

FACULTY OF FUNDAMENTAL PROBLEMS OF TECHNOLOGY
WROCLAW UNIVERSITY OF TECHNOLOGY

CARD - TERMINAL AUTHORIZATION PROTOCOL PROTECTION PROFILE

ANDRZEJ RYBCZAK
JAKUB PLASKONKA
BARTLOMIEJ PACIOREK
MATEUSZ PLATEK

WROCLAW 2013

Contents

| | | |
|----------|---|----------|
| 1 | Protection Profile Introduction | 2 |
| 2 | Security Problem Definition | 2 |
| 2.1 | Assets | 2 |
| 2.2 | Threats | 2 |
| 2.3 | Assumptions | 3 |
| 2.4 | Organizational Security Policies | 3 |
| 3 | Security Objectives | 3 |
| 3.1 | Security Objectives for the TOE | 3 |
| 3.2 | Security Objectives for the Operational Environment | 3 |
| 3.3 | Security Objective Rationale | 4 |
| 4 | Security Requirements | 5 |
| 4.1 | Security Functional Requirements for the TOE | 5 |
| 4.1.1 | FMT_SAE.1/Time-limited authorization | 5 |
| 4.1.2 | FPT_STM.1/Reliable time stamps | 6 |
| 4.1.3 | FIA_UAU.3 Unforgeable authentication | 6 |
| 4.1.4 | PT_RPL.1 Replay detection | 6 |
| 4.1.5 | FIA_UAU.2 User authentication before any action | 6 |
| 4.1.6 | FTP_ITC Inter-TSF trusted channel | 7 |
| 4.2 | Security Requirements Rationale | 7 |
| 5 | Conformance Claims | 8 |

1 Protection Profile Introduction

2 Security Problem Definition

In this chapter, we will present the security problems, which emerge in process of designing, implementing and using the Card-Terminal Authentication Protocol. We describe the threats, organizational policies and assumptions for the TOE addressed in this paper.

2.1 Assets

| Asset name | Comment | Protection Goal |
|--------------------|---|-------------------------------|
| Passwords | Passwords allow to create a secure long-term authorization between the card and terminal. Passwords are one-term only. | confidentiality and integrity |
| Communication Data | All data that is used in traffic between card and terminal (password, nonces, etc.) | integrity |
| Users Identity | Value in the card, which allows communicating terminal to determine if card-holder is allowed to gain access to the system. | integrity |
| Protected content | All organizations possessions that are available to user after successful authentication | confidentiality |

- **End-User** - The legitimate user of the system.
- **Terminal** - A device that authenticates the End-User and gives him access to the system.
- **RFID Card** - A smartcard which is able to communicate with the terminal. Holds the keys and enables End-User to authenticate.
- **Attacker** - Any entity who tries to break system security and gain unauthorized access.
- **RFID Card Authenticator** - An Entity (e.g. System Administrator, Terminal Owner) who issues RFID Cards for End Users.
- **Any human** - Any entity who has physical access to the system elements (e.g. card, terminal).

2.2 Threats

- **T.Relay-Attack**
Relay Attack is based on signal transfer between card and reader on further distance than it is usually needed. As the example, attacker's associate who is standing next to the victim can transfer all communication via e.g. WiFi to attacker who will be able to gain access.
- **T.Replay-Attack**
Attacker eavesdrops the communication between card and reader and stores it. After that, attacker repeats all information which has been previously sent by the card to the reader and gains access.
- **T.Key-Leakage**
An adversary can obtain cryptographic keys used in protocol. Keys can leak from hardware manufacturer, software engineers, could be obtained by card cloning or by using hardware backward engineering of card or terminal. The wireless communication between card and terminal could be possible source of the key-leakage.

2.3 Assumptions

- **A.End-User** (Trustworthy End-User)
The End-User of the system is assumed to be trustworthy and follow the Security Policy.
- **A.Card** (Low range communication card)
Range of radio antenna built-in into card is assumed to be low (a few centimeters).
- **A.System-Administrators** (Trustworthy system administrators)
The system administrators are assumed to be trustworthy and follow the Security Policy.
- **A.Passwords** (One-time passwords)
The passwords generated in protocol should be one-term only.

2.4 Organizational Security Policies

- **P.ValidityCheck**
TOE shall verify the validity of a card and its state before opening door to secure location.

3 Security Objectives

In this chapter we will provide security objectives, which should be met by the TOE. Security Objectives are determined on the basis of previous chapter.

3.1 Security Objectives for the TOE

- **OT.Card Uniqueness** (Fraud Detection)
The TOE shall provide information to the System Administrators if card without trusted UID will pass authentication.
- **OT.Transmission Time**
The TOE is planned to calculate communication delays. Reader calculates cards response time.
- **OT.Transmission Uniqueness**
In the TOE every transmission between card and reader is unique.

3.2 Security Objectives for the Operational Environment

- **OE.End-User** (Trustworthy End-User)
The End-User of the system shall be trustworthy and follow the Security Policy. Additionally, any problems with interfacing with the system (such as terminal denying access to secure location even though a valid card is used) should be immediately reported to the System Administrator.
- **OE.Card** (Secure and unique card)
The content of the card shall be inaccessible without cryptographic authorisation. Smartcard should be equipped in low power antenna. Each card will receive a counter or unique hash, which value will be generated after each authentication. The terminal shall distinguish two cards with same UID and different generated values.
- **OE.System-Administrators** (Trustworthy system administrators)
The system administrators shall be bound by the legal contract to not publish technical details about the system and follow the Security Policy.

- **OE.Secure Access**

The system, as well the enviroment surrounding the TOE should allow access to protected content only after successful authorization.

3.3 Security Objective Rationale

| | OT.Card Uniqueness | OT.Transmission Time | OT.Transmission Uniqueness | OE.End-User | OE.Card | OE.System-Administrators | OE.Secure Access |
|-------------------------|--------------------|----------------------|----------------------------|-------------|---------|--------------------------|------------------|
| T.Relay-Attack | | X | | | | | |
| T.Replay-Attack | | | X | | | | |
| T.Key-Leakage | X | | | | | | |
| P.ValidityCheck | | | | | | | X |
| A.End-User | | | | X | | | |
| A.Card | | | | | X | | |
| A.System-Administrators | | | | | | X | |
| A.Passwords | | | | | X | | |

The threat **T.Relay-Attack** is addressed directly by the **OT.Transmission Time** security objective. The relay attack require sending the authentication data on large distances, which would resolve in long time of response from the attackers card. The system should calculate the response time and if the safe time of response was exceeded it should halt the communication.

The threat **T.Replay-Attack** is addressed directly by the **OT.Transmission Uniqueness** security objective. The replay attack require sending the same message in effort to authenticate correctly. If the system will generate random unique values each time, the replied attacker message with resolve in different authentication result each time.

The threat **T.Key-Leakage** is addressed directly by the **OT.Card Uniqueness** security objective. Thanks to unique Card ID, when key is leaked it can be only applied to a Card with different ID. This can be easily detected.

The requirements of **P.ValidityCheck** are met by the **OE.Secure Access**. The safe enviroment which protects the valuable content behind the doors implies that the only way to access this content is to authenticate in the system.

The assumption **A.End-User** is directly addressed by **OE.End-User** which denotes that the user should be trustworthy and follow the applied Security Policy.

The assumption **A.System-Administrators** is directly addressed by **OE.System-Administrators**. The System Administrator is bound by the legal contract to not publish technical details about the system and follow the Security Policy, which meets the requirements of assumption.

The assumptions **A.Passwords** and **A.Card** are directly addressed by **OE.Card**. The card should possess a counter or unique hash which value will change on each authentication. This implies the assumption of one time passwords. Also the smartcard has to have a low range antenna which meets the assumption **A.Card**.

4 Security Requirements

The CC allows several operations to be performed on functional requirements; refinement, selection, assignment, and iteration.

The **refinement** operation is used to add detail to a requirement, and thus further restricts a requirement. Refinement of security requirements is denoted in bold text and the added/changed words are in **bold text**.

The **selection** operation is used to select one or more options provided by the CC in stating a requirement. Selections that have been made by the PP authors are denoted as underlined text and the original text of the component is given by a footnote. Selections to be filled in by the ST author appear in square brackets with an indication that a selection is to be made, [selection:], and are italicized.

The **assignment** operation is used to assign a specific value to an unspecified parameter, such as the length of a password. Assignments that have been made by the PP authors are denoted by showing as underlined text and the original text of the component is given by a footnote. Assignments to be filled in by the ST author appear in square brackets with an indication that an assignment is to be made [assignment:], and are italicized. In some cases the assignment made by the PP authors defines a selection to be performed by the ST author. Thus this text is underlined and italicized like this.

The **iteration** operation is used when a component is repeated with varying operations. Iteration is denoted by showing a slash "/", and the iteration indicator after the component identifier.

4.1 Security Functional Requirements for the TOE

4.1.1 FMT_SAE.1/Time-limited authorization

The TOE shall meet the requirement "Time-limited authorization (FMT_SAE.1)" as specified below (Common Criteria Part 2).

| | |
|------------------|---|
| Hierarchical to: | No other components. |
| Dependencies: | FMT_SMR.1 Security Roles FPT_STM.1 Reliable time stamps |
| FMT_SAE.1.1 | The TSF shall restrict the capability to specify an expiration time for <u>every information exchanged between the card and the terminal to all of the users.</u> |
| FMT_SAE.1.2 | For each of these security attributes, the TSF shall be able to <u>discard current communication session</u> after the expiration time for the indicated security attribute has passed. |

4.1.2 FPT_STM.1/Reliable time stamps

The TOE shall meet the requirement "Reliable time stamps (FPT_STM.1)" as specified below (Common Criteria Part 2).

| | |
|------------------|--|
| Hierarchical to: | No other components. |
| Dependencies: | No dependencies. |
| FPT_STM.1.1 | The FST shall be able to provide reliable time stamps. |

4.1.3 FIA_UAU.3 Unforgeable authentication

| | |
|------------------|--|
| Hierarchical to: | No other components. |
| Dependencies: | No dependencies. |
| FIA_UAU.3.1 | The TSF shall {selection: detect, prevent} detect use of authentication data that has been forged by any user of the TSF.. |
| FIA_UAU.3.2 | The TSF shall {selection: detect, prevent} detect use of authentication data that has been copied from any other user of the TSF. |

4.1.4 PT_RPL.1 Replay detection

| | |
|------------------|--|
| Hierarchical to: | No other components. |
| Dependencies: | No dependencies. |
| FPT_RPL.1.1 | The TSF shall detect replay for the following entities: {assignment: list of identified entities} . messages. |
| FPT_RPL.1.2 | The TSF shall perform {assignment: list of specific actions} card blocking when replay is detected.. |

4.1.5 FIA_UAU.2 User authentication before any action

The TOE shall meet the requirement "User authentication before any action (FIA_UAU.2)" as specified below (Common Criteria Part 2).

| | |
|------------------|-------------------------------------|
| Hierarchical to: | FIA_UAU.1 Timing of authentication. |
| Dependencies: | FIA_UID.1 Timing of identification. |

The TSF shall require each user to be successfully authenticated before allowing any other TSF-mediated actions on behalf of that user.

Hierarchical to: No other components.

Dependencies: No dependencies.

FTP_ITC.1.1 The TSF shall provide a communication channel between itself and another trusted IT product ~~that is logically distinct from other communication channels~~ and provides assured identification of its end points and protection of the channel data from modification or disclosure.

FTP_ITC.1.2 The TSF shall permit to initiate communication via the trusted channel.

FTP_ITC.1.3 ~~The TSF shall initiate communication via the trusted channel for~~
[assignment: list of functions for which a trusted channel is required].

4.1.6 FTP_ITC Inter-TSF trusted channel

The TOE shall meet the requirement "Inter-TSF trusted channel (FTP_ITC)" as specified below (Common Criteria Part 2).

The threat T.Key leakage is addressed directly by the OT.Card Uniqueness security objective. Thanks to unique Card ID, when key is leaked it can be only applied to a Card with different ID. This can be detected.

4.2 Security Requirements Rationale

| | OT:Card Uniqueness | OT:Transmission Time | OT:Transmission Uniqueness |
|-----------|--------------------|----------------------|----------------------------|
| FIA_UAU.2 | x | | |
| FTP_ITC | x | | |
| FIA_UAU.3 | | | x |
| PT_RPL.1 | | | x |
| FMT_SAE.1 | | x | |
| FPT_STM.1 | | x | |

OT:Card Uniqueness require the TOE to detect an authentication using card with untrusted UID. The SFRs FIA_UAU.2 and FTP_ITC state, that card must be authenticated before any action using trusted channel allowing administrator to detect untrusted UID, thereby meeting this objective.

OT:Transmission Time requires **FMT_SAE.1** „Time-limited authorization” and **FPT_STM.1** „Reliable time stamps”. **FMT_SAE.1** provides means to limit acceptable card response time, thus preventing relay attacks. **FPT_STM.1** provides reliable time stamps for **FMT_SAE.1**.

OT.Transmission-Uniqueness requires **FIA_UAU.3** "Unforgeable authentication" and **PT_RPL.1** "Replay detection". The **FIA_UAU.3** is responsible for detection of authentication data that has been copied or forged and has been marked by System Administrator as not-trusted. **PT_RPL.1** is responsible for detection of replayed messages and if detected to block the card.

5 Conformance Claims

References