# System Description and Risk Analysis

Cyrill Krhenbhl Silvan Egli Lukas Bischofberger

November 18, 2016

## Contents

**1 System Characterization** **3**
1.1 System Overview . . . 3
1.2 System Functionality . . . 3
1.3 Security Design . . . 3
1.4 Components . . . 3
1.5 Backdoors . . . 4
1.6 Additional Material . . . 4

**2 Risk Analysis and Security Measures** **4**
2.1 Assets . . . 4
2.1.1 Physical assets . . . 4
2.1.2 Logical assets . . . 4
2.1.3 Logical software assets . . . 5
2.1.4 Logical information assets . . . 6
2.1.5 Persons . . . 7
2.1.6 Intangible assets . . . 7
2.2 Threat Sources . . . 7
2.3 Risks Definitions . . . 8
2.4 Risk Evaluation . . . 9
2.4.1 *Evaluation physical asset: Hardware* . . . 9
2.4.2 *Evaluation physical asset: Internal network* . . . 9
2.4.3 *Evaluation physical asset: External network* . . . 10
2.4.4 *Evaluation logical asset: Firewall software* . . . 10
2.4.5 *Evaluation logical asset: CA server software* . . . 11
2.4.6 *Evaluation logical asset: CA server application* . . . 11
2.4.7 *Evaluation logical asset: CA server database* . . . 11
2.4.8 *Evaluation logical asset: Backup server software* . . . 12
2.4.9 *Evaluation information asset: User data* . . . 12
2.4.10 *Evaluation information asset: Certificates* . . . 12
2.4.11 *Evaluation information asset: Private keys* . . . 12

2.4.12 *Evaluation information asset: CRL* . . . . . 13
2.4.13 *Evaluation information asset: Server configuration* . . . . 13
2.4.14 *Evaluation information asset: Logs* . . . . . 13
2.4.15 *Evaluation information asset: Login credentials* . . . . . 13
2.4.16 *Evaluation information asset: JWT* . . . . . 14
2.4.17 *Evaluation information asset: Archive key* . . . . . 14
2.4.18 *Evaluation information asset: Root key* . . . . . 14
2.4.19 *Evaluation person asset: User/employee* . . . . . 14
2.4.20 *Evaluation person asset: CA administrator / insider* . . . 14
2.4.21 *Evaluation person asset: System administrator* . . . . . 14
2.4.22 *Evaluation person asset: Private key holder* . . . . . 14
2.4.23 *Evaluation intangible asset: User confidence* . . . . . 14
2.4.24 Detailed Description of Selected Countermeasures . . . . 14
2.4.25 Risk Acceptance . . . . . 15

# 1 System Characterization

## 1.1 System Overview

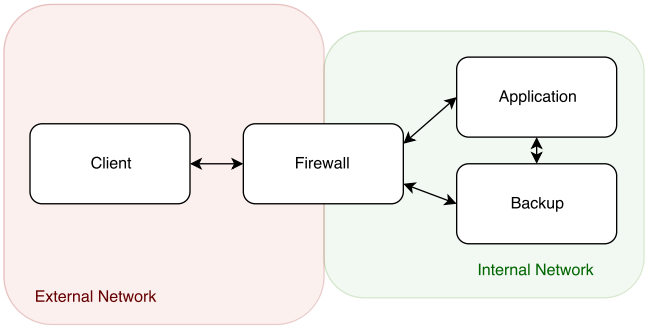


Figure 1: System overview

The mission of the system consist of providing a certificate authority (CA) service through which employees of the fictional company iMovies can request and revoke digital certificates. These certificates will be used for secure e-mail communication between employees. In the following the terms client and user will be used as a synonym for an employee of iMovies.
The architecture of the system is depicted in figure 1. The system consist of three subsystems, namely Firewall, Appserver and Backup. These subsystems form the internal network. While the firewall interfaces clients residing in the external network with the system, the Appserver's task is to control the process of issuing and revoking certificates as well as providing an interface for CA Administrators. The Backup is responsible for maintaining a copy of all system relevant data including information on users, certificates, keys, logs

## 1.2 System Functionality

## 1.3 Security Design

Describe the system's security design, including key and session management and security of data at rest and in transit.

## 1.4 Components

List all system components and their interfaces, subdivided, for example, into categories such as platforms, applications, data records, etc. For each component, state its relevant properties.

## 1.5 Backdoors

Describe the implemented backdoors.

**Hide this subsection in the version handed over to the reviewing team by setting the flag `showbackdoors` at the top of this document to `false`.**

### 1.6 Additional Material

You may have additional sections according to your needs.

## 2 Risk Analysis and Security Measures

### 2.1 Assets

#### 2.1.1 Physical assets

**Firewall:** The firewall is located in a locked and air conditioned room. There is redundant power supply for its server rack. The states of the firewall are running, compromised and down. Running means everything works as expected, compromised means an unauthorized user has had physical access to the machine and down means the firewall is not running.

**Application server:** The application server is located in the same server room with redundant power supply, but in a different rack than the firewall. The same states as in the firewall apply here.

**Backup server:** The backup server is located in the same rack as the application server also equipped with redundant power supply. The same states as in the firewall apply here.

**Internal network:** The internal network is an Ethernet local area network connecting the above mentioned components. The components are connected using layer 2 switches located in the server room. The states are running, compromised and down. A running state indicates that only authorized devices are connected to the network. A compromised state may indicate that an unauthorized user has added his own device to the network and is sniffing connections or injecting and blocking messages. A down state indicates that the network is shut down.

**External network:** The external network connects the firewall to the internet by Ethernet cable using a router that is also located in the server room. The same states as in the internal network apply here.

#### 2.1.2 Logical assets

**Connectivity:** Connections between each components and connection to the ISP. For the system to work properly, all components need to be properly connected. The states are connected and not connected.

### 2.1.3 Logical software assets

**Firewall operating system:** The operating system of the firewall is the latest Ubuntu server edition. It is managed by the system administrator who installs all relevant updates and patches within few hours after their release. The states are running, vulnerable, compromised and down. A vulnerable state indicates that the system is not up-to-date and vulnerable to known exploits. A compromised state means the system was already exploited by an attacker.

**Firewall service:** The firewall that separates the internal and external network is the latest edition of the Config Server Firewall (csf). The states are the same as for the Firewall operating system.

**Appserver operating system:** The operating system of the appserver is the same as for the firewall and the same states apply.

**Appserver webserver:** The appserver runs a nginx webserver which handles all http and https requests. It is updated by the system adminstrator. Its states are running, compromised and down. A compromised webserver allows an attacker for example to perform a man-in-the-middle attack.

**Appserver application:** The application is written in python and uses the Django framework. It manages the database and creates, revokes and provides certificates to the user. Both python and the Django framework are regularly updated by the system administrator. The states are similar to the webserver, but in a compromised state, an attacker might change the behaviour of the application.

**Appserver certificate authority scripts:** The functionality as a certificate authority is provided by a set of scripts that rely on the openssl library. The behaviour of the scripts is monitored by the system administrators. The states are the similar to the webserver, but in a compromised state an attacker also has access to certificate related functionality.

**Appserver database** The database is running MySQL and is updated and monitored for misbehaviour by the system administrator. The states are similar to the webserver, but in a compromised state an attacker has altered the database.

**Backupserver operating system:** The operating system of the backupserver is the same as for the firewall and the same states apply.

**Backupserver duplicity:** Duplicity periodically runs on the backupserver and backs up and encrypts valuable data from both the firewall and the appserver such as configurations, logs, certificates, private keys and the database.

### 2.1.4 Logical information assets

**User database:** The database contains user ids, email addresses and hashed passwords. The states are confidential and leaked. A confidential state means that only authorized system administrators and corresponding users have these informations. In a leaked state, an attacker was able to read the whole or part of the database.

**Certificates:** The certificates of each user, the certificate of the webserver and the root certificate. If a certificate is used by someone other than its owner or a certificate is used even though it was revoked, its state is invalid. Otherwise its state is valid. The severity of an invalid certificate depends on which certificate it is and if the usage of such an invalid certificate was detected, since user certificates can easily be revoked.

**Appserver configuration:** Configuration files of different services such as webserver, database, Django, certificate authority or ssh can give insight into how the system behaves and might help detect misconfigured and thus exploitable services. The states are the same as for the user database.

**Private keys:** The private keys for certificates or for ssh connections within the system. Similar states to user database, but the private key is either private or leaked.

**Crl:** The certificate revocation list has to be up-to-date and available to any user. The states are available if any user can get the list and unavailable if this is not the case.

**Backupserver configuration:** Configuration files for services such as duplicity. The states are the same as for appserver configuration.

**Logs:** Logging information about various services. The states are the same as for certificates.

**Login credentials:** Login credentials for ssh connections to different machines that may be leaked by a system administrators and login credentials from users that log into the application server. The states are the same as for the private keys, but for ssh login credential the security concern is much higher.

**JWT:** A JSON web token (JWT) describes an active connection of a user to the webserver. If an attacker manages to compromise the system in a way that he is also part of this connection, the state is compromised. For an active confidential connection the state is confidential and after the connection is closed the state is closed.

**Archive key:** The key that is used to encrypt all backed up data on the backupserver. The states are similar to the private keys.

**intermediate & root key:** The intermediate key to sign the webserver certificate and user certificates and the root key which signs the intermediate key. The states are similar to private keys.

### 2.1.5 Persons

**User/employee:** The users of the authenticated mail server, which are employees of iMovie. The state of a user is either loyal or unloyal depending on what relation he has with the company.

**CA administrator:** The CA administrators can query the certificate authority for additional information about its state but cannot modify, revoke or create any certificates (except for his own). The states are the same as for User/employee.

**System administrator:** The system administrators manages the system. The states are the same as for User/employee.

**Private key holder:** The CA administrator holds the private key of the root certificate. The states are the same as for User/employee.

### 2.1.6 Intangible assets

**User confidence:** The trust a user has in the system. This is influenced by security breaches, usability of the webserver and other factors. The user either has confidence in the system or not, which means there are two states confident and not confident.

## 2.2 Threat Sources

**Nature:** Environmental factors can hinder the execution of the system. There could be water leaks that would cause damage to servers and lost data.

**User:** The employees of iMovie can intentionally misbehave and manipulate the system or unknowingly help an attacker compromise the system.

**System administrator/Insider:** A system administrator is a more impactful threat source to the system than a user, since a compromised system administrator leads to much bigger security concerns than a compromised user.

**Script kiddies:** Script kiddies most likely do not have iMovie as their primary target, but might still try for example to infect the servers with malware to use them in a botnet. They do not have the skills to infiltrate a well protected system and so the usual security measurements and regular updates should be enough to sufficiently protect against them.

**Skilled hacker:** A skilled hacker is a big threat source and the usual security measurements most likely do not give enough protection against such an attacker. He might try to infiltrate the ca server and extract private keys to be able to imitate the webserver itself, issue arbitrary certificates or use the keys to perform man-in-the-middle attacks between employees and extract valuable information. He is most likely to be hired by a competitor or a criminal.

**Malware:** There is always the possibility of either directed or undirected malware infection if users with infected systems interact with the system.

**Organized crime:** Criminals that try to extract information from the system to blackmail people or steal valuable login credentials that are used across multiple systems.

**Competitors:** Competitors that want to undermine the reputation of iMovie, gain knowledge about company secrets or simply cause them damage.

## 2.3 Risks Definitions

| **Likelihood** | |
|---|---|
| Likelihood | Description |
| High | The threat source is highly motivated and sufficiently capable of exploiting a given vulnerability in order to change the assets 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 assets 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 assets 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. |

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

| 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 organizations 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 organizations 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 organizations mission, reputation, or interest. |

## 2.4 Risk Evaluation

In the following section we will give a risk evaluation for all possible threats and their impact on each of our assets described above.

### 2.4.1 *Evaluation physical asset: Hardware*

We can evaluate the risk for our servers and the firewall jointly as the same physical threats apply to them.

| No. | Threat | Countermeasure(s) | L | I | Risk |
|---|---|---|---|---|---|
| 1 | Nature: Component failure | Standard configuration, configuration backups, spare machines / components | *Medium* | *Medium* | *Medium* |
| 2 | Insider: Accidental or intentional destruction of components | Restrictive room access policies, spare machines / components | *Low* | *Medium* | *Low* |
| 3 | Nature: Flooding, fire etc. | Place fire alarm and sprinkler in server room, server room is located in a building on elevated level | *Low* | *High* | *Low* |
| 4 | Competitors / Organized crime: Get physical access to server room | Location of server room not public, restrictive access policy | *Low* | *High* | *Low* |

### 2.4.2 *Evaluation physical asset: Internal network*

The networking assets include the network cables and the switches/routers used in the server room.

| No. | Threat | Countermeasure(s) | L | I | Risk |
|---|---|---|---|---|---|
| 1 | Nature: Component failure | Commodity switch/router, spare cables | *Low* | *Medium* | *Low* |
| 2 | Insider: Accidental or intentional destruction of components | Restrictive room access policies, spare cables, backup switch | *Low* | *Medium* | *Low* |
| 3 | Insider: Network misconfiguration | Standard configuration, clear documentation | *Medium* | *Medium* | *Medium* |
| 4 | Nature: Flooding, fire etc. | Place fire alarm and sprinkler in server room, server room is located in a building on elevated level | *Low* | *Medium* | *Low* |
| 5 | Competitors / Organized crime: Get physical access to server room | Location of server room not public, restrictive access policy | *Low* | *Medium* | *Low* |

### 2.4.3 *Evaluation physical asset: External network*

| No. | Threat | Countermeasure(s) | L | I | Risk |
|---|---|---|---|---|---|
| 1 | Nature: ISP failure | Redundant ISP connection | *Low* | *Medium* | *Low* |

### 2.4.4 *Evaluation logical asset: Firewall software*

| No. | Threat | Countermeasure(s) | L | I | Risk |
|---|---|---|---|---|---|
| 1 | System administrator: Mis-configure firewall, purposely include backdoor | | *Low* | *High* | *Low* |
| 2 | Skilled hacker: Bypass firewall | Use restrictive access rules, regularly update system, keep access logs | *Medium* | *Medium* | *Medium* |
| 3 | Espionage / Organized crime: Bypass firewall, use zero day exploits | As above | *Medium* | *Medium* | *Medium* |

### 2.4.5 *Evaluation logical asset: CA server software*

| No. | Threat | Countermeasure(s) | L | I | Risk |
|---|---|---|---|---|---|
| 1 | System Administrator: Install bad software (e.g. sniffer), do not correctly update/configure system | Use skilled employees for the task, review system by second party | *Low* | *High* | *Low* |
| 2 | Script kiddies: DDoS | Limit incoming connections from same IP in firewall | *Medium* | *Medium* | *Low* |
| 3 | Skilled hacker / Organized Crime: Get system access | Stop all unused services, close all unnecessary ports | *Low* | *High* | *Low* |
| 4 | Malware: Use server for sending spam or distribute itself on webpages | Same as above | *HIgh* | *Medium* | *Medium* |

### 2.4.6 *Evaluation logical asset: CA server application*

| No. | Threat | Countermeasure(s) | L | I | Risk |
|---|---|---|---|---|---|
| 1 | System Administrator: ? | | *Low* | *High* | *Low* |
| 2 | Script kiddies / Skilled hacker / Organized Crime: XSS | Validate and sanitize all input | *Low* | *High* | *Low* |
| 3 | Script kiddies / Skilled hacker / Organized Crime: Eavesdrop on communication | Only use HTTPS for communication | *Low* | *High* | *Low* |

### 2.4.7 *Evaluation logical asset: CA server database*

| No. | Threat | Countermeasure(s) | L | I | Risk |
|---|---|---|---|---|---|
| 1 | Script kiddies / Skilled hacker / Organized Crime: SQL injection | Sanitize all inputs | *Medium* | *High* | *Medium* |

### 2.4.8 *Evaluation logical asset: Backup server software*

| No. | Threat | Countermeasure(s) | L | I | Risk |
|---|---|---|---|---|---|
| 1 | System administrator: Turn off backup, misconfigure backup (encryption) | Monitor backup service | *Low* | *Medium* | *Low* |
| 2 | Skilled hacker: Get access to system | Restrict access, turn off unused services, log activities | *Low* | *High* | *Low* |

### 2.4.9 *Evaluation information asset: User data*

| No. | Threat | Countermeasure(s) | L | I | Risk |
|---|---|---|---|---|---|
| 1 | System Administrator: Intentionally or accidentally modify user data | Don't allow data access to administrators | *Low* | *Medium* | *Low* |
| 2 | Script kiddies / Skilled hacker: Steal data | Always use encrypted communication, store data encrypted on backup, restrict access on user data | *Medium* | *Medium* | *Medium* |

### 2.4.10 *Evaluation information asset: Certificates*

| No. | Threat | Countermeasure(s) | L | I | Risk |
|---|---|---|---|---|---|
| 1 | User: Lose the certificate | Ability to revoke certificates | *Medium* | *Low* | *Low* |
| 2 | System Administrator: Modify data linked to certificate | Restrict data access | *Low* | *Medium* | *Low* |
| 3 | Skilled hacker: Issue bogus certificate | Don't allow user registration, log certificate creations | *Low* | *High* | *Low* |

### 2.4.11 *Evaluation information asset: Private keys*

| No. | Threat | Countermeasure(s) | L | I | Risk |
|---|---|---|---|---|---|
| 1 | User: ? | | *Low* | *High* | *Low* |
| 2 | System Administrator: | | *Low* | *High* | *Low* |
| 3 | Script kiddies: DDoS | | *Low* | *High* | *Low* |
| 4 | Skilled hacker: | | *Low* | *High* | *Low* |
| 5 | Malware | | *Low* | *High* | *Low* |
| 6 | Organized Crime | | *Low* | *High* | *Low* |
| 7 | Competitors | | *Low* | *High* | *Low* |

### 2.4.12 *Evaluation information asset: CRL*

| No. | Threat | Countermeasure(s) | L | I | Risk |
|---|---|---|---|---|---|
| 1 | User: ? | | *Low* | *High* | *Low* |
| 2 | System Administrator: | | *Low* | *High* | *Low* |
| 3 | Script kiddies: DDoS | | *Low* | *High* | *Low* |
| 4 | Skilled hacker: | | *Low* | *High* | *Low* |
| 5 | Malware | | *Low* | *High* | *Low* |
| 6 | Organized Crime | | *Low* | *High* | *Low* |
| 7 | Competitors | | *Low* | *High* | *Low* |

### 2.4.13 *Evaluation information asset: Server configuration*

| No. | Threat | Countermeasure(s) | L | I | Risk |
|---|---|---|---|---|---|
| 1 | User: ? | | *Low* | *High* | *Low* |
| 2 | System Administrator: | | *Low* | *High* | *Low* |
| 3 | Script kiddies: DDoS | | *Low* | *High* | *Low* |
| 4 | Skilled hacker: | | *Low* | *High* | *Low* |
| 5 | Malware | | *Low* | *High* | *Low* |
| 6 | Organized Crime | | *Low* | *High* | *Low* |
| 7 | Competitors | | *Low* | *High* | *Low* |

### 2.4.14 *Evaluation information asset: Logs*

| No. | Threat | Countermeasure(s) | L | I | Risk |
|---|---|---|---|---|---|
| 1 | User: ? | | *Low* | *High* | *Low* |
| 2 | System Administrator: | | *Low* | *High* | *Low* |
| 3 | Script kiddies: DDoS | | *Low* | *High* | *Low* |
| 4 | Skilled hacker: | | *Low* | *High* | *Low* |
| 5 | Malware | | *Low* | *High* | *Low* |
| 6 | Organized Crime | | *Low* | *High* | *Low* |
| 7 | Competitors | | *Low* | *High* | *Low* |

### 2.4.15 *Evaluation information asset: Login credentials*

| No. | Threat | Countermeasure(s) | L | I | Risk |
|---|---|---|---|---|---|
| 1 | User: ? | | *Low* | *High* | *Low* |
| 2 | System Administrator: | | *Low* | *High* | *Low* |
| 3 | Script kiddies: DDoS | | *Low* | *High* | *Low* |
| 4 | Skilled hacker: | | *Low* | *High* | *Low* |
| 5 | Malware | | *Low* | *High* | *Low* |
| 6 | Organized Crime | | *Low* | *High* | *Low* |
| 7 | Competitors | | *Low* | *High* | *Low* |

#### 2.4.16 *Evaluation information asset: JWT*

| No. | Threat | Countermeasure(s) | L | I | Risk |
|---|---|---|---|---|---|
| 1 | User: ? | | *Low* | *High* | *Low* |
| 2 | System Administrator: | | *Low* | *High* | *Low* |
| 3 | Script kiddies: DDoS | | *Low* | *High* | *Low* |
| 4 | Skilled hacker: | | *Low* | *High* | *Low* |
| 5 | Malware | | *Low* | *High* | *Low* |
| 6 | Organized Crime | | *Low* | *High* | *Low* |
| 7 | Competitors | | *Low* | *High* | *Low* |

#### 2.4.17 *Evaluation information asset: Archive key*

| No. | Threat | Countermeasure(s) | L | I | Risk |
|---|---|---|---|---|---|
| 1 | User: ? | | *Low* | *High* | *Low* |
| 2 | System Administrator: | | *Low* | *High* | *Low* |
| 3 | Script kiddies: DDoS | | *Low* | *High* | *Low* |
| 4 | Skilled hacker: | | *Low* | *High* | *Low* |
| 5 | Malware | | *Low* | *High* | *Low* |
| 6 | Organized Crime | | *Low* | *High* | *Low* |
| 7 | Competitors | | *Low* | *High* | *Low* |

#### 2.4.18 *Evaluation information asset: Root key*

| No. | Threat | Countermeasure(s) | L | I | Risk |
|---|---|---|---|---|---|
| 1 | User: ? | | *Low* | *High* | *Low* |
| 2 | System Administrator: | | *Low* | *High* | *Low* |
| 3 | Script kiddies: DDoS | | *Low* | *High* | *Low* |
| 4 | Skilled hacker: | | *Low* | *High* | *Low* |
| 5 | Malware | | *Low* | *High* | *Low* |
| 6 | Organized Crime | | *Low* | *High* | *Low* |
| 7 | Competitors | | *Low* | *High* | *Low* |

#### 2.4.19 *Evaluation person asset: User/employee*

#### 2.4.20 *Evaluation person asset: CA administrator / insider*

#### 2.4.21 *Evaluation person asset: System administrator*

#### 2.4.22 *Evaluation person asset: Private key holder*

#### 2.4.23 *Evaluation intangible asset: User confidence*

#### 2.4.24 Detailed Description of Selected Countermeasures

Optionally explain the details of the countermeasures mentioned above.

#### 2.4.25 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 |
|---|---|
| ... | ... |
| ... | ... |