System Description and Risk Analysis

Cyrill Krähenbühl Silvan Egli Lukas Bischofberger

November 21, 2016

Contents

1 System Characterization

1.1 System Overview

20 points

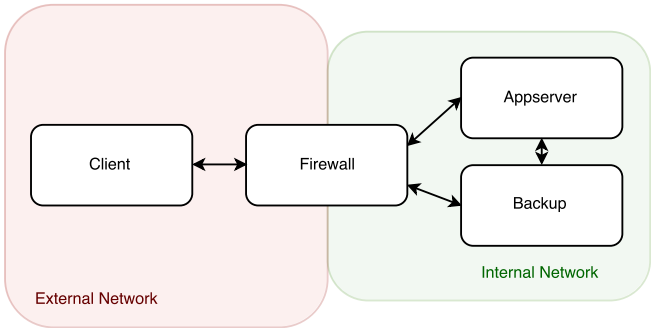

Figure 1: System overview

Describe the system's mission, the system boundaries, and the overall system architecture, including the main subsystems and their relationships. This description should provide a high-level overview of the system, e.g., suitable for managers, that complements the more technical description that follows.

1.2 System Functionality

Describe the system's functions.

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

In the following sections we describe the backdoors we implemented which should give a potential outsider control over the system, such that he can compromise the purpose of the system.

1.5.1 Easy Backdoor

We allowed a known potential vulnerability in some JWT libraries. In JWT the client specifies the algorithm used to sign the token, the library with the vulnerability allow the client to choose the 'none' algorithm. This basically allows the client to create any token with a 'none' signing algorithm where he can omit the signature. Therefore the attacker then can login as any user and perform actions in their name.

1.5.2 Hard Backdoor

The second backdoor finally exposes an open telnet connection with default credentials telnet:telnet which allows the attacker to connect to the CA server as root. To open that channel, the attacker needs to perform two actions: First we implemented port knocking on the firewall, this opens the port TODO. Then we implemented a script listening for a specific ICMP packet on the firewall which will input NAT rules to the firewall, it also sends another packet to the CA server to open the telnet port.

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 which relation he has to 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.

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.

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

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
5	Nature: Component failure	Commodity switch/router, spare cables	*Low*	*Medium*	*Low*
6	Insider: Accidental or intentional destruction of components	Restrictive room access policies, spare cables, backup switch	*Low*	*Medium*	*Low*
7	Insider: Network misconfiguration	Standard configuration, clear documentation	*Medium*	*Medium*	*Medium*
8	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*
9	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
10	Nature: ISP failure	Redundant ISP connection	*Low*	*Medium*	*Low*

2.4.4 *Evaluation logical asset: Firewall software*

No.	Threat	Countermeasure(s)	L	I	Risk
11	System administrator: Misconfigure firewall, purposely include backdoor	System administrators check for misbehaviour of other system administrators	*Low*	*High*	*Low*
12	Skilled hacker: Bypass firewall	Use restrictive access rules, regularly update system, keep access logs	*Medium*	*Medium*	*Medium*
13	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
14	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*
15	Script kiddies: DDoS	Limit incoming connections from same IP in firewall	*Medium*	*Medium*	*Medium*
16	Skilled hacker / Organized Crime: Get system access	Stop all unused services, close all unnecessary ports	*Low*	*High*	*Low*
17	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
18	System Administrator: Create certificate for some user	Log all certificate creation procedures	*Low*	*High*	*Low*
19	Script kiddies / Skilled hacker / Organized Crime: XSS	Validate and sanitize all input	*Low*	*High*	*Low*
20	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
21	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
22	System administrator: Turn off backup, misconfigure backup (encryption)	Monitor backup service	*Low*	*Medium*	*Low*
23	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
24	User: Lose their username and password	Allow them to login using a certificate	*Low*	*Low*	*Low*
25	System Administrator: Intentionally or accidentally modify user data	Don't allow data access to administrators	*Low*	*Medium*	*Low*
26	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
27	User: Lose the certificate	Ability to revoke certificates	*Medium*	*Low*	*Low*
28	System Administrator: Modify data linked to certificate	Restrict data access	*Low*	*Medium*	*Low*
29	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
30	System Administrator: Leak to external party	Only root is allowed to access private keys	*Low*	*High*	*Low*
31	Script kiddies / Skilled hacker: Steal private keys	Private keys are only accessible for root users, keys are encrypted in transfer	*Low*	*High*	*Low*

2.4.12 *Evaluation information asset: CRL*

No.	Threat	Countermeasure(s)	L	I	Risk
32	System Administrator / script kiddies / skilled hacker: Insert fake or remove real entries	Restrict write access to crl file to root	*Low*	*High*	*Low*

2.4.13 *Evaluation information asset: Server configuration*

No.	Threat	Countermeasure(s)	L	I	Risk
33	System Administrator: Leak configuration	Place configuration in standard place (secured by access policies)	*Low*	*Medium*	*Low*
34	Script kiddies / Skilled hacker: Alter configuration (e.g. weaken preferred security algorithms)	As above, additionally backup config incrementally (spot alterations)	*Low*	*High*	*Low*
35	Malware: Delete or alter configuration randomly	Backup configuration (incremental), access logs, restrictive access policies	*Medium*	*High*	*Medium*
36	Competitors / Espionage: Access configuration and use for own system	Hide internal configurations of the system from the outside	*Low*	*Medium*	*Low*

2.4.14 *Evaluation information asset: Logs*

No.	Threat	Countermeasure(s)	L	I	Risk
37	System Administrator: Accidentally or intentionally delete logs	Policy to not delete logs before they are backed up	*Low*	*Medium*	*Low*
38	Script kiddies / Skilled hacker: Insert or delete messages from the logs	Restrict access to logs to application and root	*Medium*	*Medium*	*Medium*
39	Malware: Insert random logs	Restrict access to logs to application and root	*Low*	*Medium*	*Low*

2.4.15 *Evaluation information asset: Login credentials*

No.	Threat	Countermeasure(s)	L	I	Risk
40	System Administrator: Forget login credentials	Backup offline, allow login with ssh key	*Medium*	*High*	*Medium*
41	Script kiddies / Skilled hacker: Brute force password guessing	Restrict amount of connections from same IP, enforce strong passwords	*Low*	*High*	*Low*

2.4.16 *Evaluation information asset: JWT*

No.	Threat	Countermeasure(s)	L	I	Risk
42	User: Lose JWT	Saved in browser session	*Low*	*Low*	*Low*
43	Script kiddies: Steal JWT from a not closed browser window	Short lifetime of token	*Low*	*High*	*Low*
44	Skilled hacker: Steal JWT (e.g. by malicious browser plugin)	Only store JWT in local session, short lifetime of token, enforce PW/certificate login afterwards	*Low*	*High*	*Low*

2.4.17 *Evaluation information asset: Archive key*

No.	Threat	Countermeasure(s)	L	I	Risk
45	System Administrator: Lose key (stored offline)	Store at different locations (e.g. in several safes)	*Low*	*High*	*Low*

2.4.18 *Evaluation information asset: Root key*

No.	Threat	Countermeasure(s)	L	I	Risk
46	System Administrator: Lose key (stored offline)	Store at different locations (e.g. in several safes)	*Low*	*High*	*Low*

2.4.19 *Evaluation person asset: User/employee*

No.	Threat	Countermeasure(s)	L	I	Risk
47	Competitor / skilled hacker: Steal private key to be able to read email communication	Instruct users how to safely store confidential information, regularly renew certificate, use passphrases or keys to encrypt private key on harddisk	*Medium*	*Medium*	*Medium*

2.4.20 *Evaluation person asset: CA administrator / insider*

No.	Threat	Countermeasure(s)	L	I	Risk
48	Competitor: Leak system implementation	Use standard implementations if possible	*Low*	*Low*	*Low*
49	Skilled hacker: Steal private key to have access to CA information	Use additional information to get further knowledge about the system	*Low*	*Low*	*Low*

2.4.21 *Evaluation person asset: System administrator*

No.	Threat	Countermeasure(s)	L	I	Risk
50	Skilled hacker: Steal private key to have full access to the system	Unmodifiable log files to detect intrusion into & modification of the system	*Low*	*High*	*Low*

2.4.22 *Evaluation person asset: Private key holder*

No.	Threat	Countermeasure(s)	L	I	Risk
51	Skilled hacker: Steal private key to be able to imitate the CA and sign any certificate	No possible countermeasure since all security guarantees are based on the secrecy of this key	*Low*	*High*	*Low*

2.4.23 *Evaluation intangible asset: User confidence*

No.	Threat	Countermeasure(s)	L	I	Risk
52	Competitor: Hires skilled hacker to breach the security of the system to leak customer data, which reduces the confidence of the user in the system	Increase the security of the system	*Low*	*Low*	*Low*

2.4.24 Detailed Description of Selected Countermeasures

No. of threat	Detailed Description
51?	In the case that the root key is leaked, the system does no longer have any security guarantees since the user has no longer any means of authenticating the system

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
1?	Replicated hardware to ensure redundancy in any case
7?	Let an expert from outside the company check the configuration of the internal network
12?	?
13?	?
15?	?
17?	?
21?	?
26?	
35?	
38?	
40?	
47?	Allow users to only use company certified machines to use the system which can be made more secure