System Security, Spring 2010

Exercise 2

Distribution: 12.03.2010
Hand in: 18.03.2010

1 Smart Cards

Most of you will have one or more smart cards in your purse and use them nearly every day. The range of application and also the requirements of these cards are varying. In nearly all applications of a smart card security plays a central role.

(a) What exactly is a smart card? Find information on the Internet and describe the different types of smart cards and their components.

(b) Consider three different examples of applications for smart cards and describe informally the security requirements of the card (e.g., library card, member card, ec-card).

(c) Describe the term "skimming" in context of smart cards?

2 EEPROM

A major part of a smart card or, more generally, of a tamper proof tool is an EEPROM chip.

(a) What is the function of such an EEPROM and what is its role in a Tamper Proof Tool?

(b) What is the main problem to guarantee the successful deletion of information on an EEPROM?

3 Locking System

A car manufacturer wants to equip his cars with a new locking system which works in the following way: The system is composed of a small (tamper-proof) sender embedded in the car key and a receiver in the car. Pushing a button on the sender causes it to send an radio frequency signal. The signal consists of 128-bit string which is the actual cryptographic key and which will be checked by the receiver. The range of the sender is about $20m$.

The cryptographic key length renders a brute force attack impossible and the sender can be considered tamper-proof.

(a) The system seems to be as secure as a classical lock. Do you see another possibility to break the security of the system?

(b) What can be done to avoid the attack you just described?

4 Advanced Encryption Standard

Consider the symmetric encryption algorithm AES.

(a) Which operations are applied by AES to encrypt a plaintext?

(b) What is the weak point in the design/implementation of AES that timing attacks exploit? Explain the attack in detail, using your own words! For example, mention how many messages have to be sent to the attacked server!