System Description and Risk Analysis

Bähler Alessio   Enz Andreas   Niederberger Matthias

October 18, 2017

Contents

1 System Characterization

1.1 System Overview

The System consists of three machines in a company network and a external client machine. Inside the company network we have Machine 1 housing the Core CA functionality and the legacy MySQL database. Machine 2 contains the web server with a firewall to shield it because any traffic from outside the company network will have to cross the web server machine anyway. Finally Machine 3 is used for the physical separation of the backup service, with backup daemons connecting to the other two machines.
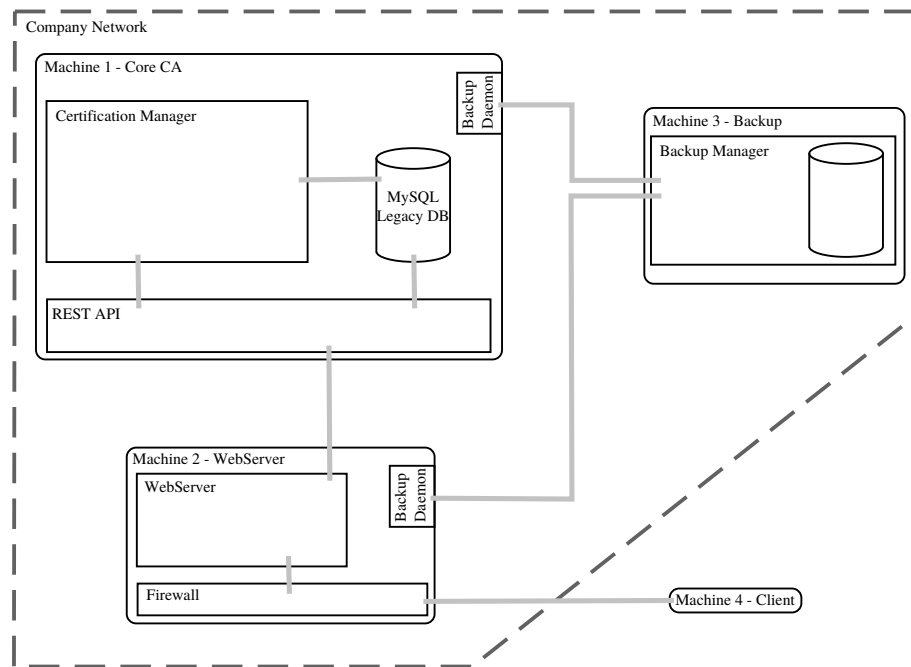

Figure 1: System Architecture of the company network including an external client machien.

1.2 Components

A short description of the components in Figure 1.

- **Certification Manager**: Manages certificate state (creation, revocation, deletion, ...). Interfaces with the web server over the REST API and directly with the legacy MySQL database. It has two main subcomponents:

  - Certification Store: A directory where keys and certificates are stored.

– Certification Generator: Built with OpenSSL

- **MySQL DB**: As provided. Interfaces with the web server over a REST AP and with the Certification Manager.

- **REST API**: Interface between Core CA machine and WebServer machine.

- **Web Server**: Accepts web traffic filtered through a Firewall. Does Authorization by checking legacy database and can request certificate state changes from the Certification Manager.

- **Firewall**: Filters traffic.

- **Backup Manager**: Periodically stores specified data in the backup database. Interfaces with Core CA and WebServer machine.

    – Backup Daemon: Sends Data to Backup machine

2 Risk Analysis and Security Measures

2.1 Assets

Physical Assets

- Web Server: physical machine hosting the Web Server Application

- Core CA: physical machine hosting the CA Application and the legacy database

- Backup: physical machine hosting the backup data

Logical Assets

- Software

    – Web Server Application
    – Core CA Application
    – legacy MySQL database
    – Backup application

- Information

    – Certificates
    – Keys
    – User data
    – Configuration files
    – Logs

Persons

- System Administrator

- CA Administrator

- Users (Employees and Informants)

Intangible Goods

- Company Reputation

2.2 Threat Sources

TODO: Name and describe potential threat sources (*not* threats!) including their motivation.

- Nature: probably not relevant since it targets availability

- Users: Employees (includes also cleaning personnel etc.) and Informants can act maliciously or be careless/poorly trained

- Competitors: may be interested in obtaining confidential information to gain an advantage, blackmail or cause harm by publishing it. May resort to Skilled Hackers to achieve their goals.

- "Victims": subjects of investigative reports that were publicly exposed and may want to get revenge by causing any kind of damage. May resort to Skilled Hackers to achieve their goals.

- Organized Crime: can directly or indirectly be "Victim", could be interested in blackmailing the Company to gain money or just to obtain important information that can be sold on the black market/used for other illegal activities.

- Malware: TODO

- Expert Hackers: A skilled hacker has expert knowledge for some systems. He can write his own code and may use unknown or unpublished vulnerabilities (from book). May itself be a "Victim" or act for monetary interests.

- Script Kiddies: This type of adversary has basic computer knowledge and uses mainly known vulnerabilities for which exploits are available on the Internet. However, he might write scripts to automate tasks or use tools to automatically create malware. His main motivations are challenge, glory and destruction (from book).

- Organizatorial Deficiencies (from SecEng slides): lack in employee training, poor/non-existing/non-enforced security measures (E.g. TODO) can weaken the overall security of the system.

- Hardware Failures (from SecEng slides): TODO

2.3   Risks Definitions

Define likelihood, impact and risk level using the following three tables [1].

Likelihood	Description
High	The threat source is highly motivated and sufficiently capable of exploiting a given vulnerability in order to change the asset's state. The controls to prevent the vulnerability from being exploited are ineffective.
Medium	The threat source is motivated and capable of exploiting a given vulnerability in order to change the asset's state, but controls are in place that may impede a successful exploit of the vulnerability.
Low	The threat source lacks motivation or capabilities to exploit a given vulnerability in order to change the asset's state. Another possibility that results in a low likelihood is the case where controls are in place that prevent (or at least significantly impede) the vulnerability from being exercised.

Impact	
Impact	Description
High	The event (1) may result in a highly costly loss of major tangible assets or resources; (2) may significantly violate, harm, or impede an organization's mission, reputation, or interest; or (3) may result in human death or serious injury.
Medium	The event (1) may result in a costly loss of tangible assets or resources; (2) may violate, harm, or impede an organization's mission, reputation, or interest, or (3) may result in human injury.
Low	The event (1) may result in a loss of some tangible assets or resources or (2) may noticeably affect an organization's mission, reputation, or inter- est.

Risk Level			
Likelihood	**Impact**		
	Low	Medium	High
High	Low	Medium	High
Medium	Low	Medium	Medium
Low	Low	Low	Low

2.4   Risk Evaluation

List all potential threats and the corresponding countermeasures. Estimate the risk based on the information about the threat, the threat sources and the

corresponding countermeasure. Adhere to the risk definitions you have given above. As a sanity check, there should be at least one high-risk entry.

2.4.1 *Evaluation Asset X*

Evaluate the likelihood, impact and the resulting risk, *after implementation of the corresponding countermeasures.* Formulate the threats in active, not passive, voice: who (threat source) does what (threat action)?

No.	Threat	Countermeasure(s)	L	I	Risk
1	...	...	Low	Low	Low
2	...	...	Medium	High	Medium

2.4.2 *Evaluation Asset y*

No.	Threat	Countermeasure(s)	L	I	Risk
1	...	...	Low	Low	Low
2	...	...	Medium	High	Medium

2.4.3 Detailed Description of Selected Countermeasures

Optionally explain the details of the countermeasures mentioned above.

2.4.4 Risk Acceptance

List all medium and high risks, according to the evaluation above. For each risk, propose additional countermeasures that could be implemented to further reduce the risks.

No. of threat	Proposed additional countermeasure including expected impact
...	...
...	...

References

[1] Computer Security: Principles and Practice. William Stallings and Laurie Brown, Prentice Hall, 2008 Applied Information Security: A Hands-on Approach, David Basin, Patrick Schaller and Michael Schlpfer, Springer, 2011