ system provides a high security enhancement for data interchange between two networks. It may even offer an alternative to conventional firewall solutions.

The Lock-Keeper™ principle was developed to find a way to exchange data between an internal high security network and an external, less secure network, such as for example, the Internet without having to create a direct connection, even if such a connection would only have to be created for a short time. Based on a rather trivial mechanism, i.e., the transfer of data between the networks via discs, the idea to develop a solution that allows the automated exchange via disc was conceived.

To this effect, the Lock-Keeper™ is based on a well-known and simple mechanism: It works like a sluice. Just like a ship sluice, the Lock-Keeper™ passes data through its gates without ever allowing a direct connection between the internal and external network.

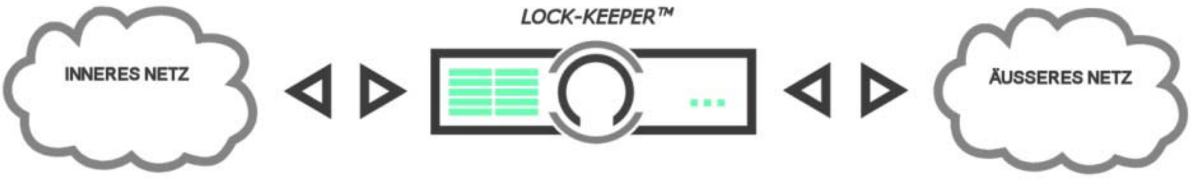

Fig. 1: Topology of Lock-Keeper™ Sluice Technology

## Network Data Exchange – How it works

The actual internal Lock-Keeper™ consists of three active PC-based components. The internal Lock-Keeper™ PC is connected with the internal high security network of the company. The external PC is connected to the less secure network, e.g., the Internet. The third Lock-Keeper™ PC, which provides the actual lock function, is set up to perform a detailed analysis of the traffic passing through. Additional components can be docked to the Lock-Keeper™.[5]

The internal Lock-Keeper™ components are connected to a patented* switch plate that restricts communication to a maximum of two LK-PCs at a time. This is ensured by switch relays (electronic switches) on the plate that switches between the connections on a physical level, i.e., interrupts the data cable power cycles.

[5] see section "Combined Security Architectures", practical examples

Consequently, the switch mechanism has dual defined status:

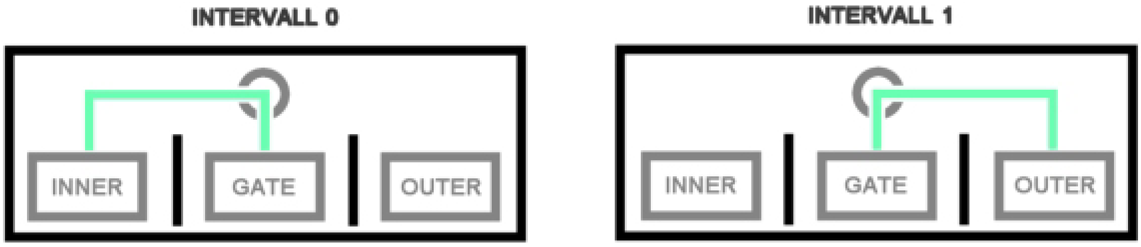

Fig. 2: Lock-Keeper™ Switch Status, <Inner> represents the computer pointing to the inside, <Outer> represents the computer pointing to the outside, <Gate> represents the computer acting as the central internal Lock-Keeper™ computer.

The lock control or the switch relay is autonomous and cannot be changed or disengaged by someone who has access to the rest of the system. Consequently, neither external hackers nor well-trained insiders are in a position to eliminate or by-pass the physical separation of the networks.

Example <User A sends e-mail via the Internet> shows the Lock-Keeper™ data transfer process quite well (see Fig. 3, below):

**Example: Sending Mail**

User A, an employee of a company utilizing the Lock-Keeper™ system sends an e-mail message to the Internet from the secure company network.

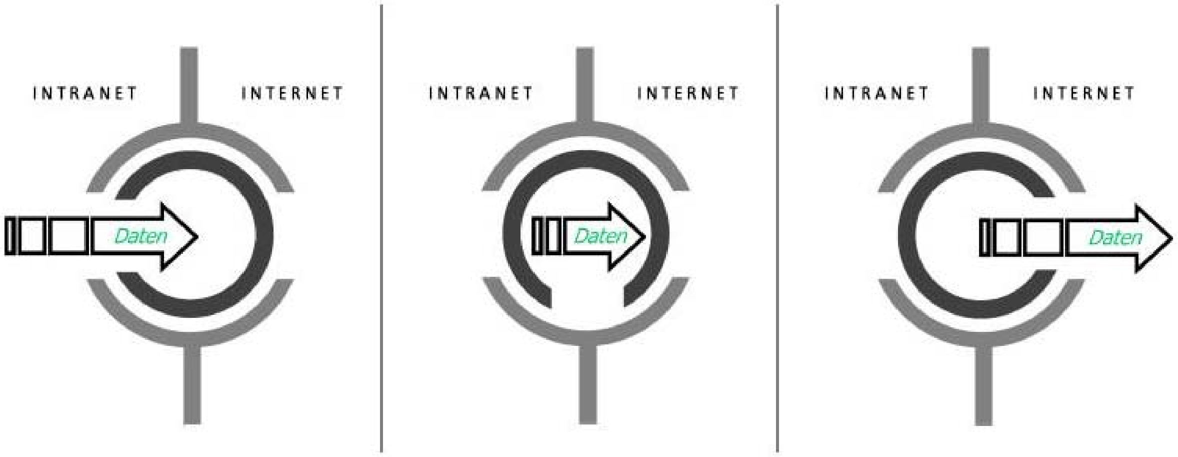

Fig . 3: The Lock-Keepers™ Function

In a first step, the user data packets (the e-mail) are send to an internal mail server that transfers them to the Lock-Keeper™. The Lock-Keeper™ stores the data on the computer pointing to the internal network. It verifies if there actually is a connection to the central computer. In the event that it cannot detect a connection it waits until the switch plates switch the lines. Now the mail is sent to the actual sluice computer (center) where it is

analyzed based on the needs and security requirements before it is allowed to make its way to the Internet. Once it has successfully passed the security check (e.g., virus scan) the central computer verifies if a connection to the outer computer, which is connected to the Internet, is in place. If this is the case, the mail is transferred and can now be forwarded to the recipient via the Internet.
There is no direct physical connection between Internet and Intranet for the duration of the transfer process described here, since unlike Firewalls, the Lock-Keeper™ doesn't just separate the data transfer on the application or protocol level, but actually interrupts the line power circuits.

Consequently, lock technology such as the Lock-Keeper™ system is immune to online attacks (see 2.2), since the pertinent security concept doesn't separate authorized from non-authorized requests (as a firewall does, see 3.1). Instead, it always stores any type of data movements between IN and ON in an intermediate memory, thus preventing all direct attacks. It does this regardless of whether an optional analysis is performed or not. On the other hand, this also means that it is hard to obtain certain services that require direct and unobstructed connections between computer networks through the Lock-Keeper™ or cannot be provided at all. In the preview we will discuss future developments and existing solutions for this area.

## 5. Firewall and Lock-Keeper™

### Firewall - Strengths

As indicated earlier, firewalls are the current standard IT security tool. The advantage of firewall technologies is their ease of use combined with relatively high levels of security. Firewalls now offer a very wide spectrum of supported functionalities and/or protocols and thus also a high standard of service quality.

Security level increases go hand in hand with reduced numbers of protocols and applications that may be authorized. In any event, however, firewall applications always allow an actual connection on the lowest layer of the network, i.e., on the "physical layer" and on the "data link layer"[6].

### Areas of Attack

It goes without saying that the ease of use that firewalls provide thanks to their large functionality affects their security standards adversely. Even though they are the standard IT security tool, firewalls have a large number of security holes and consequently pose certain risks.

i) Risk factor people

One of the central components in the operation of a firewall is the security policy. It provides the foundation on which the firewall is built, configured and operated. The enforcement of the policy frequently falls prey to lack of personnel or lack of sufficiently trained personnel. Regular maintenance and loading of security patches are just as important as the compilation of the policy and as such should only be performed by specially trained experts.

[6] vgl. OSI-Reference Model

ii) Risk factor technology

It is very hard to anticipate technological vulnerabilities. Software products (firewalls) that consist of more lines of programming code) have a greater potential for errors that are hidden in the program, regardless of whether these errors are logical or programming errors as such. These errors or "bugs" can be quite helpful to hackers trying to break in. The basic operating system on which the firewall software runs can also contain errors and consequently create "security holes".

Yet another weak area of software-based security solutions is the fact that the post-crash status is undefined. In the event of a power loss that has initiated a restart of the software, for example, the system can end up in an undefined state, which, depending on the circumstances may safeguard the functionalities of the computer, but not the security.

**Lock-Keeper™ - Strengths**

As discussed earlier, the Lock-Keeper™ lock mechanism separates the networks physically, eliminating the online status.

Consequently it is impossible, even for insiders, to neutralize or by-pass the security barrier of the network hardware separations. Software as well as accidental or intentional errors in system configurations cannot establish a direct connection through the lock because of the way the system is constructed.

In a worst-case scenario, faulty software components or incorrect and insufficient configurations can only adversely affect the data exchange as such, while the integrity of the internal network data is not endangered at any time.

Thanks to the lock concept, a crash or an attack cannot create a scenario that will connect the two networks directly with each other, since the relays stay in a defined state even after a crash (either an internal or an external connection).

**Security Versus Ease-of-Use**

We have already emphasized the fact that the Lock-Keeper™ doesn't have an online status thanks to the physical separation of the networks. Obviously this means that intended protocols also can not be run directly through the Lock-Keeper™ since they are based on online connections.
A study that we conducted did, however, reveal that most scenarios can be realized through the Lock-Keeper™ without making the application that much more difficult.
To this effect, it is, for example, not only possible to transfer mail and files via then Lock-Keeper™, but also to create a galvanized separation from the network for the internal company database that feeds data into, e.g., the website. Moreover, an encoded connection (e.g., VPN) can be realized with the help of the Lock-Keeper™. In this case the Lock-Keeper™ computers pointing to the outside act tunnel end points (see practical examples).

Services that depend on a permanent online connection are hard to protect or cannot at all be protected by the Lock-Keeper™. For example, it must be decided on a case-by-case basis whether sensible Internet surfing activities should be implemented through the Lock-Keeper™, since there is at least a two switch interval delay before the user receives a response (via cache-proxies). On the other hand, it should be evaluated if surf PCs should indeed be positioned in a high security network.

In other words, the price that must be paid to attain a secure defense mechanism against online attacks is a loss in quality of service standards. Multi-layered security architectures offer a way out of the dilemma. They allow a company to divide its own network into several sub-networks. These sub-networks are then – depending on the security level – protected by a firewall or a Lock-Keeper™. It goes without saying that firewalls and Lock-Keepers™ can also be used in combination.

### Combined Security Architectures

Typically, the IT architectures of companies with LAN Internet access are equipped with firewalls as well as virus scanners and mail analysis tools.

Since the Lock-Keeper™ consists of three internal computers each application that is currently on the market and can be loaded on the basic operating system can be installed. Several products (such as, for example, virus scanners) have already been thoroughly tested for utilization with the Lock-Keeper™.
The Lock-Keeper™ itself does provide one hundred percent online attack protection thanks to the physical separation of the networks. Moreover, it offers the option to avert off-line attacks, since the data can be evaluated for viruses, worms and Trojans on an as-needed basis as it passes through the Lock-Keeper™.

## 6. Practical Examples

The following paragraphs show a few practical examples of Lock-Keeper™ applications. Basically, virtually any service can be transparently utilized via the Lock-Keeper™ as long as it can be realized based on the <store and forward> principle.

### Mail Transfer via Lock-Keeper™

The most frequently utilized Internet service is electronic mail, which also provides a classic practical example for a typical Lock-Keeper™ application. Mail exchange can be performed transparently in both directions if the mail is transferred via the Lock-Keeper™ in the same fashion as proxies. The time delay doesn't really matter in this case since it is usually irrelevant whether mail arrives for example two minutes later.

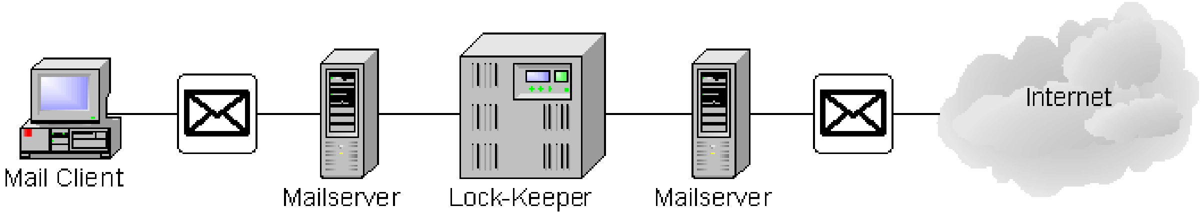

Abb. 4: Practical Example Mail Transfer

### File Transfer via Lock-Keeper™

Similar to e-mail transfer, file-transfers can also be automatically transported offline via the Lock-Keeper™. In this case, the data are, for example, copied into one or several folders, from where they are transferred by the Lock-Keeper™.

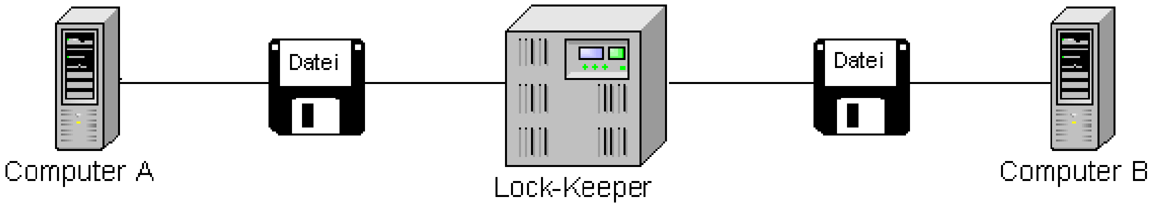

Fig. 5: Practical Example File Transfer

### Database Alignment via Lock-Keeper™

In this scenario, the Lock-Keeper™ is positioned between the actual database server of the company that contains all relevant (and possibly also very sensitive) data. The Lock-Keeper™ now offers the option to transfer data from the main database server (A) to the web server. This is done through a second database (B) that is connected to the web server online and that receives its data offline from main server A via the Lock-Keeper™. Consequently, all relevant data is immediately available when a website is accessed. There is no delay. Meanwhile, web database B aligns its data with main database A in regular time intervals.

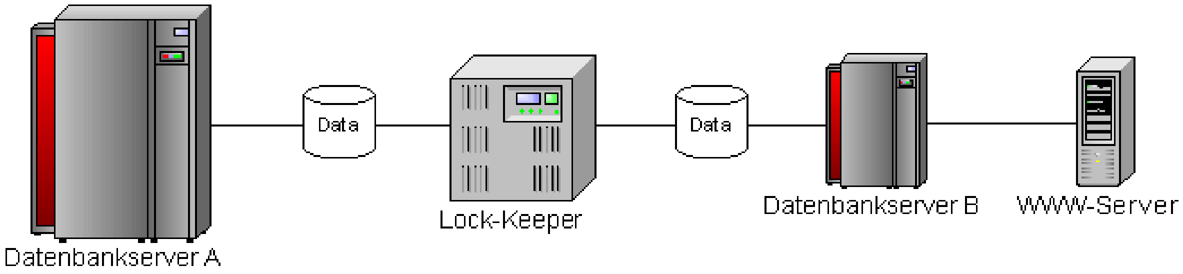

Abb. 6: Practical Example Database Alignment

### Secure Connections Between Two Companies

Given that Internet connections between two companies basically open a new door into an open network, such connections pose the same risks as the Internet does on its own. Besides the fact that data exchanged could be highly sensitive and should not be made available to third parties, there is a possibility that a potential attacker abuses the connection to a trustworthy partner company and gains access to the internal company network through this line.

The first problem can be resolved if an encoded connection (such as VPN) is established between the two companies. But the problem of a direct online connection between the two businesses remains – even if the connection is encoded – i.e., the risk is still there.

A combination of both solutions allows users to enjoy the benefits of an encoded connection while getting added security, thanks to the physical separation of the networks.

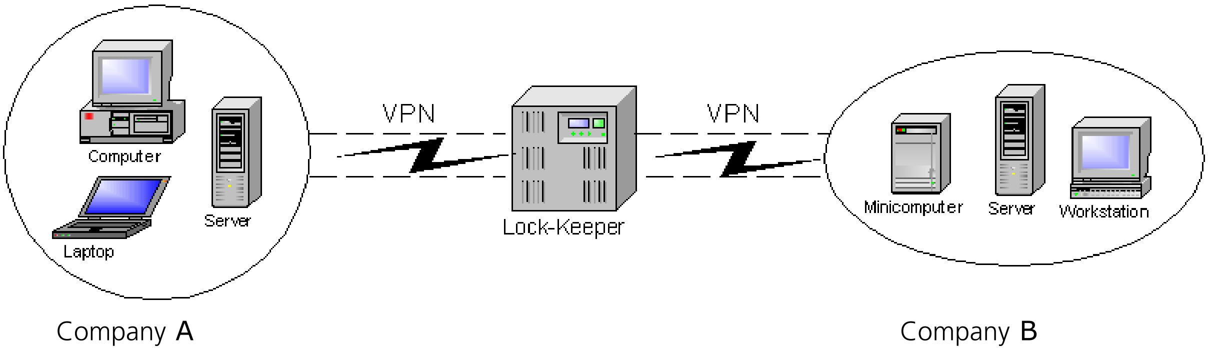

Abb. 7: VPN Connection Between Companies

### Summary and Preview

The development of modern security architectures must be driven by the changing and growing demand for electronic data interchange. Versatile and multi-medial information transfer does, however, trigger extensive vulnerabilities that come in just as many forms and expressions. The assignment of different security levels allows the harmonization of quality of service expectations and relevant security requirements. To this effect, a very wide pallet of security components that can be implemented should ideally be taken into account. In addition to and as an enhancement of conventional firewalls, Lock-Keeper™ infrastructures are now available that make secure data interchange a reality.
This review showed the basic functionalities of these systems and explained their integration into complex security architectures. We have also provided an insight into complex expansion options that allow users to overcome time constraints or service restrictions.
Options that allow for time-delayed handling of services that usually require a direct connection between the data exchange networks are currently under development to be later released as sluice technology upgrades. These developments could possibly prevent the current quality of service restrictions.

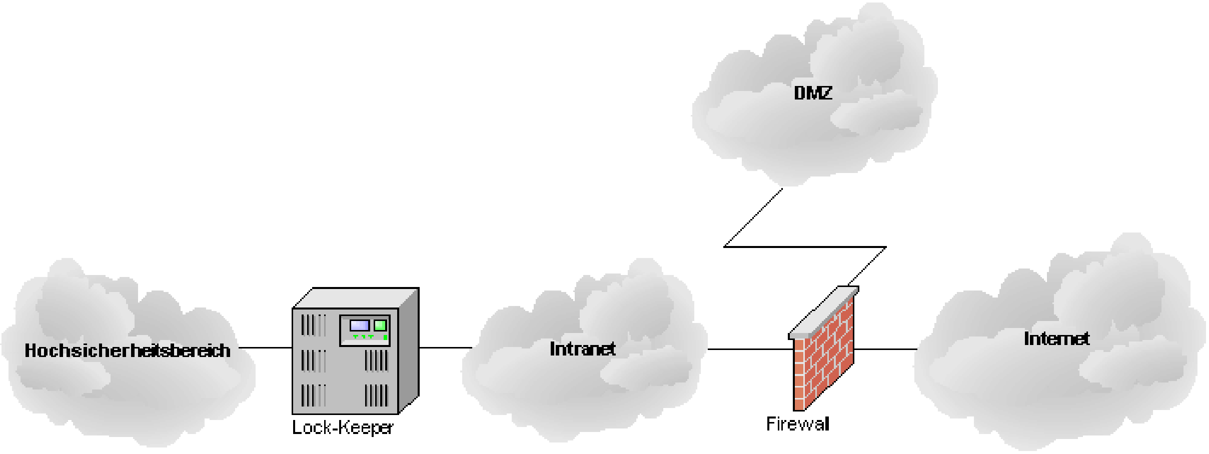

Fig 8: Utilization of the Lock-Keeper™ in conjunction with a firewall, protecting a high security area and an Intranet.

## Addendum A: Technical Specifications Lock-Keeper™

| Description | Specifications |
|---|---|
| Measurements (H x W x D ) | 86 x 482 x 573 mm (19'' 4 HE) |
| Operating power<br>Rated power<br>Frequency<br>Output | 230 V AC ± 5 %<br>0.5 A<br>50 Hz<br>350 W power adaptor |
| Ambient temperature (during operation)<br>Ambient temperature (during idle phase) | 10-30° C<br>0-40° C |
| | |

### Lock-Keeper™ System

| Description | Specifications |
|---|---|
| Internal computer cards<br><br>Lock-Keeper™ | <br><br>3 x CPU SBC PC Industrial Insertion Cards<br>3 x IBM IC35L040AVER07 7300 rpm UDMA<br>TI-LK Control plate v1.4 |
| Hardware Specification per PC card | Intel Pentium LowPower 266 Mhz<br>64 MB SDRAM |
| Connections (per card) | RJ45 FE<br>PS/2 keyboard<br>Monitor, 15 poles (3x5)<br>Serial, 9 poles (Console) |
| Operating System | SuSE Linux v. 7.2 |
| Max. internal data max. internal data penetration | 115.200 bps, serial (Lock-Keeper™ Basic)<br>100 Mbps, FE (Lock-Keeper™ Advanced) |

## Addendum B: Literature

[1] Morrie Gasser: Building a secure Computer System, Van Nostrand Reinhold, 1988

[2] William R. Cheswick, Steven M. Bellovin: Firewalls and Internet Security, Addison-Wesley, 5th printing April, 1995

[3] P. Gulbins, UNIX Version 7, bis System V.3 (Unix Version 7, to System V.3) , Springer-Verlag, 1988

[4] B. Costales, E. Allmann: sendmail, O'Reilley and Associates, 2nd edition, 1997

[5] David A. Curry: UNIX System Security: A Guide for Users and System Administrators, Addison-Wesley, 1992

[6] G. Paul Ziemba et al.: Request for Comments: 1858, Security Considerations – IP Fragment Filtering, October 1996

[7] Klaus Brunnstein: Beastware (Viren, Würmer, trojanische Pferde) Paradigmen Systemischer Unsicherheit, Sichere Daten, sichere Kommunikation, Springer-Verlag, 1994, 44-60 (Beastware (Viruses, Worms, Trojan Horses) Paradigms of Systems Insecurity, Secure Data, Secure Communication)

[8] F. Cohen: Computer Viruses: Theory and Experiments", proceedings of the 7th National Computer Security Conference, Gaithersburg 1984, 240-263

[9] 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

## Contact

**IT-Services s.à.r.l.**
**25C, boulevard Royal**
**L-2449 Luxembourg**

**Tel:** +352 46 13 3 13 – 01
**Fax:** +352 46 13 3 13 – 09

**Web:**http://www.it-services.lu/

**General Information:**
info@it-services.lu

**Join our team:**
jobs@it-services.lu