

Transport Ticketing Security and Fraud Controls

Keith E. Mayes, Konstantinos Markantonakis, Gerhard Hancke
Information Security Group Smart Card Centre
Royal Holloway, University of London
Egham, Surrey England
(keith.mayes, k.markantonakis, gerhard.hancke) @rhul.ac.uk

Abstract

For many years, public transportation systems have been an essential part of day-to-day life and so the principle of needing a “ticket” has been familiar to generations of travelers. However as technology has advanced it has become possible to make use of electronic tickets that have significant advantages both for travelers and for the transport system operators. There has been a lot of recent publicity regarding weaknesses in some electronic ticket solutions; which whilst based on some solid facts tend to suggest that transport ticket security and fraud control is primarily a smart card/RFID technology issue. However this cannot be the case as systems exist that do not use such technology; or use it along side legacy systems. This paper will consider technology problems, but will first establish the bigger picture of transport ticketing and will finally make suggestions for future evolution of such systems.

1 Introduction

Effective public transportation systems are seen as a fundamental requirement for modern society, not only to satisfy basic mobility requirements, but increasingly to ensure that time, resources and assets are used in an efficient manner thereby minimising adverse impact on the environment. Public transport offers a service and generally users need to present a ticket to prove that they are entitled to travel. Obtaining a ticket usually requires the exchange of value between the traveller and a transport operating company, such that the magnitude of exchange is appropriate to the required travel permission and underlying service costs. However, where money is exchanged for a transport service there will always be individuals who seek to avoid or unfairly reduce their fare payments (or even generate income), which will ultimately burden their fellow travellers with added ticket costs. This is nothing new and does not stem from flaws in technology, but rather in human nature. However, more recently some transport operators have turned to technology in order to reduce fraud. As reducing fraud with technology requires attention to information security, transport operators have become aware of the need for appropriate fraud and security controls. There is in fact a great deal of debate concerning the effectiveness of existing controls, although this tends to be narrowly focussed on issues related to smart card/RFID security. This can distort the overall understanding of the system aspects, which can be used as justification for both alarmist and complacent viewpoints. To expand the focus we will first return to the fundamentals of ticketing systems for transportation.

2 Ticket Basics

In an old (pre-technology) and simplistic train or bus ticketing system we would have various types of customers (travellers) plus the transport operator's staff and processes. A traveller could be characterised as shown below.

Traveller

- Identity
- Age
- Concessions
- Travel requirements/products
- Payment and/or means to pay

The actual identity of the customer was not captured although it was part of a fraud check during ticket purchase and usage e.g. an adult should not use a child's reduced fare ticket. Concession entitlements including those that are age related needed to be captured at the time of ticket purchase and issue; and be subsequently verifiable. Each traveller would have their own unique travel requirements including class of travel, departure and destination stations, time and dates of travel. There would also have been requirements for longer term seasonal use and journeys that use multiple transport operators' systems. Generally customers paid the transport operator for tickets in advance of travel. The transport operator could be characterised as shown below.

Transport Operator

- Company
- Ticket office (Seller)
- Station ticket inspector
- Train or bus ticket inspector

There were multiple transport operating companies and buying one ticket that used multiple systems was not always possible or resulted in a complex fare calculation. The ticket would be purchased at a physical ticket office and displayed to a ticket inspector in order to gain access to the train platforms. Once on the train the ticket might need to be checked by additional inspectors and finally to leave the destination platform the

ticket would once again be checked by an inspector. Clearly from a fraud control perspective a lot of faith was put into the appearance of the ticket and the visual inspection processes. Considering the examples in Figure 1, it is perhaps surprising to see how simple some tickets were.

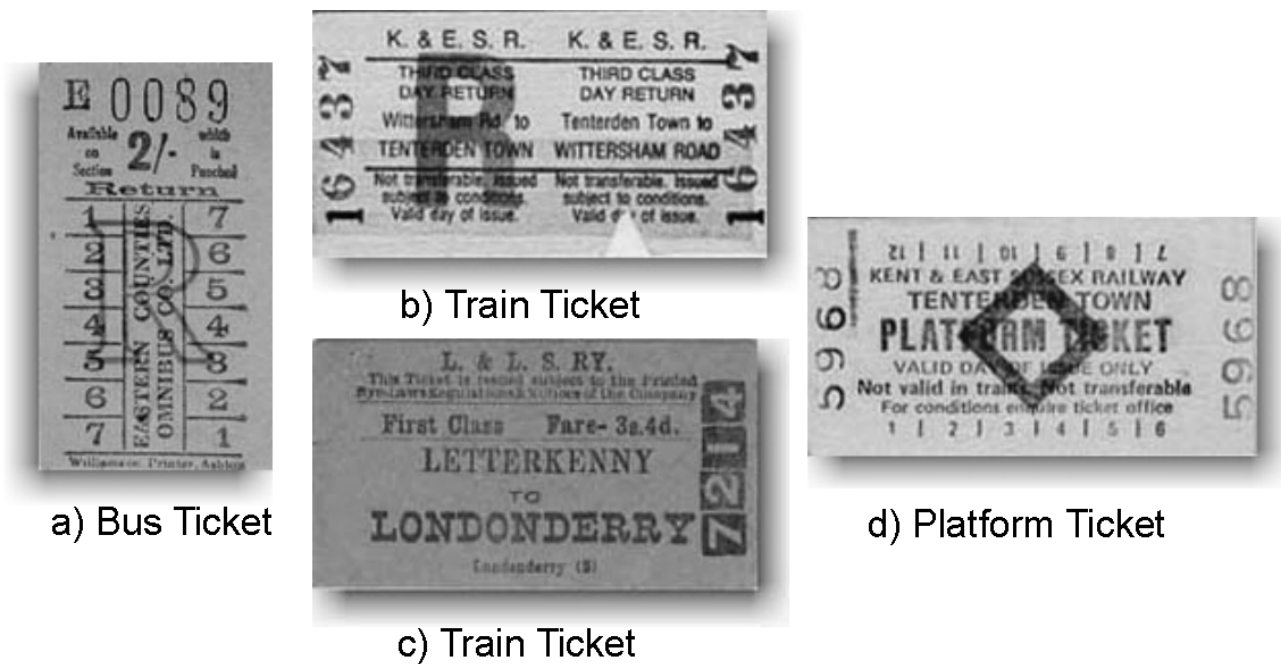


Figure 1: Old-Style Transport Tickets (courtesy Transport Ticket Society 2009 [1])

Inspection of a ticket often involved “punching” holes of various shapes to record a history of usage and verification. In Figure 1a the bus ticket is a little more sophisticated as it can also be punched in various positions. The third class return train ticket in Figure 1b was only valid for the day of issue and has been used as evident from the triangular punch. By contrast Figure 1c was a first class single, with no obvious mention of validity date and it was either not used or used but not punched. Figure 1d is included as an example of a ticket that allowed for station platform access only, with no permission to actually travel.

Considering Figure 1 as a whole, we can see that even if we assume very basic printing processes it would not have been too difficult to have created counterfeit tickets. However the real problem was fare evasion. We mentioned that great faith was placed not only in the tickets, but also in inspection. Manual/human inspection (even when efficient) takes time, which inhibits the flow of passengers into and out of stations, which not only causes queues and inconvenience, but is also error-prone and potentially dangerous. Busy stations may deal with enormous numbers of passengers and it is simply not practical and cost-efficient to employ large teams of inspectors simply to control station access and so many stations became “open” with more reliance on inspection during travel. We will consider how this development presented non-technical fraud opportunities.

3 Non-Technical Ticket Fraud

Transport ticket systems were available long before the introduction of electronics and computers, although they are relatively young compared to criminality. It is therefore no surprise that people have sought to commit fraud relating to transport and the fundamental goals have not changed much over the years i.e. travel without a ticket or the wrong ticket. To appreciate the scale of this, Transport for London estimated that abuses of its old paper ticket system (phased out almost a decade ago) resulted in losses on London Underground and busses of £10s of millions per year [2]. Some example strategies that used to be adopted by fraudsters are listed in Table 1.

Table 1 Non-Technical Fraud Strategies

	Travel without a ticket.	Travel with a ticket that is valid, but not for the intended journey.
Entry to Departure Station/Platform	1) Open station/lack of inspection.	7) If station/platform control in place, buy lowest cost ticket for entry to the chosen train/platform.
Inspection during travel	2) Luck or avoidance of inspector.	8) Journey ticket still valid when checked or avoid inspector.
	3) Claim departure station closer to destination (buy minimal journey ticket if discovered).	9) Buy minimal additional journey ticket if discovered.
Exit from destination station/platform	4) Open-station lack of inspection.	10) Open-station or ticket valid for arrival.
	5) If inspections then may avoid checks within crowds.	11) "Waved" ticket may be convincing in crowds
	6) Buy minimal journey ticket if discovered.	12) Buy minimal additional journey ticket if discovered.

Some of these exploits can be deterred by punitive fares e.g. a traveller must pay the maximum fare if found travelling without a ticket, but this risks alienating honest customers who may have had genuine difficulties with ticket purchase facilities. Figure 2 shows the number of exploits (from Table 1) that could be addressed by punitive fares.

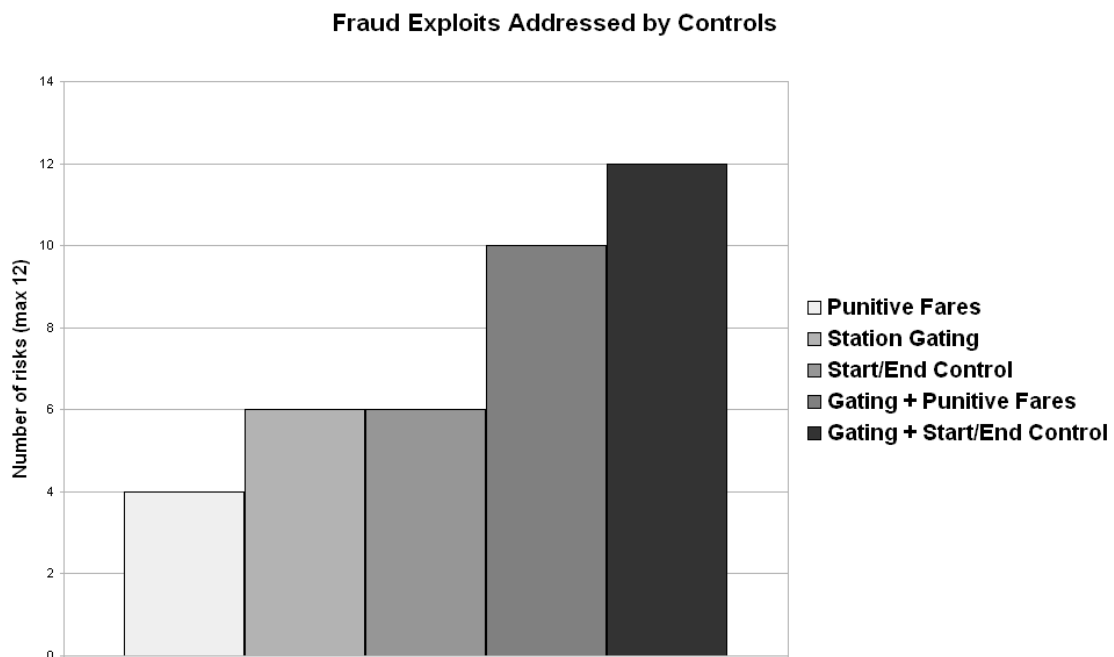


Figure 2: The Relevance of Controls to Non-Technical Fraud Exploits

Figure 2 also shows the significant impact of finding an effective solution to the station control/gating problem. In fact the combination of punitive fares and gating covers many of the exploits, but there is still reliance on inspection during travel and potential resistance from customers. An improved solution is indicated by the last column of Figure 2, in which gating is combined with the potential for checking the start and end of individual journeys thus leading to a requirement for machine readable tickets.

4 The Introduction of Machine Readable and Electronic Tickets

An important point to note from the foregoing discussions is that from a fraud control perspective, a major goal of introducing machine readable tickets was to improve revenue collection by means of rapid automated ticket checking, allowing gated stations to become a safe and practical reality. Thus improving the security of the “ticket” was not therefore the main driver; although it has of course becoming increasingly relevant.

The first machine readable tickets for transport appeared in the 1980s and were based on paper/card printed ticket, with a magnetic stripe on the rear. The data storage capability of the stripe was very limited and the contents could be easily copied, however the important point was that it was machine readable (e.g. via a reader in a station gate or barrier) and not that it was more secure than the paper ticket. Although magnetic stripe cards remained in use on credit cards for a long time (and with major fraud problems) the ticket security was fundamentally weaker as it was a one-factor authentication system (only something you have i.e. the ticket). In comparison, credit card/ATM transactions were two-factor i.e. the card you have plus a signature or a Personal Identification Number (PIN). In fact even as technology has advanced this weakness has remained by virtue of the fast-flow nature of electronic-ticketing. You cannot have, for convenience and safety reasons, slow two-factor authentications at access gates. Another difference with respect to credit/ATM cards is that the transport system transactions are effectively off-line due to the speed and practicality of managing on-line centralised transactions for mass user systems. The use of reduced security with respect to a credit/ATM card was justified by the assumption that tickets were relatively low-value. This assumption no longer holds in all systems. However, magnetic stripe tickets remain in widespread use and it is recognised that added security and fraud control must be provided by the gated system infrastructure and back-office systems.

Returning to Table 1, we can see that by permitting gated infrastructure the magnetic stripe ticket has gone a long way towards reducing non-technical fraud on transport systems. However, the type of ticket is not normally re-usable or suitable for tracking the start/end of a journey; neither is it very reliable in operation. To overcome these problems and reduce the proliferation of complex travel products, we need cards with unique IDs and re-writable storage. This permits journey history to be recorded and monitored, tickets to be disabled if fraud is suspected, travel products to be written to the card and a purse credit value to be maintained for purchasing additional travel. By providing simple and or automated top-up of the purse value there is no need for a traveller to ever queue again to buy a ticket and the use of a proximity contactless smart card provides a faster, more convenient and reliable transaction experience. Fortunately these requirements could be met with the introduction of electronic tickets based on a computer chip within a plastic card and supporting a wireless interface. Whilst this all sounds very positive, so far we have only addressed non-technical fraud and unfortunately technical fraud did not lag far behind the introduction of electronic tickets.

Having established that machine readable/electronic transport ticketing was not originally driven by ticket security concerns or dominated by technology interests, it is now appropriate to address some technical fraud issues and particularly with respect to the MIFARE Classic product [3] that has been the target for attack and proven to be vulnerable. We will start by introducing some basic comparative ratings that we can then use to compare various tickets types and technologies that may be encountered in practice. The ratings are defined in Table 2 and represent a mixture of objective (linked to best practice) and subjective criteria resulting in coarse (Low, Medium or High) scores.

Table 2 Ticket Property Comparison Ratings

Type/Score	Low	Medium	High
Functionality	Basic ID or simple read-only and/or use-once ticket	Fixed functionality, read/write, or re-usable, multiple ticket products	Flexible functionality (e.g. microprocessor), re-usable read/write, multiple ticket products
Speed	Human verification process, or ticket must be inserted, or several seconds to process	Contact-less interface, one second plus for whole transaction	Contact-less interface, few hundreds of milliseconds for whole transaction
Algorithm Strength	Proprietary or weak/broken	N/A	e.g. AES or 2/3 Key DES
Key size (Symmetric)	Less than 80 bits (ECRYPT/NIST [8, 9] – smallest general purpose key)	80-127 bits	128 bits or more (ECRYPT/NIST [8, 9] – smallest general purpose long-term key)
Hardware security	No anti-tamper measures, or proven weak/broken	Vendor statement of tamper resistance	Independent certification
Clone/counterfeit resistance	Requires little skill (amateur) and resources	Requires moderate skill (engineer) and resources	Requires considerable skill (expert) and resources

Having introduced the system of ratings it is now possible to use it to compare some examples of ticket types that may be encountered in transport systems, as shown in Table 3.

Table 3 Comparison of Example Ticket Types

Ticket Type	Description	Interface	Functionality	Speed	Algorithm strength	Key-size (bits)	Hardware security	Resistance to copying/counterfeits
Legacy								
Paper	Simple printed paper/card	Visual	Low	Low	None	None	None	Low
Mag-Stripe	Printed ticket plus magnetic stripe	Visual + stripe reader	Low	Low/ Medium	None	None	None	Low
ID only	Chip card that just presents ID	Proximity RFID	Low	High	None	None	Low – only has to prevent ID reprogramming	Low/None
Memory Card	Chip card with unprotected memory	Proximity RFID	Medium	High	None	None	Low - may prevent ID reprogramming	Low/None
MIFARE Classic [3]	Chip card with memory secured by proprietary mechanisms	Proximity RFID	Medium	High	Low – was intended as Medium	Low 48	Low – poor random number generator and tamper resistance	Low – was intended as Medium/High
Current								
DESFire EV1 [4]	Multi-mode proprietary platform, with AES/DES	Proximity RFID	High	Medium	High AES 2K3DES	High 128 Medium 112	High (EAL4+ for AES)	High
Generic Micro-processor SmartMX [5]	True “smartcard”, tamper-resistant micro-processor plus security applet	Proximity RFID	High	Low/ Medium	High (if best practice design)	High (if best practice design)	High (some platform/ applications are common criteria evaluated)	High

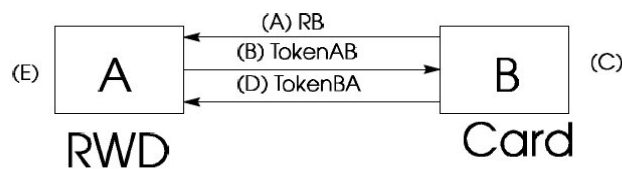
5 The MIFARE Classic

Although it has become much maligned (and did not compare well in Table 3) the MIFARE Classic [3] was in its “day” an innovative and successful product, supporting both the functionality and speed demanded for ticketing applications as well as the convenience of the contactless/RFID proximity interface, at an attractive price point. The implemented security measures have proved to be the Achilles heel, however the MIFARE Classic did at least have a security algorithm (CRYPTO1), keys and mutual authentication protocols, whereas some ticket products had virtually no security protection.

5.1 Basic Security Issues

The MIFARE Classic and indeed modern ticket solutions should satisfy some basic security requirements.

- The ticket/card needs to prove to the reader (perhaps at a station gate) that it is genuine. Likewise, the reader needs to prove to the card that it is a genuine reader. This process is called *mutual authentication*, and the goal is that both the reader and the card are convinced they are to start information exchange with a genuine peer.
- It is desirable that all information exchanged between the card and the reader is protected against unauthorised eavesdropping and modification (potentially malicious).



The tokens are structured as follows:

$$Token_{AB} = e_{K_{AB}}(R_A \parallel R_B \parallel B \parallel Text2).$$

$$Token_{BA} = e_{K_{AB}}(R_B \parallel R_A \parallel Text4).$$

Figure 3: Example Mutual Authentication Process [6]

To do this the card and reader need a cryptographic algorithm and at least one shared secret key. It is conceivable to use an asymmetric algorithm, but so far the implementations have proved too slow for widespread transport ticket usage. An example mutual authentication process is provided in ISO 9798-2 [6] and reproduced in Figure 2. The main steps of the protocol are as follows (assuming the card ID is already known);

Pass 1:

- Card B generates and sends a random number (R_B) to the reader

Pass 2:

- Reader A generates its own random number (R_A) and computes $Token_{AB}$ (using the secret key shared with the card ($e_{K_{AB}}$)), which it then sends to the card
- the card decrypts $Token_{AB}$ and by checking R_B (and the optional fields B and TextX) can infer that the token came from a legitimate reader i.e. one possessing the shared key

Pass 3:

- The card computes $Token_{BA}$ and sends to the reader
- The reader decrypts $Token_{BA}$ and by checking R_A (and potentially the optional fields) infers that it came from the legitimate card i.e. one possessing the shared key.

The exchanged random numbers can then be used to help create a session key sequence to protect the confidentiality of the exchanged messages.

The MIFARE Classic approximates to this approach, but according to recent publications is vulnerable in a number of areas; notably:

- The algorithm must be kept secret
- The key-size is small
- The random number generation is flawed
- Reliance on a simple stream cipher

5.1.1 *Secrecy of Algorithm*

A well-known cryptography principle attributed to the 19th century Dutch cryptographer Auguste Kerckhoffs [7], states that a cryptosystem should not rely on the secrecy of the algorithm for its security. Design secrets are accepted as a cause of fragility in cryptosystems, often leading to dramatic failure once design information is leaked or reverse engineered. There is a very apt comment attributed to Bruce Schneier.

“...every secret creates a potential failure point. Secrecy, in other words, is a prime cause of brittleness—and therefore something likely to make a system prone to catastrophic collapse. Conversely, openness provides ductility.”

Proprietary closed designs generally suffer from very restricted expert review and so structural weaknesses are more likely to be present than in a design evaluated by the wider expert community.

5.1.2 *Small key-size*

If an algorithm is well designed then an attacker must try to guess the key (from all possible keys) until the correct one is found. This is a form of attack that is applicable to all ciphers and it is known as *exhaustive key search* (or *brute force*) attack. The designer then has to ensure that the number of possible keys is so large, that it would be impractical for even a well equipped adversary to recover a secret key via exhaustive search. However The MIFARE Classic keys are only 48 bits in length which falls well short of international recommendations ECRYPT/NIST [8, 9]. By comparison, the Data Encryption Standard (DES) [10] is now considered obsolete (in favour of AES [11]) and a relatively low-cost exhaustive search attack was practically demonstrated [12] that could reveal its 56-bit key. We note that there are 256 times more DES key possibilities than there are CRYPTO1 keys and so it is not unreasonable to assume that an exhaustive key search against the CRYPTO1 algorithm is quite practical. The only (and very weak) protection against this was to keep the algorithm design secret so that it could not be implemented in fast FPGA key-cracker machines [13].

5.1.3 *Random numbers*

As can be seen from Figure 2 the mutual authentication is dependent on the quality of random number generation. However in the MIFARE Classic the random number generation can be predicted and controlled, compromising not only the authentication, but any session keys derived from it.

5.1.4 Simple Stream Cipher

Regardless of the algorithm and key-size used, if this results in a keystream that is simply XORed with the datastream then the solution is vulnerable to active relay [14] man-in-the-middle attacks.

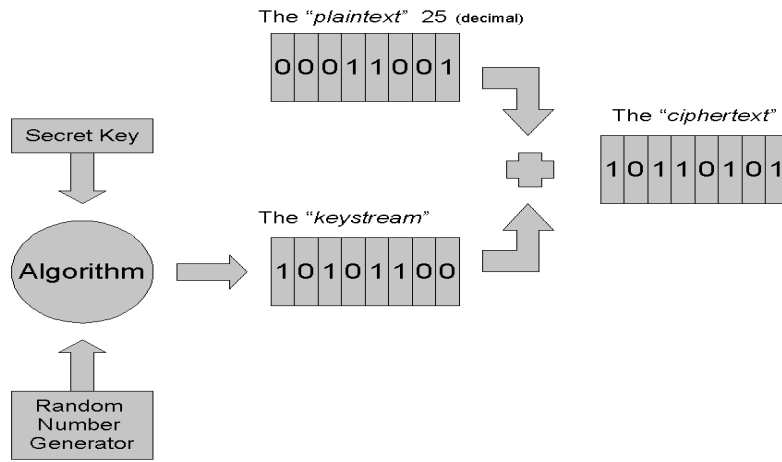


Figure 4: Simple Stream Cipher Example

By way of illustration, if the bits in the ciphertext of Figure 4 are modified there will be a corresponding change to the decoded plaintext. We can see how this could be exploited by considering an example in which the attacker has paid for £25 to be loaded onto his card; but wants the card to believe that £100 has been loaded. The attacker intercepts the message from the reader containing the ciphertext and XORs it with 01111101 (so it becomes 11001000), before forwarding the message. The decoded plaintext will then become 01100100, representing the desired load value of £100. Whilst the integrity of the plaintext may be verified by a CRC or parity bits, the attacker could also modify the CRC/parity using the same method.

5.2 Published Work

Because of the proprietary and secret nature of its design and the known small key-size, the MIFARE Classic had for some years been regarded with scepticism by security professionals, although its low cost, widespread use and lack of detected fraud or security exploits maintained its position within the transport ticket business. Opinion towards the product deteriorated rapidly following a technical presentation at the Computer Chaos Club conference towards the end of 2007; during which Nohl and Plotz [15] described their work on reverse engineering of CRYPTO1. This work was later published at the USENIX Security Symposium [16]. This inevitably led to full publication of the algorithm; however it was almost certainly not the first time that the algorithm design had been reverse-engineered or acquired by other means. For example, products are advertised by some Chinese companies that appear to mimic the functionality of the MIFARE Classic and in examination of product data sheets, it was found that at least one dated back to 2004.

The publications by Nohl et al acted as a catalyst for the Radboud University in Nijmegen who set about identifying and exposing the extent of the MIFARE Classic weaknesses. A publication at the CARDIS 2008 conference from Koning Gans et al [17] focussed on a key stream attack; exploiting the combined weaknesses of random number/nonce generation and stream ciphering. It required recording of a genuine authentication and then arranging for the original nonce to be repeated so that a recorded message could be replayed to complete a rogue authentication; after which other messages could be replayed or modified (not unlike the example of Figure 4). This attack which has similarities with other replay/relay exploits [14] relied on knowledge of some plaintext, however this was not unreasonable as aside from some manufacturer fixed data the data contents of some transaction types could be quite predictable. *The important characteristic of such attacks is that they are effective and yet do not require knowledge of the algorithm or the secret key.*

However, the definitive paper on the MIFARE Classic is from Garcia et al [18] and was presented at ESORICS in 2008. The paper published (despite legal opposition) the CRYPTO1 algorithm and developed several practical attacks based on analysis of the Linear Feedback Shift Register (LFSR) at the core of the algorithm; again exploiting the poor random number generation. Two attacks are described in detail; the first recovers the state of the LFSR by observing that it is directly affected by the nonce value and using a combination of multiple authentications with a genuine reader and pre-computation tables. In cryptanalysis terms this attack is quite feasible in terms of memory (1 terabyte) and the number of required authentication attempts (4096); but it does require considerable time to be spent at a genuine reader (2-14 minutes) which could render it impractical from a fraud perspective. More powerful is the second attack that exploits the invertibility of the algorithm filter function. The detailed explanation of this is beyond the scope of this paper; however the result is that initially only a single authentication session is needed for analysis that yields 65536 key candidates that can be then be checked against a further authentication session. This is most definitely a practical attack that is well within the processing and memory capabilities of ordinary computing equipment and does not require a lengthy stay at a genuine reader.

The ESORICS paper also mentions that the second authentication is different to the first, in a multi-sector authentication sequence i.e. the second tag nonce is encrypted with the key protecting the second sector. This almost casual statement is an important finding as it means that a tag will reveal key information (albeit combined with a nonce) instead of just a nonce. Furthermore as the paper describes methods to quickly determine the nonce, the revealed key information can then be recovered. This opens the door to attacks on genuine cards without the need to eavesdrop valid transactions or query genuine readers. This topic is expanded on in a later paper [19]. The attack assumes that at least one key is known a priori for the card, which could arise due to an Issuer's policy rather than card design fault. The Issuer best-practice would be to properly diversify keys between cards and between application sectors to avoid global (or predictable) keys. However there is always a chance of spare, common of "future-use" sectors that are left with default keys (as they protect nothing of interest) that could be used for the first authentication. There will no doubt be other papers describing MIFARE Classic attacks, but the important work seems already to have been completed.

5.3 Fraud Impact

Returning to the core theme of transport systems we should not assume that the MIFARE Classic security attacks will instantly translate into large scale fraud as there are a number of factors (technical and non-technical) that could help compensate for the problem.

Non-Technical:

- Most people are generally honest and would not risk a criminal record.
- There is little temptation when the gain from fraud is small with respect to the effort/risk.
- Experiences from paper ticket systems and conventional policing operations are applicable to counter organised fraud.

Technical/Process:

- The cards/tickets present an ID during a transaction with a reader and this can be monitored and blocked by back office systems if fraud is suspected.
- Back office systems can monitor and reconcile payments for travel with actual travel usage and block suspicious cards.
- Ticket inspectors can verify card/tickets and check stored travel history.

This is not to suggest that these measures are foolproof, but it shifts fraud towards higher-value products and increases the sophistication and skill level for the attack techniques that underpin the fraud exploits. It is of course far better to have protection from a fit-for-purpose security solution and transport system operators would be well advised to plan the eventual phasing out of the MIFARE Classic.

6 Lessons Learned and Where Next?

From the fore-going discussions it should be clear that there were strong drivers for the introduction of electronically readable transport tickets and that improving the security and authenticity of the ticket was not the primary reason. However reliance on electronic systems for the purchase and use of services puts added emphasis on information security and cryptographic algorithms, protocols and implementations. Transport ticket solutions must support the required functionality, have the performance to support fast-flow operation and be cost-effective/affordable, while also providing sufficient security protection to reasonably protect the associated data and value. Within limits, if the cost of the protection is greater than the lost revenue and the cost of investigating fraud then it is an option to simply tolerate the losses. However such situations can escalate rapidly and so transport operators take a risk with this approach and must at least be very fast to react and introduce new technology as the fraud situation deteriorates.

An ill-considered move from one technology to another risks replacing one set of problems with another, although recent problems have given increased awareness of security issues within the transport industry. The main problems with the MIFARE Classic stem from the fact that the algorithm, key-size, protocol and product design were not widely reviewed and indeed this was largely prevented by the proprietary and secret nature of the product. How much better it could have been given the limitations of its age and price range will never be known for sure. The main lesson is that algorithms should be based on widely reviewed designs, using best-practice key sizes and the overall product should be evaluated to a reasonable extent to demonstrate that its operation and security protection are fit-for-purpose.

Better still would be to break the linkage between the card platform/hardware and the transport application thus permitting their separate evolution and evaluation. This is best suited to smart cards (secured microcontroller chips/cards) and also helps remove dependence on proprietary solutions and permits multiple “chip” platforms for continuity of supply, tolerance to product faults and commercial benefit. Another advantage is that the application can be specific to a particular transport operator, without unnecessary (and potentially vulnerable) functionality bundled into an off-the-shelf proprietary product. This approach could also be used to provide standardisation of algorithm interfaces rather than the algorithms themselves. This strategy is used in the mobile communications industry and permits the use of both open and proprietary algorithms depending on the operator requirements.

In fact the emphasis should not be on one solution for ever, but evolution and co-existence of multiple solutions. If this stage is reached we could imagine a range of card/tickets being presented to a station gate reader to authorise travel. These are not necessarily cards from the transport industry, but could be bank cards, phones, passports etc. Whilst there are practical issues to overcome the recent “touch & pay” products [20] [21] based on EMV [22] cards have a lot in common with transport tickets i.e. having a proximity/RFID interface, single factor, fast-flow for low-ish value purchases.

7 Concluding Remarks

The transport ticket has been around for a long time and so too have associated problems with fraud and revenue collection. These problems were originally non-technical in nature and handled by non-technical, but human resource intensive measures. Advances in technology meant that stations could be gated (when appropriate) on entry and exit with rapid automatic ticket reading for the fast-flow needed to safely and conveniently deal with crowds of travellers. Furthermore the availability of re-usable electronic tickets meant that customers did not need to queue for ticket purchase and had less justification for not having a valid ticket for travel. These measures were effective against non-technical fraud, but being based on technology they introduced the topic of technical fraud. The deployed systems were very cost sensitive and so balanced to match the perceived threats and discourage attacks on the system, rather than establish a very high standard

of security. However, the intended level of security is not always present as evident from recent publications relating to the widely used MIFARE Classic. The design and implementation of the product has proven to be completely flawed such that just about any exploit is possible including card counterfeiting/cloning. This does not necessarily imply that there will be an upsurge in transport ticket fraud as this is affected by some non-technical issues and motivational aspects as well as the effectiveness of back-office systems and security processes. It should also be appreciated that transport operators have a lot of effective experience from combating fraud from paper tickets; where there are only limited anti-counterfeit measures. However, fraud from security breaches can escalate rapidly and so transport operators are advised to improve their ticket solutions. It is important that choosing the new solution does not just duplicate the old problems. In particular the use of proprietary algorithms should be avoided and new products should only be considered if they have been made available for independent evaluation. A more open and standardised approach is recommended as in the future transport systems may need to accommodate a range of cards, devices and protocols; such as EMV bank cards and NFC phones. The banking industry in particular could provide sophisticated controls and experience to combat fraud and security attacks on smart card systems and potentially make the deployment of transport-only cards/tickets obsolete and unnecessary.

References

- [1] The Transport Ticket Society, <http://www.transport-ticket.org.uk>
- [2] B. Dobson, "Transport for London Oyster Card", ISG-Smart Card Centre MSc Lecture notes, Royal Holloway University of London 2009.
- [3] Philips Semiconductors, MIFARE Standard Card IC MF1 IC S50 Functional Specification, revision 4.0 1998
- [4] NXP, MF3ICD8101 MIFARE DESFire contactless multi-application IC short data sheet, revision 1.0 2007
- [5] NXP, SmartMX Platform features, Revision 1.0 Short form Specification, 2004
http://www.nxp.com/acrobat_download/other/identification/095710.pdf
- [6] International Standard Organisation, (1999) "ISO/IEC 9798-2, Information technology - Security Techniques- Entity Authentication - Part 2: Mechanisms using a symmetric encipherment algorithms", <http://www.iso.org>
- [7] Auguste Kerckhoffs, "La cryptographie militaire", *Journal des sciences militaires*, vol. IX, pp. 5–83, Jan. 1883, pp. 161–191, Feb. 1883
- [8] ECRYPT. key-length recommendations <http://www.keylength.com/en/3/>
- [9] NIST, key-length recommendations <http://www.keylength.com/en/4/>
- [10] Federal Information processing Standards, Data Encryption Standard (DES), FIPS publication 46-3
<http://csrc.nist.gov/publications/fips/fips46-3/fips46-3.pdf>
- [11] Federal Information processing Standards, Advanced Encryption Standard (AES), FIPS publication 197. <http://csrc.nist.gov/publications/fips/fips197/fips-197.pdf>
- [12] Kumar Sandeep et al, "How to break DES for €8,980", CHES 2006, <http://www.crypto.ruhr-uni-bochum.de>
- [13] Jan Petzl (2006), "Cryptanalysis with a low cost FPGA Cluster", IPAM Workshop Special Purpose Hardware for Cryptography http://www.copacobana.org/paper/IPAM2006_slides.pdf
- [14] Gerhard Hancke (2005), "A Practical Relay Attack on ISO 14443 Proximity Cards", Project Report, University of Cambridge Computer Laboratory, <http://www.rfidblog.org.uk/hancke-rfidrelay.pdf>
- [15] K. Nohl, H. Plotz, Little Security Despite Obscurity, presentation on the 24th Congress of the Chaos Computer Club in Berlin (Dec 2007)
- [16] K. Nohl, D. Evans, H. Plotz, Reverse -Engineering a Cryptographic RFID Tag, USENIX Security Symposium, San Jose CA (July 2008)
- [17] G. De Koning-Gans, J.H. Hoepman, F.D. Garcia, A Practical Attack on the MIFARE Classic, proceedings of CARDIS2008, LNCS 5189 (Springer 2008)
- [18] F.D. Garcia et al, Dismantling MIFARE Classic, ESORICS 2008, LNCS5283 (Springer 2008)

- [19] F.D. Garcia et al, Wirelessly Pickpocketing a MIFARE Classic Card, (to appear in IEEE Symposium on Security and Privacy 2009)
- [20] Barclaycard “OnePulse”, <http://www.barclaycard-onepulse.co.uk/cardDetail.html>
- [21] Mastercard, “PayPass”, <http://www.paypass.com>
- [22] EMV Books 1-4 Version 4.1 2004, <http://www.emvco.com/specifications>

Biographies

Keith Mayes is the Director of the Information Security Group Smart Card Centre at Royal Holloway, University of London. His current interests are smart card/RFID/NFC security, protocols and applications; mobile communications systems; transportation systems security and risk assessment. More information can be obtained from <http://www.scc.rhul.ac.uk/people.php>

Konstantinos Markantonakis is a Reader in the Information Security Group at Royal Holloway University of London. His main research interests include smart card security and applications; secure cryptographic protocol design, Public Key Infrastructures, key management, mobile phone security. More information can be obtained from <http://www.scc.rhul.ac.uk/people.php>

Gerhard Hancke is a researcher with the Smart Card Centre, which forms part of the Information Security Group at Royal Holloway University of London. His main interests are proximity identification and the security of RFID/contactless systems. Other interests include pervasive computing and sensor networks.