Proof of concept, cloning the OV-Chip card

Public transport system in The Netherlands

ing. R. Verdult
Master student computer science,
Security of Systems at the Radboud University Nijmegen

Supervisor: **Flavio D. Garcia**

Introduction

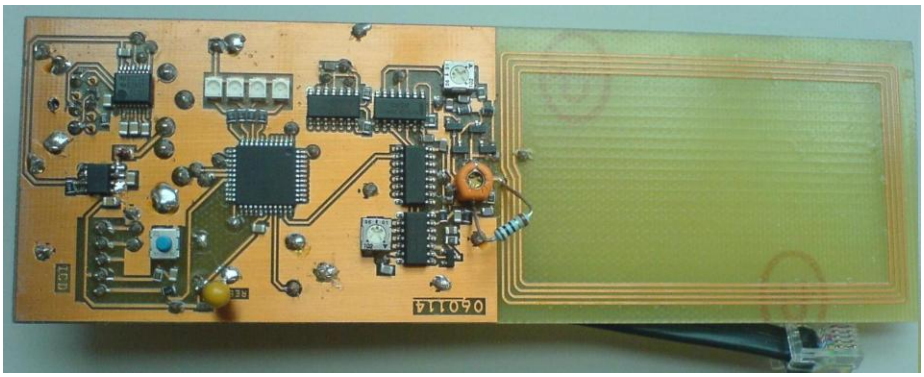
The OV-Chip is a project that digitalizes the payment system for public transport in The Netherlands. It makes use of RFID technology, which offers a contact-less transaction between a gateway and a traveling ticket. This system will eventually replace all the original paper tickets. Since the residents of The Netherlands have no choice in using this system, the university sees it as their social responsibility to have a critical look to potential security issues involving this system. Therefore, I have investigated the possibility to clone a ticket. A clone is an exact copy of the original ticket which cannot be detected by the gateway, empowering a malicious user to abuse the system

Mifare Cards

The OV-Chip uses Mifare cards which are produced by the company NXP. There are two different types being used, Ultralight and Classic. The cheaper Mifare Ultralight cards are used as disposable tickets for one or two way traveling. The Ultralight card is actually a simple piece of memory and a wireless transceiver and has no communication protection at all. The more expensive Mifare Classic card is used for subscriptions. The Classic card is generally the same as the Ultralight card, though the communication is protected by some undisclosed encryption algorithm called CRYPTO1. The algorithm has been recently reversed engineered by two students in Germany [1] and will be published later this year. This would significantly degrade the protection of the Classic card, potentially to the same level of the Ultralight card.

Custom Hardware

In my investigation I have focused myself at the disposable tickets of the OV-Chip card. These cards have some identification and travel information stored in their memory. Because they are Mifare Ultralight cards the communication is transferred in plaintext and can be observed by an eavesdropping device. We have developed such a device (Called Ghost) which is also capable of emulating and cloning any RFID tag (card). The construction costs for this device is in the order of 40 Euros.



Ghost device

Proof of Concept

The actions I need to perform to create a clone of an original card are the following.

- Buy a original two way ticket at the ticket machine
- Read out the identification code with any wireless reader
- Read out the memory content with any wireless reader
- Configure the Ghost as emulator
- Program the identification and memory content into the Ghost

Security issues

The original ticket will allow a user to travel two times. It will store the current state on the ticket itself. This can be two, one or none trips left. When I travel one trip with the Ghost I can reset the Ghost back to the state of two trips left. This means in general that I can reuse the card an unlimited number of times.

With the knowledge of the German researchers it would in principle be possible to clone a subscription card. This means that it would be possible to clone a card from a victim and use his information to check-in at the gateways. All traveling will be registered on his account.

Conclusion

It seems that the security of the OV-Chip project is not satisfactory of a critical infrastructure as the public transport in The Netherlands. It would be good if the involved parties will take these findings seriously and use them to improve the system. The moral of the story is that security by obscurity is not good for the long run.

Special thanks

The cooperation of the electronic expert Peter Dolron.
My supervisor Flavio D. Garcia for his help.
The Student Gehard de Koning Gans who works on a similar project with me.

[1] Karsten Nohl, Henryk Plötz, http://events.ccc.de/congress/2007/Fahrplan/events/2378.en.html