SECURITY OF CONTACTLESS SMART CARDS

Martin Henzl
Doctoral Degree Programme (2), FIT BUT
E-mail: ihenzl@fit.vutbr.cz

Supervised by: Petr Hanacek
E-mail: hanacek@fit.vutbr.cz

Abstract: This paper overviews the security of contactless smart card and near-field communication applications. It provides an analysis of potential threats typical to contactless communication along with available countermeasures. Some attacks are described in detail. The equipment required for selected attacks is described and results of performed tests are presented.

Keywords: Contactless smart cards, NFC, Proxmark, Libnfc, Security

1 INTRODUCTION

The reason why we are interested in the security of contactless smart cards and near-field communication (NFC) devices is that they are both used in applications that require certain level of security, such as payment systems, electronic ticketing, electronic vouchers and access control systems. There are about 100 pilot projects worldwide [1], which use NFC devices for small payments. Most banks still prefer standard contact smart cards as credit and debit cards, however, contactless cards are becoming popular and they are spreading quickly. Contactless cards are more convenient for the user to perform transactions than contact cards, however, they yield new vulnerabilities due to the radio link interface. The proper use of these technologies provides high level of security, however, many applications, especially for access control, are being developed by not security aware developers, so they can be easily attacked. This paper provides an analysis of threats typical to contactless technologies and shows some practical attack examples along with possible countermeasures.

2 CONTACTLESS TECHNOLOGIES

Contactless smart cards and near-field communication devices both use the same communication interface, adopted from RFID tags. Near-field communication is a standard designed for handheld devices such as cell phones or PDAs. It enables them to act as a contactless smart card or as a reader. Two NFC enabled devices can communicate via NFC. The contactless communication is based on mutual inductance of two coils. The active device (reader) creates an alternating electromagnetic field, which provides the passive device (card) with energy due to the electromagnetic inductance. Data are transferred from the reader to the card by amplitude modulation of the carrier (which also provides the energy to the card). A modified Miller coding with 100% modulation or Manchester coding with 10% modulation are used. The data transfer in the direction from reader to card is based on load modulation. The card sends the information by changing its power consumption. These changes can be detected on the reader and the data can be extracted. The Manchester coding with 10% modulation is used in this direction. The contactless devices work at a frequency of 13.56MHz and the maximal operational distance is about 10cm, but may differ for individual card types and NFC devices. The data transfer rate ranges from 106kbps to 424kbps. The speed of 106kbps is the minimum that every contactless card must support and at which every communication begins. All details about the communication can be found in [2].

3 THREATS

This section provides the analysis of threats specific to contactless technology. It is not a complete list of all possible attacks, only the most important threats are mentioned. The focus is on threats inherent to the wireless communication.

Eavesdropping. Eavesdropping a wireless communication is possible from a long distance. The attacker can easily intercept and alter data being transmitted over the air, which is a big drawback as compared with contact smart cards. Not only that eavesdropping is very easy with an appropriate equipment, but it can be executed without the user's awareness and without trace from distance. The countermeasure against eavesdropping is the encryption of data being transmitted.

Relay Attack. One attacker establishes the communication with the genuine smart card, the second attacker with the genuine reader, and they relay all communication over their own channel. This yields a possibility of modifying the data and thus performing a man-in-the-middle attack. Without relaying the communication, an effective man-in-the-middle attack is practically impossible because of the short communication distance of contactless smart cards. The attacker would have to communicate with both the reader and the card in the way that they would not hear each other. This requires the constellation which is not likely in the real world. The relay attack creates such a constellation and enables the man-in-the-middle attack. The man-in-the-middle attack can be avoided by mutual authentication. The attackers can relay the communication over long distances. This distance can be limited by limiting the maximum response time. By knowing the speed of light and the response time, the reader can estimate the distance from the card. It is called *distance bounding protol* and it can be used to avoid the relay attack. However, this protocol is not easy to implement, therefore not much used, and the relay attack remains dangerous [3].

Interruption of Operation. The communication between the card and the reader may be interrupted by transmitting random noise or some other signal at the same frequency. This can interrupt the proceeding transaction at any time and without any notice. The application needs to know whether the transaction was performed correctly or if there was an error. There should be a backup mechanism and backtracking which ensure that the transaction ended in a regular state. The permanent jamming of the communication can also be classified as DoS (Denial of Service) attack.

Covert Communication. Contactless smart cards have one big disadvantage from the security point of view. Unlike contact smart cards they can communicate with the reader without user's notice. The contact card must be put into the reader, so the user is always aware of the communication (if the card is in his possesion and is not stolen). However, in case of contactless cards, the fraudulent reader can remotely communicate with the card without notice even if the card is in the user's possession. The possible countermeasure is a strong mutual authentication.

There can also be a DoS attack performed without the user's notice, for example on a prepaid card. The service the user has prepaid can be denied for example by debiting all monetary units from the card at a distance. The attacker has to understand the communication protocol between the card and reader in order to send desired commands to the card. Much easier attack is emptying or destroying the smart card by inappropriate electromagnetic waves. The only countermeasure is the Faraday cage.

Radio Frequency Analysis. This is a side channel attack developed from power analysis and electromagnetic analysis performed on contact smart cards [4]. It employs the fact that the electromagnetic field surrounding the card depends on the actual power consumption of the card, because the card is powered by this field. In contrast to contact smart cards, the electromagnetic field can be measured without the need of physical damaging the card. This attack requires the card being in possession of the attacker. The attacker can then learn some sensitive data from the card.

4 PRACTICAL ATTACKS

In this section I will show two experimental attacks. The first attack was performed on a real access control system which uses Mifare Classic cards. The vulnerability which I have found and used for this attack could be disposed by proper implementation, which will be also described. The second attack shows the menace of relay attacks and how these attacks can be performed. I will also describe the equipment useful for RFID, contactless smart card and NFC research.

4.1 RESEARCH EQUIPMENT

The most important device designed for RFID research is Proxmark 3. For experimental attacks I have also selected the popular NFC reader ACR122 which is used in many applications, but which can also be turned into a powerfull research tool with the *libnfc* library.

Proxmark 3 is a RFID research device with open-source design. It incorporates the FPGA unit, used for low level signal processing, and the ARM processor, that implements the transport layer. It can be used as a sniffer, as a reader or as a card, using various protocols. Proxmark 3 supports both low frequency (125kHz - 134kHz) and high frequency (13.56MHz) signal processing, so it can be used for contactless smart cards. There is also an alternative to Proxmark 3, the OpenPCD together with OpenPICC, which are also free hardware designs. OpenPCD works as a reader (Proximity Coupling Device), OpenPICC as a card (Proximity Integrated Circuit Card).

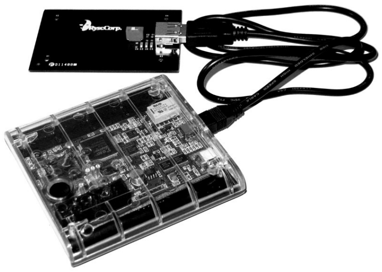

Figure 1: Proxmark 3 with connected high frequency antenna.

4.2 MIFARE CLASSIC ATTACK

I have examined the real access control system which uses the Mifare Classic smart cards. The security features of the Mifare Classic card are UID, PRNG and proprietary encryption algorithm CRYPTO1. The UID is set in the factory and cannot be altered. It is used in the anticollision procedure and for identification purposes. The PRNG is used for authentication and the CRYPTO1 for encrypting the communication after a successfull authentication.

There have been some attacks on the Mifare Classic in the past. Nohl and Ploetz [5] have reverse engineered (by physical dismantling and analyzing the hardware of the chip) the Mifare Classic and exposed several weaknesses, such as that the nonce is generated by a Linear Feedback Shift Register (LFSR) which shifts every $9.44\mu s$, which is exactly one bit period in the communication. Hence there is a possibility to get the same nonce after $0.618s$ if the communication with the card is established at the exact time, which enables the attacker to replay the authentication and successfully authenticate. The security of Mifare Classic was build on the principle ”Security by obscurity”, which is bad. There are other attacks on Mifare Classic, such as [6]. For example [7] shows multiple attacks that are feasible without access to the genuine reader by just wirelessly communicating with the card.

Now I will focus on the examined access control system. I have used Proxmark 3 to eavesdrop the communication between a genuine card and a genuine reader. By analysing the communication, I have found out that the tested system uses only the UID of the card for verifying the user's identity. If the UID presented by the card is stored in the backend database, the access is granted. There is no authentication between the card and the reader, no encrypted communication, there is no sensitive information stored on the card except of the UID. The UID is not protected, the card presents its UID every time it approaches any reader, because the UID is used in the anticollision procedure. The anticollision procedure ensures that at least one card in the reader's field will communicate with the reader. If there are more cards in the field, one is always selected. I have used Proxmark 3 to eavesdrop the communication and get my card's UID. Then I programmed the Proxmark 3 so it can replay the anticollision procedure with my UID and card type identifier. Figure 2 shows the constellation.

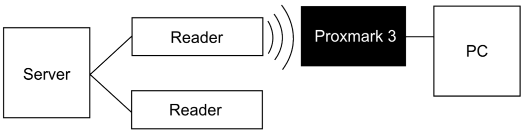

Figure 2: Attack on access control system.

My PC was sending commands to the Proxmark 3 via USB. The Proxmark 3 communicated with the reader situated by door, which was connected to the server that has access to the backend database. With the programmed device I was able to get access to locked door without the genuine card. The eavesdropped and replayed anticollision procedure is following (with obfuscated UID):

```
RDR: 26                          REQA (7bits)
TAG: 04 00                       ATQA)
RDR: 93 20                       SEL cascade 1
TAG: 08 ab cd ef 81              CT (1B), UID (4B), BCC (1B)
RDR: 93 70 08 ab cd ef 81 a1 eb  SEL
TAG: 09 3f cc                    SAK
```

The tested access control system relies only on UIDs. The attacker can get the UID without authenticating to the card and then replay it. The access control system could be much more secure if it was using UID together with some shared secret stored in a cryptographically protected memory. It would increase the security with current hardware. Even better would be using of Mifare DESFire cards, because of the previously presented Mifare Classic vulnerabilities.

4.3 RELAY ATTACK

Relay attack is the most dangerous attack on contactless smart cards, because it is very hard to protect from it. The major danger is in that the attacker can use someone's smart card without his aware and for example pay with it in a shop far away. There was a study [8] which showed a possible relay attack on e-passports, which allow the maximal response time of $4.949s$, according to the standard. This is long enough to relay the communication even over TCP/IP. There is a possibility of using NFC devices for these attacks. Two mobile phones equiped with NFC can communicate with each other via GSM. One of them communicates with the genuine reader, the second with the genuine card. They relay everything over their shared communication channel. Figure 3 shows the constellation of devices for the relay attack. The attackers do not have to build complicated hardware, the NFC enabled phones are now accessible to everyone and are relatively cheap. This can be dangerous and an increase of relay attacks can be expected. However, there is one obstacle for such devices. There are two types of UIDs - unique (for identification) and random (for untraceability). Random UIDs always start with $0x08$. NFC devices can set their UID to random type with arbitrary value, but always starting with 0x08. The unique UID can not be changed. So if the attacked application does not use random UIDs and checks unique UIDs, NFC mobile phones can not be used for relay attacks. NFC device ACR122 with the *libnfc* library can be used for a relay attack, it can forge any UID, which solves the previous problem.

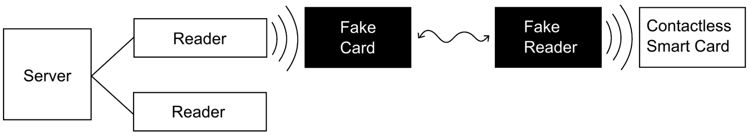

Figure 3: Relay attack.

5 CONCLUSION

Most of the described attacks can be avoided by implementing proper countermeasures. The only attack which is practically unavoidable is the relay attack. The user can use the Faraday cage to protect the card from being read from distance, however, when the attacker has access to the card, the relay attack can be executed. This has to be taken into account. Smart card and NFC application issuers mostly don't publish their algorithms for scientific feedback, hence there could be many bugs that might remain hidden for a long time using such a system. So there is a space for further research.

6 ACKNOWLEDGEMENT

The research has been supported by the Czech Ministry of Education in frame of the Research Intention MSM 0021630528: Security-Oriented Research in Information Technology, MSM 0021630503.

REFERENCES

[1] NFC trials, pilots, tests and live services around the world, 2011. [Online]. Available: <http://www.nearfieldcommunicationsworld.com>.

[2] Dominique Paret: RFID and Contactless Smart Card Applications. John Wiley & Sons, 2005.

[3] Gerhard Hancke: A practical relay attack on iso 14443 proximity cards. Technical report, 2005.

[4] Helena Handshuh: Contactless technology security issues. Information Security Bulletin, 2004. [Online]. Available: <http://www.chi-publishing.com/samples/ISB0903HH.pdf>

[5] Karsten Nohl, David Evans, Starbug Starbug, and Henryk Plötz: Reverse-engineering a cryptographic rfid tag. In Proceedings of the 17th conference on Security symposium, pages 185-193, Berkeley, CA, USA, 2008. USENIX Association.

[6] Gerhard Koning Gans, Jaap-Henk Hoepman, and Flavio D. Garcia. A practical attack on the mifare classic. In Proceedings of the 8th IFIP WG 8.8/11.2 international conference on Smart Card Research and Advanced Applications, CARDIS '08, pages 267-282, Berlin, Heidelberg, 2008. Springer-Verlag.

[7] Flavio D. Garcia, Peter van Rossum, Roel Verdult, and Ronny Wichers Schreur: Wirelessly pickpocketing a mifare classic card. In Proceedings of the 2009 30th IEEE Symposium on Security and Privacy, pages 3-15, Washington, DC, USA, 2009. IEEE Computer Society.

[8] M. Hlavac and T. Rosa: A note on the relay-attacks on e-passports - the case of czech e-passports. IACE ePrint archive 2007/244, 2007.