Lock-Keeper – A High Security Solution based on Physical Separation

Feng Cheng, Christoph Meinel

Internet Technologies and Systems
Hasso Plattner Institute, Potsdam, Germany
Agenda

- Introduction
- The Lock-Keeper Architectures:
  - SingleGate Lock-Keeper
  - DualGate Lock-Keeper
- Lock-Keeper Security
  - Experiments: Penetration Testing
  - Deploying Virtual Machines in Lock-Keeper
  - Lock-Keeper based Strong Authentication
- Usability Discussion: Lock-Keeper Applications
- Conclusions
Introduction (1)

■ New Challenge of Security
  □ Attacks targeted on the whole private network has been more and more severe and dangerous.
    - online attack and offline attacks
    - known attacks and unknown attacks
    - Insider attacks and outsider attacks

■ If you are connected to the network, you would be always at the risk of being attacked.

■ The ultimate method to secure a network is to disconnect it
  - Physical Separation.
Physical Separation:

Find a way to exchange data between two networks – usually classified as a high security internal network and a less secure external network - without establishing a direct, physical connection, no matter how short-lived such a connection would be.
Introduction (3)

- **Lock-Keeper** is an implementation of Physical Separation Technology, which can guarantee both *security* and *usability* simultaneously.
- Lock-Keeper patents from ten countries/districts
- In 2005, we started a cooperation with “Civil and National Security” Department of Siemens Switzerland
- Siemens Switzerland has produced a commercial version of the Lock-Keeper (OEM) and now the system is offered by Siemens International in worldwide
The Lock-Keeper system consists of

(1) Three independent active computers

- “INNER” computer is connected to the internal, high security network
- “OUTER” computer on the opposite side is connected to external, less secure network, e.g., the Internet
- “GATE” computer provides the actual lock function
The Lock-Keeper system consists of

(2) A patented switch module

- Switch module completely controls connection and communication
- Function and timing of the switch module is completely autonomous and can not be affected by any software
- Neither external attackers nor insiders can change or bypass physical separation of the networks

LK Switch-PCB
(3) **Software in the Lock-Keeper System:**

- Basic operating system on the Lock-Keeper computers allows the integration of third-party security software into the Lock-Keeper system, e.g.
  - Virus scanner to be placed on the GATE
  - Extra software firewalls to be placed on INNER and/or OUTER

- **Lock-Keeper Secure Data Exchange Software (LK-SDE)** provides different application modules, so that following functionalities can be provided transparent to the users:
  - Mail Exchange
  - File Exchange
  - Database Replication
  - Secure Web-Services Provider
  - Any customer applications
The Lock-Keeper Architecture (4)

LK-SDE Software – Protocol Separation

**OUTER**
- File X Module
- Mail X Module
- DB Syn./Rep. Module
- Web Services Module
- VPN Module
- ... Others
- Other App. Module

**GATE**
- Enhanced OS
- Basic Data Exchange Module
- Data Scanning Module

**INNER**
- File X Module
- Mail X Module
- DB Syn./Rep. Module
- Web Services Module
- VPN Module
- Other App. Module

Enhanced OS
Extended version: DualGate Lock-Keeper

- Second “GATE” and extended switch mechanism
- Keeps the property of “Physical Separation” but improves performance

GATE does **actively** start all communications.

There is NO possibilities to **actively** access GATE
Penetration Testing Lock-Keeper vs. Firewalls (1)

- **Test scenario 1:**
  - SMTP through Firewall (just port 25 is open)

- **Test scenario 2:**
  - SMTP through Lock-Keeper

- Experiments performed by our attack simulating and measurement tool called SNAPP, “Smart Network Attack & Penetration Platform”

- Attack Graph is used as a metric to compare different protection mechanisms and their overall security
Penetration Testing-Lock-Keeper vs. Firewalls (2)

Test Scenario I: SMTP through Firewall

- The attack graph shows several possibilities to attack the target host.
- In our experiment SNAPP successfully establishes a VNC session to the target host and get full access of it!!
Penetration Testing - Lock-Keeper vs. Firewalls (3)

Test Scenario 2: SMTP through Lock-Keeper

- Lock-Keeper is used to protect the same internal mail server
- Lock-Keeper’s OUTER is vulnerable to DoS attacks, but in contrast to the firewall solution, the protected mail server is not affected.
Deploying Virtual Machines in Lock-Keeper (1) - Motivations

- A hacker does possibly succeed in compromising INNER and/or OUTER e.g. by means of a DoS-attack shown in the attack graph
- That’s because the application modules on INNER/OUTER provide normal network services to the outside
  - The OS or other application modules can be intruded to when the hacker gets full access to any one of these application modules
- It is difficult to restore the system in case of a destruction
- Maintaining the Third-Party security software for Data Scanning module on GATE is not convenient
  - Admin can NOT connect GATE normally because of switching.
  - GATE does and can NOT provide any services
Deploying Virtual Machines in Lock-Keeper (2)

VMs on INNER/OUTER
- Applications supported by the Lock-Keeper are realized by several application VMs.
- **Application Separation** and **User Separation**

VM on GATE
- The third-party virus scanning or content filtering tools can be installed on VM
- Administrator can create or change the Data Scanning VM Image-file locally, and then copy it to GATE when he/she logsins on the LK-GATE system → **offline maintaining**
- Due to the VM isolation, the process and result of the data scanning can not be affected by anyone else → **offline scanning**
Lock-Keeper Security (7)

**Lock-Keeper based Strong Authentication (1)**

- An organization’s portal, which offers services and/or remote access for authorized persons, provides the **single open point** of the internal network and therefore is an attractive attack point.

- After **bypassing** or **penetrating** conventional authentication mechanisms deployed by the portal, hackers can easily intrude into the internal network through its normal direct connection with the outside world.

- Some Sensitive information, e.g. user profile, privacy or policy, required by most authentication approaches or access control schemes, is vulnerable in the **online** state.
Lock-Keeper Security (8)

Lock-Keeper based Strong Authentication (2)

- After customer’s request has received on OUTER, it is reunited into a standard file-based Lock-Keeper Message Container (LKMC).
- On GATE, a complete authentication procedure will be performed accordingly based on “Certificate Store” and “Policy Database”.
- Other authentication techniques can be easily integrated.
Usability Discussion: Lock-Keeper Applications (1)

Securing **file exchange** between internal and external systems by Lock-Keeper

Most utilized service, however, is **mail exchange** between internal and external networks
Lock-Keeper may secure **database synchronization** and protect core database server.
Secure Web Services Provider

- Complete protection of the internal WS provider and its network
- Secure verification of the passing SOAP traffic
- Implementation: external proxy + WS-Router (OUTER) + SOAP Verification (GATE) + WS-Invoker (INNER)
Combination with third party security products

Lock-Keeper can easily be combined with all other kinds of security tools, like Firewalls, Intrusion Detection Systems and/or Encryptors without any additional efforts to provide a full scale security solution.
Conclusions (1)

Lock-Keeper Benefits on Security and Usability

- Implementation of Application-Level Gateway in a “Physical Separation" device: the highest security level of the protected network is guaranteed.

- Realizations of Protocol/Application/User separation help to prevent any kinds of direct communications between users (both client role and server role) in separated networks.

- Compare to traditional relay mechanism (e.g. packets store-and-forward), GATE, which has no services provided, is impossible to be actively accessed by INNER/OUTER or other LK-Outside hosts.

- Insider Attacks (e.g. from an offlinely planted attack agent) is hard to send the sensitive internal information out through the Lock-Keeper.
Conclusions (2)

Lock-Keeper Benefits on Security and Usability

- In cases of any failures (from Human factors or technical factors) when Lock-Keeper doesn’t work normally, the internal network and its hosts can still keep to be disconnected and secure.

- **Psychological factor, provided by such physical separation with the untrusted world, helps to get more trustworthiness**

- Extra functionalities and productivities with enhanced security
  - Integrated Server for File-Mail Exchanges
  - Secure Replication between Heterogeneous Databases
  - Flexible deployment of third-party security mechanism – offline scanning/offline maintaining
  - Strong and federated authentication for SOA
Many thanks for your attention

**For more Information:**

- Hasso-Plattner-Institut
  Universität Potsdam
  Postfach 90 04 60, D-14440 Potsdam
  - [http://www.hpi.uni-potsdam.de/~meinel/](http://www.hpi.uni-potsdam.de/~meinel/)

  or

- Siemens Schweiz AG – Civil and National Security
  Freilagerstr. 40, CH-8047 Zürich
  - [http://www.siemens.ch](http://www.siemens.ch)