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
Card	To authenticate in the system, user will use a smartcard, which he will receive from system administrator. Smartcards will use Mifare Classic standard, which provides basic operations and simple counter.	integrity
Terminal	Device provided by trusted third party. It will cooperate with Mifare Classic smartcards. The terminal will authenticate user if correct smartcard is provided.	integrity
Passwords	Passwords allows 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

and rest of actors

2.2 Threats

- Relay Attack
- Replay Attack
- Card cloning
- Key leakage
- Compromisation of algorithm