Radboud Universiteit Nijmegen

08-33A

Nijmegen, March 12, 2008

Dismantling contactless smartcards

On March 7, 2008 researchers and students of the Digital Security group of the Radboud University Nijmegen have discovered a serious security flaw in a widely used type of contactless smartcard, also called RFID tag. It concerns the "Mifare Classic" RFID card produced by NXP (formerly Philips Semiconductors). Earlier, German researchers Nohl and Plötz pointed out security weaknesses of this cards. Worldwide around 1 billion of these cards have been sold.

This type of card is used for the Dutch `ov-chipkaart' [the RFID card for public transport throughout the Netherlands] and public transport systems in other countries (for instance the subway in London and Hong Kong). Mifare cards are also widely used as company cards to control access to buildings and facilities. All this means that the flaw has a broad impact. Because some cards can be cloned, it is in principle possible to access buildings and facilities with a stolen identity. This has been demonstrated on an actual system. In many situations where these cards are used there will be additional security measures; it is advisable to strengthen these where possible.

The Digital Security group found weaknesses in the authentication mechanism of the Mifare Classic. In particular:
1. The working of the CRYPTO-1 encryption algorithm has been reconstructed in detail.
2. There is a relatively easy method to retrieve cryptographic keys, which does not rely on expensive equipment.

Combining these ingredients we succeeded on mounting an actual attack, in which a Mifare Classic access control card was successfully cloned. In situation where there are no additional security measures, this would allow unauthorised access by people with bad intentions.

Background
The Mifare Classic is a contactless smartcard developed in the mid 90s. It is a memory card that offers some memory protection. The card is not programmable. The cryptographic operations it can perform are implemented in hardware, using a so-called linear shift feedback register (LSFR) and a "filter function". The encryption algorithm this implements is a proprietary algorithm CRYPTO-1 which is a trade secret of NXP. The security of the card relies in part on the secrecy of CRYPTO-1 algorithm, which is known as "security by obscurity".
Mifare Classic cards are typically used for authentication. Here the goal is that two parties prove who they are. This is done by demonstrating that they know some common secret information, a so-called shared secret (cryptographic) key. Both parties, in this case the Mifare card and the card reader, carry out certain operations and then check each other's results to be sure of whom they are dealing with.
Authentication is needed to control access to facilities and buildings, and Mifare cards are commonly used for this purpose.
Successful Authentication is also a prerequisite to reading or writing part of the memory of the Mifare Classic. The card's memory is divided into sectors, each protected by two cryptographic keys.
Proper key management is a subject in its own right. Roughly speaking, there are two possibilities:

1. All cards and all card readers used for a some application have the same keys for authentication. This is common when cards are used for access control.
2. Each card has its own cryptographic keys. To check the keys of a card, the card reader should then first determine which card it is talking to and then look up or calculate the associated key(s). This is called key diversification. It is claimed that this approach is used for the Dutch public transport card.

Security weakness of the Mifare Classic
The Digital Security group found weaknesses in the authentication mechanism of the Mifare Classic. In particular:
1. The working of the CRYPTO-1 encryption algorithm has been reverse engineered, and we developed our own implementation of the algorithm.
2. We found a relatively easy method to retrieve cryptographic keys, which does not rely on expensive equipment.
To reverse engineer the CRYPTO-1 encryption algorithm we used flawed authentication attempts. If one does not precisely follow the rules of the prescribed protocol, one can obtain some information about of the way it works. Combining such information is was possible to reconstruct the algorithm.
Once the algorithm is known, one can find out the keys that are used by a so-called brute force attack, i.e. simply trying all possible keys. In this case the keys are 48 bits long. Trying all the keys then requires around nine hours on advanced equipment, according to the recent TNO report 34643 "Security Analysis of the Dutch OV-chipkaart", published February 26th 2008.
However, here too certain flaws in the authentication protocol could be exploited, as we discovered. This leads us to the second point: there is a way to relatively easily retrieve the key without carrying out a lengthy brute force attack. This can be done by first carrying out many failed authentication attempts, which do provide some information. Storing the results of this in a big table, one can look for a match and retrieve the key. The table only has to be constructed once, and can be prepared in advance by repeatedly running the CRYPTO-1 algorithm on a fixed input.
Our proof-of-concept demonstration of this attack still required many authentication attempts once this table had been constructed. Recording these attempts took several hours, but could be carried out by a hidden antenna to eavesdrop on a card reader. It seems that the complexity can be further reduced, possibly dramatically so, making the attack much simpler.

Exploiting these weaknesses
Once the secret cryptographic key is retrieved, there will be possibilities for abuse. How severe these possibilities are will depend on the situation. If all cards share the same key, then the system will be extremely vulnerable. This may be the case if cards are used for access control to buildings and facilities, both in the private and public sector. There is however no information on how common this is.
For such a setting we demonstrated an actual attack, where a card of, say, an employee can be cloned by bumping into that person with a portable card reader. The person whose identity is being stolen may then be completely unaware that anything has happened.
In a situation where diversified keys are used, abuse will be more difficult, but not impossible. No actual attacks have been demonstrated for such a scenario.

Countermeasures
At the technical level there are currently no known countermeasures. Shielding cards when they are not in use, e.g. in a metal container, reduces the risk of an attacker secretly reading out a card. However, when the card is being used, it is still possibly to eavesdrop on the communication, with a hidden antenna near the access point.
Strengthening of traditional access control measures is therefore advisable. Access to sensitive facilities will (or should) be protected by several protection mechanisms anyway, of which the RFID tag is only one.

German Hackers
In December 2007, Karten Nohl and Henryk Plötz announced that they had reconstructed CRYPTO-1 at a hackers' conference in Berlin. We have been in touch with them, and our work builds on their results. However, Nohl and Plötz kept some information about CRYPTO-1 to themselves. To reverse engineer CRYPTO-1, they carried out a physical attack, where they studied the layout of the hardware implementing the algorithm on an actual Mifare Classic chip. Their approach is completely different from

ours, as we only exploited weaknesses of the protocol and did not look looking at the hardware implementation.

Publication
When discovering a security flaw there is a dilemma on how to handle this information. Immediate publication of the details can encourage attacks and do serious damage. Keeping the flaw secret for a long period may mean that necessary steps to counter the vulnerability are not taken. It is common practice in the security community to try to strike a balance between these concerns, and reveal flaws after some delay.
This is the approach we have taken. On Friday, March 7 2008, the government was informed, because national security issues might be at stake. On Saturday, March 8, experts of the Dutch Signals Security Bureau (NBV) of the General Intelligence and Security Service (AIVD) visited Nijmegen to assess the situation, where they concluded that the approach we demonstrated was an effective attack. On Sunday, March 9, NXP was informed, and on Monday, March 10, Trans Link Systems (the company developing the Dutch public transport card). We spoke to representatives of both companies about the technical details, and are collaborating with them to analyse the impact and think of possible countermeasures. On Wednesday, March 12, minister Ter Horst has informed
Parliament.

About the Digital Security Group
The Digital Security Group at the Radboud University Nijmegen consists of about 25 researchers. The research focuses on two themes: software security and identity-centric security. Over time, the group has developed a considerable expertise in the field of smartcards. The group has for instance advised on technical aspects of the electronic passport that was introduced last year. The group is also active in the areas of electronic voting, RFID, privacy, and cyber crime. For more information see our webpages at http://www.ru.nl/ds

More information is available via the science editors of the Radboud University, tel +31-24-3616000, email: info@communicatie.ru.nl