System Description and Risk Analysis

Cyrill Krhenbhl Silvan Egli Lukas Bischofberger

...

Page limit: 30 pages.

Contents

1 System Characterization **2**
1.1 System Overview . . . 2
1.2 System Functionality . . . 2
1.3 Security Design . . . 2
1.4 Components . . . 2
1.5 Backdoors . . . 2
1.6 Additional Material . . . 3

2 Risk Analysis and Security Measures **3**
2.1 Assets . . . 3
2.1.1 Physical assets . . . 3
2.2 Threat Sources . . . 3
2.3 Risks Definitions . . . 4
2.4 Risk Evaluation . . . 4
2.4.1 *Evaluation Asset X* . . . 5
2.4.2 *Evaluation Asset y* . . . 6
2.4.3 Detailed Description of Selected Countermeasures . . . 6
2.4.4 Risk Acceptance . . . 6

1 System Characterization

1.1 System Overview

20 points

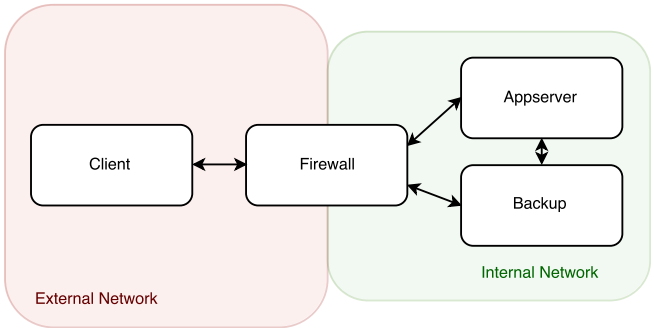

Figure 1: System overview

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

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.

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

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

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.

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.

logical: - connectivity

software: - firewall os - firewall service - appserver os - appserver webserver - appserver application - appserver ca scripts - backupserver os - backupserver duplicity

information: database - certificates - appserver application configuration (webserver, database, django, ca, ssh) - private keys - crl - backupserver application config - Logs - Login credentials - jwt - archive key - ca key (intermediate & root key)

persons: - user/employee - ca administrator - system administrator - private key holder

intangible: - user confidence

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

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: 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

2 points

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

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

2.4 Risk Evaluation

7 points

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

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.

corresponding countermeasure. Adhere to the risk definitions you have given above.

2.4.1 *Evaluation Asset X*

Evaluate the likelihood, impact and the resulting risk, *after implementation of the corresponding countermeasures*. For each threat, clearly name the threat source and the the 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
...	...
...	...