System Description and Risk Analysis

Bähler Alessio Enz Andreas Niederberger Matthias

October 28, 2017

Contents

1 System Characterization

1.1 System Overview

The System consists of three machines in a company network and external client machines that connect over the Internet. 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 and the company network because any traffic from the internet 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.

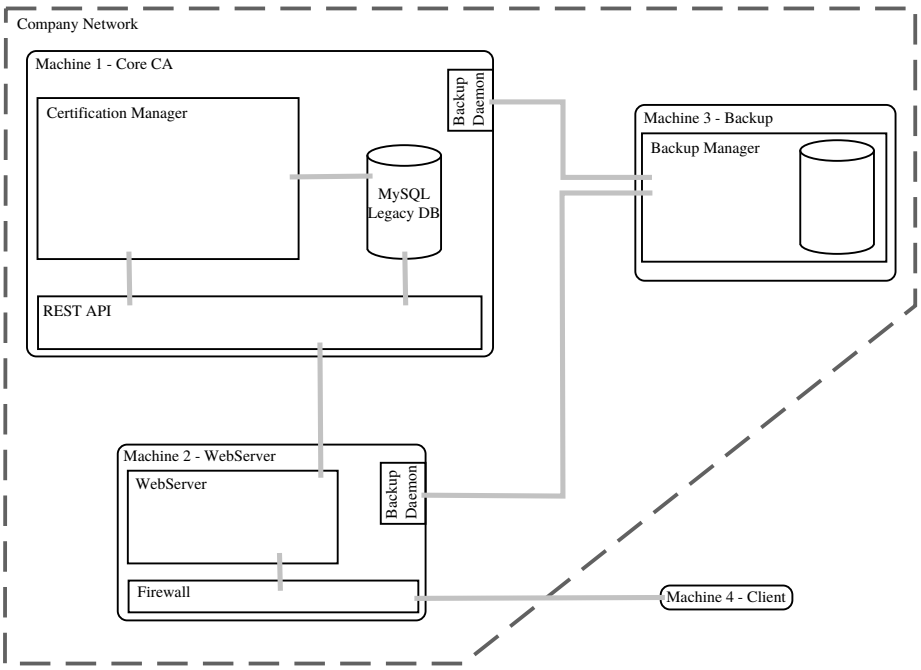

Figure 1: System Architecture of the company network including an external client machine.

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 API 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 Web Server 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. Must be available and enable secure and tamper resistant communications with the clients.
- Core CA: physical machine hosting the CA application and the legacy database.
- Backup: physical machine hosting the backup data.
- Internet Connectivity: Modem and lines connecting the WebServer to the Internet.
- Internal Network: LAN via physical lines and a switching modem.

Logical Assets

- Software
  - Web Server Application
  - Core CA Application
  - Legacy MySQL database/application/driver?
  - REST API
  - Backup Daemon
  - Backup Manager

  - Firewall

- Information
  - Certificates
  - Keys
  - User data
  - Configuration files
  - Logs

Persons

- System Administrator: maintains the system by applying software updates, controlling system logs to search malicious behaviours that could lead to security issues and ensuring that the machines hosting the systems components are working properly. He therefore has access to sensitive data, in the form of a remote connection well as physical access to all components.
- CA Administrators: are able to verify the current state of the CA.
- Users: Employees and Informants that both use the system to obtain certificates which allow them to communicate securely with the WebServer.
- Management

Intangible Goods

- Company Reputation
- Confidentiality of informant identities.

2.2 Threat Sources

- Nature: Floods, lightning strikes, earthquakes can damage the physical infrastructure.
- 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: may be non-directional or self-spreading and have different goals, e.g. Ransomware, Trojans.
- 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: lack in employee training, poor/non-existing/non-enforced security measures, such as unsanitized user input, can weaken the overall security of the system.
- Hardware Failures

2.3 Risks Definitions

Definition of Likelihood, Impact and Risk level using the following three tables from [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	Med	High
High	Low	Med	High
Med	Low	Med	Med
Low	Low	Low	Low

2.4 Risk Evaluation

Potential threats and countermeasures with the inferred risk.

2.4.1 *Evaluation Web Server*

No.	Threat	Countermeasure(s)	L	I	Risk
1	Expert Hackers: mount MitM attack to spy on and tamper with communications between Clients and WebServer. This allows the hackers to learn in particular a user's password and private keys.	HTTPs connection with Server side authentication	*Med*	*High*	*Med*
2	Victim: resorts to Script Kiddies to launch DDoS attack on WebServer and cause damage, disruptions, maybe even ask money to stop	Simple DDoS protection like SYN cookies against syn flood	*High*	*High*	*High*

2.4.2 *Evaluation Backup*

No.	Threat	Countermeasure(s)	L	I	Risk
1	User: exploits physical access to Backup Machine and obtains backup data.	Physical protection of System Components, Disk Encryption	*Low*	*Med*	*Low*

2.4.3 *Evaluation System Administrator*

No.	Threat	Countermeasure(s)	L	I	Risk
1	Expert Hacker: steals System Administrator credentials	Enforce Strong Passwords, Increase security sensibilization/awareness	*Med*	*High*	*Med*
2	Organizatorial Deficiencies: illness or injury impede its work and the System is left unattended in case of problems/attacks	Good Documentation and making sure that not only one person knows the system	*High*	*Med*	*Med*

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