System Description and Risk Analysis

Bähler Alessio Enz Andreas Niederberger Matthias

...

Page limit: 30 pages.

Contents

Recall the following guidelines when writing your reports:

- *Adhere to the given templates.*
- *Refer to the security principles in the book for justification.*
- *Use clear terminology:*
  - *secure = confidential + authentic. Be clear about which properties you are writing.*
  - *Are pairwise distinct: certificate, private key, public key, archive to of certificate with private key. Please avoid mixing these up.*
- *Refer to the source document of your risk definitions if appropriate.*
- *For the risk evaluation, formulate the threats in active, not passive, voice: who (threat source) does what (threat action)?*
- *Use a spell checker before hand-in!*

1 System Characterization

1.1 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 access control, 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

TODO: 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

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

Physical Assets

- Web Server Machine
- Core CA Machine
- Backup Machine

Logical Assets

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

Persons

- System Administrator
- CA Administrator
- Users (Employees and Informants)

Intangible Goods

- Company Reputation

2.2 Threat Sources

TODO: Name and describe potential threat sources (*not* threats!) including their motivation.

- Nature: probably not relevant since it targets availability
- 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: TODO
- 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 (from SecEng slides): lack in employee training, poor/non-existing/non-enforced security measures (E.g. TODO) can weaken the overall security of the system.
- Hardware Failures (from SecEng slides): TODO

2.3 Risks Definitions

Define likelihood, impact and risk level using the following three tables. TODO: source from book.

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	Medium	High
High	Low	Medium	High
Medium	Low	Medium	Medium
Low	Low	Low	Low

2.4 Risk Evaluation

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. Adhere to the risk definitions you have given above. As a sanity check, there should be at least one high-risk entry.

2.4.1 *Evaluation Asset X*

Evaluate the likelihood, impact and the resulting risk, *after implementation of the corresponding countermeasures.* Formulate the threats in active, not passive, voice: who (threat source) does what (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
...	...
...	...