ETH zürich

Applied Security Laboratory
Prof. David Basin AS 2017

# Evaluation Criteria for the Applied Security Laboratory Project

## 1 Introduction

For the project for the *Applied Security Laboratory* course each group is required to perform the following tasks for a fictional Certificate Authority:

1. Requirements analysis;
2. Risk analysis, resulting in appropriate countermeasures;
3. Secure system implementation including two backdoors;
4. System description;
5. System review of another group's system.

The results of these tasks must be documented using the two provided templates, which contain a total of three parts:

**System Description and Risk Analysis Report:** This report consists of the description of the system that the group designed and implemented, as well as of the risk analysis that was carried out (two parts).

**Security Review Report:** This document describes the approach taken by the group and the results of the security review of another group's system.

The overall rating (70 pts) of the project is split into the four parts:

1. Risk Analysis (20 pts);
2. System Description and Implementation (20 pts);
3. Security Review (20 pts);
4. Final presentation of own and reviewed system (10 pts).

The evaluation criteria of each of the above parts are described in the following sections.

# 2 Risk Analysis

## 2.1 Goals

The students perform a complete risk analysis for the fictional company, including the identification of assets, threat sources, the definition of the terms likelihood, impact, and risk, as well as the identification and evaluation of threats and countermeasures. The risk analysis is based on the book and follows the instructions provided in the distributed template.

## 2.2 Evaluation Criteria (20 pts)

**Assets (3 pts):** Identify and describe all important assets and the required security properties.

**Threat sources (3 pts):** For the identified assets, determine and describe all relevant threat sources including their motivation.

**Risk definitions (2 pts):** Give sensible definitions of the notions of *likelihood* and *impact* such that the different levels allow one to clearly rate the different threats and countermeasures.

**Risk evaluation (7 pts):** List all relevant *threats* based on the assets and threat sources. For each threat, identify appropriate *countermeasures*. Then evaluate the *remaining* risk according to the risk definitions above.

**Presentation (5 pts):** The risk analysis part of the report is clearly written, statements are justified and described in detail, and are correct and precise.

# 3 System Description and Implementation

## 3.1 Goals

This section of the report describes the system architecture, design, and implementation. It includes a high-level overview of the system, a description of its functionality, components and subsystems, interfaces, and backdoors. The system description must follow the instructions provided in the template.

## 3.2 Evaluation Criteria (20 pts)

**System design and description (7 pts):** The report is complete, i.e., all subsections given in the template are present and addressed in reasonable detail. Design decisions regarding security are motivated and justified.

**Implementation (9 pts):** The system implementation meets the given requirements. Assumptions can be made to resolve possible ambiguities in the requirements, but these must be justified. We give one point for the complete implementation and correct description of each of the following requirements.

Functional requirements (1 pt each):

1. Certificate issuing;
2. Certificate revocation;
3. CA administrator interface;
4. Key backup;
5. System administration and maintenance.

Security requirements (1 pt each):

1. Access control with regard to the CA functionality and data, in particular configuration and keys;
2. Secrecy and integrity with respect to the private keys in the key backup;
3. Secrecy and integrity with respect to user data;
4. Access control on all components.

**Presentation (4 pts):** The report is clearly written, statements are justified and described in detail, and are correct and precise.

# 4 System Review

## 4.1 Goals

After exchanging the final system description and the corresponding virtual machines, the student groups carry out a systematic review of another group's system and report. This includes a critical evaluation of their report (system description and risk analysis) as well as of their system implementation. The students must follow a clear strategy to analyze the other group's system using different testing and analysis techniques, including *black-box* and *white-box* testing. **All critiques must be justified.**

## 4.2 Evaluation Criteria (20 pts)

**System description (4 pts):** The system description of the other group's report is evaluated. It must follow the instructions provided in the template. Weak points and omissions are identified. Particular attention is given to the critical evaluation of the proposed security architecture and measures.

**Risk analysis (4 pts):** The risk analysis of the other team is critically evaluated. It must follow the instructions provided in the template. Weak points and omissions are identified.

**Implementation (4 pts):** The functionality and security of the system is systematically tested and compared to the requirements and the risk analysis. The review report includes the results of

- testing the implementation of functional and security requirements (completeness and correctness),
- evaluating the implementation of the identified countermeasures (completeness, security, and correspondence with risk analysis), and
- analyzing the system using black-box testing and white-box testing.

**Comparison (3 pts):** The review contains a comparison of the system designs and implementations of the two groups and points out highlights of each of the two systems.

**Presentation (5 pts):** The report part is clearly written, statements are justified and described in detail, and are correct and precise.