

Overview of Security Threats for Smart Cards in the Public Transport Industry

Konstantinos Markantonakis, Keith Mayes
Information Security Group Smart Card Centre
Royal Holloway University of London
Egham, Surrey, United Kingdom
{K.Markantonakis, Keith.Mayes}@rhul.ac.uk

Damien Sauveron
XLIM
University of Limoges
France
Damien.Sauveron@xlim.fr

Ioannis G. Askoxylakis
Institute of Computer Science
Foundation for Research &
Technology – Hellas
asko@ics.forth.gr

Abstract

The advantages of utilising smart card technology, more importantly contactless smart cards, in the transport industry have long been realised. In this paper we provide an overview of the generic security issues and threats encountered whenever smart cards are utilised within the transport industry. To help highlight the issues, we analyse the different types of cards, their hosted applications, along with certain requirements on the relevant card issuing authorities.

1. Introduction

Among the main driving factors towards the success of smart card technology are the capabilities of performing security sensitive operations along with maintaining the integrity of the internally stored information. These characteristics enable the wide deployment of smart card based services in a variety of applications and sectors. Smart cards are increasingly used as authentication and encryption vehicles in mobile phones, as bankcards, and as the carrying medium for various payment and access control applications.

The advantages of utilising smart card technology, more importantly contactless smart cards, in the transport industry have long been realised. As a consequence there are a number of major schemes currently operating in various cities worldwide (e.g. Oyster in London, Octopus in Hong Kong, CharlieCard in Boston) and many more schemes (e.g. in Holland) are in various stages of development. In these schemes the cards are used as a new ticketing medium aiming to reduce fraud, increase passenger flow and convenience.

Due to the sensitive and important role of the smart card device within the overall smart card based system it is evident that the card as well as the infrastructure components be designed to withstand various attacks and attempts of fraud during their lifecycle. This has implications on both physical and logical security levels, which are of vital importance and at the same

time act as the driving factor for the adoption of the technology.

In this paper we provide an overview of the generic security issues and threats encountered whenever smart cards are utilised within the transport industry. Furthermore, the threat requirements are also taking into account the general characteristics of the overall system design and whenever possible relevant countermeasures are suggested.

2. Smart Card Technology in Public Transport

This report does not attempt to comment in anyway about the suitability of the different smart card technologies applied to different transport scenarios and sectors. However, we present some candidate smart card technology for the transport industry and where possible comment on its advantages and disadvantages. The sections below introduce three card types that may be appropriate for practical use within the transport industry.

2.1. Low Cost Smart/Chip Card Technology

The low cost smart cards cover a variety of technologies in a variety of application and sectors. This category is the most limited of the three in terms of memory and processing capabilities. Indeed the processing capability may be so restricted that there is some debate as to whether it should be called a “smart” card or simply a “chip” card. The chip is embedded in a low cost carrier medium such as a piece of thin plastic substrate, cardboard or even thick paper.

2.2. Contactless Smart Card Technology

Most contactless smart cards can be read from a distance of about 10 cm, and in some cases they can be read without being removed from a wallet or purse. Apart from the difference in the communication interface and the thickness of the plastic cover there are no other real logical differences from traditional

contact cards, in terms of processing power, memory capacity and cryptographic capabilities. The main characteristics of contactless smart card technology (e.g. physical robustness, enable fast passenger flows, relatively secure, etc.) indicate that it is currently the best available solution for the transport industry and as a result different types of cards are used in a number of projects all over the world.

2.3. Dual Interface Smart Card Technology

A dual interface or “combi” card, as the name implies, combines a contact and contactless interfaces for the underlying chip functionality. Therefore, the card may allow access to the same data using contact and contactless smart card readers. However, it is also possible to combine a contact and contactless chip on the same card such that they are completely independent. We will focus our discussions on the single chip “dual interface” card.

3. The Operational Environment

In this section we highlight the operational requirements of smart card technology in the transport industry in terms of the parties involved, their control over different aspects of the overall ticketing systems and also their motivation. The following requirements are not exhaustive and the goal is to categorize them so that they will help us to define the security boundaries for our analysis.

3.1. The Entities Involved

There are different entities involved in any smart card transport based scheme. For the sake of simplicity and completeness we draw attention to the following:

- The **smart card** is often a credit card sized plastic card (it can also be a low cost carrying medium like paper based) embedded with an integrated chip. In general the chip offers certain processing power along with volatile and non-volatile storage memory (the types of memories will be described later on).
- The **cardholder** is defined as the person to whom the card was issued. It is assumed to be the party that has possession of the smart card on a day-to-day basis. It should also be noted that the cardholders serve a dual role. Under certain circumstances they might have every interest in retaining the integrity of the system (e.g. when they receive a refund for a card based purchase). On the other hand they could be the originators of

attacks that will result in direct or indirect benefits from fraud.

- The **card issuer**, as the name implies, is the party that issues the smart card. It is a common requirement of smart card issuers that they always retain control of the card.
- The **smart card application developers** are responsible for developing the smart card hardware and software including any applications and often the underlying operating system. Therefore, we assume that this category does not impose a major risk factor within our analysis.
- The **terminal** represents the device that allows the card to communicate with the outside world. Some terminals might be directly controlled by the cardholder such as a card reader connected to the cardholders PC or indirectly by tampering with a Point-of-Sale (POS) terminal machine at a train station gate
- The **back office systems** are responsible for manipulating card, cardholder and transaction (journey related) data.
- The **smart card manufacturers** are often the card distributors as they often manufacture and directly deliver the cards to transport operators. It is assumed that smart card manufacturers are trusted entities that follow all the necessary best practices for the protection and secure distribution of cards.
- The **attackers** involve any party with an interest to attack the security of the overall system. These could include traditional hackers, academics, but also cardholders.

3.2. General Observations Regarding Existing Smart card Technology

It is widely believed that smart cards have a lot to offer in security sensitive applications by supporting cryptographic algorithms and secure storage of sensitive information. When the card utilises cryptographic algorithms and well designed security protocols it can be used as a tamper resistant token for authorisation and access control. Over the last few years major hardware and software improvements have taken place in order to improve the security of the smart card device. As a result the high-end smart card technology deploys adequate security functionality that it is relatively difficult to penetrate. Technological improvements will continue to take place as smart card attacks become more and more sophisticated.

It is important to note that smart cards can not offer complete security, not because they have restricted functionality but simply because absolute security can not be guaranteed by a single device. The overall

security of a smart card based system is as vulnerable as its weakest link. For example, even if the most sophisticated smart card technology is deployed, it is highly probable that the security objectives will not be met if the underlying security protocols are weak. In the transport industry for example, other system components should be properly implemented and they should be considered equally important, i.e. proper station gating, and back office system development. The latter observation re-emphasises the fact that smart cards are a very important component within the system architecture but they should not be considered in isolation.

Another concept that requires further consideration is that as smart card technology and applications become more widely deployed the incentives for attacks will increase. The larger the number of cards and the more applications are involved the greater the potential for attacks to be mounted. The potential of breaking into one application can act as the starting point for attacking others, especially when applications reside in the same card. When multiple applications are involved in a single card, it will be a security conscious option to consider a high end multi application smart card operating system like Java Card and Open Platform, Multos, etc. Furthermore, as smart card security evaluation experience (e.g. using The Common Criteria) increases both cards and applications should ideally be evaluated to adequate security levels (e.g. EAL4+).

3.3. Revenue Protection and Fraud

Among the main benefits of introducing smart cards in the transport industry is claimed to be fraud reduction. It is true that smart cards offer the industry far more sophisticated security features compared with the magnetic stripe system and moreover with the paper based tickets. However, it must be remembered that reducing fraud will not necessarily produce a corresponding increase in revenues. For example, it could be the case that some people, when denied the chance to travel without their ticket being inspected may choose not to travel at all or use an operator who does not prohibit fraud in an aggressive way. However, there may be an indirect benefit to operators as by carrying fewer passengers there is more available capacity for genuine customers. The latter may encourage new customers or help to satisfy existing customers. Of course the high initial investment is a barrier to deployment of smart card solutions but there is the promise of reduced costs in the longer term.

Revenue protection is perceived differently by the various entities within the transport industry. For the

purpose of this report ticketing fraud includes fraudulently produced tickets and “overriding” as a result of not properly checking the ticket validity at the exit points. For the former type of fraud smart card technology can offer substantial benefits, as it is relatively more difficult to forge. However, the potential benefits will depend on how much counterfeit fraud is currently taking place. For the latter type of fraud, it is reiterated the fact that smart cards can successfully cover certain aspects of the problem. But no solution will be effective unless the tickets are properly inspected for the duration of the journey or at their destination (e.g. adequate gating is required and sometimes additional visual ticket inspection might be considered necessary).

3.4. Motivation and Complementary Architectural Issues

It must always be remembered that there is no absolute security. Breaking into a system should be considered possible when the right amount of money and time are properly invested. Therefore, the main effort in designing a secure system, e.g. a smart card based ticketing system, will be to identify the balance between the required security to adequately counter the threats and the available security (taking into account the characteristics of the current technology and the relevant cost). For example, a city wide, low cost fare system may have a different security model to a national travel scheme. Identifying all the possible threats (all not be possible) well in advance may not be a trivial task but it will certainly help in the proper system design and subsequent operation. Threats should also be prioritised according to their significance in order to assist the requirements definition and assist in the selection of the appropriate countermeasures and the design of an efficient system.

The transport operators might also require that its employees use smart card technology in order to authenticate themselves to fare collection devices. Therefore, staff fraud will have to be taken into consideration. In addition to the above types of threats we also have to consider third party individuals or organised groups that might obtain an interest in defrauding the system.

In order to enhance the overall security of a smart card based transport system, additional components will be required that might not be directly related to smart cards. These additional components will complement the smart card security and also strengthen the overall system operation.

Smart card ticketing based solutions may assume that the ticket medium is inspected both at the

beginning and also at the end of the journey. This ensures that the exact fare is calculated on the spot and subsequently an appropriate amount is extracted from the card. Although there are alternative options (e.g. a fixed amount is withdrawn from the card, at the beginning of a journey, and depending on the actual distance the monetary difference is either returned to the card or requested from the card), almost all of them rely on the fact that station gating is properly implemented.

In order to enhance the overall system security, it would be helpful that certain back office systems perform further checks on all journeys, in order to identify any irregularities and update the card hot lists accordingly. This will of course require adequate networking of all the ticketing machines and POS terminals with the back office systems. Communication is required at least once a day in order for relevant information to be exchanged.

Most of the ticketing applications require the existence of an electronic purse within the card to provide the means of payment. Often, this electronic purse is proprietary for each system or card issuer. Although the existence of an electronic purse makes the whole idea feasible and flexible, at the same time it acts as an incentive for attacking the system.

Some of the above observations suggest ways of providing countermeasures against certain vulnerabilities but at the same time introduce new issues that need to be taken into account. In the next section we observe some of these issues and whenever possible we also provide the relevant countermeasures.

4. Smart card Attacks and Threats Analysis for the Transport Industry

The aim of this section is to provide criteria to categorise the different types of attacks, threats against different types of smart cards, the participants involved, and the required skills and level of expertise, etc [2].

For the purpose of this study, a smart card attack is defined as an attempt by an entity to bypass the physical or logical security of the card and/or its inter-dependent applications and systems, in order to obtain unauthorised direct or indirect access to information, benefits or entitlements.

4.1. Attacks Against Smart Card Component

There are two types of non volatile memory in a smart card. The Read Only Memory (ROM) hold's persistent information (e.g. the smart card operating system, applications), which is written (masked) during the manufacturing phase. The most common type of

memory that allows information to be written or deleted at any point in the cards lifecycle is the Electrically Erasable Programmable Read Only Memory (EEPROM). Therefore, the target of an attack can be the security sensitive information stored internally within the card. The aim of the attack will be to obtain access to such information and use it to compromise the security of the card or some other principal entity in the smart card scheme.

A smart card attack can also target the operation of cryptographic primitives (e.g. the generation of cryptographic keys or execution of an application) of the actual smart card microprocessor. The aim of this attack will be to force the smart card microprocessor to perform certain operations that will compromise its security. For example, to allow the microprocessor to update the ticket entitlement in the card and at the same time avoid deducting the payable amount from the purse. The range of attacks on smart cards can be classified into three basic categories i.e. logical, physical and side-channel.

4.1.1. Logical attacks

The logical types of attacks attempt to identify and exploit any vulnerabilities or weaknesses in the design of the smart card operating system (SCOS) [6, 17] or the smart card application. This may take the form of presenting the card with invalid commands, formats, field lengths or attempts to overflow buffers. The advantage of these attacks is that they are cheap, relatively simple to perform and do not necessarily damage the card. However, provided that reputable application developers and smart card suppliers are used then rigorous design (and sometime peer reviews) and development processes should have eliminated the logical vulnerabilities.

4.1.2. Physical attacks

These types of attacks can be mounted by an entity obtaining physical access to the smart card. Therefore the attacker can be either the cardholder, a member of staff, or even a third party that somehow manages to get hold of some legitimate cards.

There are many different ways to perform physical attacks on smart card microprocessors, some require low cost equipment [13] and other require sophisticated and expensive equipment. Typical attacks, in the latter category, include attempts to read the contents of the EEPROM memory of the card (by using powerful electron microscopes) [7], to re-activate burned fuses by focusing ion beams or even using laser cutter microscopes to modify the architecture of the chip. In most cases a number of chips may have to be

destroyed before an attack is considered successful. In order to provide adequate countermeasures the smart card manufacturers provide constant improvements (Dielectric "passivation layers", wire mesh layers and non standard bus systems) on their chip designs, in order to make it more difficult for these attacks to take place.

Whilst physical attacks have focused on smart cards used in other industries there is no reason why they cannot be applied to transport [4]. The main question is whether a criminal group can find a business case to justify the cost and effort required for such an attack.

4.1.3. Side-Channel Attacks

Side channel attacks have been of concern to the smart card industry because they require modest levels of equipment and do not necessarily damage the card. The majority of attacks have monitored the supply current of the working smart card in order to infer how particular processes run and to extract secret information such as keys stored on the card [9]. Similar results have been obtained in laboratory conditions by carefully positioning a tiny antenna over certain areas of a smart card chip. Attacks can be applied to normally operating processes or by applying external input to introduce faults [5].

There are some industry review of contactless card security [8, 15] but up to recently there was relatively little is said about side-channel attacks on contactless cards (compared to cards with contacts), primarily because there was no direct and convenient measurement of current consumption [10]. However, current variations may result in detectable RF field fluctuations which may then be processed. The radio communication link may also assist the attacker if it proves possible to locally eavesdrop on normal card usage.

4.1.4. Further Considerations for Transport Cards

All the three types of cards identified in section 2 are subject to the aforementioned attacks. The low-cost cards may be particularly vulnerable as in order to lower the cost of the card certain security compromises (e.g. not evaluated by peer review process) might have been considered. It must be taken into account that although low cost cards might be used for one way tickets this does not imply that the value of the ticket will be low, e.g. long distance one-way train tickets. Similarly, the cardholder flexibility versus security must be very carefully balanced.

Therefore, it is recommended that all cards should be used with extra care in an environment where risk is considered minimal and security is supported by

additional countermeasures. The other two types of cards (contactless and dual interface) are often relatively more expensive and they are expected to be able to withstand the "entry-level" [14] of physical and logical attacks.

One possible usage scenario for a transport smart card is when it is not necessary to be removed from the passenger's wallet in order to be presented in the acceptance terminal. In that case, since no immediate visual inspection can be made, the likelihood of an attack is increased. For example, consider the misuse of a child fare card.

As mentioned previously the existence of a back office system that will perform regular checks will significantly supplement the overall security of the system and for example may be able to check the origin and destination of a journey to subsequently verify the corresponding purse balance. However, corresponding actions to block or blacklist the card can be effort intensive and generally it is far better to apply design effort to raise the system's resistance to attack rather than trying to detect when something goes wrong.

4.2. Publicity Attacks

The "publicity" attacks usually come from researchers and individuals seeking fame and recognition. Although initially these types of attacks might not be considered extremely damaging, they actually are, as they eventually attack the brand image.

In case a smart card application (residing in a multi-application smart card) is compromised, it is often the case that all the accompanying applications receive the bad publicity. In that case restoring the brand image can be extremely daunting. For example, suppose a loyalty point application, an electronic purse application and a ticketing application are all residing in the same card. Let us suppose that the loyalty application is compromised and due to the fact that it is used alongside the transport application the latter also receives negative publicity.

The "publicity" attacks can have a devastating effect both on the actual project and the organisations involved. The creation of a widely recognized and successful brand image often requires a huge investment in time money and effort.

4.3. Indirect Gain Attacks

The indirect gain attacks are relatively more difficult to be identified as they exploit vulnerabilities in various components of the system and they are usually identified following the system being fully

operational. For example, an attacker exploits vulnerabilities in the protocol or the messages being exchanged to/from the smart card. A more indirect action includes an employee of the transport company obtaining access to previously used cards (from the lost-and-found or recycled bouquet) that might hold some residual value and attempt to sell them or re-use them.

Both the indirect gain attacks and publicity attacks can be prevented in the same way as with any other type of attack. That is, by eliminating the prospect of taking place in the first place. This can be partially guaranteed by selecting appropriate smart card technology along with well-designed and properly integrated systems that will be able to withstand relatively sophisticated attacks. Furthermore, it is necessary that the proper security and auditing procedures (e.g. for the card distribution destruction and replacement) be in place in order to ensure the smooth operation of the system.

4.4. Attacks by Rogue Terminals

This is the classical type of attack that alarmed both cardholders and card issuers in the past [3]. Whenever a smart card is presented to a legitimate terminal, the terminal should be trusted that it will perform all the operations as expected. For example, consider the case of a cardholder buying a ticket from an unattended POS terminal in the street. The cardholder is prompted to pay £1 for the ticket price but the terminal deducts more (e.g. £5) from the purse. It is likely that the rogue transaction will be identified when the back-office systems or the cardholder inspects the card log files or the card transaction statements/receipts respectively, but this may be too late to take effective action.

The countermeasures for this type of attack include a combination of methods. Firstly, communication (at the protocol and application level) with the outside world should only be allowed between authenticated entities. This might require that cards should be powerful enough to perform adequate cryptographic operations (i.e. authentication of the terminals) prior to establishing any communication. This option might increase the overall complexity of the system due to cryptographic key management and longer transaction times. Secondly, legitimate terminals should be able to obtain certain details of the last journey and purse transactions every time a card is presented. Subsequently, the terminals will have to transmit this information to the back office systems and, as part of the further processings, any irregular or under/over priced journeys could be identified.

4.5. Attacks Against the Terminal and/or Interface

For terminals that reside under the cardholder's control (e.g. a PC connected reader) there is always the risk that the communication might be intercepted and/or manipulated. However, if the communication protocol and the applications are properly designed and communication is adequately protected (e.g. encrypted or signed) the likelihood and the effects of an attack are minimised.

Irrespectively of the terminal characteristics or the relevant cardholder control, there is the risk of the card being removed from the terminal before the transaction is completed. The duration of a typical contactless transaction in a transport application may be between 140-300ms. This means that the time frame, that an attack can be mounted, is relatively small. In cases where the terminal is not under the immediate control of the cardholder (e.g. entry gates or POS) it becomes even more difficult to control the timing of such an attack. Moreover, most of the cards provide the functionality of transaction atomicity [11]. This means that well designed applications will guarantee that transactions will either take place in full or do not take place at all.

Another category of attacks is stolen terminals e.g. those carried by the transport operator employees in order to issue tickets and receive payments. As a result fake terminals could be developed in order to issue tickets and receive payments. The main countermeasure against this type of attack is that a terminal will require a form of communication with the back-office systems, at a regular interval, in order to enable them to work properly for the next few days. In that way the period for which a terminal can operate without being inspected both physically and logically is minimised.

4.6. Attacks by the Card Issuer or Other Program Participants

Among the major factors that influence the success of almost any smart card program, in terms of being widely accepted and attracting new cardholders, is the concept of trust. It is crucial that the card issuer is considered as a trusted entity. However, the issuer may be a large company with many employees and so the necessary procedures should be in place in order to ensure that only trusted and authorized personnel have access to the appropriate mission critical systems.

The scenario is more complicated for multi-application cards with applications from various parties. In this case someone might consider that any single party can attack the other's interest in the card.

For example, let us examine the scenario in which an issuer, i.e. a transport operator, issues a smart card along with a payment application and a loyalty application both from different providers.

There are multiple countermeasures that will prevent any of the participants taking advantage of the interests of another entity within the card. First of all, most proprietary and open multi-application smart card operating systems should prevent any undocumented and unauthorized communication to take place between two applications [12]. At the same time most multi-application smart card operating systems aim to enforce strict issuer control of the card. That means that the issuer is always aware of which applications are residing in the cards at any point in time and any application downloads or deletions are pre-authorized. This empowers the card issuer with the flexibility to decide whether an application comes from trustworthy origins before it is actually allowed to be downloaded into the card.

The likelihood of issuer attacks is minimized when proper smart card application software engineering processes are utilized for the development of the smart card applications. Additionally, extra reassurance can be drawn from the security functionality of the underlying operating system.

Protection against attacks from third party participants can be provided by well-designed back office systems. They should be in a position to identify any card discrepancies as they can perform checks on current and previous stages of the card lifecycle.

Third party attacks can be prevented, to some extent, by proper application code inspection through off-line, or even on-line [16], smart card application code verification procedures, i.e. before or during the application download respectively.

4.7. Further Issues for Consideration

Smart Card Distribution and Storage should always be considered as a sensitive process. Especially within the transport industry where smart cards will have to be transported pre-personalised within various sites, e.g. from the manufacturer to the issuer and from the issuer to the various storage locations at the various points of sale. Therefore, card transportation and distribution should always take place via approved couriers.

Furthermore, if the keys used for card enablement (e.g. in order to protect the cards during their transportation through various sites) remain secret then the cards will remain relatively secure.

Smart Card Destruction and Replacement is also a sensitive operation. It must be guaranteed that the selected cards are properly disposed of and furthermore any residual value within the electronic purses is properly reclaimed. The monetary refunds procedures should be adequate in order to prevent staff from exploiting residual value stored in lost or non working cards, or even attackers picking old cards and creating disposal clones.

Smart cards and security evaluations are considered essential in the light of the increased sophistication of the security attacks.

We believe that for the transport industry to safeguard its assets it should consider the use of smart card security evaluations and peer reviews in order to increase confidence in smart card ticketing schemes.

Abuse of Concessionary Scheme or Season Tickets is an existing type of fraud against which smart card technology will provide little direct protection. A cardholder can always lend his/her smart card (e.g. bearing the discounted entitlements) to third parties. Therefore, without any proper visual inspection of the ticket medium this type of fraud will continue to exist after the introduction of smart card technology. However, the associated transaction logging by the back end systems may detect excessive or unusual usage patterns and so indirectly the card system may combat such fraud.

Staff Fraud is a type of fraud that smart card technology will offer some direct protection as certain staff procedures (ticket issuing, access control) will be safeguarded by the additional functionality offered by smart card system. However, some new fraud opportunities may arise with respect to the handling of lost and stolen cards.

In general, staff fraud can be very creative and difficult to anticipate and so proper organisational procedures should be in place, so that opportunities are restricted.

5. Conclusions

From a technology point of view all the components that assist the deployment of smart cards in the transport industry are available. Selecting the best available technology will probably reduce certain risks but at the same time will increase the overall cost of a migration program. Furthermore, the proper system integration, installation and operation should be considered as critical phases.

Smart cards tend to be replaced every 2-3 years, at least in the banking sector, in order to catch up with recent technological developments. Selecting the appropriate smart card technology is a very critical step for the transport operator as the appropriate balance between price and offered technology should be

identified. Similarly, there are other issues (back-office systems, station gating, POS terminals, third party applications, etc.) that will have to be considered for an effective chip migration.

It is often the case that a multi-application smart card approach will appear attractive as it may allow the transport operator to share the cost of the card with other interested parties such as banks. However, this needs to be carefully considered as the cost reduction may be eroded by the increased complexity of the solution's architecture and its operational management.

Additionally, in parallel to the smart card ticketing system, it is necessary to have the necessary "fall back" systems that will allow the transport operator main procedures to operate with relevant confidence in case there are any major problems with the operation of the fully automated system.

Acknowledgment

The authors would like to thank Gerhard Hancke for his helpful comments.

6. References

- [1] *Common Criteria*. www.commoncriteria.org, 2006.
- [2] R. Anderson and M. Kuhn. Tamper resistance — a cautionary note. In *The 2nd USENIX Workshop on Electronic Commerce Proceedings, Oakland, California*, pages 1–11. USENIX Association, November 1996.
- [3] Mike Bond. Chip and pin (emv) point-of-sale terminal interceptor. <http://www.cl.cam.ac.uk/~mkb23/interceptor/>, March 2006.
- [4] Nicolas T. Courtois, Karsten Nohl, and Sean O'Neil. Algebraic attacks on the crypto-1 stream cipher in mifare classic and oyster cards. *Cryptology ePrint Archive*, Report 2008/166, 2008. <http://eprint.iacr.org>.
- [5] Eli Biham and Adi Shamir. Differential Fault Analysis of Secret Key Cryptosystems. In *CRYPTO '97: Proceedings of the 17th Annual International Cryptology Conference on Advances in Cryptology*, pages 513–525, London, UK, 1997. Springer-Verlag.
- [6] J. Elliot. The maos trap [smart card platforms]. *Computing & Control Engineering Journal*, 12, Issue 1:4–10, February 2001. ISSN: 0956-3385.
- [7] Jacques Fournier. Security attacks, countermeasures and testing for smart cards. Presentation in the MSc in Information Security, February 2008.
- [8] HID. Rfid tags and contactless smart card technology comparing and contrasting applications and capabilities, 2005.
- [9] P. Kocher, J. Jaffe, and B. Jun. Differential power analysis. In M. Wiener, editor, *Advances in Cryptology CRYPTO '99*, volume 1666 of *Lecture Notes in Computer Science*, pages 388–397. Springer-Verlag, 1999.
- [10] S. Mangard M. Hutter and Martin M. Feldhofer. Power and emattacks on passive 13.56 mhz rfid devices. In *Workshop on Cryptographic Hardware and Embedded Systems, CHES 2007*, volume 4727 of *LNCS*, pages 320–333. Springer-Verlag, September 2007.
- [11] P. Peyret, G. Lisimaque, and T. Y. Chua. Smart cards provide very high security and flexibility in subscriber management. In *IEEE Transactions on Consumer Electronics*, volume 36(3), pages 744–752, August 1990.
- [12] H. C. Pohls and J. Posegga. Smartcard firewalls revisited. In J. Domingo-Ferrer, J. Posegga, and D. Schreckling, editors, *Smart Card Research and Advanced Applications - Proceedings of the 7th IFIP WG 8.8/11.2 International Conference, CARDIS 2006*, volume 3928 of *Lecture Notes in Computer Science*, pages 179–191. Springer-Verlag, April 2006. Tarragona, CAT, Spain.
- [13] Markus G. Kuhn Ross J. Anderson. Low cost attacks on tamper resistant devices. In M. Lomas et al., editor, *Security Protocols, 5th International Workshop, Paris, France*, volume 1361 of *LNCS*, pages 125–136. Springer-Verlag, 1997.
- [14] Keith Mayes, Konstantinos Markantonakis, "Smart Cards, Tokens, Security and Applications", *Springer Verlag, January 2008*, ISBN: 978-0-387-72197-2.
- [15] Alain Vazquez. what future for contactless card security? Eurosmart, May 2001.
- [16] Xavier Leroy. On-Card Bytecode Verification for Java Card. In *E-SMART '01: Proceedings of the International Conference on Research in Smart Cards*, ISBN 3-540-42610-8, pages 150–164, London, UK, 2001. Springer-Verlag.
- [17] Constantinos Markantonakis, "The Case for a Secure Multi-Application Smart Card Operating System", Information Security Workshop 97 (ISW97), September 1997, Ishikawa, Japan, In *Lecture Notes in Computer Science (LNCS)*, volume 1396, pp.188-197