TNO Information and Communication Technology

Nederlandse Organisatie voor
toegepast-natuurwetenschappelijk
onderzoek / Netherlands Organisation
for Applied Scientific Research

Brassersplein 2
P.O. Box 5050
2600 GB Delft
The Netherlands

www.tno.nl

T +31 15 285 70 00
F +31 15 285 70 57
info-ict@tno.nl

TNO report 34643

Security Analysis of the Dutch OV-Chipkaart®

Public excerpt of TNO report 34642

Authors	Not disclosed
Reviewer	Not disclosed
Project	Security Analysis of the Dutch OV-Chipkaart®
Project number	035.32279
Project manager	Not disclosed
Contractor	Trans Link Systems
Date	February 26th 2008
Classification	UNCLASSIFIED

Contents

1 Introduction

1.1 Background

Preparations are currently underway to introduce the so called OV-Chipkaart® as a common means of payment for all forms of public transport in The Netherlands. This contactless chipcard, which can be loaded with a balance in Euros and specific travel products, will eventually replace all current ticket manifestations. The responsibility for establishing an integral OV-Chipkaart system as well as issuing the actual cards has been assigned to Trans Link Systems (TLS), a consortium of public transport companies Connexxion, GVB, RET, HTM and NS.

The actual OV-Chipkaart has three specific manifestations: a personalised, an anonymous and a disposable version. The first two are based on the Mifare Classic 4K chipcard as offered by card manufacturer NXP, formerly known as Philips Semiconductors. Underlying the disposable version is the less sophisticated Mifare Ultralight card, produced by the same vendor.

In December 2007, the security of the Mifare Classic 4K card became the subject of debate. This was invoked by a presentation given at a conference of the Chaos Computer Club (CCC) in Germany. In this presentation, mention was made of severe weaknesses in the Mifare Classic card that would effectively render it useless for a variety of applications. Most importantly, the presenters claimed to have developed detailed knowledge of the secret cryptographic algorithm CRYPTO1. The secrecy of this algorithm is an important aspect of the overall security model for the OV-Chipkaart.

The CCC presentation received wide attention in a variety of media as well as at the level of national politics. In order to acquire a precise understanding of the problem, TLS commissioned TNO to perform an independent investigation into both credibility and impact of the aforementioned vulnerabilities.

1.2 Purpose and scope

The purpose of this investigation is to identify and assess the risks that the aforementioned development introduces with respect to the Dutch OV-Chipkaart and establish a viable strategy for controlling these risks adequately. With respect to scope, the following is of importance:

- The analysis is explicitly not limited to immediate risks stemming from the attack capabilities already demonstrated by the CCC presenters. Rather, the emphasis of this investigation is on the eventual implications if current capabilities are developed further. Here, important aspects include the potential damage for stakeholders and end users and the extent to which a criminal organisation might develop a business case for illicit exploitation of the OV-Chipkaart.
- TNO chose to adopt a broad scope for the purpose of assessing risks and possible remedies. Most importantly, despite the fact that the CCC claims specifically relate to the Mifare Classic card, all consequent risks were assessed in light of the OV-Chipkaart system as a whole, i.e. the card itself as well as the infrastructure via

which it is used and managed. Here, the aim has been to ensure a well balanced overall perspective.
- At the start of the investigation, the Dutch government put a lengthy set of questions forward to TLS for inclusion in the scope. These questions were adopted.

Notwithstanding the above, the investigation was performed under the constraints that the available time frame was 5 weeks, the assignment commissioned by TLS posed requirements on the scope and specific vendor information was not disclosed to TNO. This imposed certain limits on the aspects that could be covered. To maintain a feasible assignment, a specific set of activities was explicitly excluded:

- TNO has not conducted hardware tests to verify the claims presented at the CCC conference in Germany. The credibility of these claims was assessed purely on the basis of the presentation itself and TNO's own knowledge of chipcards and cryptographic algorithms.
- Any potential risks to the OV-Chipkaart system that are not the immediate effect of the aforementioned CCC claims were not analysed in this investigation. As a direct consequence, the Mifare Ultralight card, which serves as a basis for the disposable manifestation of the OV-Chipkaart, is not addressed. This card does not incorporate the CRYPTO1 algorithm and is therefore not directly affected by the CCC claims.
- Neither the claims of the CCC presenters nor the findings from this investigation were verified against the formal specifications of the CRYPTO1 algorithm. These specifications are kept secret by chip manufacturer NXP and were therefore not available to TNO in any form.
- TNO did not investigate the possibility of performing so called "side channel" attacks such as Differential Power Analysis[1] on the card. This would require knowledge of the CRYPTO1 algorithm as well as implementation details of the card, neither of which was available to TNO.
- Within the context of this investigation, TNO did not produce design specifications to accompany the strategic way forward. Rather, the focus is on outlining possible countermeasures and providing insight into the remedial effects thereof.

Note that all deliverables produced in this investigation were written in English to accommodate an independent review by international peers, as announced by the Dutch government.

1.3 Document outline

Chapter 2	This chapter provides a detailed description of the approach followed in this investigation. This includes specific security aspects analysed, parties consulted and deliverables produced.
Chapter 3	Here, an overall perspective is presented on the complete set of findings that resulted from the investigation.
Chapter 4	This chapter presents the overall conclusions as well as the recommended way forward.

[1] For further explanation see http://www.cryptography.com/resources/whitepapers/DPA.

2 Approach of the investigation

This chapter provides a detailed description of the approach followed by TNO for this investigation. Here, the emphasis is on explaining the various phases of the analysis and the specific issues that were analysed in each phase. The chapter concludes with an overview of resulting deliverables.

2.1 Analysis phases

Figure 1 depicts the various phases that comprised the investigation, including the primary issues addressed in each.

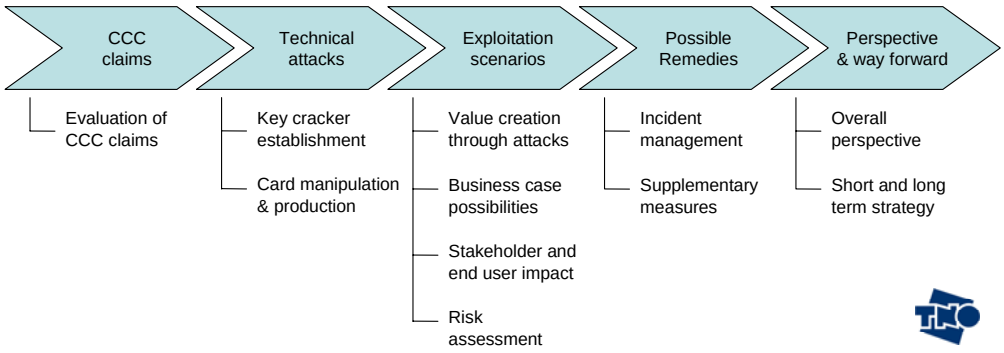

Figure 1: Summary of investigation approach

Here, the specific setup of each phase has been as follows:

1. **Evaluation of CCC claims**
   The CCC presentation incorporated a variety of claims regarding vulnerabilities in the Mifare Classic card and the CRYPTO1 algorithm that it employs. In this phase, the credibility of each of these claims was evaluated. Since verification against the formal CRYPTO1 specification was not possible (see Chapter 1), TNO developed an expert opinion based solely on the presentation itself. Most importantly, this phase resulted in an appraisal of the extent to which the CRYPTO1 algorithm was indeed reverse engineered by the CCC presenters.

2. **Identification and evaluation of technical attacks**
   In this phase, possibilities to perform a successful technical attack on the Mifare Classic 4k card were assessed. This analysis was built on the assumption of a fully compromised CRYPTO1 algorithm, since this provided the most thorough insight into attacks that might eventually take place. The analysis involved several aspects of interest:
   - Possibilities to establish a key cracker, via which the secret cryptographic keys of individual cards might be retrieved. Among the factors weighed were an appraisal of hardware involved, including the corresponding time and financial investment, and the extent to which an attacker might be capable of retrieving input data for a key search (so called *plaintext-ciphertext pairs*). Note that the investigation also addressed the possibility to retrieve the master keys from which individual card keys are deduced via a process of diversification.

- Specific possibilities to manipulate a genuine card or produce a device that could pose as one. Here, situations where an attacker is capable of retrieving cryptographic keys and those where an attacker does not possess such information were analysed separately. With respect to illicit card production, a distinction was made between attackers employing so called emulators and attackers that use a blank Mifare card as their starting point.

The analysis of technical attacks required insight into certain specific characteristics of the CRYPTO1 algorithm. Since the specifications of this algorithm are not public, extensive interaction with chip manufacturer NXP was established to obtain the required information to the maximum extent possible. With respect to the key cracker issue, specific information was obtained through interaction with the university of Bochum, Germany, where this topic is a subject of research.

3. Identification and evaluation of exploitation scenarios

This phase focused on the question to which extent the technical attacks might offer a malevolent party possibilities to exploit the OV-Chipkaart system to its benefit by means of value creation. To this end, exploitation scenarios were identified and evaluated, thereby addressing the following issues:

- Possibilities to obtain actual public transport products on the basis of the technical attacks evaluated in the previous phase
- The extent to which these possibilities might offer criminal organisations a viable business case for conducting attacks
- The damage that might be induced to both stakeholders and end users of the OV-Chipkaart system in the event of actual incidents

Based on these factors, all exploitation scenarios identified were subjected to a risk assessment. Here, probability and impact of actual incidents were weighed to establish the severity of each scenario.

4. Assessment of possible remedies

In this phase, the extent to which exploitation scenarios might be curtailed through specific remedies was evaluated. Here, the following possibilities were contemplated:

- The extent to which the mechanism of managing incidents as already present within the OV-Chipkaart system should be considered effective and adequate in light of the attacks and exploitation scenarios analysed. Here, insight into the capabilities of the current fraud detection and blacklisting setup was established through extensive interaction with TLS as well as Octopus Cards Limited, the manufacturer of the underlying system. The analysis integrally involved both the present setup and possible enhancements to it. Among the factors addressed were detection accuracy and speed and the potential workload on the mechanism as a whole.
- The extent to which supplementary remedies might be adopted to prevent attacks from occurring. To this end, a variety of measures was suggested by both TLS and chipcard manufacturer NXP. These suggestions were weighed against the characteristics of attacks and exploitation scenarios to assess (potential) effectiveness.

Apart from (expected) effectiveness, evaluation of these remedies incorporated factors such as technical feasibility, implementation effort and future-proofness.

5. **Establishment of overall perspective and way forward**
   Here, all findings of the previous phases were combined into an overall perspective on the security of the OV-Chipkaart. Based on this, a way forward was proposed for both the short and long term.

Primarily on the basis of the overall perspective developed in the final phase, TNO subsequently established a set of conclusions and recommendations from the investigation as a whole.

2.2 Deliverables produced

The investigation resulted in two closely related, but by their nature fundamentally different deliverables:

- A classified report in which all details of the investigation are elaborated, made available to the direct stakeholders only
- A public excerpt of the classified report, deemed suitable for wider distribution

This explicit distinction is required because the classified report incorporates details of potential technical attacks and exploitation scenarios, the disclosure of which in itself might theoretically subject the OV-Chipkaart system to risk. Moreover, some information contained in the classified report is subject to intellectual property rights (including proprietary know-how) of third parties such as NXP and was made available to TNO under strict confidentiality arrangements.

Having stated the above, the need is also recognised to share the insights that were established during the investigation with a broader audience. Here, important considerations are the involvement of the Dutch government in the OV-Chipkaart system and the widespread public interest in its security level. To accommodate this need, TNO also produced a public excerpt of the classified report from which all sensitive details were removed. This public excerpt incorporates:

1. A detailed description of the approach followed by TNO for this investigation
2. A comprehensive account of phase 5 - overall perspective and way forward.
3. A comprehensive account of the conclusions and recommendations that were established on the basis of the investigation as a whole.

To affirm that the maximum degree of openness has been pursued, it is emphasised that the text incorporated in the public excerpt was taken nearly literally from the corresponding chapters in the classified report.

Note that preliminary results of phase 1 – the evaluation of CCC claims – were already reported separately. Similar to the above, this yielded both a classified deliverable and a public derivative thereof[2].

[2] *Reaction to Computer Chaos Club presentation on Mifare cards in December 2007*, available via http://www.tno.nl/downloads/tno_ict_reaction_ccc_presentation_170108.pdf.

3 Overall perspective on the analysis

From the analysis of CCC claims it is apparent that the CRYPTO1 algorithm underlying the security functionality of the Mifare Classic 4k card either has been broken or will be in the near future. Analysis has shown that once this is the case, establishment of a key cracker to retrieve the secret cryptographic keys of individual cards will become realistic. This is primarily due to the fact that the 48-bit keys employed in the algorithm are too small to withstand so called *brute force* or *key search attacks*. Based on current technology, an investment of around $9,000 (hardware only) will suffice to develop a key cracker that retrieves an individual key within a few hours. Here, it is noted that attackers need to retrieve multiple keys of a single card to gain control over it.

The establishment of a key cracker will provide malevolent parties with a variety of exploitation scenarios. If no measures are taken, the OV-Chipkaart system may therefore encounter certain levels of fraud and abuse. Here, the following considerations are of importance:

- It is more than likely that a “proof of concept” of OV-Chipkaart exploitation on the basis of a key cracker will be established in the near future. This might for instance be initiated by a university.
- The analysis has shown that there is at least the theoretical possibility that criminal organisations will develop a business case for OV-Chipkaart abuse. Although commercial viability could not be fully assessed, this possibility indicates the need to seriously anticipate criminal exploitation.

To a certain extent, the exploitation scenarios identified in the investigation may be controlled via the present mechanism of fraud detection and blacklisting and the adoption of specific supplementary measures. There are, however, categories of exploitation scenarios for which the remedies identified will complicate but not fully avert the underlying technical attack. Moreover, for some scenarios the remedy deemed most suitable has intrinsic limitations, for instance because it can only be effective under the premise of a limited number of attacks. A certain level of residual risk is therefore unavoidable.

The above does not necessarily imply that migration to a different card is the only possible way forward. On economic grounds, a conceivable approach would be to enhance existing measures and adopt supplementary remedies to such an extent that the degree of residual risk is acceptable from a business perspective. For comparison TNO refers to the financial branch, where it is quite common to accept specific risks associated with credit and debit cards. Here, if a customer becomes the victim of fraud, he is usually compensated afterward. According to TLS, such compensation is also specified in the terms and conditions under which the OV-Chipkaart is offered to the market.

Despite the above possibility, TNO concludes that the Mifare Classic 4k card will eventually need to be replaced. Here, the following considerations are essential:

- As technology progresses, a new generation of computation hardware will emerge that offers better performance at substantially lower cost. This will render the various exploitation scenarios less complicated than they are now.

- It is quite conceivable that upon disclosure of the CRYPTO1 algorithm, it will turn out to incorporate specific vulnerabilities that greatly simplify technical attacks. Numerous stream cipher algorithms have shown such characteristics in the past. Here, it is emphasised that, because of its obscure nature, the CRYPTO1 algorithm has never been reviewed by the international community of cryptographic experts.

These developments are likely to catalyse the amount of fraud and abuse attempts, ultimately causing the process of managing incidents to become uncontrollable. For the long run, therefore, TNO recommends migration to a different card with stronger security characteristics.

An important issue is of course the time limit for migrating. From the analysis, TNO deduced that adopting a subset of the identified remedies will increase the life span of the card in its current technical form. As soon as (criminal) attempts at abusing the system assume a large scale, however, these remedies will start losing their effectiveness. In order to assess the time span that remains before the OV-Chipkaart system arrives in this situation, it is meaningful to consider the developments that need to take place beforehand:

- Establishment of a fully functional key cracker, the details of which will only be available to the responsible researchers upon initial implementation.
- Publication of research results, eventually yielding widely spread knowledge of the key cracker's existence and functional setup among security experts and hackers
- Adoption of the key cracker for fraudulent activities. Here, criminals will also need to establish a business case and some mechanism for distributing fraudulent cards.

Possibly, the final step could be the emergence of hardware and software tools through which the task of cracking cards might become available to the masses. For reference, we refer to past examples in which equipment to crack GSM SIM cards was offered for sale on the Internet.

The amount of time involved in each of these developments cannot be exactly quantified upfront, in part because it depends on the amount of effort that will be invested by specific entities. It is apparent, however, that the overall route towards large scale illicit exploitation of the OV-Chipkaart system is at present still substantial. TNO estimates that it will take at least some years until such a situation occurs. From a risk management perspective, a viable anticipation strategy would be to:

1. Ensure that approximately 2 years from now, a situation has been established where migration to a successor of the Mifare Classic 4k can be initiated at any given moment and executed within a limited time span. Regarding the latter, a reasonable target would be to aim for a migration time of approximately half a year.
2. Determine the exact moment of migration on the basis of fraud and abuse rates actually observed within the OV-Chipkaart system and comparable infrastructures throughout the world. To this end, a continuous process of monitoring and assessing developments will be required.

This approach would ensure adequate anticipation of risk whilst at the same time maximising the life span of the current OV-Chipkaart to its full potential.

An essential implication of the above analysis is that – according to TNO's appraisal – continuation of the present card will eventually evoke a situation in which a certain level of fraud and abuse is unavoidable. Ultimately, the decision to either accept or alleviate this risk is up to the business owners of the system.

4 Conclusions and recommendations

4.1 Conclusions

Based on the investigation as a whole, which was conducted within a predefined scope, TNO established the following overall conclusions:

- In light of recent developments, the Mifare Classic 4k as it is currently employed within the OV-Chipkaart system will eventually need to be replaced by a card with stronger security characteristics.
- The need for migration is not acute. Adoption of a set of remedies at the infrastructure level will enable continuance of the present card for at least some years. Moreover, a viable strategy would be to establish migration readiness rather than actually initiating such migration in the short term.
- Scenarios for exploiting the system yield a limited impact on cardholders. On the spot robbery of travel products or purse value is not realistic. In one specific scenario, however, the cardholder will need to be financially compensated. With respect to privacy, the only personal trait that can be disclosed through attacking the card is a birth date. Moreover, the identity of the cardholder is only reflected in the printed matter on the card and not in any way stored in the chip.

With regard to more specific aspects of the underlying investigation, the following is concluded:

- As the majority of CCC claims regarding weaknesses in Mifare Classic cards is credible, it is more than likely that the secret CRYPTO1 algorithm underlying the security functions of this card either has been reverse engineered or will be at some point in the near future.
- Once all details of the CRYPTO1 algorithm have become public, establishment of a key cracker to retrieve the secret cryptographic keys of individual cards will become realistic. Based on current technology, an investment of around $9,000 (hardware only) will suffice to develop a key cracker that retrieves an individual key within a few hours.
- Using the keys retrieved with a key cracker to obtain the master key from which these were derived is not possible.
- Possession of card keys will enable an attacker to manipulate or clone legitimate cards and produce so called emulators. Notably, attackers might also produce fully functional cards that have not in any way been derived from an officially issued OV-Chipkaart and via specific methods manipulate cards even without any knowledge of the corresponding keys.
- Any occurrence of a cloned card is likely to have a physical appearance that strongly deviates from a regular OV-Chipkaart. Although the possibility of producing clones that resemble genuine cards cannot be fully ruled out, a crucial requisite to this end can presently not be met.
- Although TNO cannot state with full certainty that criminal exploitation of the card vulnerabilities will indeed occur, the analysis has shown that there is at least the

theoretical possibility that criminal organisations will develop a business case to this end.

- The fraud detection system employed within the OV-Chipkaart infrastructure is capable of producing indicative signals for all exploitation scenarios identified within the investigation, should an incident occur. Combining this with the possibility of adopting supplementary remedies cannot avert the fact that continuance of the card in its current form implies acceptance of a degree of residual risk.

4.2 Recommended way forward

Based on the above overall assessment, this section will present a recommended way forward for both the short term and the long term.

4.2.1 Short term

To alleviate risk in the short term and maximise the life span of the card in its current form, it is recommended that a subset of remedies analysed in the investigation be adopted as soon as possible. For confidentiality reasons, the measures TNO specifically proposes to this end cannot be specified here. They are, however, elaborately detailed in the classified report underlying this public excerpt.

Note that although the proposed measures will not fully dispel all of the risks identified, the residual risk upon implementing them is believed to be sufficiently manageable for some years.

4.2.2 Long term

As explained in the previous section, the Mifare Classic 4k will eventually need to be replaced. Here, the recommended strategy is to establish migration readiness within approximately 2 years, whilst determining the exact moment of migration on the basis of fraud and abuse rates actually observed. Since the process of preparing for card migration is by no means straightforward, it is recommended that the available time span be exploited in full by initiating such preparations as soon as possible. Here, the following issues should be addressed:

1. **Select a suitable next generation card**
   Based on a thorough evaluation of candidate cards, a viable successor for the Mifare card should be selected. It is important to recognize that this is certainly not a straightforward task. Each candidate is likely to incorporate specific attractive characteristics. Some alternatives might incorporate exceptionally strong security features, whereas others might be particularly attractive from a migration perspective. In practice, a trade off of some sort will need to be made.

   For the purpose of selection, a requirements specification should be developed that incorporates the findings of this investigation, i.e. defines (cryptographic) features to avert the attacks and scenarios identified, as well as requisites with respect to migration. It is recommended to employ this requirements specification in an RFQ with a variety of card vendors.

2. **Develop a feasible migration path**
   Once the successor card has been selected, a meticulous migration path should be developed. Here, at least the following aspects should be addressed:

- Assessment of impact on the various elements of the OV-Chipkaart infrastructure when introducing the successor card. For example read and write devices will probably need to be adjusted to accommodate the (cryptographic) characteristics of the new card.
- Interaction with equipment vendors to assess the extent and time path according to which they can fulfil change requests that have arisen from the aforementioned impact assessment
- Interaction with the selected card vendor to establish a feasible time path for the delivery of OV-Chipkaart capable instantiations of their product in the volumes required
- Development of a practicable methodology to take currently operational OV-Chipkaart instantiations out of circulation. Here, a conceivable option is a migration path in which card replacement is aligned with the risk severity of specific card manifestations. As an example, the possibility might be considered to start with the migration of personalised OV-Chipkaart.

Ultimately, a situation should be established where card migration can be initiated at any given moment and carried out within a time span of approximately half a year. Here, it is emphasised that the constraint of fast migration may require specific elements of the infrastructure to be adapted well before the actual migration is initiated.