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 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

- **End-User** - The legitimate user of the system.
- **Terminal** - A device that authenitcates 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 eavedrops 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.Terminal** (Secure terminal)
  The terminal is assumed to be resistant to backward-engineering and theft. Any attempt of the latter should result in invalidation of information stored inside it.
- **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 will be met by the TOE.

3.1 Security Objectives for the TOE

- **OT.Card Uniqueness** (Fraud Detection)
  The TOE shall provide information to the System Administrators if card with trusted UID will not 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.Terminal** (Secure terminal)
  The terminal shall be resistant to backward-engineering and theft. Any attempt of the latter shall result in terminal unconditionally blocking any further attempts of gaining access to secure location, so the incident is acknowledged by system administrators as soon as possible.

- **OE.Card** (Secure and unique card)
  The content of the card shall be inaccessible without cryptographic authorisation.
  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.Protocol** (Secure protocol)
  The protocol should be built using only well documented cryptographic elements that are proven to be safe.

3.3 Tabelka

	OT.Card Uniqueness	OT.Transmission Time	OT.Transmission Uniqueness	OE.End-User	OE.End-User	OE.Terminal	OE.Card	OE.System-Administrators	OE.Protocol
T.Relay-Attack									
T.Replay-Attack									
T.Key-Leakage									
P.ValidityCheck									
A.End-User									
A.Terminal									
A.Card									
A.System-Administrators									
A.Passwords									

4 Security Requirements

5 Conformance Claims