published as: F. Cheng, Christoph Meinel, Th. Engel, G. Müllenheim, J. Bern, D. Thewes: A Complete Solution for Highly Secure Data Exchange: Lock-Keeper and its Advancements;
Proceedings of the Fourth International Conference on Parallel and Distributed Computing, Applications and Technologies (PDCAT 2003);
IEEE PDCAT 2003, Chengdu (China), 2003, pp. 201-205.

A Complete Solution for Highly Secure Data Exchange: Lock-Keeper and its Advancements

Feng Cheng, Christoph Meinel ,Thomas Engel,
Institute of Telematics,
University of Trier, 54292 Trier, Germany
Email:{cheng , meinel, Engel}@telematik-institut.de
Web: www.telematik-institut.de

Gerhard Müllenheim, Jochen Bern, Dominik Thewes
IT-Services s.à r.l.
25c, boulevard Royal, L-2449 Luxembourg
Email: {muellenheim, bern, thewes}@it-services.lu
Web: www.it-services.lu

Abstract-The Lock-Keeper is a new network security solution which can provide secure data transfers between two different networks without having to establish a direct physical connection. By means of the Lock-Keeper system, the possibility of direct attacks to the protected network can be eliminated. An actual system, the SingleGate Lock-Keeper, is used as an example to introduce the Lock-Keeper concept in detail, including its architecture[1], functionalities, applications, vulnerabilities and benefits. Based on this system, a new advanced DualGate Lock-Keeper including another "gate" unit is proposed that can provide more efficient and secure data exchange and make extensions of the Lock-Keeper applications possible.

Keywords: Network Security, Physical Separation, Data Exchange, Lock-Keeper, Gate

1. Introduction

With the development of network technology, more and more computers are connected to open networks such as the Internet. This is the result of an ever-growing need for information exchange for businesses, government offices, academic researchers and various other users and also results in ever-expanding possibilities for data transfer. In other words, nowadays, there are a lot of important and confidential resources on the web easily available to employees, partners, customers, contractors, or even everyone else. However, all these data flows over public networks have also created many dangerous opportunities for attacks. Whenever data are transferred on the web, especially between a company's internal network and an outside source, there are multiple risks, for example viruses, worms, unauthorized accesses, etc. Thus, the task of securing private data and simultaneously permitting secure data exchange has become a primary problem for most network applications.

Today, a large number of security technologies, such as firewalls, anti-virus tools, or intrusion detection systems, are offered to protect the data exchanges and electronic communications. Nevertheless, in spite of the ubiquity and constant development of such solutions, networks and their attached resources still remain quite delicate and vulnerable. So far, all these methods are not enough to satisfy ever-increasing security requirements, and none of proposed security solutions can acquire psychologically complete trusts.

The Institute of Telematics in Germany has proposed a new security solution named Lock-Keeper in 1998 [1, 2, 3, 4]. Based on the simple principle that "the ultimate method to secure a network is to disconnect it", the Lock-Keeper can guarantee higher levels of security and entirely prevent specific intruder attacks by physically separating the communicating networks. In recent years, the patented Lock-Keeper system has been developed and improved to be more mature, dependable and applicable. This paper will introduce the Lock-Keeper and its up-to-date advancements in detail.

The next section is a review of the original Lock-Keeper system, also called the SingleGate Lock-Keeper, including the principle, implementation architecture, functionalities and shortcomings of the SingleGate Lock-Keeper. An advanced Lock-Keeper system, the DualGate Lock-Keeper, is introduced in the third section. In the last section, we summarize and add an outlook to further development of this unique security solution.

2. Review of the SingleGate Lock-Keeper System

As mentioned above, data exchange is the fundamental element and also the basic functionality of networks. To a certain extent, network security depends mainly on the security of data and its exchange. Almost all the existing security solutions, regardless of their differing implementation principles, also provide protection of data and its exchange. Up to now, firewalls have established themselves as popular and crucial tools in providing such protection [5]. This section will introduce an alternative but more complete security solution, the SingleGate Lock-Keeper system.

2.1 Lock-Keeper Sluice Technology

Firewalls are mostly based on the packet filtering principle which analyzes TCP/IP packets by verifying the sender and the receiver IP addresses. They also monitor the TCP ports to ensure that the selected service

In Proceedings of the 4th International Conference on Parallel and Distributed Computing, Applications and Technologies (PDCAT 03), August 26~28, 2003, Chengdu, China.

is authorized for use. However, there are also various methods that allow others to bypass the analytical mechanisms of a firewall. Moreover, a conceptual weakness of the firewall can enable unauthorized parties to access the internal data despite firewall protection. The root of the problem lies in this security measure's basic functionality. A firewall should be able to divide requests into authorized and unauthorized. It must authorize the former and deny the latter. During highly criminal attacks, the unauthorized attacker usually falsifies the access information by illegally obtaining an authorized access and therefore passes the firewall successfully.

Unlike firewalls which separate the data transfer on the application or protocol level, the Lock-Keeper system separates the communicating networks at a physical level. The Lock-Keeper principle was developed to find a way to transmit data between two different networks – usually classified as a high security internal network and a less secure external network - without having to establish a direct, even physical, connection, no matter how short-lived such a connection would be.

Fig. 1 The Lock-Keeper Sluice Technology

To this effect, the Lock-Keeper is based on a well-known and simple mechanism: It works like a sluice, as indicated in Figure 1. Just like a ship sluice, the Lock-Keeper system transfers data through a gate without ever creating a direct connection between the internal and external network. In this way, attackers and malign data have no opportunities to break into the internal network by any means of online attacks because of the physical network separation. From another point of view, because of this simple principle, the Lock-Keeper technology is very easy to be understood, implemented, and used. "Keep it simple, if it is complex, it's probably wrong" [6]. Such a simple, useful solution can be accepted psychologically by the confounded persons.

2.2 Architecture of the SingleGate Lock-Keeper

As an implementation of the Lock-Keeper sluice technology, a SingleGate Lock-Keeper consists of three active, autonomous, PC-based components. The innermost Lock-Keeper Computer ("INNER" in Figure 2) is connected to the internal high security network, for example an intranet of a company. The Computer on the opposite side ("OUTER" in Figure 2) is connected to the less secure network, e.g., the Internet. The third Lock-Keeper Computer, also called GATE Computer ("GATE" in Figure 2), which provides the actual lock function, is set up to perform a detailed analysis of the traffic passing through.

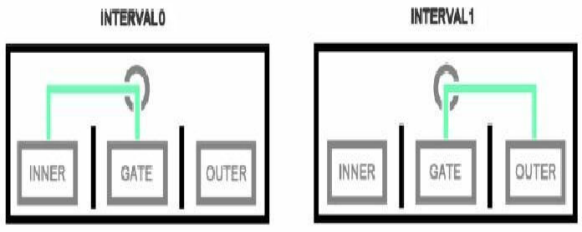

Fig. 2: SingleGate Lock-Keeper Switch Status

All three components are connected to a patented switching unit that restricts their communications. Only "INNER" and "GATE" or "OUTER" and "GATE" can be connected at any time. This is ensured, in terms of implementation, by relays (switches) on a printed circuit board (PCB) that enables and disables connections on a physical level, i.e., interrupt the data cables. The function and timing of this unit is autonomous and can not be changed or disengaged by someone who has access to the rest of the system. Thus, neither external attackers nor insiders can change or bypass the state of the physical separation of the networks.

Each Lock-Keeper Computer has its own components (CPU, RAM, a hard disk, network cards, etc) . On each computer, there are also an independent operating system and the Lock-Keeper software which implements the transfer and verification of the data. Besides these three PC-based components, the SingleGate Lock-Keeper system also contains the abovementioned PCB controlling the connections between the GATE Computer and the two other units ("INNER" and "OUTER"). As indicated in Figure 2, the switch mechanism has two defined states.

Fig. 3: The SingleGate Lock-Keeper Function

As indicated in Figure 3, the data is sent to and stored on one of the two external Lock-Keeper Computers ("OUTER" in the example of Figure 2) firstly. This external Lock-Keeper Computer verifies whether there currently is a connection to the GATE Computer available. In the event that it cannot detect a connection, it will wait until the switch connects the lines. After this step, the data is transferred to the GATE Computer where it is analyzed based on the needs and security requirements. Once it has successfully passed the security check, for example virus scanning, the GATE Computer verifies whether a connection to the other external Computer ("INNER" in the example case) is in place. If this is the case, the data is transferred and can

now be forwarded to the outside of the Lock-Keeper system.

Here, it is worth to point out that the basic operating system on the GATE Computer makes it possible to integrate some general third-party security software [6] into the Lock-Keeper system, which can provide more extensive protection to the data exchange. For example, we can install virus scanning software [7] or mail analysis tools [8] to check the data. It is also possible to install content filtering tools [9] which can provide similar functionalities as traditional firewalls. Moreover, some accounting and statistics [10] can also be done on the Lock-Keeper to monitor and record the system access and the network usage. With the help of these security measures, the Lock-Keeper Keeper system enhances the security level of the protected network.

2.3 Functionalities and Applications

As discussed earlier, the lock mechanism of the Lock-Keeper separates the lower structures of networks physically, eliminating the online status. Thus, it is impossible, even for insiders, to get across the security barrier of the network hardware separations. Crashes or attacks can never create a scenario that will connect the two networks directly to each other, since the relays stay in a defined state (either an internal or an external connection). On the other hand, software, as well as accidental or intentional loopholes in the system, can never establish a direct connection through the lock, either. In a worst-case scenario, faulty software components or incorrect or insufficient configurations can only adversely affect the data exchange as such, while the integrity of the internal network data is never endangered at any time.

Thanks to this lock concept, the Lock-Keeper provides higher levels of security and completely prevents specific intruder attacks. We have seen a variety of scenarios where the security level could be raised by the Lock-Keeper without making the application more difficult. The most frequently utilized service which can be protected by the Lock-Keeper system is data exchange, for example mails or files transfer, between internal networks and external networks. It is also a typical practical example of Lock-Keeper utilization. By the Lock-Keeper system, the most important database of a company, e.g., a web or FTP server, which possibly contains some secret and sensitive data, can be separated from other computers. Anyone, either the employee or the legal partner of a company, has to get their required data after passing the checking process of Lock-Keeper. This application can be used to implement remote access services and become a perfect substitution to current utilized VPN technology, Virtual Public Network [11], which is very complicated and expensive because of the employment of an encoded connection.

Theoretically, the Lock-Keeper system can protect almost all the network services, because it can provide a complete security protection for ordinary data exchanges.

2.4 Drawbacks

Just like the physical disconnection of the networks makes the Lock-keeper system a complete security solution for data exchanges across the networks, it also brings a lot of limitations and problems for either applications or extensions of Lock-Keeper. The file transfer through the SingleGate Lock-Keeper includes the duration of file queue, data transmit, file checking and the useless waiting time. The maximum capacity of data transmit by the current SingleGate Lock-Keeper is less than 1.3 MB/s. What is more, much time is obliged to be spent on waiting for the establishment of connections. The performance of the SingleGate Lock-Keeper is not enough to provide network services that depend on a permanent online connection. In other words, a lot of intended network protocols can not be run directly through the Lock-Keeper system. For example, web browsing, which is currently the most popular use of networks, can not be easily protected by the SingleGate Lock-Keeper, since there is at least a two switch interval delay before the user receives a response. So the most important drawback of a SingleGate Lock-Keeper is the low speed of data transfer, or in other words, the latency imposed on the data transfer is quite high.

Improving the performance of the SingleGate Lock-Keeper for data transfer and decreasing the latency has become a key to extend usability of the Lock-Keeper system. For this purpose, some possible measures for Lock-Keeper improvements had to be considered and implemented.

3. DualGate Lock-Keeper System

The development of modern security architectures will be driven by the changing and growing demand for secure data exchange. The shortcoming of the SingleGate Lock-Keeper in terms of latency limits its utilility and also provides great potentials for its improvement. In this section, an advanced Lock-Keeper system, the DualGate Lock-Keeper, will be proposed.

3.1 Architecture of the DualGate Lock-Keeper

Another GATE Computer is introduced into the SingleGate Lock-Keeper system. We call the Lock-Keeper system with two GATE Computers the DualGate Lock-Keeper.

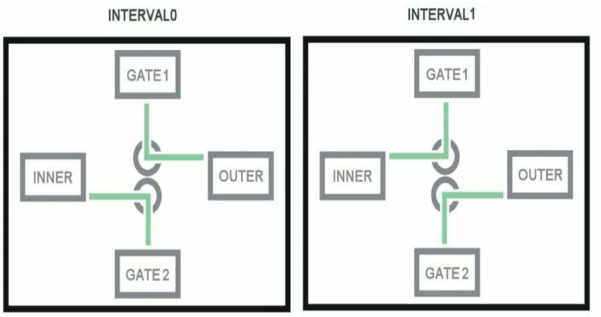

Fig. 4: DualGate Lock-Keeper Switch States

With the addition of another GATE Computer, the PCB and its switch mechanism is modified accordingly. The new principle is to automatically establish two separate, disjoint connections at the same time. As indicated in Figure 4, the switch mechanism has two defined states in that either GATE1 is connected to INNER and GATE2 to OUTER, or the other way around.

Besides modifications of the Lock-Keeper hardware, an updated core software had to be developed to control and harmonize data transfers through the two connections. A strict and proper file queuing algorithm which is responsible for generating two queues of files to be transferred on both external Computers ("INNER" and "OUTER") is also required. This is because, unlike the SingleGate Lock-Keeper which permits the unique GATE Computer to choose the files, the DualGate has to prepare files for two GATE Computers ("GATE1" and "GATE2") separately.

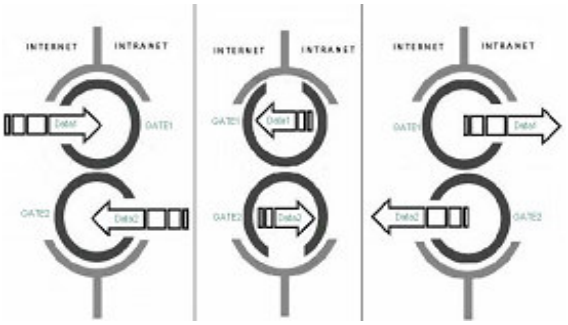

Fig. 5: The DualGate Lock-Keeper Function

When the two connections have been established successfully, the GATE Computers will examine the file queues on their respective connected external Computer and then get a file that has been prepared to be transferred in the next step. As indicated in the left picture of Figure 5, the GATE1 Computer retrieves Data1 queued on the OUTER Computer which is connected to the Internet, and the GATE2 Computer retrieves Data2 from the INNER Computer. Thus, two data transfers will be processed at the same time. After all of Data1 (resp. Data2) has been transferred to the GATE1 (GATE2) Computer, the data will be checked independently by the third-party security software on the respective GATE Computer, similar to the corresponding state of the SingleGate Lock-Keeper. These states can be described as the middle picture of Figure 5. The result will be used to determine whether the data should be transferred to its target or not, as indicated by the right picture of Figure 5.

3.2 Improvement Analysis

The transfer process of a file needs two intervals on the current Lock-Keeper system. The first is to transfer data from the two external computers to one of the two Gate Computers and the second is to deliver the data from the Gate Computer to the other external computer (and then into the connected network). The duration of one interval is determined by the fixed physical connection interval, i.e., enforced by the PCB. In fact, in order to reduce the idle time which may be added by the additional frequency of connection partner changes, the connection interval is set beforehand as a relatively large value. On the other hand, both data transfer and content filtering require a single file as the basic transmission unit. Thus, we must spend at least two intervals in transferring a file with the size of even only one byte. This is not reasonable and also a major obstacle to the popularity of the Lock-Keeper system.

Increasing data transfer capacity in a single cycle is another solution to enhance the data transfer functionality of the Lock-Keeper system. Use of a properly optimized core software managing the data transfer with minimal idle time is an absolute necessity.

By the employment of two gate units, two files can be transmitted at the same time, even in two different directions simultaneously. So the Lock-Keeper file transfer speed can theoretically be improved twofold. In addition, in the new system every Computer will always have a communication partner ready to receive data. There will be no idle Computer during the whole process. Every file which will be transferred can enter the transfer process instantly and will never require any additional waiting time. Thus, compared to the SingleGate Lock-Keeper, the DualGate Lock-Keeper is more efficient.

4. Conclusion

By the Lock-Keeper system, either SingleGate or DualGate, a complete security protection for data exchange can be achieved. The concept of Lock-Keeper technology breaks through the traditional mode of data transfer which is based on continuous connections and makes a thorough network security solution possible. Networks which employ Lock-Keeper systems are immune to any online attacks. Instead, the Lock-Keeper system always stores any type of data transferred between two networks in an intermediate memory, thus

preventing all direct attacks. However, the functionalities of the current Lock-Keeper system, even the DualGate Lock-Keeper system, also can not satisfy the ever-expanding security requirements. Data transfers offered by the Lock-Keeper system are not fast enough to accommodate all the web services, since the long latency is a big constraint. Moreover, how to combine Lock-Keeper systems with a suitable and powerful third-party security tool is also a crucial point for the extension of Lock-Keeper applications. A Lock-Keeper system with a short latency, fast data transfer and extensive interfacing to the third party security software is the object of Lock-Keeper technology development.

References

[1] Ernst-Georg Haffner, Thomas Engel, Christoph Meinel, The Flood-Gate Principle - a Hybrid Approach to a High Security Solution, Proceedings of the International Conference on Information Security and Cryptology(ICISC'98), December 18-19, 1998, Seoul, South Korea.

[2] Ernst-Georg Haffner, Thomas Engel, Christoph Meinel, Techniques for Securing Networks against Criminal Attacks, Proceedings of the International Conference on Internet Computing(IC'00), June 26-29, 2000, Las Vegas, USA.

[3] Ernst-Georg Haffner, Thomas Engel, Christoph Meinel et al., The Lock-Keeper™ Architecture, Technical Report of IT-Services, 2001.

[4] http://www.telematik-institut.de/patente_und_produkte/patente/lockkeeper.html.

[5] William R. Cheswick, Steven M. Bellovin, Firewalls and Internet Security, Addison-Wesley, 1995.

[6] Tobin Sears, Internet Access and Security Solutions: Description of Security Features and Benefits, Technical Report of Network Appliance, Inc., 2003.

[7] Klaus Brunnstein, Beastware (Viren, Würmer, trojanische Pferde): Paradigmen systemischer Unsicherheit, sichere Daten, sichere Kommunikation, Springer-Verlag, 1994.

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

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

[10] http://www.webwasher.com/en/products/contentrep/index_cr.htm.

[11] Paul Ferguson and Geoff Huston, White paper: "What is a VPN?", Revision 1, April 1998.