



Brassersplein 2
Postbus 5050
2600 GB Delft

Retouradres: Postbus 5050, 2600 GB Delft

Trans Link Systems
T.a.v. de heer Drs. J. Kok
Stationsplein 151 - 157
3818 LE AMERSFOORT

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

Datum
16 januari 2008

Onze referentie
2008PUBLIC022

E-mail
Frank.vanaken@tno.nl

Doorkiesnummer
+31 15 285 71 57

Doorkiesfax
+31 15 285 73 82

Onderwerp

Begeleidingsbrief bij TNO Rapport "Reaction to CCC presentation on Mifare cards in December 2007"

In de afgelopen jaren heeft TNO in opdracht van Trans Link Systems diverse analyses uitgevoerd gericht op de technische beveiliging van componenten in het OV-chipkaartsysteem, sommige op hoog niveau en sommige in detail. Zo is ook in 2004 de beveiliging van de kaart en Mifare Classic 4K chip als onderdeel van een quick scan op hoog niveau onderzocht. Trans Link Systems heeft TNO laten weten open te willen zijn over de uitkomsten van deze analyses. Tegelijkertijd geldt dat meer inzicht op korte termijn afbreuk kan doen aan de totale beveiliging van het systeem. TNO begrijpt dat standpunt en laat de keuze aan Trans Link Systems hoe hiermee om te gaan. TNO zal haar medewerking verlenen aan Trans Link Systems om alle rapportages beschikbaar te stellen aan een commissie van experts en/of een onafhankelijke partij ter toetsing.

Op opdrachten aan TNO zijn van toepassing de Algemene Voorwaarden voor onderzoeksopdrachten aan TNO, zoals gedeponeerd bij de Rechtbank Den Haag en de Kamer van Koophandel Haaglanden; de Algemene Voorwaarden zullen op verzoek worden toegezonden.

Recentelijk heeft TNO op verzoek van Trans Link Systems een spoedonderzoek gedaan naar de onmiddellijke risico's als gevolg van het bericht dat in Berlijn twee onderzoekers de OV-chipkaart zouden hebben gekraakt. Dit rapport treft u hierbij aan. Op een aantal plaatsen is informatie verwijderd omdat het vertrouwelijke informatie van derden betreft. De strekking van het rapport wordt daardoor niet aangetast.

Hoogachtend,

A handwritten signature in black ink, appearing to be 'G. van Oortmerssen', written over a horizontal line. The signature is fluid and somewhat abstract, with several loops and a long horizontal stroke extending to the right.

Prof. dr. ir. G. van Oortmerssen
Algemeen Directeur

TNO Corporate Staff Departments

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



Return address: P.O. Box 6034, 2600 JA DELFT, THE NETHERLANDS

Corporate Security
Schoemakerstraat 97
P.O. Box 6034
2600 JA Delft
The Netherlands

www.tno.nl

T +31 15 269 48 41
F +31 15 269 66 55
TNO-Beveiliging@tno.nl

Date
17 January 2008

Our reference
BMTNO2008011703

Direct dialling
+31 15 269 48 42

Subject

Declassification of memorandum concerning research Mifare card

The original memorandum with subject "Reaction to Computer Chaos Club presentation on Mifare cards in December 2007", generated by TNO on January 14th 2008 was classified CONFIDENTIAL. Reason for classification was protection of potentially sensitive data of the customer Trans Link Systems.

Based on the fact that Trans Link Systems published the content of the memorandum on January 16th 2008 during a public discussion in the Dutch parliament and subsequent press releases, the document is now to be regarded and handled as DECLASSIFIED, open information.

All pages of the report will be marked accordingly.

A handwritten signature in blue ink, consisting of several overlapping loops and a long horizontal stroke at the bottom.

H.H.M. Ernst
Corporate Security Officer TNO

The General Terms and Conditions for research assignments to TNO, as filed with the Registry of the District Court in the Hague and with the Chamber of Commerce and Industry for Haaglanden, shall apply to all instructions given to TNO; the General Terms and Conditions will be sent on request.

Memorandum ~~CONFIDENTIAL~~
DECLASSIFIED / UNCLASSIFIED

To
(Name of Trans Link Systems employee not published)

From
(Name of TNO employee not published)

Subject
Reaction to Computer Chaos Club presentation on Mifare cards in December 2007

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

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

Date
14 January 2008

Our reference

Direct dialling

1 Introduction

1.1 Background

In the second half of 2005, Trans Link Systems introduced a contactless chip card system for public transport in The Netherlands. This system, which is called the 'OV-chipkaart' system, is provided by the East West consortium and partly operated by Trans Link Systems.

One of the chip cards that is used in the system is the Mifare Classic 4K card, which is manufactured by NXP (formerly owned by Philips) and used in many contactless chip card systems around the world. In a presentation in December 2007 at a conference of the Computer Chaos Club (CCC) in Germany, two people claimed to have discovered weaknesses in the Mifare Classic cards that make these cards useless for all but the simplest of applications.

In response to that presentation, Trans Link Systems commissioned TNO Information and Communication Technology to do two investigations:

1. A very fast investigation to assess immediate risks for the Dutch OV-chipkaart system on the basis of the presentation given on the CCC conference.
2. A more thorough investigation, to assess not only the immediate risks, but also the risks of potential future discoveries of the CCC presenters or other people expanding on their work.

This memorandum presents the results of the first investigation. The second investigation will be initiated shortly; its results to be presented at a later stage.

1.2 Objective and scope

The objective of this assignment is:

1. To assess the credibility of the claims presented at the aforementioned CCC conference regarding weaknesses in the Mifare Classic cards
2. To assess the short term risks these claims imply for both the OV-chipkaart system and its users

~~CONFIDENTIAL~~

DECLASSIFIED / UNCLASSIFIED

Date

14 January 2008

Our reference

Page

2/2

The scope of this assignment is strictly limited to an analysis of the material presented at the aforementioned CCC conference. Here, the focus is to assess the impact of current attack capabilities the presenters claim to have. For an exact analysis of (supplementary) risks that may or will emerge as the work of these presenters is expanded further, TNO refers to the second investigation that is to be initiated shortly.

2 The CRYPTO1 algorithm

The Mifare Classic 4K card makes use for its security of the so-called CRYPTO1 algorithm, a cryptographic algorithm. This algorithm is used for the encryption of the data exchange between the card and the card reader and for the secure authentication of the card and the reader to each other. The encryption must secure the confidentiality of the exchanged data and prevent copying or manipulation of travel products and purse value; the authentication must make sure that the public transport can only be accessed with genuine cards.

The CRYPTO1 algorithm is a proprietary algorithm, designed by NXP and kept secret from anybody but NXP and a number of licensed manufacturers of the Mifare Classic cards.

The security of the card is in part based on the secrecy of the algorithm. The algorithm is used in combination with secret keys with a length of 48 bits. These secret keys reside on the card and enable the functions mentioned above, i.e. authentication and confidentiality. These keys should never be known outside the cards, not even to the owner of the cards, because if someone is in possession of these keys, he can for example write false products on the card or alter existing products.

The used key length of 48 bits is considered to be very short, because it is not resistant against attacks in which someone tries to find the value of the keys with so-called *full key search attacks*. In a full key search attack, the attacker tries all combinations of the key bits until he has come up with the right combination. To be able to carry out a key search attack, an attacker needs to know the exact algorithm in which the key is used, otherwise he is not able to determine whether he has found the right combination or not. Therefore the fact that the CRYPTO1 algorithm is secret, protects against this kind of attacks.

3 The CCC presentation

In the CCC presentation in December 2007 the authors have claimed the following:

1. to have discovered the complete CRYPTO1 algorithm;
2. that this fact makes the card vulnerable to full key search attacks, because the key length is only 48 bits; the authors claim this can be done in one week using \$100 hardware, or in one day using \$700 hardware;
3. that there is no non-linearity in the algorithm, making it possible to step back in the algorithm to find older keys and that the combination of the bits from the shift

~~CONFIDENTIAL~~

DECLASSIFIED / UNCLASSIFIED

~~CONFIDENTIAL~~

DECLASSIFIED / UNCLASSIFIED

Date

14 January 2008

Our reference

Page

3/3

register is not well spread, making it even easier to find the keys than with a full key search;

4. to have discovered serious weaknesses in the random number generator on the card;
5. to have discovered weaknesses in the way the secret key is combined in the algorithm with the Card ID;
6. that these findings render all cards that use this algorithm, among which the Mifare Classic 4K card, useless for all but the simplest applications.

Notably, the latter claim implies that the current Mifare 4K card is not suitable for public transport and electronic purse applications. Each of these claims will be assessed in the following paragraph.

4 TNO assessment of the presentation claims

This paragraph will discuss how credible TNO Information and Communication Technology considers the claims of the presentation to be and what their specific consequences are. Here, the same numbering is used as in the previous section. Note that TNO has no knowledge of the CRYPTO1 algorithm, so judgements have been done solely on the basis of the CCC presentation.

1. **Because the authors have only presented parts of the algorithm, the claim to have discovered the full CRYPTO1 algorithm, cannot be fully verified at this moment. However, TNO is of the opinion that either they *have* fully retrieved the algorithm, or will do so in the near future.** To start with, they have certainly located the part of the chip where the cryptographic algorithm has been implemented. They have also presented in great detail the logical build-up of the algorithm and in full detail the random number generator, even including the used generator polynomial. However, their oral claim that the whole system does not contain non-linearity, is in contradiction with a statement of NXP to TNO that actually the algorithm does contain non-linearity. This may indicate that the CCC authors have not found all details yet. However, TNO suspects that this is merely an error in their oral presentation. (Fragment not published by TNO due to third party confidentiality agreements) In the presentation they make a statement that seems to indicate that they know the algorithm *does* contain non-linearity.

That the authors have not revealed the entire algorithm may be some kind of hacker's ethics to not expose the full details until the attacked party has had time to react. This was also explicitly stated by one of the presenters. A second reason may be fear of legal actions by NXP.

2. **If the CRYPTO1 algorithm is known, this indeed makes the Mifare Classic 4K card vulnerable for a key search attack, as a key length of 48 bits is too small to resist this kind of attacks.** Even keys with 56 bits, together with much more complicated algorithms than the CRYPTO1 algorithm, have been broken by dedicated hardware. The mentioned estimated amount of financial investment required, however, seems far too low; TNO's estimation several years ago was higher by a factor of 50. This is not too relevant, however, because both amounts

~~CONFIDENTIAL~~

DECLASSIFIED / UNCLASSIFIED

~~CONFIDENTIAL~~

DECLASSIFIED / UNCLASSIFIED

Date
14 January 2008

Our reference

Page
4/4

will probably be gladly invested by criminals, if the business case for their attack is positive. As a consequence, malicious retrieval of card keys is likely to be demonstrated in the near future. If keys of a card *are* retrieved by attackers, they can, with a complicated attack, write fraudulent travel products on the corresponding card, manipulate existing products and increase the purse value. (Fragment not published by TNO due to third party confidentiality agreements)
Note that attackers need to retrieve multiple keys of a single card to be able to do that.

It is also possible that an attacker eavesdrops and records the communication between a customer's card and the card reader, conducts a key search attack on this data off-line and retrieves keys and user data of the card. This user data may include date of birth and balance of the e-purse. An on-line attack is not possible because of the time needed to retrieve the keys.

Because each card has individual unique keys, breaking one card does not break other cards as well. Each card has to be broken individually with a newly initiated attack.

3. **The authors have presented little evidence for their claims that the algorithm contains severe cryptographic weaknesses.** At the moment, therefore, it is not possible to reliably estimate whether or not this is true. If this really were the case, this would mean that the keys would be easier to find than with a full key search. However, as it is by all means possible to do a full key search on a 48-bit key, there is not much need to speed up the attack with complicated reasoning and hardware. This fact is also acknowledged by the presenters.
4. **The weaknesses discovered in the random number generator of the card are very credible, judged by the amount of detail they were presented with.** Based on a first analysis TNO believes that it is at least theoretically possible to use these weaknesses. (Fragment not published by TNO due to third party confidentiality agreements)
5. **The revealed way of the combination of the secret key and the Card ID is quite credible, judged by the amount of detail it was presented with.** In a first analysis TNO deems the corresponding attack not to be serious, since it requires the attacker to have found the key of an operational card (key_x in the presentation) which they are not able to do. The latter will be discussed in greater detail in the next section, Section 5.
6. **That the discoveries of the presenters make the Mifare Classic 4K unfit for public transport applications, is too quickly judged.** The OV-chipkaart system, for example, does not solely rely on the standard security of the card for its safety. There are other mechanisms in place, like fraud detection and blacklisting, with which fraudulent operations with cards are detected and the cards refused in the system. A thorough investigation will have to be done to judge whether the overall security architecture is sufficient to secure the system enough to destroy positive potential business cases for attackers and to protect the public to a sufficiently high degree. This will be the subject of the second investigation, mentioned in the introduction.

~~CONFIDENTIAL~~

DECLASSIFIED / UNCLASSIFIED

~~CONFIDENTIAL~~

DECLASSIFIED / UNCLASSIFIED

Date

14 January 2008

Our reference

Page

5/5

5 Short term risks

To assess the short term risk for the OV-chipkaart system and the people using the system, it is necessary to look at a negative claim the presenters made. They stated that they did not yet fully build hardware to do a full key search, a key cracker, although they say they started. But they merely showed a picture of a different, comparable project. They also explicitly stated that they are not yet able to break the keys.

This is a very credible negative claim, because they would have been very eager to present such a success to the public.

The fact that they have not fully built a key cracker yet, means that on short term the system is not at risk from a key breaking attack by the authors of the presentation and does not have to fall back on measures like fraud detection and blacklisting of cards for this reason.

It will certainly cost the attackers time to build such a key cracker; they have to implement the CRYPTO1 algorithm fully correct and highly parallelize their attack in order to be able to search the whole key space in a reasonable amount of time. They also have to figure out a way to gather plaintext/ciphertext pairs, the input for the key cracker. The time needed to complete the attack is estimated by TNO at approximately half a year. And then the attack is in the hands of the authors of the presentation, not in the hands of criminals. This might become the case only after further publications.

6. Conclusions

TNO is of the opinion that many of the claims of the CCC presentation are quite credible, judged by the amount of detail they have been presented with, for example:

- The fact that the random number generator on the card shows weaknesses;
- The fact that the combination of the key and the Card ID could have been done in a stronger way.

The claim that the authors have reverse engineered the entire CRYPTO1 algorithm cannot be fully verified on the basis of the presented results. TNO is of the opinion, however, that either they *have* fully retrieved the algorithm, or will do so in the near future.

Of these items the last one is the most serious one, as TNO shares the opinion of the authors of the presentation that knowledge of the CRYPTO1 algorithm enables a hardware attack in which the keys of the card can be retrieved, by building a so-called key cracker.

The fact that the presenters have not fully built a key cracker yet, means that on short term the system is not at risk from a key breaking attack by the authors of the presentation. The time needed to complete the attack is estimated by TNO at approximately half a year. During that time, the system does not have to fall back on measures like fraud detection and blacklisting of cards for this reason.

~~CONFIDENTIAL~~

DECLASSIFIED / UNCLASSIFIED

CONFIDENTIAL

DECLASSIFIED / UNCLASSIFIED

If keys of a card *are* retrieved by attackers, however, they can write fraudulent travel products on the corresponding card, manipulate existing products and increase the purse value. (Fragment not published by TNO due to third party confidentiality agreements)

A thorough investigation will have to be done to judge whether the overall security architecture that exists in the OV-chipkaart system is sufficient to secure the system enough to destroy positive potential business cases for attackers and to protect the public to a sufficiently high degree.

Date

14 January 2008

Our reference

Page

6/6

CONFIDENTIAL

DECLASSIFIED / UNCLASSIFIED