

System Description and Risk Analysis

Fabian Zeindler

Leonhard Helminger

Marc Ghwiler

08.10.2013

Contents

1 System Characterization

1.1 System Overview

The system's main mission is to provide a Public Key Infrastructure (PKI) for the fictional company "iMovies". Each user (authenticated by his credentials, which are stored in a legacy MySQL database or his already created private key) can change his user information (first and last name, his email address and his password), create and revoke certificates and download the private key matching to his created certificates. To achieve this goal it implements a Certificate Authority and the following user interfaces:

User web interface Simple interface to change credentials, create/revoke certificates

Admin panel Dedicated interface to see the current CA's state

Key backup Backup of every signed certificate and the according private key

System administration Administrators have SSH access to every server

1.2 System Functionality

1.2.1 User Interface

A simple web interface which allows each user to log in either with his credentials from the legacy MySQL database, or one of his previously generated certificate and private key combinations. Once logged in the user can view his information (last name, first name and email address), change his password and update his information (last name, first name and email address). Additionally it is possible for the user to let the system issue a new certificate (based on his possibly changed credentials) and download the certificate with the newly generated private key in PKCS#12 format.

1.2.2 Administration Interface

A simple web interface (not the same as the user web interface) where CA administrators can consult the current CA state after a log in process which requires the CA administrators to authenticate themselves with their certificate. This includes the number of issued certificates, the number of revoked certificates and the current serial number.

1.2.3 Certificate Issuing and Revocation

...

1.2.4 Key Backup

To prevent the loss of any information, that was encrypted with an issued certificate, every issued certificate and the according private key are archived.

1.2.5 System Administration and Maintenance

Each server is remotely accessible per SSH. ... (Log in only with a SSH key, no password authentication, not accessible from outside the LAN/port forwarding or something like that)

1.3 Components and Subsystems

The components (as depicted in Fig. ...) are as follows:

Main Firewall A virtual machine running a software firewall in front of the whole internal network. It forwards TCP Packets on port 80 and port 443 to the web server, TCP packets on port 2211 to the web server, TCP packets on port 2220 and 2221 to the legacy db firewall, TCP packets on port 2230 and 2231 to the CA-Core firewall and TCP packets on port 2240 and 2241 to the archive firewall. It accepts TCP packets on port 2200 which is the port, the internal SSH daemon is bound to.

Web server A virtual machine running ...linux. It only accepts connections from the main firewall. The only running daemons on this server are a SSH daemon listening on port 2211 to administrate the server and a HTTP daemon listening on ports 80 and 443.

Legacy DB Firewall A virtual machine running a software firewall in front of the legacy database server. It forwards TCP connections on port 2221 and TCP connections from the web server on port 3306 to the legacy database. Additionally a SSH daemon is running on port 2220 to allow administrators to remotely administrate the firewall.

Legacy DB A virtual machine running ...linux. It only accepts connections from the legacy db firewall. The only running daemons on this server are a SSH daemon accepting connections on port 2221 to administrate the server and a MySQL daemon on port 3306.

CA-Core Firewall A virtual machine running a software firewall in front of the CA-Core server. It forwards TCP connections on port 2231 and TCP connections from the web server on port 443 to the CA-Core. Additionally a SSH daemon is running on port 2230 to allow administrators to remotely administrate the firewall.

CA-Core A virtual machine running ...linux. It only accepts connections from the CA-Core firewall. The only running daemons on this server are a SSH daemon listening on port 2231 to administrate the server and a not yet decided service listening on port 443.

CA-Core Storage A database running directly on the CA-Core server. It stores all data sets that need to be permanently stored by the CA-Core.

Archive Firewall A virtual machine running a software firewall in front of the CA-Core server. It forwards TCP connections on port 2241 and TCP connections from the CA-Core on port 443 to the CA-Core Storage. Additionally a SSH daemon is running on port 2240 to allow administrators to remotely administrate the firewall.

Archive A virtual machine running `...linux`. It only accepts connections from the Archive firewall. The only running daemons on this server are a SSH daemon listening on port 2241 to administrate the server and a not yet decided service listening on port 443.

1.4 Interfaces

1.4.1 Web Interface

1.4.2 Legacy DB Interface

1.4.3 CA-Core Interface

1.4.4 Archive Interface

2 Risk Analysis and Security Measures

2.1 Information Assets

Describe the relevant assets and their required security properties. For example, data objects, access restrictions, configurations, etc.

2.2 Threat Sources

Name and describe potential threat sources.

2.3 Risks and Countermeasures

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. For this purpose, use the following three tables.

Impact		Likelihood	
Impact	Description	Likelihood	Description
High	...	High	...
Medium	...	Medium	...
Low	...	Low	...

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

2.3.1 Evaluation Asset X

Evaluate the likelihood, impact and the resulting risk, after implementation of the corresponding countermeasures.

No.	Threat	Implemented/planned countermeasure(s)	L	I	Risk
1	<i>Low</i>	<i>Low</i>	<i>Low</i>
2	<i>Medium</i>	<i>High</i>	<i>Medium</i>

2.3.2 Evaluation Asset y

No.	Threat	Implemented/planned countermeasure(s)	L	I	Risk
1	<i>Low</i>	<i>Low</i>	<i>Low</i>
2	<i>Medium</i>	<i>High</i>	<i>Medium</i>

2.3.3 Detailed Description of Selected Countermeasures

Optionally explain the details of the countermeasures mentioned above.

2.3.4 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 countermeasure including expected impact
...	...
...	...