Smart Cards

Paulo Leal
Faculdade de Ciências
Universidade do Porto
up201101503@fc.up.pt

José Reisinho
Faculdade de Ciências
Universidade do Porto
up200901635@fc.up.pt

Carlos Fernando
Faculdade de Ciências
Universidade do Porto
up201002603@fc.up.pt

José Valente
Faculdade de Ciências
Universidade do Porto
up201102801@fc.up.pt

***Abstract*—*Smart Cards* Smart Cards (SC) are currently present in the life of most of us. Mobile phones, banks, personal identification, social security, public transportation, healthcare, computer systems... All of these are areas that make use of this technology in order to provide easy access and increased security. But.. Are we really safe?**

I. Introduction

This paper aims to provide some insight, via our research, of the current state of technologies used in SC as well the modern day uses of SC.

More specifically we intend to describe the security aspect of SC regarding both software and hardware, stating the protocols that are in use, analyzing their flaws, describing possible attacks, and whenever possible proposing/mentioning solutions that could prevent their nefarious use.

We approached this by determining the current types of SC, their capabilities and functions; the who and why attacks would happen; analyzed possible attacks (and concurred that Logical Attacks, Physical Attacks, and Side Channel Attacks are the primary sort of them); and gave examples to some of these attacks.

II. State of the Art

Smart Cards are a type of chip card, meaning that they are a plastic card with an embedded computer chip. The computer chip used can be either a memory chip, used for storing values and data, or a microprocessor which processes the data stored. Transactions are made with the stored or processed data via a reader in a computing system.

A. Why SC?

Smart Cards have their main use in authentication, access control and privacy protection. These facets of the technology are often shown by its proliferation in EMV[1] transactions, phone SIM cards or hotel key-cards.

Observing the technologies possibilities it is easy to see why it is used frequently. It allows to store information reliably and to control its access, making it very attractive to store information like a patient's history for health care professionals. It allows for the running of public key encryption in order to identify its bearer, permitting user access control for restricted areas and to allow transactions(credit cards). Smart Cards also allow for the usage of an electronic purse, storing a monetary value to use in small purchases. This allows not using card readers that require a phone connection to the host computer and reduces the need for ticketing machines and similar devices.

Fig. 1. Smart Card

These characteristics make Smart Cards a very useful facilitator to plenty of industries making them a very important technology currently.

B. Types of SC

A multitude of technologies and uses are applied in SC, whether a card possesses processing capabilities or acts as a 'dumb' storage and the different uses of memory are approached in this section, as well as some of the security measures used. [2] [3]

1) Contact Cards: The most common type of smart card, they function via electrical contacts that are located on the outside area of the card, which connect to a card reader whenever the card itself is inserted. These contacts are bonded to an inner chip present in the card.

2) Memory Cards: These cards have no processing power for data management and communicate via synchronous protocols, there are two operations that can be done to a fixes address in the card : Read, and Write.

- Straight Memory Cards (SMC) - Should be thought of as a modern day floppy disk; Has no data processing capability and cannot identify itself to the reader which requires the system to know what type of card is being used. SMC can be easily duped and cannot be tracked by on-card identifiers.

- Protected or Segmented Memory Cards - Cards which possess logic in order to control the access to the memory of the card, they can be set to write-protect some, or the entirety, of the memory array. In some cases a password or system key may be used to configure restricted access to both reading and writing on the card. Can have multi-functionality by dividing the card into smaller logical segments. These cards are not as easily duplicated but they can be impersonated although tracking is available via an on-card identifier.
- Stored Value Memory Cards - Designed for the purpose of storing values or tokens these cards are either disposable or rechargeable. Many incorporate security measures, like passwords, hard-coded at the time of manufacture. The memory arrays of these cards are set-up as counters and there is barely any memory left for other functions. The number of memory cells depends on the application but they are cleared each time they are used and once all of them are cleared the card becomes useless and is either thrown away or the clearing reversed in the case of a rechargeable card.

3) CPU/MPU Multifunction Cards: Multifunction SC divide the card memory in order to create smaller independent sections (or files) that can be assigned to a particular function or application, thus possessing on-card dynamic data processing capabilities. This kind of chip utilizes a Card Operating System (COS) in order to manage data in its organized file structures, which permits multiple uses of the same card. These cards utilize modern transaction and encryption technologies which provide secure identification of users and allows for information updates without replacing the cards. Some of these cards support even Public Key Encryption (PKE) with on-board math processors.

4) Contactless Cards: SC that use Radio-Frequency Identification (RFID) in order to communicate with the reader without a physical connection or physical contact, in which the card is read when it is passed within a certain degree of proximity of the reader. They operate with very limited memory and, generally, in read-only mode, at certain frequencies (125MHz, and 860MHz to 960MHz).

5) Multi-Mode Communication Cards: These cards include multiple methods of communication such as ISO7816[4] and UHF gen 2[5]. Further denomination such as Hybrid or Dual Interface are determined in the way they are constructed.

- Hybrid Cards - Cards that have multiple chips, while having each chip connected to a corresponding interface are called Hybrid Cards.
- Dual Interface Cards - Dual Interface Cards use a single chip that controls its interfaces.
- Multi-Component Cards - These kinds of SC are generally specifically constructed for a determined market solution. They are often patented uses with several required specifications.

III. Threats

A. Who pose as attackers?

1) Insiders: Those who have a legitimate access to what they are attacking. Which means they are a trusted part of the infrastructure required by that which they attack, this forces most protocols, as a prevention method, to adopt a ”trust but verify” approach.

2) Outsiders: Those who do not have a legitimate access to that which they are attacking. This means that, more often than not, the attacker must first gain access to either the infrastructure or the communication paths that are used for the protocols, usually this access is acquired through nefarious methods.

There are however many possible reasons to attack and break, or at the very least attempt to, the security of these devices.

B. Why do they attack SC?

1) Personal: So long as there is an object/system/protocol that is claimed to be secure someone somewhere will have the itch to go and break its security to, if nothing else, acquiring the bragging rights of having been the first person to figure out how to do so.

2) Monetary: This type of attacker is after that, which the love for is the root of all evil: Money. And since these devices are considered secure and are used by the banking industry as ”keys” to our life savings why not obtain the key so that they also become the attacker’s life savings?

3) Political: With the advent of the access pass some areas require it as an added access key for authentication and traffic control, for example, the American Department of Defense (DOD) Common Access Card (CAC), which might provide an attacker physical/virtual access to areas or information he was not supposed to be able to reach.

Based upon [6][7]

IV. Attacks

There is a wide number of attack possibilities as well a a great variety of parties involved in a smart card-based system, thus we are able to categorize the attacks in various ways. Striving for simplicity, we have divided them into three main categories:

1) Logical Attacks - Protocol or software implementation exploitation
2) Physical Attacks - SC/PoS Hardware modification and analysis
3) Side Channel Attacks - Usage of physical phenomena to analyze or modify the SC behavior

A. Logical Attacks

Communication between a Smart Card and a terminal is performed via a single communication channel, a serial interface, that allows commands to be issued and performed by the card.

Attack Vectors:

- Parameter Poisoning and Buffer Overflow - This can be achieved through 'misuse' of the command parameters. This vulnerability aims to allow execution of arbitrary code in the target system and can be triggered using a malicious smart card. On November 3rd, 2010, a buffer overflow vulnerability was reported in the code handling the smart card's serial number on the OpenSC Library. This vulnerability made this type of attack possible. [8]
- Hidden Commands - Usage of hidden commands left from a previous application or from the initialization of the card. These may be used to retrieve or modify data in the SC. There is a surprising number of command options that may be supported by the card and Logical Attacks focus on these to try and trick smart cards into allowing data modification or leak of confidential data. Technically, a SC is able to recognize about 65000 unique commands. Although the practical use of the card only requires a handful of these, others may still be left in the card from a previous initialization phase or previous application. Some of these commands are, for example:
  - SELECT: Open a file or directory.
  - READ: Read a file
  - UPDATE: Change the contents of a file
  - AUTHENTICATE: Authenticate the SC to the external world
  - VERIFY: Check a cardholder's PIN code
- Malicious Applets - Most Java Cards lack an on-card bytecode verifier, which can be found on regular Java. Theoretically, this opens up the possibility of malicious code as a means of attack. Another possible flaw is the application separation on SC that support multiple applications. If the attacker is able to either abuse a vulnerable application or download a malicious one, these may be able to compromise sensitive applets.
- File Access - Command access permissions determine the required security procedures to access a file. Not only may the access permissions allow more access than needed for some files, they may also be disrupted when complex interactions occur when there is the need to access several applications in one session, creating a possible attack path.
- Communication Protocol - The communication between a SC and a terminal is handled by a protocol that controls the data flow and error recovery. A possible approach to attack this protocol is to sending messages outside the scope of the current state thus trying to gain access to secure information. A well known example is the use of an error correction facility in this protocol. It works by storing operation results within a small buffer in the RAM of the SC. The receiver of a message can request it's re-transmission whenever it is not correctly received. If a terminal asks for re-transmission of a message that has not been sent, a bad protocol implementation may return the buffer contents. The same may happen if the buffer length field is not properly initialized, compromising the entire contents of the SC memory. This issue is similar to a recent vulnerability in OpenSSL, named Heartbleed. [9]
- Cryptographic Protocol - As in any other secure system, Cryptography is key. If a protocol is not correctly implemented, it may be possible to attack the card with, for example, a replay attack. Other issues may also arise, like less secure cryptographic fallback protocols that the SC will revert to, in the event of a malfunction. There's also the possibility of the random number generator being predictable, which can compromise the whole cryptographic process. (..NSA?)

B. Physical Attacks

Physical attacks on SC are hardware oriented and their goal is to reverse engineer the functions contained in the chip. These attacks usually require high-end laboratory equipment.

Attack Vectors:

- Microscopes - Reverse engineering of the chip can be done using a SEM (Scanning Electron Microscope) or even an Optical microscope. Despite the small size of a chip's features (below one micron), the use of a good optical microscope may still yield results and allow the attacker to reconstruct the circuit or operating system with the use of automated tools. SEM's are a lot more powerful as not only do they allow seeing much smaller details, they also allow visualization of current flow. By analyzing high and low voltage (Voltage Contrast) in a chip, an attacker can distinguish between active and inactive parts of the chip while it's performing a function and even go as far as to see the actual contents of the RAM memory cells.

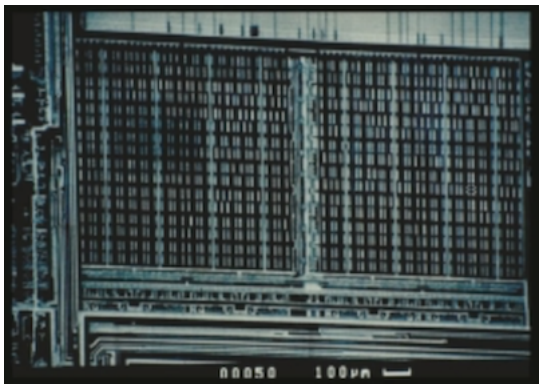

Fig. 2. Voltage Contrast of RAM Cell [10]

- Chemical Solvents, Corrosion and Staining Materials - A SC silicon chip is attached to a facade that contains the contacts and is then covered with epoxy resin which then glues the chip to the card. This creates a physical security layer as an attacker has to remove most of the

epoxy layers that cover the chip. Polyimide is sometimes used as an extra layer to make the chip's surface harder to see. We then have the passivation layer, just above the chip's metal layers. This also needs to be removed in order to be able to successfully perform an analysis of the chip. Removing these layers is a thorough process and requires very aggressive and dangerous chemicals, which implies that it should only be executed by experts in a chemistry lab. The chip is often rendered non-functional after Etching, given the aggressive nature of hydrofluoric acid.

Fig. 3. Etched SC Chip [10]

- Probe Stations - These stations allow tiny needles to be positioned on arbitrary wired of a naked chip. This allows, if the data bus is located, capture of the data exchange between the CPU and the memories. Using a logic analyzer we can also retrieve running program code and program data. We can force the chip to accept data that will overwrite the original data or even change the micro-instructions in order to give the processor a different execution path.
- Focused Ion beam (FIB) - By shooting ions (instead of electrons like in the SED) into the circuit, it is possible to make changes to the circuit. Adding different gases to the ion beam also allows the creation of wires, insulators and semiconductors. This technology makes repairing a damaged circuit possible as well as changing the circuit to, for example, redirect signals to external wires.

C. Side Channel Attacks

Side Channel attacks focus on the utilization of physical phenomena, like electricity and radiation, to analyze and manipulate the behavior of a SC chip. These attacks do not require physically opening the card and can be performed without damaging it.

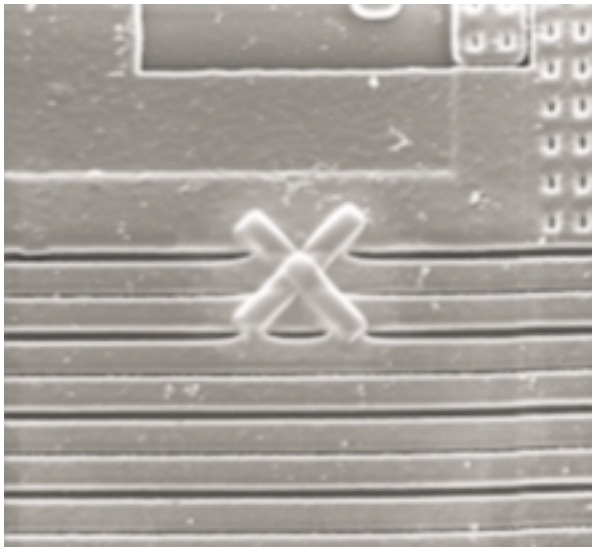

Fig. 4. Cross-shaped probe pad (FIB) [10]

Attack Vectors:

- Power Consumption Analysis - By analyzing the power consumed by a chip, an attacker can learn a lot about the ongoing processes, as electric current is used during operation by the semiconductors and its measurement can yield various details about the information being processed.
- Electromagnetic Radiation Analysis - Much like power consumption analysis, this can also provide valuable information about the ongoing processes and information being processed, as transistors produce a small amount of electromagnetic radiation.
- Power Glitching - By tampering with the power delivered to the SC, glitches may occur, as microprocessors are supposed to operate using a stable voltage. These glitches will affect stored values and depending on the internal SC capacities, the values will be influenced differently, resulting in a possible misinterpretation of the real value.

Power Consumption Analysis and Power Glitching are the most common types of Side Channel Attacks, as they are cheap to perform and offer a high chance of success.

D. Other Attacks

There are other threats that do not fall into any of the above categories:

- Eavesdropping - This attack aims to intercept and alter data being transmitted over the air
- Denial/Interruption of service - Attack that aims to disrupt the communication between the card reader and the card

V. Countermeasures

A. Logical Attacks

Smart Card sensitivity to logical attacks directly depends on code complexity. The more complex the software, the bigger the probability of a bug in it's implementation. There are some possible countermeasures:

- Formal Verification - Through the use of mathematical models, we can prove function safety.
- Testing - Validating the implementation experimentally reduces the risk of leaving a bug behind.
- Structured Design - Dividing software in small functional blocks makes it easier to not only understand the functions but to validate them.
- Standardization of Interfaces and Applications - Re-usage of proven software decreases chances of flaws.
- Convergence to the Java Card Operating System - This is an object oriented language designed especially for security, which makes it more secure than older monolithic systems that do not implement application separation.
- Evaluation Labs - These are laboratories that evaluate the security of a SC and issue a formal report/certificate.

B. Physical Attacks

Physical security has risen significantly over the most recent years. This derives from the growth of the SC industry, which led to the creation of a mass market, thus making it possible for manufacturers to afford and use advanced equipment and change the design of the chips into something far more sophisticated. Possible countermeasures for physical attacks:

- Feature Size - The advance of technology greatly aids in terms of component size. By reducing the transistor and wire sizes on the chip's surface, not only are we able to make them too small for probing station needles, we are also making them exponentially harder for optical microscopes to analyze.
- Protective Layers - It is possible to use a top layer containing a grid that carries a protective signal. If said signal is interrupted, memories are erased and processes halt. It is still possible to bypass such a layer with a great amount of skill so, by using a large number of non-correlated signals and frequently changing them would reduce the ability of an attacker to succeed.
- Multi-Layering - This technique refers to the act of hiding sensitive data lines (buried layers) under other layers which contain less sensitive connections. This is a currently common solution.
- Sensors - Sensing environmental variables like temperature, light, power supply and clock frequency can help disable the chip if it surpasses certain threshold, as it probably indicates that an attack is trying to perform analysis or even power glitching the chip, for example.
- Glue Logic - This term refers to mixing functional blocks in the chip, so that it is no longer easy to identify functional building blocks by analyzing the chip's physical structures.
- Bus-Scrambling - By scrambling the data bus between various building blocks, we hinder an attacker's attempt to intercept any data as he needs to have complete knowledge of the scrambler logic first, forcing him to perform reverse engineering of it.

C. Side Channel Attacks

1) Hardware:

- Reducing Electromagnetic Emissions - This can be achieved by lowering the power signal and balancing the circuits inside the chip.
- Increasing Amplitude Noise Level - Execution of concurrent random processes.
- Prevent Alignment of Traces - Computation of differential traces requires them to be aligned. By timing noise with process interrupts and variable clock speeds, we are able to prevent or at least hinder good trace alignment.

2) Software:

- Random Process ordering - Parallel substitutions in an algorithm (similar to S-boxes in the DES) can be performed in a random order to reduce relevant signals.
- Random Delays - Performing random delays and alternating paths to add timing noise will not only hinder the
- Eliminating Time Dependencies - Power Analysis by visual inspection of traces can be done when the function durations depend on key values. A time-constant implementation of key operations helps prevent this attack.
- Intermediate Value Blinding - By adding random data to the real data and later subtract it in the intermediate path avoids leaking of useful information. This blinding will cause non-linear intermediate functions to output wrong results so they must be carefully designed in order to compensate for the deviations caused by random data.

3) Application level:

- Retry Limitation - By introducing limits to successive failures, we are able to block the card and prevent differential analysis.
- Control and Visibility Limitation - By limiting the input and output we are able to prevent differential analysis, as an attacker cannot use it if only part of the input can be chosen or only part of the result is returned.

D. Power Glitching

- The usage of sensors, like state above, is currently the most common strategy used against this kind of attack. This strategy, however, may affect the card's functionality in some terminals or climates.
- Validation of results is also performed by calculating the output twice and comparing both.
- It is also essential to implement software and application countermeasures in order to detect and recover from fault injection.

VI. Real life example

In 2011 a criminal group found a way to create about 40 forged smart cards which where used for banking purposes in France/Belgium[11], these cards were supposed to be protected by pre-existing physical, link, network, and transport layer protocols such as ISO/IEC 7816 and 14443.

This attack was perpetrated by an outside attacker and targeted both the protocol that establishes communications between the smart card and the Point-of-Sale (PoS) which was done via a physical Man-In-The-Middle (MITM) attack. This MITM attack was done by the illegal acquisition of several VISA cards whose microchips were removed afterwards. For the purpose of being re-attached to a mix-and-match of plastic cards and microchips so that they didn't belong to the same original card.

This constituted the physical part of the attack and as both the microchip, and the plastic card, both possessing anti-forgery countermeasures, were legitimate and therefore capable of passing most at-a-glance inspections on their legitimacy.

Finally after all this a second microchip, a common run-of-the-mill hobbyists microchip, was placed and wired on top of the first (Fig 5) , while ensuring that the card itself was still usable in a normal PoS.

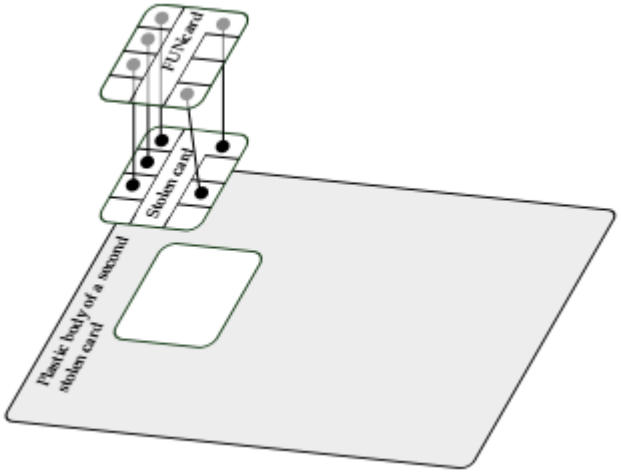

Fig. 5. Schematic of the card[11]

The second microchip was the MITM its function, although puzzling at first due to the forensic countermeasures implemented by the attackers, became apparent with a cryptanalysis tool known as side-channel analysis. This analysis revealed that all but one of the normal interactions between the card and the reader were redirected to the legitimate card (Fig 6). The one interaction that wasn't sent through but was answered by the foreign illegitimate card was the card validation request by the PoS which returned the correct signal no matter the pin inserted. This allowed the PoS to charge the bank account associated with the legitimate microchip, so long as another action was taken to prevent the detection of the fraud and this was the expenditure of only small amounts of money to try

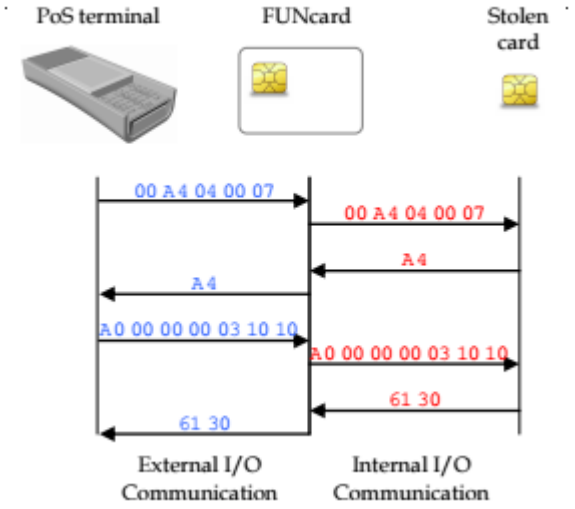

Fig. 6. Schematic of the MiTM attack[11]

to fly as low under the radar as possible and to avoid the PoS systems to look for on-line validation of the card which might prove problematic for the forged card to surpass.

This scheme was eventually discovered and dismantled it is estimated that it brought around 600.000 euros in damages which was used to acquire various items to redistribute through the black market.

VII. Conclusion

SC currently present themselves in several factors II-B, from contact II-B1 to contactless II-B4, with and without processing capabilities II-B2 II-B3, and single or multiple applications cards II-B5. Being utilized mainly for authentication, privacy, and access control purposes II-A makes them prone to attacks from nefarious users, either Insiders III-A1 or Outsiders III-A2 for Personal III-B1, Monetary III-B2, or Political III-B3 motives.

Attacks on SC can mainly be classified in Logical IV-A (those that attack protocols used or exploit software in the card), Physical IV-B (SC / PoS Hardware modification and analysis), or Side Channel Attacks IV-C (those that use of physical phenomena to analyze or modify the cards behavior).

After research, proposed changes to prevent Logical Attacks would be using mathematical models to prove safety or validating the software implementations, in which dividing software into smaller blocks in order to more easily validate them, although utilizing already proven designs prevents the need for validation. Plainly put, the more complex the software utilized is the higher the probability that a bug or an exploit can be used V-A.

Countermeasures for Physical Attacks would involve reducing transistor and wires sizes, including a top layer with an, active, protective system that carries a signal, or just by plain including more layers and using some to mask sensitive data in hidden ones. Although physical security has gotten

significantly better in the past years changes to card design are necessary to prevent some current attacks V-B.

Reducing the chip's power signal or masking it with noise would prevent some hardware attacks, using a similar substitution algorithm to DES S-Boxes to reduce relevant signals, performing random delays, eliminating time dependencies, and using random data meshed with real data (Intermediate Value Blinding) would avoid leaks and help in regards to software attacks. Lastly, introducing limits to successive failures, and limiting the input and output help with application level attacks V-C.

SC can be considered 'safe' by todays standards there's much that can be done to prevent modern day attacks, as we've referred, even if the means to do so are presented as a re-factor of the current physical model of the card, or as preventing the use of overly designed (highly complex) software. Privacy, or the security of sensitive data should be looked at as a necessity and not a commodity, seeing as that, in several cases presented throughout this paper, that could have already been lost.

REFERENCES

[1] Europay, mastercard, visa. [Online]. Available: https://www.emvco.com

[2] Cardlogix smart identity made simple. [Online]. Available: http://www.cardlogix.com/support/documentation.asp

[3] J. Abbott, "Smart cards: How secure are they?" [Online]. Available: https://www.sans.org/reading-room/whitepapers/authentication/smart-cards-secure-they-131

[4] Iso7816. [Online]. Available: http://www.cardwerk.com/smartcards/smartcard_standard_ISO7816.aspx

[5] Uhf gen 2. [Online]. Available: http://www.gs1.org/epcrfid/epc-rfid-uhf-air-interface-protocol/2-0-1

[6] B. Schneider and A. Shostack, "Breaking up is hard to do: Modeling security threats for smart cards." [Online]. Available: https://adam.shostack.org/smart-card-threats.pdf

[7] Internet security glossary, version 2. [Online]. Available: https://tools.ietf.org/html/rfc4949

[8] Opensc – get serial number" stack-based buffer overflow. [Online]. Available: https://labs.mwrinfosecurity.com/assets/154/original/mwri_opensc-get-serial-buffer-overflow_2010-12-13.pdf

[9] Cve-2014-0160 (heartbleed). [Online]. Available: https://cve.mitre.org/cgi-bin/cvename.cgi?name=cve-2014-0160

[10] M. Witteman, "Smart card security analysis." [Online]. Available: https://www.riscure.com/archive/ISB0707MW.pdf

[11] D. N. Houda Ferradi, Rémi Géraud and A. Tria, "When organized crime applies academic results a forensic analysis of an in-card listening device." [Online]. Available: https://eprint.iacr.org/2015/963.pdf