2007

ePassport security under the microscope

Matthew Sirotich
University of Wollongong

ePassport security under the microscope

Abstract

This paper focuses on ePassport security which utilizes RFID chip technology. ePassports are increasingly being used by governments to enhance the border entry and exit process. The paper briefly describes the nature of RFID technology and its characteristics pertaining to different aspects of security. The approach taken in this study is two-fold: experimental in the first instance, followed by a proof of concept (POC). The experimental study uses metrics to draw conclusions pertaining to the security, safety and privacy viability of the ePassport. Conclusions drawn from the experimental work are used to inform a proof of concept (POC) which provides one possible solution to eradicate the current issues related to the existing ePassport implementation. The proposed ePassport system is then compared to the existing ePassport using the defined metrics to determine which system provides the end user with the most privacy and security. The basic premise for this study is that if new technology is instituted to increase state security, then it should not be plagued with problems which would only increase national security concerns.

Disciplines

Business | Social and Behavioral Sciences

Publication Details

Sirotich, M. (2007). ePassport security under the microscope. In K. Michael & M. G. Michael (Eds.), The Second Workshop on the Social Implications of National Security (pp. 257-280). Wollongong: University of Wollongong.

18

ePassport security under the microscope

Matthew Sirotich

Honours Candidate, School of Information Systems and Technology, University of Wollongong

Abstract

This paper focuses on ePassport security which utilizes RFID chip technology. ePassports are increasingly being used by governments to enhance the border entry and exit process. The paper briefly describes the nature of RFID technology and its characteristics pertaining to different aspects of security. The approach taken in this study is two-fold: experimental in the first instance, followed by a proof of concept (POC). The experimental study uses metrics to draw conclusions pertaining to the security, safety and privacy viability of the ePassport. Conclusions drawn from the experimental work are used to inform a proof of concept (POC) which provides one possible solution to eradicate the current issues related to the existing ePassport implementation. The proposed ePassport system is then compared to the existing ePassport using the defined metrics to determine which system provides the end user with the most privacy and security. The basic premise for this study is that if new technology is instituted to increase state security, then it should not be plagued with problems which would only increase national security concerns.

Keywords: ePassport, radio-frequency identification, security

1 Introduction

A radio frequency identification (RFID) tag is a "tiny, inexpensive chip that transmits a uniquely identifying number over a short distance to a reading device, and thereby permits rapid, automated tracking of objects" (Jules, 2005a p. 1). Fundamentally it is a device which responds to queries from readers with a unique identification (UID) number. This paper deals exclusively with passive tags which do not have their own power source and gain their power from reader interrogations. As the medium for interaction is radio waves, the tag must be relatively close to the reader because the intensity of the radio waves (and all other electromagnetic waves) obeys the inverse square law. This law states that as the distance increases, the intensity (I) decreases inversely by the square of the distance (d) (Centre, unknown).

I.e. $I = \frac{1}{d^2}$

Once a message has been transported from the reader to the tag via electromagnetic waves the tag will power itself through inductive conductance and reply with its UID and optional information such as a Universal Product Code or some predefined value. The reader will now capture this information and transmit it to a back-end system. When this information is received it will be processed and possibly shaped into structured queries (commands that search, alter etc a database) that may be used to update databases (Wamba, 2006).

RFID is a wireless technology and hence interactions are not necessarily observed meaning that there is the potential for transactions to occur in stealth. With attributes like this, security conerns regarding tracking and much more are coming into question (Want, 2004).

2 The cornerstones of security

Before this paper can proceed an understanding of what is implied by security must be defined. Security is the provision of confidentiality, integrity, and availability (Bishop, 2002).

- *Confidentiality* is the ability to keep a secret a secret, it is the provision to ensure your private effects remain under your control. Access control mechanisms help provide a user with confidentiality, such access control mechanisms are passwords, tokens, biometrics, cryptography etc.
- *Integrity* is the assurance that data is correct and not malformed, i.e. it represents wholly and truthfully the information it was intended to or originally documented to. Two techniques exist to provide integrity which are prevention (which ensure only authorized people edit data) and detection (the act of determining when data has been altered such as a chesksum).
- *Availability* is the assurance that the data is accessible by authorized parties at all times.

Cryptographic operations, data hashing and pseudo random number generation are normally used to provide this security. A typical example of data hashing is the MD5 scheme which "takes as input a message of arbitrary length and produces as output a 128-bit "fingerprint" or "message digest" of the input" (Abzug, 1991). In the RFID context it is however currently impossible (Brainard, 2004) for a passive tag to carry out these calculations as they do not have their own power source and gain their power from reader interrogations. As this is the case other techniques such as embedded checksums must be applied to these RFID tags to ensure their security.

3 RFID security approaches

Molnar et al (2005) take into consideration that the challenge is to provide privacy protection without raising tag production and running costs. With this in mind they developed the theory of privacy for RFID through *trusted* computing. This proof of concept explains that tags will be developed to be used with dedicated readers that contain a trusted platform module (TPM) which is also known as a trustworthy reader. This ensures that a tag's privacy is respected and hence data that is not meant to be read by the reader is not read. The threat model they define is that the reader can be compromised, but the TPM cannot as it is a tamper-resistant hardware module. The reader is split into 3 distinct portions, the:

- Reader Core – is the radio interface, basically an RFID reader as we know them today
- Policy Engine – software that controls reading to ensure it is preserving privacy
- Consumer Agent – enables users and organizations to interrogate the reader to ensure it is conforming to privacy standards (a monitoring tool).

When scanning of a tag is to occur, the policy engine receives a request for read secrets, this is then passed to the TPM which determines if the reader core is valid. If all checks are passed the data is given to the trusted root and the policy engine is executed (Molnar, 2005). Yet the authors seem to cast doubt over their own proof of concept. While they state that "these ideas could be implemented today," they go on to admit that "significant engineering challenges remain" before the product can be shipped" (Molnar, 2005, p. 3). Seeing as this implementation of a TPM is yet to be built and tested and a growing distain for trusted computing is evolving, it can be assumed that this technology is under scrutiny by community groups. Schoen (n.d.) is of the belief that *trusted computing* is not the answer as it delivers users new risks of anti-competitive and anti-consumer behaviour. Another risk is that manufacturers of trusted computing hardware may produce their products with 'defects' (Schoen, n.d.).

Another interesting security implementation for RFID tags that again places the trust in the hands of the reader is the technical proposal of Jules (2005) which

describes 'the privacy bit'. In this technical proposal a bit called the *privacy bit* is added to the tags memory which tells readers if the tag is in private or public mode. The theory relies solely on the readers being trustworthy and that restrictions are placed on the firmware or software to ensure the readers respect tag privacy (Jules, 2005a). As stated, this theory places the reliance of trust on the reader, what if rogue readers were used such as those described by Newitz (2006)? Researchers such as Westhues (2003) can devise their own readers, and it can be assumed that unscrupulous people creating their own readers will not ensure that their devices are respectful of tag privacy. Jules (2005) admits that the technology has not yet been released and also admits that standards bodies have not accepted the idea, however Jules is relying on developers to realize the problems of consumer privacy and maybe then his solution may have a chance (Jules, 2005a).

The *kill command* is another technical approach which finally puts the onus on the tag to be trustworthy. The tag has a built-in command such that when the tag is authenticated to a reader, the reader can send the kill command to the tag and the tag will self destruct rendering itself unusable. The issue however is that no confirmation is given to whether the command was successful or if the command even reached the reader. Karjoth et al. (2005) have presented a revised version where visual confirmation can be observed as the kill command is a manual process of removing a pull tab which is part of the antenna. When this tab is removed the tag can no longer send or receive messages, nor power itself and hence is rendered useless (Karjoth, 2005). While this option is attractive and appears to be the most viable and most secure, it does not suit many environments as the user may wish for the tag to operate for their own purposes. This kill command is however currently enabled on RFID tags in circulation and is the first of the listed security technologies to be used by consumers and businesses.

Finally blocker tags present a new perspective, instead of relying on encryption and trust, deception is used. This system allows a tag to generate a set of 2k UID's which floods the reader with responses and leave it up to the reader to determine which UID is the real one (Brainard, 2004). Whilst this approach is very promising and has been shown to work in field studies and does not require changes to current RFID systems, it can be categorised as malicious because the flooding process can be described as a Denial-of-Service (DOS) attack (Jules, 2005a).

4 Established RFID security issues

As shown in section 3 there are avenues that can be followed to secure RFID systems, however, each approach has its own respective limitations. This downside means that the RFID security technique is flawed, as RFID systems cannot provide any guarantees on confidentiality, integrity and availability as is explained below:

- Access is not always authenticated. Westhues's (2003) device enables him to read RFID tags in passing and gather the data off the tag.

- Integrity cannot always be preserved. Integrity is provided via detection and prevention. From the security approaches in section 3, it is obvious that none implement either of these,
- Availability can be compromised. As detailed by Jules (2005a) denial-of-service attacks can cause the reader to reset.

The major threats posed by RFID systems in humancentric applications are *tracking* (the act of following a tags movements based upon its UID response to interrogations) and *inventorying* (allowing a user to identify object(s) being carried by another person) (Jules, 2006). Whilst this threat seems to contradict the reason RFID tags exist (to track and find objects), in humancentric applications the user needs to have the ability to be anonymous. Inevitably these shortcomings result in personal security threats as people can be followed based upon the UID numbers emitted by their personal effects. More seriously alarming though, personal information can be edited and read by anyone with the technology and the know-how (Westhues, 2003).

5 RFID in ePassports and possible security attacks

An ePassport is just like an existing passport however it has an RFID tag inserted in it which essentially holds the same information that is stored on the biographical page of the passport.

> The same information as a passport's data page- passport holder's name, nationality, gender, date of birth, and a digitized photo. It will also store the passport number, issue date, expiration date, and type of passport (Department, 2005).

The RFID chip is simply a second data source which is used to verify the printed data on the passport and hence identify the bona-fide holder with increased confidence. The rationale behind the ePassport is to provide better protection against misuse and tampering, reduce identify fraud, enhance border protection and provide fast and efficient passport checks (Trade, n.d.). Civil libertarian groups especially however question the motivation for the rapid implementation of the ePassport.

To use an ePassport, a user opens their passport to the biographical page and presents it to the identification machine. This machine will read the specially prepared area called the *machine readable zone* (MRZ) which provides the identification machine with the 'key' to decrypt the public key (PKI) ciphertext which safeguards the data. Once this step is complete, a check occurs to ensure the data on the RFID matches the data on the passport's biographical page (Trade, n.d.; Launch of ePassport, 2005). The US state department has taken an experimental approach to proving the security of their ePassports (which follow the same ICACO design standards as Australia's), however how secure this system is has been kept a secret. Extensive testing has occurred however the department is not releasing their findings (Gonsalves, 2005).

The most deep-rooted problem with RFID passports is not to do with the technology itself, but the policies which govern the technology in the passport domain. Coffee (2006) explains that "[a] passport with a failed e-chip remains a valid travel document". The reason this must be emphasised is because RSA laboratories report that an RFID chip can be deactivated with nothing more than a microwave (Labratories, n.d.). Furthermore RFID's utilize the radio wave medium to communicate, hence any transmission can be observed by a rogue reader within the right range. Eavesdropping is a major security issue for RFID not just because it is hard to stop, but harder still to detect (Juels, 2005b). Whilst the government has employed Faraday cages into its ePassport design, it is not inconceivable that an ePassport could become even a fraction open when being carried in a bag or purse hence allowing it to become compromised (Lamb, 2006). On the successful capturing of a signal through eavesdropping, the perpetrator is given the options of:

1. using the signal in a replay attack: send the same signal again at a convenient time such as when posing as the victim (Answers.com, n.d.) or;
2. an offline attack: where the signal is taken and interrogated to possibly break the encryption etc (Chuvakin, 2004).

Moses (2006) has also documented claims by Laurie, which reveal that it is possible to skim peoples' information from their ePassport. This is contradictory to the statements made by the Department of Foreign Affairs and Trade spokeswoman that one canoe "compromise the security of Australia's ePassport.". The department states that there is no way to read the RFID tag without first obtaining the key which is printed in the machine readable zone on the biographical page of the passport. However this information is simply a mixture of the date of birth, expiry date of the passport and the passport number which Laurie explains can be determined through sources such as online airline bookings (Moses, 2006). Due to this evidence it is clear that another method must be constructed which allows this technology to provide privacy and security for its users.

A reader can be set to continuously scan for ePassports, when one of interest is found the user can follow the RF waves much like following an electronic beacon. Critics such as Munro (2007) believe that the new ePassport systems could be used to track a user quite simply if readers are placed in the right position. When considering Gonsalaves (2005) claims that the RFID tags in passports can actually be read from up to 30 feet, it is no wonder that conspiracy theories surrounding the potential for governments to track passport holders are on the increase. These notions are highlighted by the likes of Lamb (2006) who state that "[t]here's clearly something else that they [the government] have in mind here, and we believe that they want the ability to track people without their knowledge." These claims are continuously given more force when it is considered that the US government continued with the deployment of ePassports even after receiving 98% negative feedback from the public regarding the proposal (Lamb, 2006). Whilst these claims

are not supported by current technical evidence, they do carry some weight.

Finally, the ePassport places all of the user's personal information along with a digital photo onto an RFID chip. It is all there for the taking, in one *basket* and plans are in progress to use the same basket for even more. The ePassport was designed conforming to guidelines provided by the (International Civil Aviation Organisation (ICAO), one of the design aims for the ePassport is to "[provide] a path to the use of ePassports to facilitate biometric or e-commerce applications" (Kaliski, 2005). This increases the exposure of the ePassport and increases the risk of skimming and tracking. All in all it is just giving unscrupulous people more opportunities to steal your identity. All the user's information is in a single location (the RFID chip) for the taking. If someone does break into the chip they will have all the centrally stored personal information and the owner would not even know it. Whilst this theft of information could occur in a more clandestine fashion, simply by stealing the passport and copying the information from the biographical page, the difference is that someone may notice their passport physically missing, however they would never know if someone remotely had broken into their chip and stolen their data.

6 Assessment of RFID's in ePassports

Before a new, more secure implementation of an ePassport is possible, it is a necessity to first asses the current technology being utilised. The rationale behind these experiments is to create metrics by which to measure and assess security in RFID which can then be reflected in an ePassport system. Not only are these experiments paramount in assessing the current implementation of RFID tags in ePassports, they are also central in creating a revised implementation of the ePassport which will eliminate predecessor faults. The completion of each forthcoming experiment will culminate in a value which will be either 'breached' or 'resisted breach' as defined by the unit of measurement.

6.1 The Experiments

The following experiments were carried out with either Standard Apparatus 1 or Standard Apparatus 2.

6.1.1 Standard Apparatus 1

The apparatus used was a Motorola/Symbol XR400 RFID reader connected to 2 antennas configured in a non portal configuration. This system had an adjustable reading range of approximately 3 meters to 1 centimetre. The antennas were facing opposite directions and separated by a distance of 2 meters. The apparatus was configured to scan continuously for Class 0 and Gen2 tags. Whilst this system had an excellent read range, and was highly configurable with regards to scan frequencies, distances and types, it did not have the capabilities to read the actual data stored on the tag.

6.1.2 Standard Apparatus 2

The apparatus used was a BlackBay handheld RF scanner which was configured to scan for ISO, Milfare, I-code and other protocols. This scanner had an extremely limited range of less than 5 centimeters and hence was limited in its usefulness, however it did allow for the data in tags to be read and stored.

6.2 Experiment 1- Injection attack on RFID

Aim: To determine the possibility of malforming database queries to cause detrimental database functions.

Hypothesis: *Injection attacks* are malformed database queries which trick the database into doing something otherwise illegal. This could be actions such as editing a certain entry or dropping an entire table. This form of attack has occurred time and time again over the internet in which interactive forms retrieve user data (which may be malformed) and edit a central database according to the data retrieved (Buehrer, 2005; Orso, 2005). It is to be assumed then that injection attacks are possible for RFID systems as the only object changing in the two instances is the medium upon which information is delivered to the back-end system (http to wireless communications).

Method: The 'Standard Apparatus 2' was used to read a set of 3 RFID tags. The tags ID and data were as follows:

ID	**Data**
1111111111AAAAAAAAAAA1439	Item1
1111111111AAAAAAAAAAA1438	Item2;Drop Table Data_table;
1111111111AAAAAAAAAAA1440	Item3

An SQL server is constructed with a table named 'Data_table' consisting of a single column called data. This SQL server then interfaces with a simple program which extracts the data held in the 'docked' scanner and constructs SQL queries which insert the scanned data into the database such as "INSERT INTO Data_table VALUES("EXTRACTED DATA FROM SCANNER");".

Results: After the program updates the database with the first data element in the docked scanner the database reflects:

Data_table

data
Item1

After the second data element is processed, the database reflects: 'ERROR, NO SUCH TABLE'

After the third and final data element is processed, the database reflects: 'ERROR, NO SUCH TABLE'.

Security breach: Breached.

Conclusion: It has been shown that the malformed tag data deleted all items and the entire database. After the second tag was added an error was reported stating that the table specified 'Data_table' did not exist. This hence proves the hypothesis correct and it can be stated that an Injection attack can occur on a database system if the strings used to create the structured query are not parsed correctly.

6.3 Experiment 2- Blocking a reader

6.3.1 Part A - Faraday cage

Aim: To create a more secure Faraday cage in which to encase the ePassport to address the current Faraday cage faults found by Flexills (2006).

Hypothesis: Currently a Faraday cage exists in the cover of the ePassport but as Flexills (2006) pointed out, if the ePassport is thrown into a bag or purse and opens only slightly, it is possible to read the passport. To overcome this, a purse like design which is lined with a foil will alleviate the issues and prevent reads from occurring unless the passport is removed from the purse.

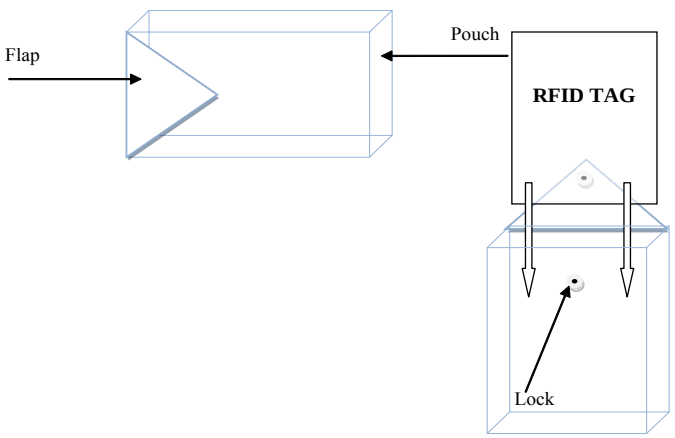


Figure 1- A Faraday Cage

Method: The Standard Apparatus 1 is used to firstly read a tag to create a control. Alfoil was then used to fashion the below pouch allowing enough space in the pouch to snugly fit the RFID tag.

Once complete the tag is placed into the pouch as shown and the flap locked into place. The Standard Apparatus 1 is then set to continuously scan for the tag. The flap is then opened and the scanning is allowed to continue. Finally remove the RFID tag completely from the pouch and ensure the tag can still be read.

Results: The control tag returns its tag ID when it is not encased in the pouch but when placed inside the pouch with the flap shut the tag ceases to respond

at all. Even when the flap is opened, the tag still does not respond. When the tag is completely removed from the pouch the tag can be read and replies with the correct tag ID.

Security Breach: Not applicable.

Conclusions: The new pouch enclosure design is by far a more secure method to house an ePassport. The experiment proves that the tag cannot be read when it is housed in the pouch, even if the flap is not secured. The current ePassport Faraday enclosure is susceptible to reads when the ePassport is partially open hence suggesting that the proposed enclosure will provide a higher degree of security.

6.3.2 Part B - External wave injection

Aim: To disrupt the reading of a tag for a short amount of time enabling a tag to pass by a reader unnoticed.

Hypothesis: An RFID tag uses radio waves as its transmission media, hence some device producing radio waves may disturb the transmission from the tag to the reader or visa versa (Australia, 2007). This phenomenon will prevent the tag from being read by a reader by either invoking destructive interference which degrades the message such that sense cannot be made from it, or abolishes the message all together. This occurrence will therefore enable the RFID tag to pass by the reader unnoticed.

Method: Apparatus 1 is set up along with a Sony Ericsson S700i (GSM with 900MHZ radio transmission). The Sony Ericsson is placed 5 cm behind a tag (class 0). The reader is then set to continuously scan the tag, which is hence read continuously. The phone is then set to initiate a phone call (emit a large amount of wave interference). The read rate is then assessed and then compared to the rate recorded when the phone call is terminated.

Results:

Condition	**Read rate**
Before phone is introduced to system	Approximately 1 read per second
Phone introduced, call not initiated	Approximately 1 read per second
Call initiated	0 reads per second

Security breach: Breached.

Conclusion: A large amount of wave injection into an RFID system can disrupt reader interrogations causing tags to pass by unnoticed. This application could be used to allow a user to pass by in stealth or even temporarily disable the chip in the ePassport, reverting it to a basic passport.

6.4 Experiment 3- Skimming an RFID tag

Aim: To determine the possibility of tracking a user and skimming information off their RFID enabled objects in a small scale example.

Hypothesis: Well-placed readers will provide enough information to allow inference to take place to a high degree of confidence. These readers will not only enable the tracking of a user, but also provide information about the RFID enabled items being carried. This occurrence is highly intrusive and provides the system owners the ability to profile and keep tabs on the user's tag.

Method: The Standard Apparatus 1 is used but the antenna configuration is modified to better model a real life implementation. Firstly 2 more antennas are added to the reader and all readers read ranges are reduced to 35% (this approximately reduces the read distance to 1.05 meters). The antennas are now spaced out around a room such that the antennas read zones do not cross over and allow dead zones (areas where no reader is monitoring the space) to occur to represent larger distances between read points. The antennas themselves represent buildings or public places. At selected antennas, tags are positioned to represent items that a user may wish to take. A user is now given a tag with a recorded tag ID and encouraged to move around the room at their own discretion and pick up any tags (items) as they please. As the user now moves around the room with their unique tag ID they are tracked via the antennas, each time a user enters an antennas zone, a log is formed with a time stamp. This log reflects the time the tag ID was interrogated and the tag ID itself. As the user picks up tags (items) and makes the transition to another zone, it will be evident that they are carrying the tag as it will show up in a new zone with their unique tag ID.

Results: Table 1 below represents the recorded events. The antennas were named North, East, South and West for obvious reasons.

The table shows a user (1111111111AAAAAAAAAAA1437) started at the Northern area. Two items were also positioned at the South and East areas. The user progresses to the Eastern area and continues to slowly move into the southern areas. Here they pick up an item (1111111111AAAAAAAAAAA1436) and continue moving with this item into the Eastern area.

Security breach: Breached.

Conclusion: It is possible to track a user, skim for information regarding what they are carrying and hence profile the user. The occurrence of this security breach allows the RFID infrastructure owners to become ever more pervasive in the user's life. It allows the surveiller to know when a user carries out an act, when they purchase something, when they are at a certain location and so much more. This breach allows for the formation of a 'Ralker' (RFID Stalker) which under other mediums is outlawed and only lawfully granted to governments under certain circumstances.

Table 1- Experiment 3 results

TAG ID	**TIME STAMP**	**TAG TYPE**	**ANTENNA**
1111111111AAAAAAAAAAA1437	***09:07PM 2/10/07***	***CLASS 0***	***NORTH***
1111111111AAAAAAAAAAA1436	09:07PM 2/10/07	CLASS 0	SOUTH
1111111111AAAAAAAAAAA1431	09:07PM 2/10/07	CLASS 0	WEST
1111111111AAAAAAAAAAA1437	***09:08PM 2/10/07***	***CLASS 0***	***EAST***
1111111111AAAAAAAAAAA1437	***09:08PM 2/10/07***	***CLASS 0***	***SOUTH***
1111111111AAAAAAAAAAA1437	***09:08PM 2/10/07***	***CLASS 0***	***EAST***
1111111111AAAAAAAAAAA1436	09:09PM 2/10/07	CLASS 0	EAST

6.5 Experiment 4- Killing an RFID tag

Aim: To destroy an RFID tag such that it will no longer respond to reader interrogations.

Hypothesis: An RFID tag contains a small circuit board, like all circuit boards too much voltage or current will cause the board to overheat. As an RFID tag gathers its electricity from electro magnetic frequency (EMF) radiation, it is assumed that a large burst of EMF radiation will cause the circuit board to overheat.

Method: An RFID tag is firstly scanned to ensure that it is in working order. The tag is then placed into a microwave and set on high for 10 seconds. The tag is then removed from the microwave and scanned to determine if the tag is still usable.

Results: The RFID tag read correctly before entering the microwave, however after 10 seconds in the microwave the RFID tag failed to respond to reader interrogations. Whilst in the microwave a bright glow was recorded coming out of the RFID tag, this was assumed to be the circuit board of the RFID tag *frying*.

Security breach: Breached.

Conclusion: The microwave appliance emits short 2.5 GHz waves called microwaves when it is turned on. These high frequency waves caused an increased voltage to flow inside the induction coil into the circuit board. This hence proved that if a large burst of EMF waves comes into contact with an RFID tag it can be destroyed.

6.6 Experiment 5- Flooding a reader

Aim: To flood a reader with so many requests, the reader either shuts down or

allows tags to pass by its reading range unnoticed.

Hypothesis: It is possible to flood a reader, but not overly practical as the amount of tags required will not be easily concealable or manageable.

Method: Countless class 0 tags are placed within a single antenna's read range. One tag with a known ID is kept out of the read range to test if it can pass by unnoticed. The reader is then turned on and the known tag is moved into the read range and then removed from the read range. The known ID is then searched for to determine if it has moved into the system unnoticed.

Results: A flood could not be created within the laboratory as not enough tags were available to cause the reader to read incorrectly. This was shown by the tag appearing each time it was introduced into the system and then removed.

Security breach: Resisted breach.

Conclusion: A flood attack on a reader is theoretically possible, however may not practically be possible if a read range was reduced to 10 cm. There would not be enough room to position enough tags to cause the flood to occur (for a summary of results from each experiment, see table 2 below).

Table 2- Summary of experiments and meta-analysis and their effects on ePassports

Security Breach	Does it impede on the privacy and security meant to be provided by the ePassport?
Skimming	A user could be followed and profiled, a smart bomb could be created if commonalities in data were found.
Injection attack	A database could be destroyed hence rendering the ePassport system useless.
Faraday cage failing	The failing Faraday cage in the current ePassport allows for rogue reading in stealth.
Killing a tag	A tag can be killed and hence reduce an ePassport back into a paper-based passport. Hence no added security.
Copying a tag and mimicking	An ePassport could be copied and the encryption taken home to be used in an offline attack to decrypt the data.

6.7 Compare experimental results with the work of Wethues

The work of Wethues (2003) has to be assessed in a meta analysis as the technical requirements needed to build his device are beyond the scope of this study. To provide credibility to Westhues's findings as this study could not test his creation, Newitz's (2006) article is cited as it describes the device in question. Wethues (2003) has developed a device which is capable of reading an RFID tag, copying the unique ID emitted by that device and then replaying the captured ID to a reader. Simply put, Westhues has created a 'replay attack' over the RFID medium. The device has a small read range and requires the user to almost brush past the tag they wish to

copy, however if the device is set up near a read point, the read distance is magnified enormously as the card is being 'excited' by another reader. This phenomenon allows the device to read tags from behind a wall or over a distance (Westhues, 2003).

To provide the much needed credibility to these claims, Newitz (2006) describes an encounter she has with Westhues. The author describes watching Westhues walk past an Internet security company, CEO James Van Bokkelen with a concealed antenna in the palm of his hand. Wethues returns to Newitz and plugs his device (via USB) into this laptop to determine if a signal was correctly recorded. Convinced that a successful read occurred, Westhues proceeds into the office building and sets his device to 'mimic' mode and waves his antenna in front of the proximity reader. Newitz (2006) concluded this device to be a complete success because the door in front of them unlocked and opened. This occurrence reinforces that RFID tags are not secure and can be copied at will. Furthermore, if this device was brought into the ePassport domain, the device owner could walk through an international airport stealing people's passport details in stealth. They could then return home and begin cracking the encryption hiding the data sets. With this information they can begin to commit fraud and identity theft.

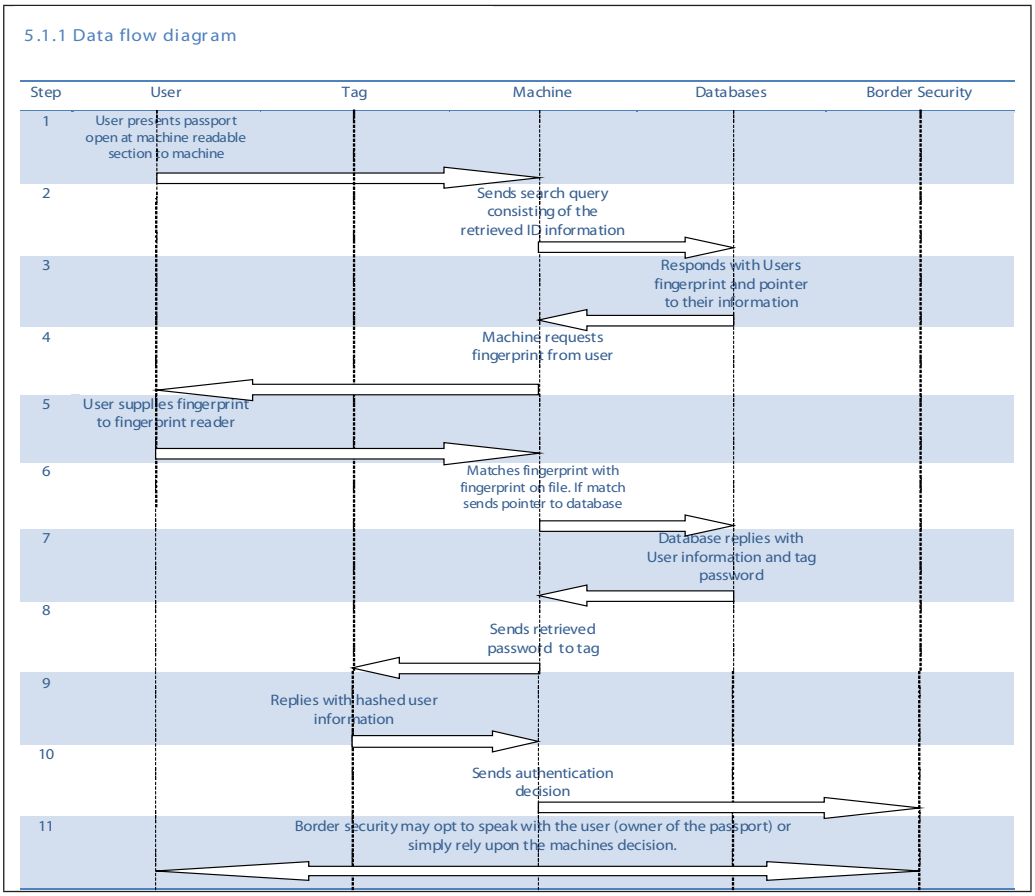
It has been shown that the current implementation of the ePassport was not well-thought out and allows for unscrupulous people to steal personal information and misuse this information. Through the meta analysis it has been shown that it is possible to steal information using an RFID device and record the data. This data could then be used in an offline attack as described by Sterling (2006) and Lettice (2007). The added security that the ePassport is intended to provide is shown to be non substantial but also shown to reduce the data security of its users. With this knowledge it is assumable that another implementation must be sort after such that the intended benefits can actually be achieved.

7 Proof of Concept

This paper has identified a number of shortcomings with the current ePassport technology. The proof of concept below is aimed at developing an ePassport which is more secure than the existing one by:

- Removing the ability to skim and track the ePassport by implementing a user verification system for the tag.
- Removing the flimsy encryption system and replacing it with a multi-tiered security system without a single point of failure.
- Providing a better implementation of the Faraday cage to deter rogue scanning.

Figure 2- Message Flow Diagram



7.1 Steps Explained

Step 1: The user opens their passport to the machine readable zone and places it on the read point of the machine. The machine will then scan the passport to retrieve the data from the MRZ.

Step 2: The data that has been obtained from the passport is now used to construct a database query. This data is simply date of birth, first name, last name etc (information that is already contained on the passport). The query is then issued to a database and a return is expected. This is the first layer of security, as a query that retrieves no records means that the identity this person is attempting to masquerade does not exist.

Step 3: If a match is found in the database, the users 'fileprint' (Khanna, 2004) and a pointer to the user's information in the second database is returned.

Step 4: The machine requests that the user place their fingerprint over the fingerprint reader so that a 'searchprint' (Khanna, 2004) can be obtained.

Step 5: User supplies their own fingerprint ('searchprint') as the machine requested.

Step 6: The 'searchprint' and 'fileprint' are now compared, if a positive match is

found then the pointer to the next database will then and only then be followed. If the pointer is to be followed, the database will be queried with the pointer to directly access the information required. This is the second step of security which proves that the identity claimed belongs to that physical person through biometrics.

Step 7: The database replies with the user's information (which is everything that would be printed on the passport such as date of birth, names, etc.) along with a tag password. This tag password exists in a 1–to-1 relationship by which only one password exists for each unique tag.

Step 8: The retrieved password is issued to the tag. The tag will only respond with its information when it receives the correct password. This system provides a third step in security to ensure that the RFID chip within the passport is the correct chip for this identity, if the correct password was not encountered the chip would not respond. As a further security precaution, incorrect passwords could be sent at random to the tag to ensure the tag is not compromised and programmed to respond to anything. This password system is adapted from the *kill-tag* system which when the correct password is received the tag calls its kill function and disables itself. However this adaptation replaces the kill function with a reply function and removes the standard reply function entirely as this proposed system never intends for the tag to reply under any other circumstances.

Step 9: If the correct password was encountered, the response is a hash string which is an ordered concatenation of the user's information and password which is then put through the MD5 hashing scheme.

Step 10: The machine will now hash the database retrieved user information and compare the hash output to that obtained from the passport. This is the fourth step in security which ensures that the information on the tag does actually represent the bona-fide user. The reason the tag stores a hashed version rather than plain text version is to ensure that skimming of tags can reap no reward. An authentication decision (passed or denied) is determined by this comparison.

Step 11: This authentication decision can then either be sent to a border security office manning the checkpoint at which point the officer may wish to conduct a visual check also. Conversely, this system can be used on an unmanned checkpoint and the decision will either allow the traveller to continue their journey, or prevent them from continuing any further.

7.2 Questioning the "key" to the ePassport system

Currently ePassports use 3DES encryption for the data on the RFID tags. Whilst this is an industry standard technology, the issue lies in the allocation of the key to decrypt the data. When designing the current ePassport, ICAO decided that the key to decrypt the data was to be composed using a concatenation of the passport number, holders date of birth, and passport expiry date (in that particular order). If an unscrupulous user was able to copy the passport data as detailed in the meta-analysis above, and could combine this with a high level phishing attack, the

key space could be reduced considerably as detailed by (Sterling, 2006). To alleviate this issue the proposed solution uses message digests. A *message digest* can never be reversed to show the original data hence nobody can ever steal your information from your passport in stealth. The issue with message digests is that because their never reversed to their original form, somebody could make an ePassport to just hold your message digest and nobody would be any the wiser. Whilst this is theoretically possible, it is not very practical. In order to succeed in this form of attack, the attacker would:

1. have to know the unique password for the ePassport he/she was trying to copy; and
2. have to have the same fingerprint as the legitimate user; and
3. have to look exactly like the legitimate user.

7.3 Layers of security provided by the proposed system

There are 4 layers of security offered by the proposed system.

Layer 1: The data that defines a unique user is used as a query in the passport holders database. If a match is not found it obviously shows that the passport does not exist and hence the owner is attempting to act fraudulently. If a match is found, it verifies that the user does actually exist and the document presented is legitimate.

Layer 2: To ensure that the person claiming to own the details in the passport actually does, a biometric test is used. The user's fingerprint ('searchprint') is taken and compared to the 'fileprint' which belongs to the passport. If a match occurs, it proves that the passport does belong to the bona-fide user.

Layer 3: Now that it has been established that the correct user is the holder of the right passport, it is necessary to ensure that the right chip is in the passport. This step prevents a person from cloning a passport and installing a fake RFID tag in it instead. A unique password which corresponds to the passport in question is sent to the tag. Upon receiving the correct password the chip will respond with data, however if an incorrect password is encountered, the tag will remain dormant and ignore all requests. To ensure someone has not altered the tag to respond at any time, a sequence of passwords can be sent to the tag, all incorrect but one. If the tag responds to an incorrect password, it can be assumed that the tag has been tampered with.

Layer 4: The tag in the passport only stores hashed user values which are created via a one way function and hence can never be reverted back to their original form. This security feature preserves user data as personal information can never be skimmed off the tag even if the right password is found. This means that smart bombs cannot be made to be denominational as the hash string will not reveal information regarding the country of origin etc.

7.4 Confidentiality

Preservation 1: The proposed system's kill tag approach prevents a rogue reader

from tracking users as it is assumed that a rogue reader will not have the tags unique password. Assuming this, a rogue reader will never get any form of response from a tag. Hence the tag owner can travel at ease as their identity is never disclosed.

Preservation 2: In the event that a rogue reader does determine the tags unique password, the information retrieved is in actual fact useless. The tag only stores hashed information which according to the design and manifest behind hashing, can never be processed back into its original form. Hence if a breach occurs and a rogue reader does steal tag data, they have not stolen anything of worth.

7.5 Integrity

The integrity of this system lies in the comparison processes of stored information to retrieved information. The system uses a multi-tiered authentication verification process, by which a user makes an authentication claim (i.e. delivers a passport to the machine) and must then verify that they actually own the passport (via a fingerprint scan). This is again demonstrated when the tag must prove that it belongs to the right passport which belongs to the bona-fide user by communicating with the machine, if, and only if the correct password is received. This phenomenon culminates in a final authentication and verification process by which the tag's hash string is compared to the on file hash string. This multi-tiered process aims at ensuring that changes to data cannot occur, but ultimately if they do occur, one of the tiers of authentication and verification will determine the fraudulence.

7.6 Availability

The user verification system for the tag is a simple means to provide the availability characteristic as this scheme requires a password to read the tag. It is assumed that only a bona-fide user will have the password and hence only makes the tag available to intended users.

7.7 Databases

The user verification system for the tag is a simple means to provide the availability characteristic as this scheme requires a password to read the tag. It is assumed that only a bona-fide user will have the password and therefore the tag is made available to intended users alone.

The reason the two databases (figure 3) are set up into an array is a performance consideration and is intended to reduce the search space and hence allow for practical searching. Using Australia as an example, the top 20 surnames are tabulated and the total frequency of each of the first letters is recorded in figure 4.

The 'W' category holds 160,303 occurrences and when put into perspective accounts for 20.9% of the top 20 occurrences. Applying this figure to the Australian population as a total (approximately 20 million) to provide a rough generalization, it is possible to see that the W database may hold approximately 4 million entries. Considering that 'Google' can search its indexes and return 2,370,000,000 entries

for the letter 'e' in 0.09 seconds it is hence assumed that the intended database model will function efficiently. Data was tabulated using Wikipedia (2007) who gathered their results from IP Australia, Government of Australia.

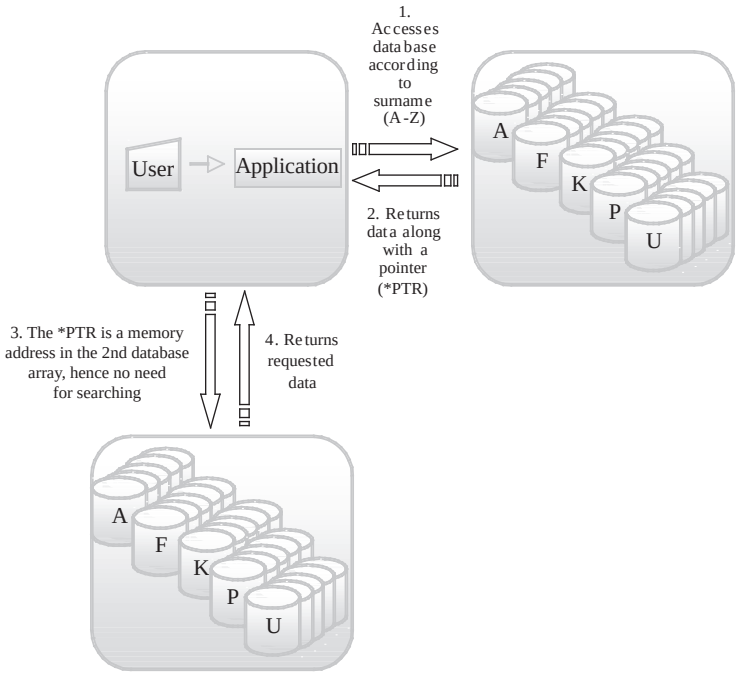


Figure 3- Accessing records from the database

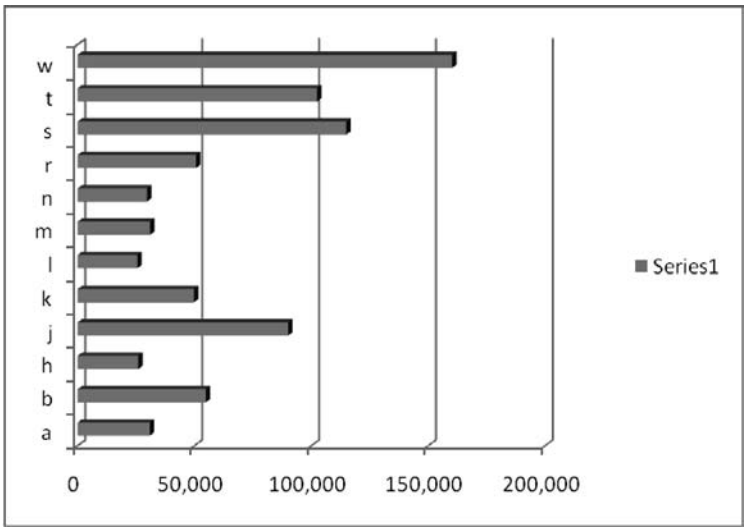


Figure 4- Letter-specific databases for faster searching on surname

7.8 Policy

Currently border security will accept an ePassport with a faulty RFID chip as a legitimate identification document (table 3). This policy is a critical mistake as it circumvents the reason the ePassport was created. If an unscrupulous person disables an RFID chip, the ePassport is now only as secure as a passport without an RFID chip. This is obviously a problem or else why would the government have wished to introduce an ePassport? To remedy this, the policy surrounding the proposed implementation of an ePassport will define a passport with a faulty RFID tag as an illegitimate identification document and will take note of the owner for further investigation.

Table 3- ePassport comparisons

Possible security breach	**Current ePassport**	**Proposed ePassport**
Tracking	Breach	Resisted Breach
Killing	Breach	Resisted Breach
Injection attack	Breach	Breach
Blocking security device	Breach	Resisted Breach
Wave injection attack	Breach	Breach
Steal information	Breach	Resisted Breach
Flooding	Resisted Breach	Resisted Breach
TOTAL	Breach=6, Resisted Breach=1	Breach=2, Resisted Breach=5

Tracking: The proposed ePassport can only be tracked if the right password is issued to the tag or else no response will be obtained, however the current ePassport will respond to anything.

Killing: Both implementations are susceptible to a tag being destroyed however the policy for the proposed implementation ensures that this occurrence does not lead to a breach.

Injection attack: Both systems are perceptible to an injection attack if their back-end systems are not configured correctly.

Blocking security device: The Faraday cage that houses the current ePassport fails if the passport is only slightly open (this may occur if thrown into a bag). The proposed enclosure stops the ePassport from opening, hence preventing an inadvertent read window.

Wave injection attack: Both systems are perceptible to this attack as it attacks the core technology.

Steal information: The current ePassport contains encrypted information which can be decrypted, the proposed implementation keeps one way message digests of the data which can never changed back into the information's original form.

Flooding: Both the new and the proposed system would require so many tags

to actually produce a flooding attack that they could not all be concealed.

8 The irony of it all

"[A]ny system is only as secure as its weakest point of entry" (Microsoft, n.d.).

Whilst this quote was not originally used in the context of ePassports, it applies itself with the same meaning. By reviewing the process of obtaining a passport in Australia the weakest points are quickly identified which render all attempts to secure a passport useless. Figure 5 shows the relationship between these important personal documents. It also shows that the single point of failure is the birth certificate. Zill (n.d.) also takes this point of view and denotes a *birth certificate* is "a "weak" document because it is relatively easy to forge and has no photo or fingerprint requirement (Zill, n.d.). Following the schema presented, once a birth certificate is obtained, a Medicare card can also be obtained. A driver's license is the next obvious progression as both a Medicare card and birth certificate are in possession. Finally, a passport can be obtained as all the vital government documents are in possession. The previous chronological investigation shows that a passport is not made secure by enhancing the technologies and policies surrounding it, as an illegitimate passport can easily be obtained using fake seminal documents. It is important however to realize that the basis of this paper is not to solve the existence of fraudulent passports, but to ensure that if this particular RFID technology 'must' be used, that the technology is applied in such a way that it does not cause new afflictions upon society.

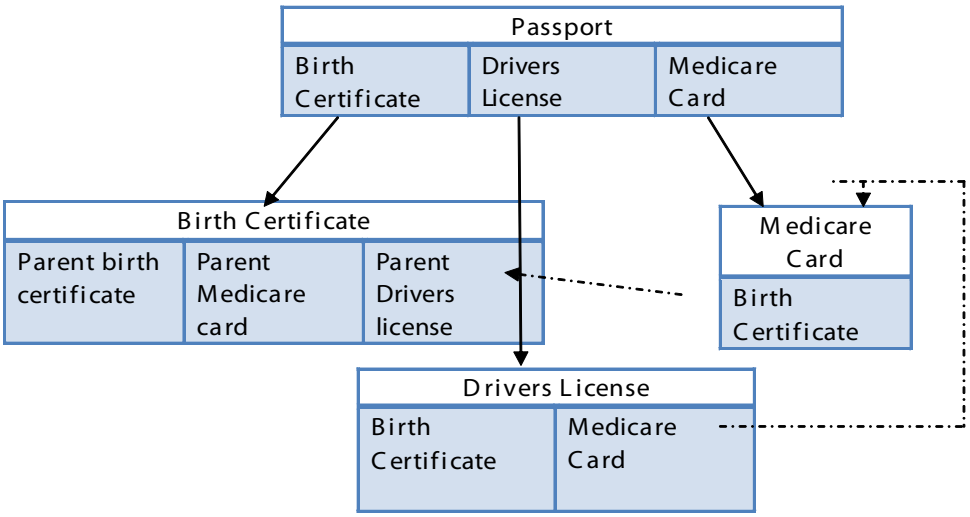


Figure 5- Important personal identification documents

References

Abzug, M, T. 1991. MD5 Homepage (unofficial). Abzug, M, T. [Online] 1991. [Accessed: 13 April, 2007] http://userpages.umbc.edu/~mabzug1/cs/md5/md5.html.

Answers.com. n.d. Replay attack. Answers. [Online] Computer Language Company Inc., n.d. [Accessed: 14 April 2007] http://www.answers.com/topic/man-in-the-middle-attack.

Australia, Commonwealth of. 2007. Mobile Telephones Scientific Background. Australian Radiation Protection and Nuclear Safety Agency. [Online] 2007. [Accessed: 30 August 2007] http://www.arpansa.gov.au/mobilephones/mobiles1.cfm.

Bishop, M. 2002. Computer Security: Art and Science. s.l.: Addison Wesley Professional, 2002.

Brainard, J. Jules A. 2004. Soft Blocking: Flexible Blocker Tags on the Cheap. Washington: Communications of the ACM, 2004.

Buehrer, G, T. Weide, B, W. Sivilotti, P, A, G. 2005. Using Parse Tree Validation to Prevent SQL Injection Attacks. Columbus: ACM, 2005.

Centre, Radiation Emergency Assistance. n.d. Definitions related to radiation. Radiation Emergency Assistance Centre/Training Site. [Online] n.d. [Accessed: 4 November 2007] http://orise.orau.gov/reacts/guide/definitions.htm.

Chuvakin, A. Peikari, C. 2004. Protect Yourself Against Kerberos Attacks. WindowsDevCenter. [Online] O'Reilly, 2004. [Accessed: 14 April 2007] http://www.windowsdevcenter.com/pub/a/windows/excerpt/swarrior_ch14/index1.html.

Department, U.S. State. 2005. U.S. passports get tagged. s.l.: Expanded academic ASAP, 2005.

Coffee, P. 2006. Passport to a Void Promise; Solving the wrong problem in the wrong way is a stupid tech trick. eWeek. Aug 2006, Vol. 23, 34, p. 16.

Flexills. 2006. RFID Passport Shield Failure Demo. YouTube. [Online] Flexills, 2006. [Accessed: 15 April 2007] http://www.youtube.com/wath?v=-XXaqraF7pl.

Gonsalves, C. 2005. A Ticket to Trouble; RFID-enabled passports pose privacy, security risks. eWeek. 2005, Vol. 22, 19, p. 33.

Jules, A. Riverst, L, R. Szydlo, M. 2003. The Blocker Tag: Selective Blocking of RFID Tags for Consumer Privacy. Washington: Communications of the ACM, 2003.

Jules, A. 2005a. RFID Privacy: A technical primer for the non-technical reader. MA: RSA Labratories, 2005a.

Kaliski, B. 2005. ravel Security and Function Creep: Thinking about the ePassports in the Long Term. Speaking of security. [Online] 2005. [Accessed: 15 April 2007] http://www.rsa.com/blog/entry.asp?id=1019.

Karjoth, G. Moskowitz, A, P. 2005. Disabling RFID Tags with Visible Confirmation: Clipped tags are silenced. Workshop on Privacy in the Electronic Society. November 7, 2005.

Khanna, R. 2004. Systems Engineering for Large-Scale Fingerprint Systems. [book auth.] N. Bolle, R. Ratha. Automatic Fingerprint Recognition Systems. New York: Springer-Verlag, 2004.

Labratories, RSA. n.d. FAQ on RFID and RFID privacy. RSA Labratories. [Online] n.d. [Accessed: 15 April 2007] http://www.rsa.com/rsalabs/node.asp?id=2120#13.

Lamb, G, M. 2006. New 'e-passports' raise security issues; Despite official assurances, some worry that thieves might read chip- toting US passports. Boston: s.n., 2006, p. 13.

Launch of ePassport press conference. Downer, A. 2005. Canberra: http://www.foreignminister.gov.au/transcripts/2005/051025_ePassport.html, 2005.

Lettice, J. 2007. How to clone a biometric passport while it's still in the bag. The Register. [Online] The register, 3 2007. [Accessed: 8 August 2007] www.theregister.com/2007/03/06/daily_mail_passport_clone/.

Microsoft. n.d. Microsoft's approach to secure government systems. Microsoft Government. [Online] Microsoft, n.d. [Accessed: 1 October 2007] http://www.microsoft.com/industry/government/securityprivacy.mspx.

Molnar, D. Soppera, A. Wagner, D. 2005. Privacy for RFID through Trusted computing. Workshop on Privacy in the Electronic Society. November 7, 2005.

Moses, A. 2006. Passport hacker warns of identity risk. Sydney Morning Herald. [Online] 2006. [Accessed: 14 April 2007] http://www.smh.com.au/news/security/passport-hacker-warns-of-identity-risk/2006/12/12/1165685661999.html.

Munro, K. 2007. SECURITY MATTERS: Broadcast your details with an RFID. February 28, 2007, p. 1.

Newitz, A. 2006. The RFID Hacking Underground. Wired. May 2006, 14.05.

Orso, William G.J. Halfond and Alessandro. 2005. AMNESIA: Analysis and Monitoring for NEutralizing SQLInjection. California: ACM, 2005.

Schoen, S. n.d. Trusted Computing: Promise and Risk. Electronic Frontier Foundation. [Online] n.d. [Accessed: 13 April 2007] http://www.eff.org/Infrastructure/trusted_computing/20031001_tc.php.

Staake, T. Thiesse, F. Fleisch, E. 2005. Extending the EPC Network - The Potential of RFID in Anti-Counterfeiting. Symposium on Applied Computing. March 13-17, 2005.

Sterling, B. 2006. Arphid Watch: Find Own Foot, Aim Hastily, Pull Trigger. WIRED. [Online] WIRED, 17 11 2006. [Accessed: 8 August 2007] http://blog.wired.com/sterling/2006/11/arphid_watch_fi.html.

Thorsteinson, P, G. Ganesh, G, A. 2003. .NET Security and Cryptography. Upper

Saddle River: Prentice Hall, 2003.

Trade, Department of Foreign Affairs and n.d. The Australian ePassport. Australian Government: Department of foreign affairs and trade. [Online] n.d. [Accessed: 20 April 2007] http://www.dfat.gov.au/dept/passports/.

Wamba, S, F. Lefebvre, L, A. Lefebvre, E. 2006. Enabling Intelligent B-to-B eCommerce Supply Chain. ICEC'06. 2006.

Want, R. 2004. Enabling Ubiquitous Sensing with RFID. Computer. 2004, Vol. 37, 4.

Westhues, J. 2003. Proximity Cards. cq.cx. [Online] October 2003. [Accessed: 29 March 2007] http://cq.cx/prox.pl.

Wikipedia. 2007. List of most common surnames. Wikipedia. [Online] Wikipedia, 05 2007. [Accessed: 1 October 2007] http://en.wikipedia.org/wiki/List_of_most_common_surnames#Australia.

Zill, O. n.d. Crossing borders: How terrorists use fake passports, visas and other identity documents. PBS. [Online] PBS, n.d. [Accessed: 1 October 2007] http://www.pbs.org/wgbh/pages/frontline/shows/trail/etc/fake.html.