

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 |
| 2.2 | Threat Sources | 3 |
| 2.3 | Risks Definitions | 3 |
| 2.4 | Risk Evaluation | 4 |
| 2.4.1 | <i>Evaluation Asset X</i> | 4 |
| 2.4.2 | <i>Evaluation Asset y</i> | 4 |
| 2.4.3 | Detailed Description of Selected Countermeasures | 5 |
| 2.4.4 | Risk Acceptance | 5 |

1 System Characterization

1.1 System Overview

20 points

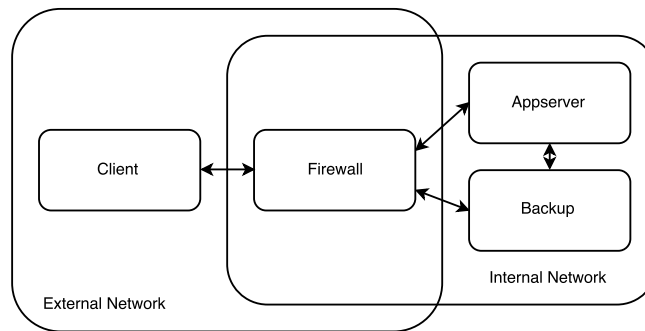


Figure 1: System overview

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

3 points

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

2.2 Threat Sources

3 points

Name and describe potential threat sources including their motivation.

2.3 Risks Definitions

2 points

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

| 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

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 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 | ... | ... | <i>Low</i> | <i>Low</i> | <i>Low</i> |
| 2 | ... | ... | <i>Medium</i> | <i>High</i> | <i>Medium</i> |

2.4.2 Evaluation Asset y

| No. | Threat | 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> |

2.4.3 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 |
|---------------|--|
| ... | ... |
| ... | ... |