Forschungsbericht Nr. 03 - 5

Lock-Keeper Technology - A New Network Seurity Solution

Feng Cheng, Paul Ferring, Christoph Meinel
Forschungsgruppe Institut fuer Telematik
FB IV-Informatik
Universitaet Trier, 54286, Trier, Germany
{cheng, ferring, meinel}@ti.uni-trier.de

Lock-Keeper Technology - A New Network Security Solution

Feng Cheng, Paul Ferring, Christoph Meinel
Forschungsgruppe Institut für Telematik
FB IV-Informatik
Universität Trier, 54286, Trier, Germany
{cheng, ferring, meinel }@ti.uni-trier.de

Abstract

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 internal data and systems from unauthorized access. This paper will introduce a novel security solution named Lock-Keeper, which can provide data transfer by physically separate connections. By means of the SingleGate Lock-Keeper system, a simple implementation of this idea, the possibility of direct attacks to a protected network can be eliminated entirely and data can be exchanged between two networks through a completely secure and reliable way. As an advanced implementation of this technology, the DualGate Lock-Keeper is proposed by including another new "gate" unit. Along with this development, not only the Lock-Keeper performance on data transfer, especially the transmit speed, is improved significantly, but also some other new good characteristics appear simultaneously. All these improvements make the DualGate Lock-Keeper more efficient, flexible and applicable. Moreover, an architecture and its working principle of the Lock-Keeper Cluster which is built up by the combination of two or more independent Lock-Keeper systems are analyzed in detail. Thanks to this lock concept, the Lock-Keeper can provide higher levels of security and completely prevents specific intruder attacks. A lot of scenarios, which can be protected by the Lock-Keeper, are revealed in this paper.

Keywords: Network, Security, Physical Separatation, Lock-Keeper, Gate

1. Introduction

With the development of network technology, more and more computers are connected to open networks such as the Internet on a global basis. 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.

So far, 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.

This paper will introduce a new security solution named Lock-Keeper and its up-to-date advancements in detail[1, 2, 3, 4, 5]. 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.

The next section will use the SingleGate Lock-Keeper as an example to explain the Lock-Keeper principle in detail. The DualGate Lock-Keeper, including its architecture, functionalities, new characteristics and performance improvements, is introduced in the third section. Some detailed information about the Lock-Keeper Cluster will be described in the fourth section. The fifth section will propose some practical examples of the Lock-Keeper applications. In the last section, we summarize and add an outlook to further development of this unique security solution.

2. The Lock-Keeper Principle and the SingleGate Lock-Keeper

Currently, almost all the security solutions, regardless of their differing implementation principles, are applying themselves to protect data and its exchange. Up to now, firewalls have established themselves as popular and crucial tools in providing such protection [6]. This section will analyze firewall techniques and their shortcomings, and then introduce an alternative but more complete security solution, the Lock-Keeper technology. The term “Lock-Keeper technology” defines the patented process of data exchange (by the use of the sluice mechanism, see Figure 1.) between physically separated networks.

2.1 Firewalls and their Drawbacks

Firewalls are mostly based on the packet filtering principle. A firewall may be a hardware device or a software program. It can analyze TCP/IP packets by verifying IP addresses of the sender and the receiver and also can monitor the TCP ports to ensure that the selected service is authorized, too. See Figure 1.

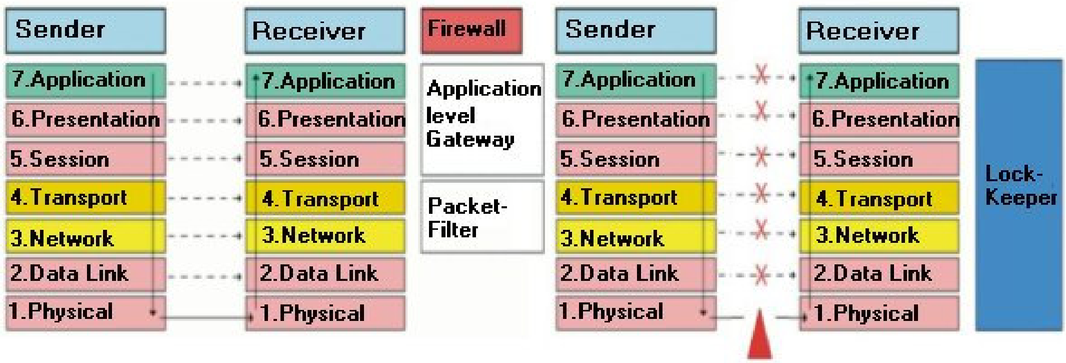

Figure 1. Comparison between Lock-Keeper and Firewall

However, any misconducts or carelessness cannot be controlled by firewalls. Policies involving the use and misuse of passwords and user accounts must be strictly enforced. These are management issues that should be raised during the planning of any security policy, but that cannot be solved with firewalls alone. On the other hand, just like any other security solutions, firewalls are also designed to allow a wide range of "acceptable" behavior. A firewall should be able to divide requests into authorized and unauthorized. It must authorize the former and deny the latter. This conceptual weakness enable unauthorized attackers easily to obtain an internal IP address and then gain access to valuable internal data which has been thought to be protected safely behind the firewall. In a word, the functional principle of this system poses an inherent security risk. In addition, the operating system on which the firewall is based also provides lots of opportunities to attack and compromise the system. Moreover, caused by the complexity of firewalls and their security polices, firewalls are often expensive, hard to configure and they are comprehended only by security experts. “Keep it easy, if it is complex, it’s probably wrong”. Drawback on this psychological factor also makes firewalls untrustworthy.

2.2 Proposal of the Lock-Keeper technology

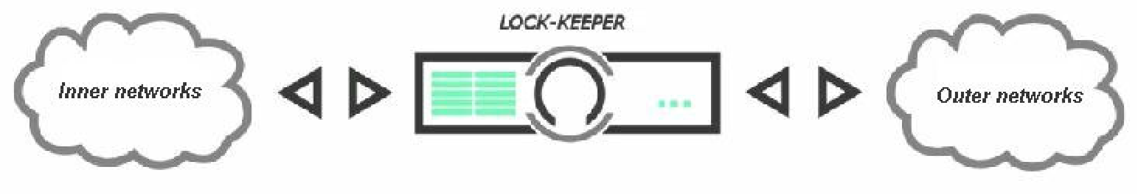

Figure 2. Topology of the Lock-Keeper Sluice Technology

Unlike firewalls which separate the data transfer on the application or protocol level, the Lock-Keeper system[1, 2, 3, 4, 5] separates the communicating networks at a physical level, see Figure 1. 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. To this effect, the Lock-Keeper is based on a well-known and simple mechanism: It works like a sluice, as indicated in Figure 2. The Lock-Keeper system transfers data through a gate without ever creating a direct connection between the internal and external network. In this way, it can be guaranteed that 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. Compared with the complicated firewalls, both the principle and the possible architecture of the Lock-Keeper are simple, clear and easy to be understood. By reason of the psychological advantages, the proposal of the Lock-Keeper technology helps to change the saying from "Build it first, secure it later" to "Secure it first, build it later"([1], [6]).

2.3 The SingleGate Lock-Keeper

As an implementation of the Lock-Keeper sluice technology, a SingleGate Lock-Keeper consists of three active PC-based components, see Figure 3. The innermost Lock-Keeper Computer is connected to the internal high security network, for example an intranet of a company. The Computer on the opposite side is connected to the less secure network, e.g., the Internet. The third Lock-Keeper Computer, also called GATE Computer, which provides the actual lock function, is set up to perform a detailed analysis of the traffic passing through.

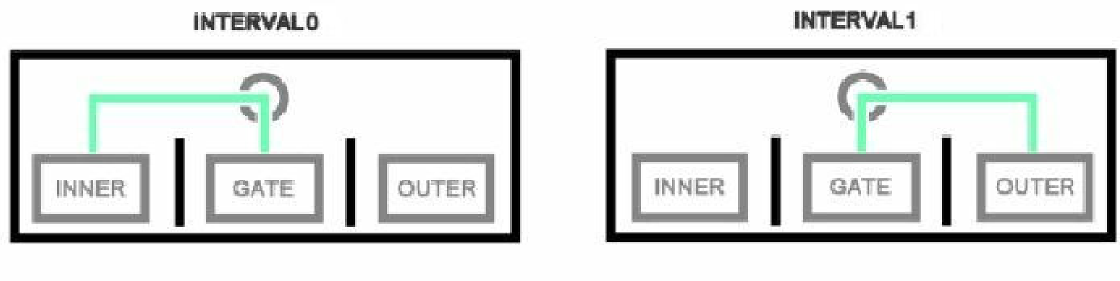

Figure 3. SingleGate Lock-Keeper Switch Status

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 by relays (switches) on a printed circuit board (PCB) that enables and disables connections on a physical level, i.e., interrupt the data cables. As indicated in Figure 3, the switch mechanism has two defined states. 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, hard disk, network cards, etc). On each computer, there is also an independent operating system and some other additional programs which help to transfer or verify data.

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 [7] into the Lock-Keeper system, which can check data traffics during they pass the GATE computer and provide more extensive protection to the data exchange. For example, we can install virus scanning software [8] or mail analysis tools [9] to check the data. It is also possible to install content filtering tools [10] which can provide similar functionalities as traditional firewalls. Moreover, some accounting and statistics [11] 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 system enhances the security level of the protected network.

2.4 Functionalities

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 errors 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.

3. The DualGate Lock-Keeper System

The development of a security solution is always driven by the changing and growing demands. The architecture of the SingleGate Lock-Keeper has many constraints which have restricted its applications. In this section, an advanced, flexible, and applicable Lock-Keeper system, the DualGate Lock-Keeper, will be introduced in detail.

3.1 Improvement Analysis

Just like the physical disconnection of the networks makes the Lock-Keeper system a complete security solution for data exchanges on the network, it also brings a lot of limitations and problems for either applications or extensions of Lock-Keeper. The data transfer through the SingleGate Lock-Keeper may not be rapid 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. If we take "cycle" as the description of the time span for data transfers between two computers, the Lock-Keeper system needs two cycles, one to transfer data from the two external computers to GATE computer and the second to deliver the data from the GATE computer to the other external computer. The duration of one cycle is determined by the fixed physical connection interval, i.e., enforced by the PCB. On the other side, if the GATE does not happen to connect with the source external computer, data must wait there for the switch change. The maximum of overhead waiting time may be a switch interval. So it has become a big drawback of a SingleGate Lock-Keeper that the latency imposed on the data transfer is quite high which limits its utilizations.

However, it has also provided great potentials for the Lock-Keeper improvement. The performance on the data transfer and the long latency has become key factors to extend usability of the Lock-Keeper system. On one hand, use of a properly optimized core software to increase the capacity of data transferred in a single cycle is a solution to enhance the data transfer functionality of the Lock-Keeper system. On the other hand, Employment of adjusted hardware components to manage the data transfer with minimal overhead is another absolute necessity.

3.2 Architecture of the DualGate Lock-Keeper

As indicated in Figure 4, 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.

With the addition of another GATE computer, the PCB and its switch mechanism is modified accordingly. The new switch 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.

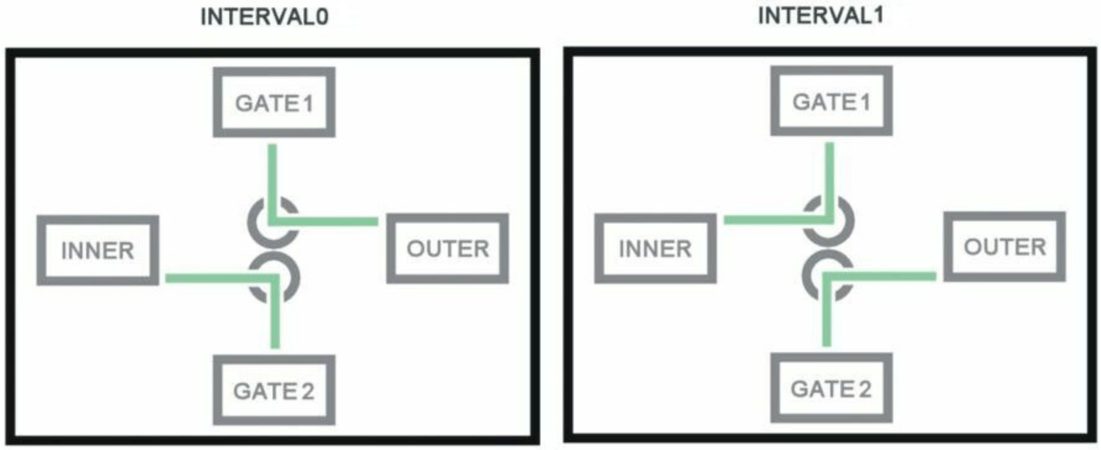

Figure 4. The DualGate Lock-Keeper Switch States

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. The mechanism of the file queuing is flexible and can be determined optionally by different application requirements.

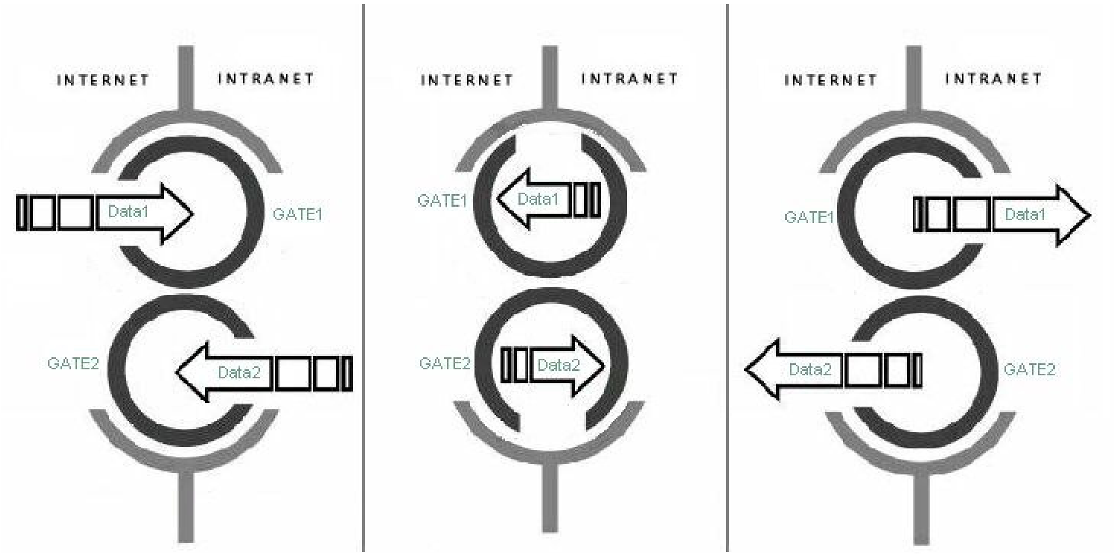

Figure 5. The DualGate Lock-Keeper Function

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 flows will be processed at the same time. After all of “Data1” (resp. “Data2”) has been transferred to the GATE1 (or 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.

3.3 Functionalities and New Characteristics

By using two Lock-Keeper gates, we can transmit two files at the same time, even in two different directions simultaneously. 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. In other words, by adding another GATE computer, we can adequately use all the resources of the system. In addition, some new useful characteristics go perfectly with this development. Thus, compared to the SingleGate Lock-Keeper, the DualGate Lock-Keeper is more efficient. Improvements of the DualGate Lock-Keeper can be summarized like this:

- Increasing the transmit capacity(TC)

By means of this modification, the Lock-Keeper file transfer speed can be improved twofold. In theory, the DualGate Lock-Keeper may be able to reach the same overall throughput between inner and outer as a direct and permanent Fast Ethernet connection which is important for extending the Lock-Keeper applications.

- Reducing the minimum round trip time of small messages through the Lock-Keeper

Small messages which can be transmitted during one interval between two hosts can reach the target in a minimum time of two intervals. By the DualGate Lock-Keeper, the external computers are always connected with one of the two gates. Files can be transferred as soon as they arrive the respective external computers without any other redundant waiting time. It is very important for achieving the optimal quality of service(Qos).

- Using the whole time for transferring files between connected hosts

A constant data flow can be created and kept as long as the file queue is not processed completely which is important for reaching optimal transmit throughput.

- Implementing a few file queuing algorithms

As which has mentioned above, some file queuing algorithms, such as “First in First out” (FIFO), “Last in First out” (LIFO), “Weighted File Queuing” (WFQ) or any other criteria can be implemented in the DualGate

Lock-Keeper. The flexibility of file transfer sequence can meet different requirements which is important for customizing the system and to enable different types of applications.

3.4 Performance Improvements

Table1. Comparison between the SingleGate Lock-Keeper and the DualGate Lock-Keeper

	Transfer Duration (s)	
Experiments	Experiment A (total size: 1GB, file number: 1)	Experiment B (total size: 1GB, file number: 44)
The SingleGate Lock-Keeper	694 (best situation, Delay = 50s)	3306 (best situation, Delay = 17s)
The DualGate Lock-Keeper	726 (unoptimized, Delay = 60s)	852 (unoptimized, Delay = 60s)

As shown in the table 1, in the experiment A, we use respectively both Lock-Keeper systems to transfer a file with 1 GB. The result shows that a DualGate Lock-Keeper system, whose delay (60s), is not be optimized has nearly the same performance for transferring a single file as the best situation which an optimized SingleGate Lock-Keeper system can get. However, the experiment B, which transfers a file queue, for example a queue of 44 files, shows that the speed of the data transfer is improved significantly.

Because of some good properties and the performance improvements, the DualGate Lock-Keeper can provide more efficient, flexible and applicable security protections for the data exchange between networks.

4. Lock-Keeper Cluster

From another point of view, both the architecture and the working process of the DualGate Lock-Keeper is very similar to a cluster of two SingleGate Lock-Keeper, except for throwing off two unwanted external computers. In the same way, two DualGate Lock-Keepers can also be integrated into a DualGate Lock-Keeper Cluster. It can be anticipated optimistically that the DualGate Lock-Keeper Cluster would possess more powerful performance and advantageous characteristics. In this section, a possible architecture and correlative discussion of a DualGate Lock-Keeper Cluster will be proposed.

4.1 Architecture of the DualGate Lock-Keeper Cluster

As indicated in the Figure 6, two DualGate Lock-Keeper system are integrated tighter and installed between the unreliable external network(Internet) and the protected internal network(an intranet).

Compared with the improvement from a combination of two SingleGate Lock-Keeper to a DualGate Lock-Keeper, in the DualGate Lock-Keeper Cluster, four external computers, two INNER computers and two OUTER computers, are required to make the control mechanism of connections more easy and at the same time make the implementation architecture more simple. In addition, the performance of the file queuing and data transfer can also be improved by the employment of four external computers.

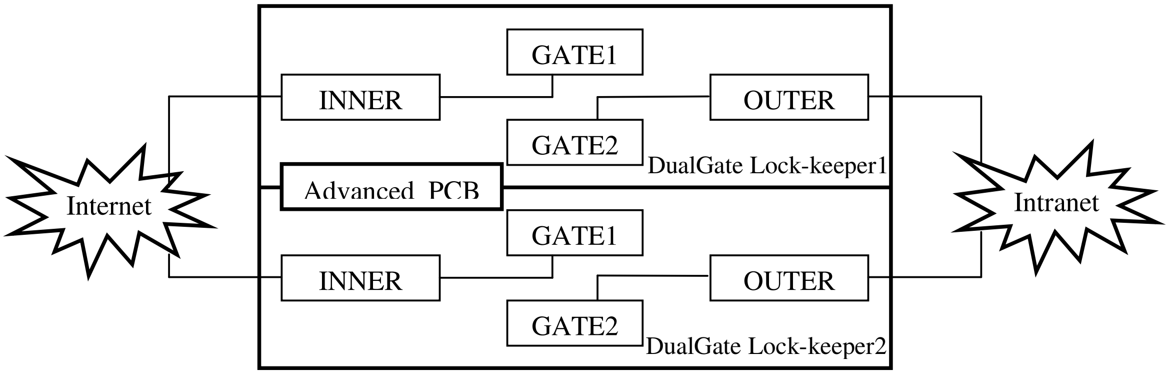

Figure 6. The DualGate Lock-Keeper Cluster

Besides the two DualGate Lock-Keeper system, there is an advanced printed circuit board(PCB) which synchronizes working processes of two DualGate Lock-Keeper. The running of this PCB is automatic and can not be controlled by any other components either hardware or software of the system. The detailed switching function of this PCB will be described in the following.

4.2 Working principle of the DualGate Lock-Keeper Cluster

According to the basic concept of the Lock-Keeper technology, any direct physical connections between two networks are all forbidden. Therefore, when the DualGate Lock-Keeper Cluster runs, there may be only four permitted states of connections between external computers and gate computers in the two DualGate Lock-Keeper, as shown in the Table 1. This switching mechanism is guaranteed by both the abovementioned advanced PCB outside of the DualGate Lock-Keeper system and two inside Lock-Keeper PCBs.

Table 2. the Change of connection state of the DualGate Lock-Keeper Cluster

	DualGate Lock-Keeper1		DualGate Lock-Keeper2	
Connection State	GATE1 – OUTER GATE2 – INNER	GATE1 – INNER GATE2 – OUTER	GATE1 – OUTER GATE2 – INNER	GATE1 – INNER GATE2 – OUTER
< t_0	... …	... …	... …	... …
t_0	1	0	1	0
$t_0 + T/2$	1	0	0	1
$t_0 + T$	0	1	0	1
$t_0 + 3T/2$	0	1	1	0
> $t_0 + 2T$	… …	… …	… …	… …

With the help of the outside advance PCB, the connections in different DualGate Lock-Keeper can be synchronized according to different requirements. Here is only an example of the connection state change mode, see Table 1 and Figure 7. The time difference of connection switches of the two DualGate Lock-Keeper1 is **T/2**. T is the duration of a Lock-Keeper interval.

In order to improve the efficiency of the file processing and optimize the data flows in the cluster system, a new file queue algorithm is appointed on the external computers of both the DualGate Lock-Keepers to help data choose the best and optimal transfer path.

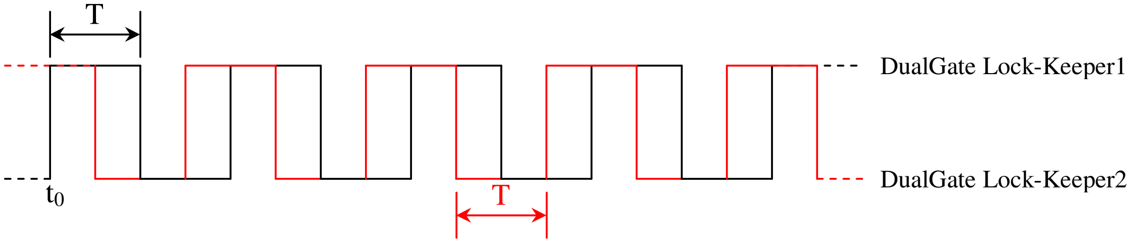

Figure 7. The change of connection state “GATE1 - OUTER GATE2 - INNER”

Now we can suppose an application scenario. There is a short message which will be transferred from the external network to the internal network, and then after being processed in the internal network, the response for this message is required to be transferred back. Three suppositions are proposed: 1. the message is so small that the transfer duration between two hosts can be neglected, 2. the content checking duration of the small message can also be neglected, 3. the message can be processed completely in half an interval. For this task, two intervals(**2T**) is required when we employ one DualGate Lock-Keeper(which has been indicated in the Section 3.3). However, using the DualGate Lock-Keeper Cluster can decrease the duration to one interval(**T**). For example, in the time $\mathbf{t_0}$, the message M enters into the system. Then, the file queue algorithm will choose the DualGate Lock-Keeper2 (abbr. DL2) as the proper transfer path. The reason is that after only half an interval (i.e. in the time $\mathbf{t_0+T/2}$), the connection states of DL2 will be changed before the DualGate Lock-Keeper1 (abbr. DL1), see Table 1 and Figure 7. That means, after a duration of **T/2**, the message M can be transferred from the OUTER computer of DL2 (DL2-OUTER) to the INNER computer of DL2 (abbr. DL2-INNER) by the GATE1 of DL2(abbr. DL2-GATE2). Then, the message M will be processed in the internal network and the response of M will be ready to transfer towards outside. At that time, the GATE2 of the DL1(abbr. DL1-GATE2) is chosen as a best path because it will change the connection states after half an interval. And then, in the time $\mathbf{t_0 + T}$, the response of M can reach the OUTER computer of the DL1(abbr. DL1-OUTER). The detailed description of the whole process can be shown by the Table3.

So by the use of this DualGate Lock-Keeper Cluster, the minimum round trip time of a small message can be decreased to one Lock-Keeper switch interval. It is very useful for providing security protection for such services as web browsing by the Lock-Keeper technology.

In addition, the reliability of the system can also be enhanced by using the DualGate Lock-Keeper Cluster. If there is something wrong with one of the two DualGate Lock-Keeper, the other one could still be able to work normally. The method for searching the optimal path can help every files pass the Lock-Keeper as soon as possible. The waiting time either in the file queue or on the gate is shortened significantly.

Table3. The transfer process of a small message and its response.

Time	Position	operation
t_0	DL2-OUTER → DL2-GATE1	transfer
$(t_0, t_0+T/2)$	DL2-GATE1	wait
$t_0+T/2$	DL2-GATE1 → DL2-INNER → Intranet	transfer
$(t_0 +T/2, t_0 + T)$	Intranet → DL1-INNER → DL1-GATE2	process & transfer
$t_0 + T$	DL1-GATE2 → DL1-OUTER	transfer

In addition, the reliability of the system can also be enhanced by using the DualGate Lock-Keeper Cluster. If there is something wrong with one of the two DualGate Lock-Keeper, the other one could still be able to work normally. The method for searching the optimal path can help every files pass the Lock-Keeper as soon as possible. The waiting time either in the file queue or on the gate is shortened significantly.

5. Lock-Keeper Applications

Thanks to this lock concept, the Lock-Keeper provides higher levels of security and completely prevents specific intruder attacks. We can reveal a lot of scenarios which can be protected by the Lock-Keeper. The most frequently utilized service which can be protected by the Lock-Keeper system is data exchange, for example mail or file 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 reinforce to current utilized VPN technology, Virtual Public Network [12]. Theoretically, the Lock-Keeper system can protect almost all network services, because it can provide a complete security protection for ordinary data exchanges. This section will propose some practical examples of the Lock-Keeper applicationsn

5.1 Mail Transfer via Lock-Keeper

Electronic mail has now become the most frequently utilized Internet service. It also provides a classic practical example for a typical Lock-Keeper application, see Figure 8. 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.

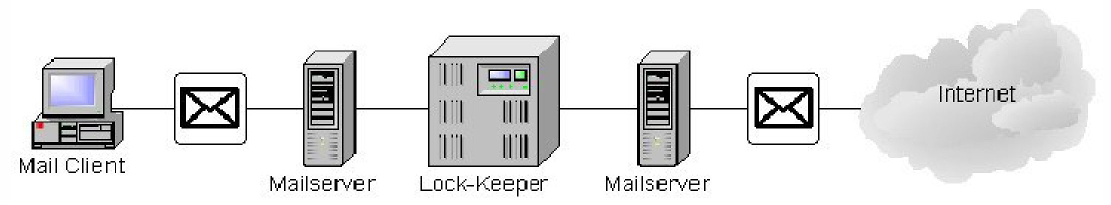

Figure 8: Practical Example Mail Transfer

5.2 File Transfer via Lock-Keeper

Similar to e-mail transfer, file-transfers can also be automatically transported offline via the Lock-Keeper, see Figure 9. In this case, the data are, for example, copied into one or several folders, from where they are transferred by the Lock-Keeper.

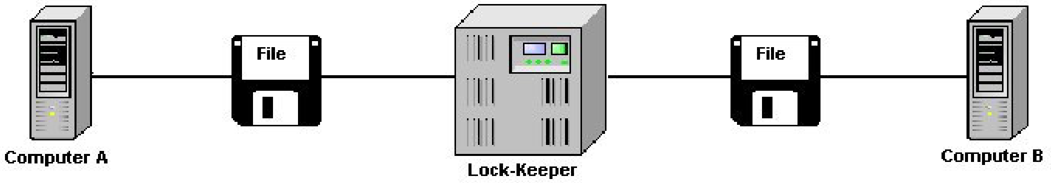

Figure 9: Practical Example File Transfer

5.3 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, see Figure 10. 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.

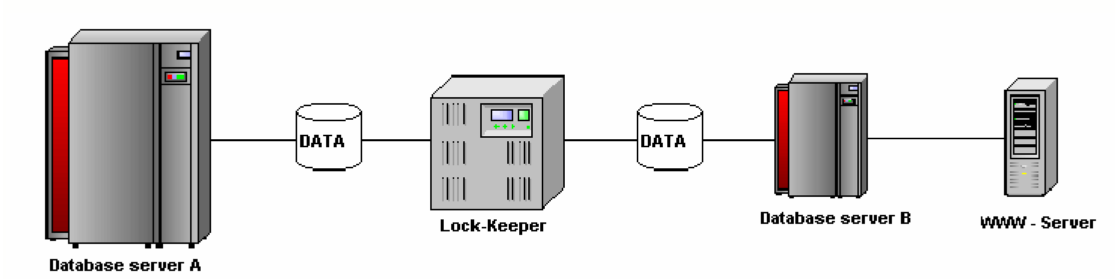

Figure 10: Practical Example Database Alignment

5.4 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.

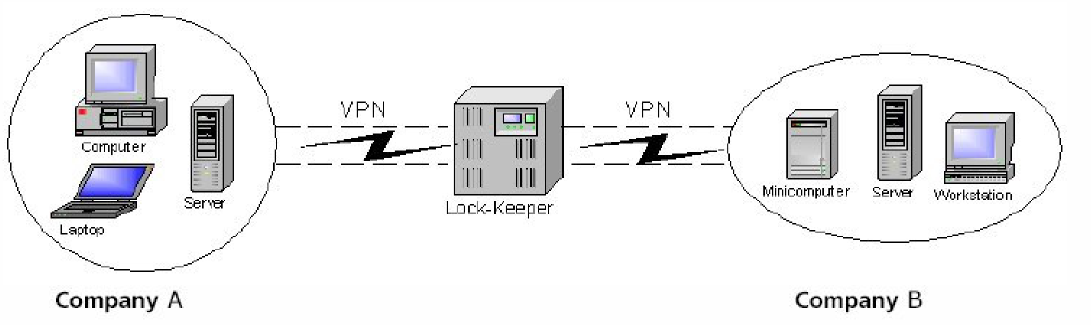

Figure 11: VPN Connection Between Companies

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, see Figure 11.

6. Conclusion

By the Lock-Keeper system, either the SingleGate Lock-Keeper, the DualGate Lock-Keeper or the Lock-Keeper Cluster, a complete security protection for data exchange can be achieved. This review showed the basic functionalities of these systems and explained their integration into complex security architectures. 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. In addition to and as an enhancement of conventional firewalls, the Lock-Keeper techology can be able to be one of the most efficient solutions for network security.

Acknowledgements

We are thankul to Thomas Engel, Ernst-Georg Haffner, Jochen Bern, Gerhard Müllenheim, Dominik Thewes, Thomas Wagner, Michael Noll for their contributions to the previous works of the Lock-Keeper Technology.

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

[4] Feng Cheng, Christoph Meinel, Thomas Engel, et al., "A Complete Solution for Highly Secure Data Exchange: Lock-Keeper and its Advancements", in Proc. of the Fourth International Conference on Parallel and Distributed Computing, Applications and Technologies (PDCAT'03), Chengdu, China, August 27-29, 2003, pp. 201-205.

[5] Feng Cheng, Paul Ferring, Christoph Meinel, et al, The DualGate Lock-Keeper: A Highly Efficient, Flexible and Applicable Network Security Solution, Proceedings of the 4th ACIS International Conference on Software Engineering, Artificial Intelligence, Networking, and Parallel/Distributed Computing (SNPD'03), Lübeck, Germany, October 16-18, 2003, pp. 152-159.

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

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

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

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

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

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

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