Security and Trusted Hardware Applications
Week #3 Tutorial

Pedro Antunes - up201507254

May 30, 2022

U. PORTO

FC FACULDADE DE CIÊNCIAS
UNIVERSIDADE DO PORTO

Instructor: Bernardo Portela

1

The main characteristics associated with a smart card are:

- Reduced size and made of flexible plastic - typically is the same size as a credit card;
- Store and process information with a micro-controller under a gold plate, containing a single silicon integrated circuit chip with memory and microprocessor;
- Tamper-resistant (it is possible but it needs sophisticated tools to break the circuit chip, and then smart card gets unusable);
- Self-contained, i.e no external power is required;
- It has a unique identifier and can neither be forged nor copied.

When there is storage of information by a system, there are attack vectors that can allow an attacker to gain unauthorized access to this type of sensitive information.

Therefore, when there is sensitive information that needs to be stored persistently or temporarily, it is necessary to use secure storage methods to protect the stored sensitive information.

Smart cards are a secure storage option that can be easily carried to any physical location due to their characteristics.

2

Security by obscurity means that we are using cryptographic implementations without actually knowing the methods and paths used to produce a response to what has been requested. Thus, it is not possible to validate or prove that something is or is not done right. For example, we cannot say that there are no backdoors behind some obscurity software/hardware, because we have no way of looking at the construction of the software/hardware and really proving whether or not it has backdoors or other features.

Proprietary algorithms assimilate to the uncertainty of security by obscurity. In contrast to this, open-source algorithms that follow certain implementation standards give us better guarantees that there is indeed real security with certain assumptions. This is because, there is a large community trying to break the implementations of these systems and this is what actually gives strength and security to these implementations.

3

A half-duplex communication means that the communication channel can only be used by one of the entities in the communication. For example, a communication from a smart card to a reader, the smart card communicates to the reader and the reader after this communication is over communicates its response, or vice versa.

Smart cards always begin in receive mode and use a data structure called APDU (Application Protocol Data Units). This structure facilitates half-duplex communication by having precisely a command APDU structure that makes requests or triggers some event, and a structure that responds to a command APDU called a response APDU.

4

Physical attacks are typically invasive attacks that damage and modify the smart card chip circuits such that the smart card becomes unusable. However, there are non-invasive physical attacks that involve trying to remove information about what procedure and computation the smart card performs, such as voltage and temperature manipulation or clock times.

In opposite, malware attacks are not invasive to the point of physically damaging the smart card. These attacks are characterized by software that is silently injected into the card and then looks for functionalities on the card that allow it to exploit and unlock the secret key. For example, expecting the user to sign some information by entering a secret PIN. Usually there is a PIN request for each use of the smart card. One way this malware acts would be, after the user enters the PIN, to launch a new request for the user to enter the PIN again but now in malicious software.

Software countermeasures can and must be implemented to try to stop problems like this. However, these countermeasures prevent malware attacks more easily than physical attacks. In the presence of physical attacks and through software, we can force constant-time processing of the smart card and prevent possible timing attacks and temperature measurements. However, invasive attacks aimed at damaging the chip and we cannot prevent this with software countermeasures.

Two countermeasures to malware attacks are the use of a single-access device driver architecture and defining one private key for every PIN entry, and thus preventing information from malicious actors being signed by the smart card user key.

5

a) The ISO/IEC 14443 refers to contactless smart cards for proximity systems.

b) The usage of these cards in the modern world is increasing every day, specially after covid-19 pandemic. Nowadays, we can easily find these systems in bank cards, public transportation cards, or educational institution cards.

c) The technique used for communication is NFC (Near Field Communication), a protocol of RFID (Radio Frequency Identification) family. Specifically, NFC is a branch of High-Frequency (HF) RFID and is designed to be a secure form of data exchange.

d) The NFC protocol entities communicate via radio waves. Consists in two devices - the NFC tag and the NFC reader exchange information in NFC data exchange format.

An NFC tag sends radio waves to activate the antenna in a receiving device. The recipient validates the information to complete information exchange. The technology works over a very short distance — approximately 4 inches. NFC tags work without a battery and draw power from another device.

An NFC reader connects to only one NFC tag at a time, minimizing accidental transactions. During NFC payments, encrypted data exchange happens between NFC chips. Card details can be stored on a smartphone, which then acts like a traditional card.