published as: F. Cheng, P. Ferring, Christoph Meinel, G. Müllenheim, J. Bern: The DualGate Lock-Keeper: A Highly Efficient Flexible and Applicable Network Security Solution;
In Proceedings of the 4th International Conference on Software Engineering, Artificial Intelligence, Networking, and Parallel/Distributed Computing (SNPD 2003);
SNPD 2003 Lübeck (Germany), 2003, pp. 152-159, isbn: 0-9700776-7-X.

The DualGate Lock-Keeper: A Highly Efficient, Flexible and Applicable Network Security Solution

Feng Cheng, Paul Ferring, Christoph Meinel,
FB IV- Informatik,
University of Trier, D-54286 Trier
Email:{cheng , ferring, meinel}@ti.Uni-trier.de
Web: www.telematik-institut.org

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

Abstract

[a]*The idea of data transfer by physically severed connections has been applied in a simple realization of the Lock-Keeper technology, the SingleGate Lock-Keeper system. By means of it, 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 changes 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 two DualGate Lock-Keeper are analyzed in detail in this paper.*

Keywords: Network, Security, Physically Severed Connection, Lock-Keeper, Dual Gate

1. Introduction

Nowadays there are large amounts of important and confidential resources on the web easily available to employees, partners, customers, 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 and worms, or unauthorized accesses, etc. Users who connect their computers to the network must be aware of these dangers and their implications. Thus, the task of protecting the critical private networks and simultaneously permitting secure data exchange has become a primary problem for most network applications.

So far, lots of security technologies, such as firewalls, anti-virus tools, or intrusion detection systems, are offered to protect the data and their exchanges. Nevertheless, in spite of the ubiquity and constant development of such solutions, networks and their attached resources still remain quite delicate and vulnerable. All these methods are not complete and powerful enough to satisfy ever-increasing security requirements. 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 completely prevent specific intruder attacks by physically separating the communicating networks([1]~[5]).

The next section is a review of the Lock-Keeper technology. The SingleGate Lock-Keeper system is used as an actual implementation example. The DualGate Lock-Keeper, including its architecture, functionalities and new characteristics, is introduced in the third section. Some detailed information about the Lock-Keeper Cluster will be described in the fourth section. In the last section, we summarize and add an outlook to further development of this unique security solution.

In Proceedings of the 4th ACIS International Conference on Software Engineering, Artificial Intelligence, Networking, and Parallel/Distributed Computing (SNPD'03), October 16-18, 2003, Lü beck, Germany.

2. The Lock-Keeper Technology

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.

Figure 1. Topology of the Lock-Keeper Sluice Technology

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 monitor the TCP ports to ensure that the selected service is authorized, too.

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[6]. In addition, the operating system which the firewall is based on, provides lots of opportunities to attack and compromise the system, too. Moreover, caused by the complexity of firewalls and their security polices, firewalls are often expensive, difficult to configure and they are comprehended only by security experts. " Keep it easy, if it is complex, it's probably wrong" [6]. Drawback on this psychological factor also makes firewalls untrustworthy.

2.2 Proposal of the Lock-Keeper technology

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. 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. 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. In comparison to 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]).

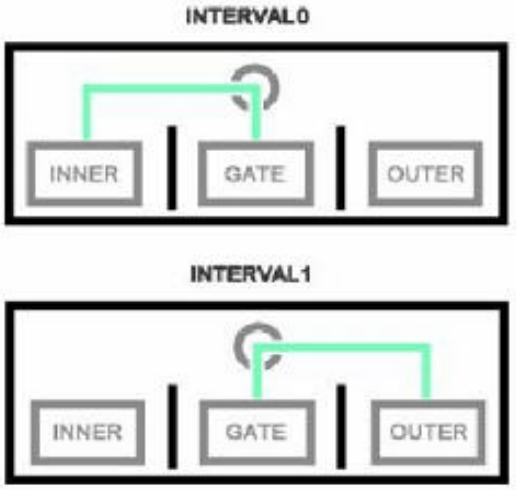

Figure 2. The states of the SingleGate Lock-Keeper switch interval

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 2. The innermost Lock-Keeper Computer(INNER) is connected to the internal high security network, for example an intranet of a company. The Computer(OUTER) 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.

All three components are connected to a patented switching unit that restricts their communication. 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., interrupts the data cables. As indicated in Figure 2, the switch mechanism has two defined states(interval 0: INNER and GATE connected to each other, interval 1: GATE and OUTER connected to each other). 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.

It is important 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 traffic during it is passing the GATE computer to provide more extensive protection to the data exchange. For example, it is possible to 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 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 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.

By the means of this lock concept, the Lock-Keeper provides higher levels of security and completely prevents specific intruder attacks. There are 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. 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, can only get their required data after passing the checking process of Lock-Keeper. This application can be used to implement remote-access-like services as an alternative 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.

3. The DualGate Lock-Keeper System

The requirements of secure data exchange on one side and comfortable services on the other lead to a conflict. The development of modern security architectures are always driven by the changing and growing demands for the data exchange. 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

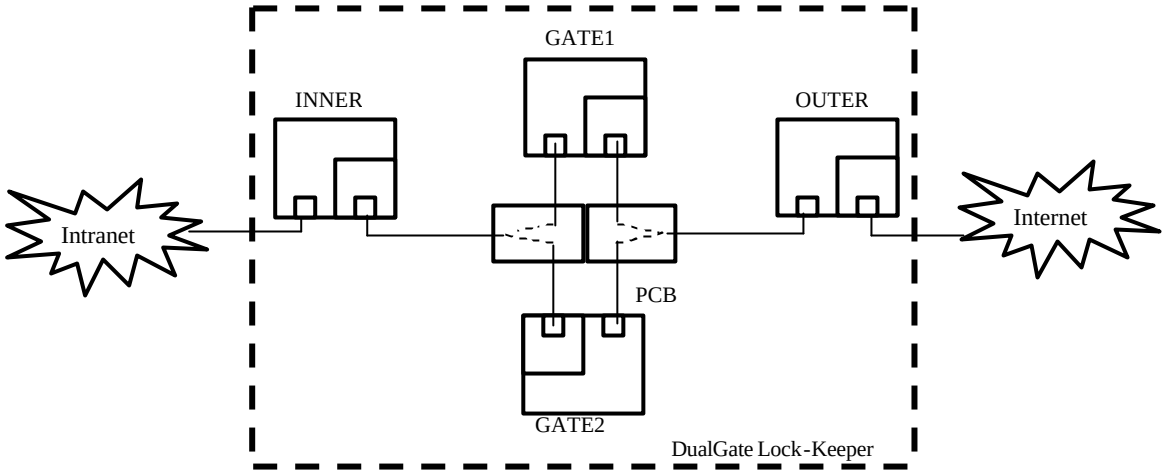

Figure3. The DualGate Lock-Keeper System

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 fast enough to emulate 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 uses 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 3, 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.

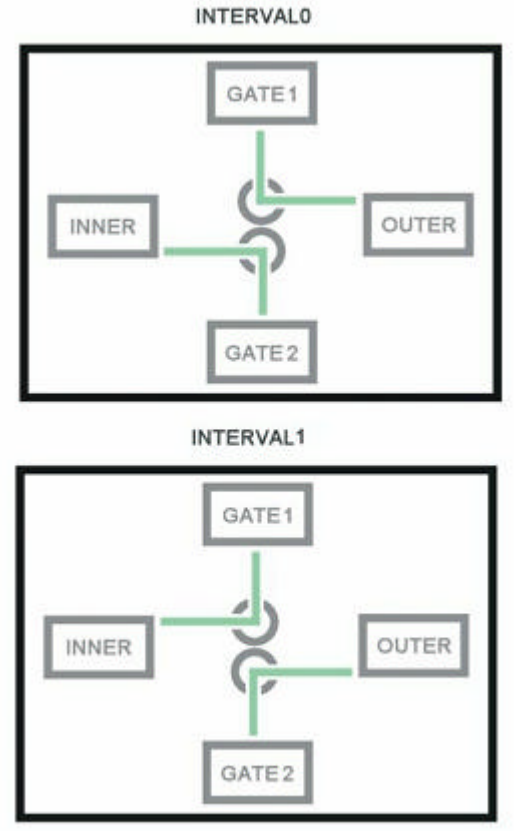

Figure 4. The states of the DualGate Lock-Keeper switch interval

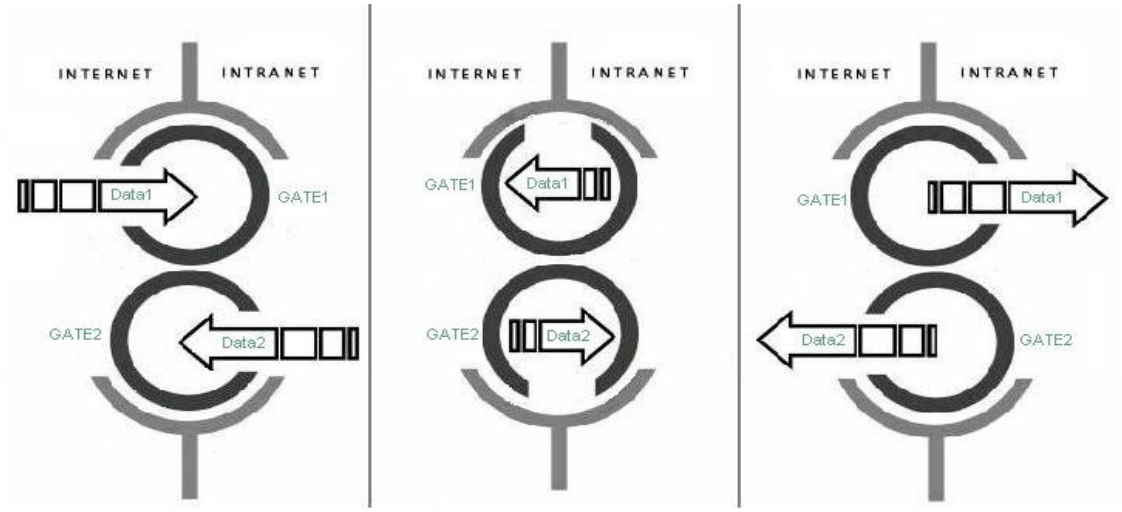

Figure 5. The DualGate Lock-Keeper Function

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

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. Moreover, 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.

Because of these good properties, the performance of the DualGate Lock-Keeper has been improved significantly which makes the DualGate Lock-Keeper a highly effecient, flexible and applicable network security solution.

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.

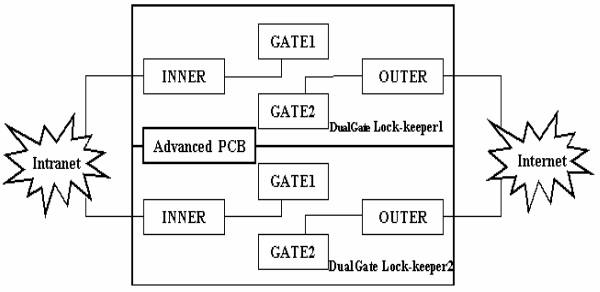

Figure 6. The DualGate Lock-Keeper Cluster

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 1, 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.

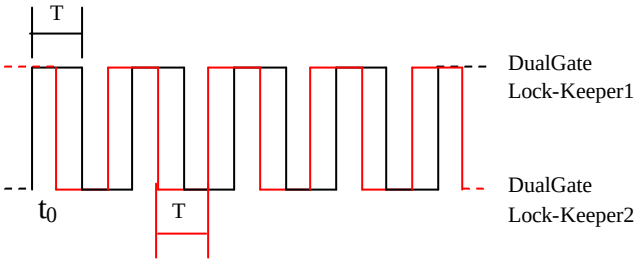

Figure 7. The change of connection state "GATE1 – OUTER GATE2 – INNER"

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(**2 T**) 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 Table 2. 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.

Table2. The transfer process of a small message and its response.

Time	Position	operation
$\mathbf{t_0}$	DL2-OUTER—— DL2-GATE1	transfer
$\mathbf{(t_0, t_0+T/2)}$	DL2-GATE1	wait
$\mathbf{t_0+T/2}$	DL2-GATE1——DL2-INNER —— Intranet	transfer
$\mathbf{(t_0+T/2, t_0+T)}$	Intranet—— DL1-INNER —— DL1-GATE2	process & transfer
$\mathbf{t_0 + T}$	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. Conclusion

As a high secure, easy to understand and construct, simple solution, the Lock-Keeper technology can provide complete protection for data exchanges and private networks. The concept of Lock-Keeper technology breaks through the traditional data transfer mode 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. The performance can be improved by the DualGate Lock-Keeper system proposed in this paper. The proposal of the DualGate Lock-Keeper Cluster can make the Lock-Keeper technology applicable for protecting more network services.

References

[1] Ernst-Georg Haffner, Thomas Engel, Christoph Meinel, "The Flood-Gate Principle - a Hybrid Approach to a High Security Solution", in Proc. of the International Conference

on Information Security and Cryptology(ICISC'98), Seoul, South Korea, December 18-19, 1998.

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

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

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

[5] 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.

[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.