Practical Attacks on Proximity Identification Systems (Short Paper)

Gerhard P. Hancke
University of Cambridge, Computer Laboratory
15 JJ Thomson Avenue, Cambridge CB3 0FD, UK
gh275@cl.cam.ac.uk

Abstract

The number of RFID devices used in everyday life has increased, along with concerns about their security and user privacy. This paper describes our initial findings on practical attacks that we implemented against 'proximity' (ISO 14443 A) type RFID tokens. Focusing mainly on the RF communication interface we discuss the results and implementation of eavesdropping, unauthorized scanning and relay attacks. Although most of these attack scenarios are regularly mentioned in literature little technical details have been published previously. We also present a short overview of mechanisms currently available to prevent these attacks[1].

1. Introduction

RFID devices are used for logistics, access control, cashless payment systems and even travel documents [11, 21, 22]. No physical contact needs to be made with the reader, which simplifies operation and increases transaction speeds. This lack of human interaction has however led to fears that this technology could be abused and as a result most RFID discussions have centered around privacy concerns. Consumer groups claim that information about the user could be acquired without consent, and therefore rallied against the "big brother" potential of RFID technology. And as RFID devices are used for transactions of increasing value they also become the target of a lone attacker, who if able to read the device while in somebody's purse or wallet, might be able to engage in the act of digital theft while standing next to or walking past his victim. This has understandably driven research into RFID security. For a full academic overview it would be best to consult comprehensive sources on RFID security and privacy research [2, 16].

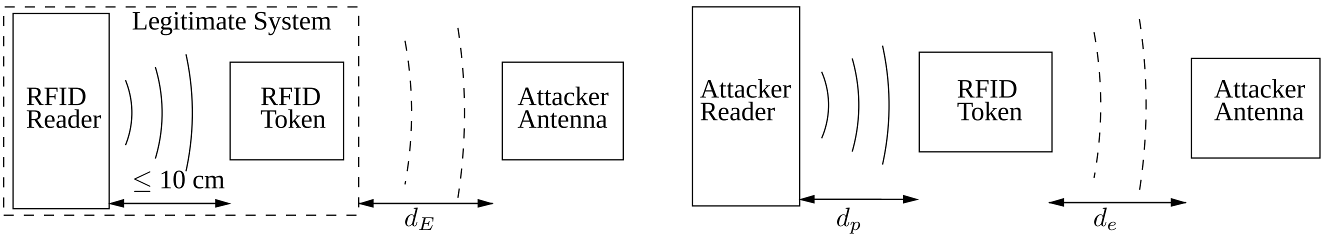
Even though several papers make claims about the possibilities of relay and eavesdropping attacks on RFID devices they don't always describe implementations or show results. Kfir and Wool [20] published the most relevant paper where they modeled a contactless smart card system and simulated the distances achievable for reader→token and token→reader communication in the context of a relay attack. As discussed in section 2, RFID is a general term for any near field communication device. A contactless smart card is not the same as a tag used in logistics so if somebody can read a razor's tag from 1 m it cannot be assumed that the same is true for an e-passport. Different scenarios also exist for eavesdropping, as discussed in section 3, and therefore the experimental setup should be known in order for the information to be useful. These factors also add to the confusion surrounding current reports about RFID eavesdropping. The American Civil Liberties Union (ACLU) demo, where a passport was read from 3 feet, used "similar" RFID technology to the real e-passport [1], and no further info was released after press reports that the US National Institute of Science and Technology (NIST) eavesdropped the RFIDs to be used in US passports from as far away as 30 feet [29].

This paper describes our implementation of practical eavesdropping and relay attacks against RFID devices. It should be mentioned beforehand that we did not aim to compete with a professional RF testing institution. We simply worked towards proof of concept and practical descriptions of attacks, as might be implemented by an attacker with some RF knowledge and finite resources. We present and discuss some preliminary unauthorized scanning and eavesdropping ranges achieved during our experimentation. These result are intended as a starting point for further research in this field, which would be helpful in determining an accurate threat model for RFID systems.

2. RFID Background

RFID is a collective term for near field communication devices and in reality refers to devices adhering to a number of different standards. In the HF band interfaces have been standardized for "proximity" (ISO 14443 [12]), "vicinity" (ISO 15693 [13]) and "near field" (NFCIP-1/ECMA340,

[1] Appears in the Proceedings of IEEE Symposium on Security and Privacy 2006, pp. 328–333, Oakland, USA, 21–24 May 2006.



(a) Passive eavesdropping. d_E is the distance from a token/reader pair, operating within specifications, to where an attacker can eavesdrop a two-way communication sequence .

(b) Active scanning. d_p is the distance at which the token can be powered from an attacking reader and d_e is the distance from the powered up token at which an attacker can eavesdrop a two-way communication sequence

Figure 1. Distances related to different eavesdropping attack methods

ISO 18092 [15]) devices, with maximum operating ranges in the order of 10 cm to 1 m. A further standard, ISO 18000 [14] defines possible communication interfaces for LF, HF, and UHF bands. The EPC Class-1 standard [6] is well known for UHF item management tags, which also operate at a much longer range. Our experiments were conducted in the HF band using tokens conforming to the ISO 14443 A standard, which is used by popular commercial products such as Philips Mifare (and is also one of the standards specified for e-passports [18]). It also corresponds closely to the “near field” standard so attacks could be extended to work in this environment.

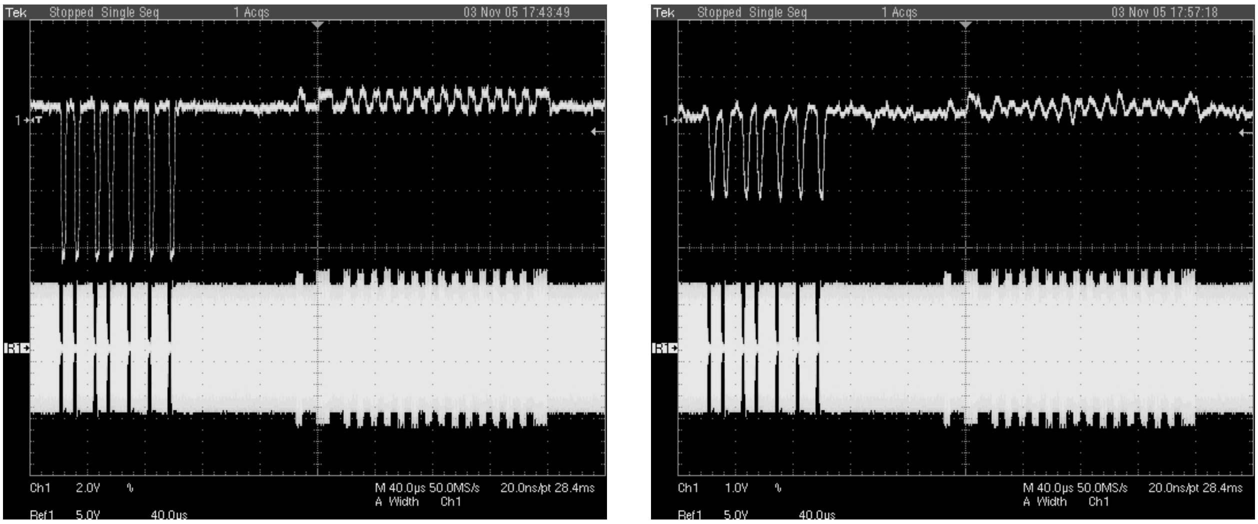
RFID tokens receive both data and power from the carrier transmitted by the reader. Within the HF band this is based on the principle of mutual inductance and coupling two coils via their magnetic field. In the ISO 14443 A standard the data from the reader to the token is modulated onto a 13.56 MHz carrier using 100% Amplitude Shift Keying (ASK). Modified Miller coding is used because the 3 μs pulses, where the carrier is absent, are short enough to allow the resonant circuit in the token to maintain the power level while also receiving data. The token’s response is Manchester coded and modulates a 847 kHz subcarrier, again using ASK, with the result then load modulated onto the main carrier. Load modulation varies the impedance of the token’s resonant circuit by switching additional resistive or capactive loads in time with the data stream, therefore achieving amplitude modulation of the reader’s carrier. The data rate for both reader→token and token→reader is 106 kbits/s [7]. An example of a communication exchange is shown as reference in Figure 2(a).

3. Eavesdropping

Some people see near field communication as secure because the specified communication range is small, $\leq$ 10 cm, with most commercial readers only operating at a range of 1 or 2 cm. Eavesdropping of signals is therefore an obvious attack in the RF environment. There are two main attacks to consider. Passive eavesdropping is the interception of communication between a legitimate reader and a token. Active eavesdropping, or scanning, involves a malicious reader that could try and access a token without its owner’s consent. In practice the attacker would have to provide power and communicate with the token over a longer distance than normally specified, as the owner might become suspicious of somebody in his personal space. The fact that an attacker is not bound by the same transmission limits [5] adhered to by industry designers makes this attack practical.

There are different distance parameters involved in eavesdropping experiments. Figure 1 gives an overview of these parameters. For active eavesdropping the first step is to activate the token and the second step is to retrieve the token’s response. We define d_p as the distance from which an attacker’s reader can activate the token by providing power and communicating information. We also define d_e, which is the distance at which the attacker can recover the token’s response. If the attacker only uses one antenna for active scanning d_p would equal d_e. We propose the scenario where two antennas are used, which allows for more flexibility. d_e is not limited by d_p and different types of antennas can be used for powering/transmitting and receiving. Consider a case where a simple loop antenna, which is efficient for generating the magnetic field (H) required for power transfer but ineffective for receiving, can be hidden close to the target token. A much larger and complicated antenna can then be placed further away for eavesdropping on the communication. For passive eavesdropping we define d_E as the distance, from the token, where the attacker can recover a two-way communication sequence between a reader and token. In effect this can be seen as a special case of active eavesdropping with d_p in the order of 2 cm.

To further complicate matters we must make a distinction between the eavesdropping range of reader→token ($d_{R\rightarrow T}$) and token→reader ($d_{T\rightarrow R}$) communication. The token→reader communication is very dependent on the mutual magnetic coupling and near-field characteristics of the system. The effect of the load modulation on the carrier



(a) $d_E = 110$ cm.

(b) $d_E = 400$ cm.

Figure 2. Data captured by passive eavesdropping (top) compared with a reference of the transmitted amplitude modulated data (bottom). In each picture the left hand side of the trace shows the reader→token communication, with token→reader shown on the right.

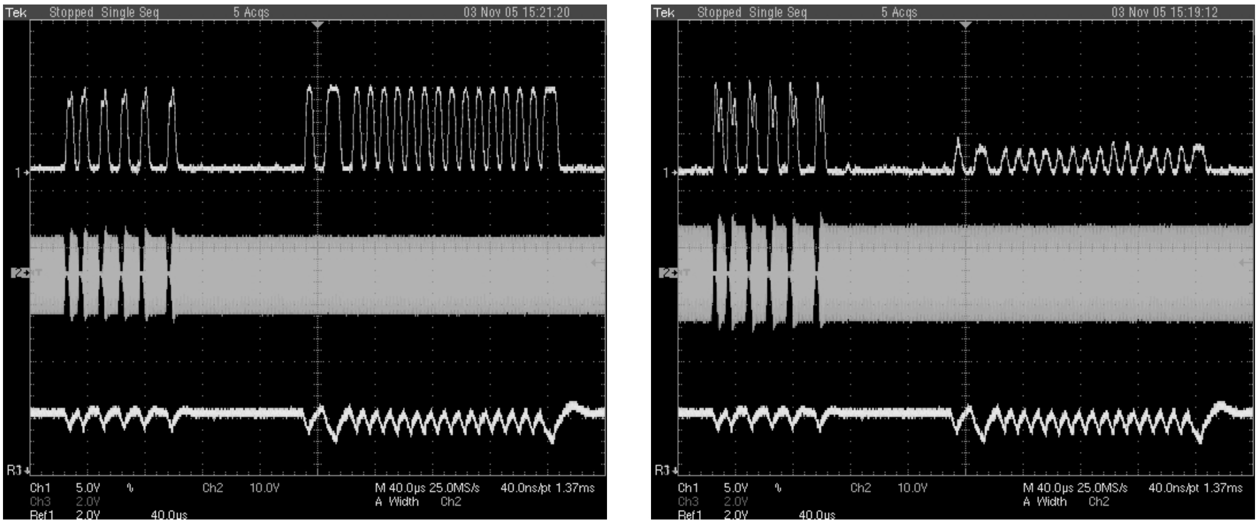
is also much smaller in amplitude when compared with the ASK modulation used for reader→tag communication. For our results we define that a successful eavesdropping attack recovers both reader→token and token→reader communication. d_E and d_e is therefore equal to the value of $d_{T\to R}$ in each case.

3.1. Passive Eavesdropping

For the attacker's antenna we used the Dynamic Sciences R-1250 Wide Range receiver with the R-1150-10A Portable Antenna Kit. The R-1250 is a superheterodyne receiver operating from 100 Hz – 1 GHz with selectable bandwidths from 50 Hz – 200 MHz. The antenna kit includes a set of H-field ferrite core antennas for field-strength measurements in the 100 Hz – 30 MHz range. Looking at the H-field is of particular interest when taking into account the magnetic nature of proximity devices. The wide range receiver allows users to quickly scan a range of frequencies looking for compromising transmissions. Once the frequency and bandwidth of the data is determined the receiver holds no real advantage over a simple amplitude demodulator so not every attacker needs one. We then continuously queried a Philips Mifare token using a commercial ISO 14443 A reader capable of reading a token from approximately 2 cm. The reader is build around the Philips MF RC530 contactless reader IC, which is capacitively coupled to a 60x45 mm loop antenna, and is implemented as shown in the relevant manufacturer's data sheets [24]. Figure 2(a) shows examples of recovered data for two different values of d_E. In Figure 2(a) the two-way communication is still clearly visible. The token's response in Figure 2(b) is much more noisy but the data sequence could still be recovered using a simple comparator with hysteresis. The token→reader communication became indistinguishable from the surrounding noise as d_E exceeded 400 cm even though the reader→token communication was still visible. Please note that the difference in trace magnitude between Figure 2(a) and Figure 2(b) does not accurately reflect signal degradation as the receiver's amplifier settings were readjusted at each distance to best recover the signal. Even though we can confirm that eavesdropping is possible up to 4 m our result is well short of the 9 m described in the NIST report and at this stage we cannot reject or support their claim. It is very feasible that the value of d_E could be increased with application specific antennas, more complex signal processing or simply running the experiments in an environment with less background RF noise.

3.2. Active Scanning

We created an attacking reader by amplifying the carrier and data signal from the reader, described in section 3.1, and transmitting it using larger loop antennas. For the attacker's antenna we used the same antennas and wide range receiver as we used for passive eavesdropping. We then experimented with different antennas sizes (A5, A4 and A3) and RF amplifiers (0.5 W, 1 W, 2 W and 4 W). Reference



(a) A5 antenna with 1 W amplifier, $d_p = 15$ cm and $d_e = 75$ cm.

(b) A5 antenna with 1 W amplifier, $d_p = 15$ cm and $d_e = 145$ cm.

Figure 3. Data captured through active eavesdropping (top), the reader's command (middle) and a reference token's response as seen by the pick-up coil (bottom)

designs, performance trade-offs and theoretical limits for these antennas and amplifiers are publicly available [26,27].

3.2.1 Reader to Token

We set up each antenna/amplifier combination and measured the maximum distance where we could activate a token. To test whether a token had been powered and received the data correctly we used a pick-up coil in close proximity to see if it generated the correct response. The results are shown in Table 1 and are as expected. d_p is proportional to the antenna radius/transmitted power. $d_{R \rightarrow T}$ is of no significance as the attacker is transmitting the reader→ token data.

	0.5 W	1 W	2 W	4 W
A5 (148x210 mm)	15 cm	16 cm	17 cm	19 cm
A4 (210x297 mm)	20 cm	23 cm	23 cm	25 cm
A3 (297x420 mm)	22 cm	25 cm	26 cm	27 cm

Table 1. d_p for each antenna/amplifier setup

3.2.2 Token to Attacker's Antenna

After activating the token the next step is to retrieve the token's response. The best result for d_e was obtained using the A5 antenna with the 1 W amplifier and is shown in Figure 3(b) along with a comparative measurement at roughly half the maximum distance. This was a surprising result as we expected the range to increase but we only achieved d_e = 50 cm using the same antenna with the 4 W amplifier and d_e = 135 cm using the same amplifier with the A4 antenna. This could be attributed to a number of factors. The amplitude of the load modulation was absolute and not proportional to the amplitude of the carrier signal. As the carrier is amplified the load modulation effect gets smaller relative to the entire signal. Essentially the modulation index is decreased each time the carrier is amplified and the SNR decreases accordingly. This was the same for tokens from different vendors with the same card-type form factor. The amplitude of the reflected load modulation decreased as d_p increased. Even though the token can be activated at the distances mentioned before it had to be moved closer to the loop antenna to create a sufficient effect in order to be eavesdropped. That negated the advantage of larger antenna/amplifier combinations. Analysing the spectrum of the transmitted signal from the reader showed some carrier leakage into the sidebands. When the carrier is amplified the receiver has difficulty isolating the sidebands and the input amplifiers saturate before the small data signals can be seen. In a specially design attacking reader care could be taken as to the spectral properties of the carrier signal which should allow for the recovery of smaller sideband signals, hence increasing d_p and d_e. The threat of this attack seems slightly diminished as d_p ended up quite small for the best case of d_e. That said, 15 cm is enough to execute an attack in a crowded area and easily allows reading of a card in somebody's pocket or bag.

4. Relay Attacks

This is any attack where information passes through the attacker's hardware on its route between the legitimate reader and the token and presents a practical example of the grand master chess problem. An attacker can use two transponders in order to relay the information that a reader and a token exchange during a cryptographic challenge-response protocol. A proxy-token device is placed near the real reader and a proxy-reader device is placed near the real token, possibly unknown to its holder. Information can therefore be forwarded over a great distance if a suitable communication medium is chosen between the proxy-token and proxy-reader. As a result, the reader will report that it has verified the presence of a remote token and provide access to the attacker.

We implemented a practical relay attack and achieved a relay distance of 50 m using a cheap FSK RF link [9]. The timing constraints were not as strict as defined in the standards, and allowed sufficient time to relay messages, even with the 20 μs delay our hardware introduced. The necessary hardware parts were easily obtainable and the cost of the whole system was well under \$100, with most of the cost being an OEM RFID reader. The system was then modified using a FPGA development board to implement an adjustable delay so that the maximum attacking window could be determined. It was possible to buffer and delay the data for a period of time on the condition that it was clocked out on the rising edge of the reader's clock. We systematically increased the delay and tested the system by reading the token's ID. At 750 μs the system still functioned as normal. Errors started occurring when the delay reached 1 ms and no data was read once the delay reached 5 ms. The allowed time delay might be dependent on the reader and its setup, so the experiment should be repeated with a few readers to get an accurate result. We also considered the possibility that an attacker could alter data before relaying it back to the reader. Using the same experimental system we successfully modified a token's ID response, which is unencrypted and only uses a byte wise XOR for integrity. This offers possibilities for further work on how this could effect older payments systems using stream ciphers with limited integrity checking.

5. Countermeasures

We briefly discuss how tokens are protected and to what extend the current mechanisms and card data can be compromised by the attacks mentioned in the previous sections. Passive eavesdropping could be negated by implementing confidentiality and privacy mechanisms while active scanning is prevented by authentication. Papers on RFID security concentrate on minimalist cryptography protocols for EPC type tags. Suggested authentication and privacy protocols use pseudonyms and hash locking [17,23]. Further protocols suggest modifying the anti-collision protocols [28] or providing blocking tags [19]. Few of these ideas are currently implemented with the EPC standard only specifying a 32-bit password and kill code option to prevent active scanning. ISO 14443 tokens generally provide stronger algorithms such as RSA, DES, AES with some vendors providing proprietary algorithms, e.g. Philips Crypto1. These tokens have a fixed Unique Identifier (UID) used for anti-collision that could be used to track a specific card and the subsequent Protocol and Parameter Selection (PPS) could provide more information about the origin/use of the card before security mechanisms are invoked. Some access control systems, despite the cryptographic capability of their tokens, simply use the UID for access control purposes in the same way as old style proximity cards and are therefore vulnerable to a simple replay attack. The International Civil Aviation Organization (ICAO) new password standard, using ISO 14443 tokens, only specifies mandatory "Passive Authentication" which only proves that the data is authentic. "Basic Access Control", which would provide confidentiality, is an optional feature and if not implemented would allow the attacker to eavesdrop the passport owner's personal information [18].

Relay attacks cannot easily be prevented by cryptographic protocols that operate at the application layer of an RFID protocol stack. An attacker executing a relay attack cannot avoid causing a delay in the system. Distance-bounding or secure-positioning protocols are therefore a possible defense. Brands and Chaum [4] described the first distance-bounding protocol based on timing the single-bit round-trip delay in a cryptographic challenge-response exchange in order to prevent relay attacks. Since then a number of protocols based on technology such as RF [3], Received Signal Strength (RSS) [8] and Ultrasound [25] have been proposed. These protocols are not ideal for RFID devices as some require excessive power and processing resources while little attention was paid to practical considerations such as noise and error correction. Kuhn et al. [10] proposed a new distance bounding protocol for RFID devices. Further research in this area might lead to protocols with sufficient resolution to prevent unauthorized readers from accessing tokens from outside a trusted boundary.

6. Conclusion

The RF communication interface of 'proximity' tokens are vulnerable to practical attacks. We showed that an eavesdropper can intercept a two-way communication sequence between a legitimate reader and token from 4 m and that it is also possible to scan a token's response from approximate 1.5 m aways after activating it from a distance of

15 cm using a magnetic loop antenna. We also showed how relay attacks can successfully spoof the location of authentication tokens and that the permissible system delay further provides an opportunity for attacks on the system's integrity by allowing enough time for the modification of legitimate communication sequences.

Currently these attacks are only at the proof of concept stage and it is likely that further work would yield better results, e.g. digital signal processing or specially designed receivers could all increase the eavesdropping range. Nevertheless the current implementations still present a credible threat as these are within the capabilities of an attacker with a limited budget and some RF/electronic knowledge. It would also be interesting to see similar results for tokens using standards other than ISO 14443 A, e.g. ISO 14443 B. We hope that the results we presented can serve as a starting point for more research into security aspects of RFID communication interfaces.

References

[1] ACLU's Barry Steinhardt RFID demonstration. http://blogs.pcworld.com/staffblog/archives/000609.html

[2] G. Avione. *Security and Privacy in RFID systems*. http://lasecwww.epfl.ch/˜gavoine/rfid/

[3] P. Bahl and V.N. Padmanabhan. *RADAR: an in-building RF-based user location and tracking system*, Proceedings Nineteenth Annual Joint Conference of the IEEE Computer and Communications Societies, pp 775–784, March 2000.

[4] S. Brands and D. Chaum. *Distance Bounding Protocols*, Advances in Cryptology EUROCYPT '93, Springer-Verlag LNCS 765, pp 344–359, May 1993.

[5] CEPT/ERC REC 70-03 relating to the use of short range devices. Annex 9: Inductive applications.

[6] EPC Class-1 Generation-2 UHF RFID Conformance Requirements Specification v. 1.0.2

[7] K. Finkenzeller, *RFID Handbook: Radio-frequency identification fundamentals and applications*, Wiley, 1999.

[8] K.P. Fishkin and S. Roy. *Enhancing RFID privacy via antenna energy analysis*, RFID Privacy Workshop, 2003.

[9] G.P. Hancke. *A practical relay attack on ISO 14443 proximity cards*. http://www.cl.cam.ac.uk/˜gh275/relay.pdf

[10] G.P. Hancke and M. G. Kuhn. *An RFID distance bounding protocol*, Proceedings IEEE/CreateNet SecureComm, pp 67 – 73, 2005.

[11] International Civil Aviation Organization (ICAO). Document 9303 Machine Readable Travel Documents (MRTD). Part I: Machine Readable Passports, 2005.

[12] ISO 14443. *Identification cards – Contactless integrated circuit cards – Proximity cards*.

[13] ISO 15693. *Identification cards – Contactless integrated circuit cards – Vicinity cards*.

[14] ISO 18000. *RFID for Item Management: Air Interface*.

[15] ISO 18092 (ECMA-340). *Information technology – Telecommunications and information exchange between systems – Near Field Communication – Interface and Protocol (NFCIP-1)*.

[16] A. Juels. *RFID Security and Privacy: A Research Survey*. http://www.rsasecurity.com/rsalabs/node.asp?id=2937

[17] A. Juels. *Minimalist cryptography for RFID tags*, International Conference on Security in Communication Networks, Springer-Verlag LNCS 2864, pp 107–123, 2003.

[18] A. Juels, D. Molnar and D. Wagner. *Security and Privacy Issues in E-passports*, Proceedings IEEE/CreateNet SecureComm, pp 74 – 88, 2005.

[19] A. Juels, R.L. Rivest and M. Szydlo. *The Blocker Tag: Selective Blocking of RFID Tags for Consumer Privacy*, Proceedings ACM Conference on Computer and Communications Security, pp 103–111, 2003.

[20] Z. Kfir and A. Wool. *Picking virtual pockets using relay attacks on contactless smartcard systems*. Proceedings IEEE/CreateNet SecureComm, pp 47–58, 2005.

[21] London Transport Oystercard. http://www.oystercard.com

[22] Mastercard PayPass.

[23] D. Molnar and D. Wagner. *Privacy and Security in Library RFID Issues, Practices, and Architectures*, Proceedings ACM Conference on Computer and Communications Security, pp 210–219, 2004. http://www.paypass.com/

[24] Philips Semicondcutor, Contactless Reader Components – Data Sheets and Application Notes. http://www.semiconductors.philips.com/products/identification/readers/contactless/

[25] N. Sastry, U. Shankar and D. Wagner. *Secure verification of location claims*, Proceedings ACM Workshop on Wireless Security, pp 1–10, September 2003.

[26] ST Microelectronics, *How to Extend the Operating Range of the CRX14 Contactless Coupler Chip*, Application Note AN1954, 2005.

[27] Texas Instruments, *HF Antenna Design Notes*, Technical Application Report 11-08-26-003, 2003.

[28] S.A. Weis, S.E. Sarma, R.L. Rivest and D.W. Engels. *Security and Privacy Aspects of Low-Cost Radio Frequency Identification Systems*, First International Conference on Security in Pervasive Computing, Springer-Verlag LNCS , pp 201–212, March 2003.

[29] J. Yoshida. *Tests reveal e-passport security flaw*. http://www.eetimes.com/showArticle.jhtml?articleID=45400010