Overview of Micro-payment Technology

Vishal Bharat Sharma
Macquarie University
Sydney, Australia
vishal.sharma@students.mq.edu.au

Abstract

Micropayment systems are the electronic payment systems used to make small value payments. In these systems the technology used is Radio Frequency Identification (RFID) which offers number of advantages over other current technologies in use in payment systems. Number of the benefits offered by RFID technology has attracted business and authorities for its use. But the recent security researches on this technology had brought number of its vulnerabilities into light, which made authorities to think again before accepting it as a one-stop solution to current technology's shortcomings. The aim of this work is to provide an overview of the RFID technology in context to payment systems, to discuss about its basic working, requirements and issues. The possible outcome of this project would be the detailed analysis of RFID, its main security issues and possible suggestions (by experts) that can be used to overcome these current security issues.

1 Introduction

The Payment systems are one of the fundamental pillars of modern economies and can be defined as a collection of technologies, laws, protocols, and customs that make it possible for people and companies to pay money to each other (Kniberg, 2002). All payment systems have definite characteristics and qualities and they find their application on the basis of these qualities and characteristics. Payment systems currently in use can be divided into mainly two types. **Traditional payment system**, a system in which hard cash is used to pay for making payment. The fundamental problem with this system is that two parties can't exchange money without meeting; third party is needed, which slows down process. Another problem with cash is that it has a fixed set of denominations, which makes it difficult to handle extremely large or extremely small transactions. Another system in use is **electronic payment system**, in this system all the payments are made digitally – usually through network connection. All the payment systems which use cards, mobile and internet falls under this category. Mobile and internet support some specific types of payments only and require credit card or net-banking account, are not considered in this report. The cards are the main source of payments in electronic payment system. Although these cards are widely used, but they posses some limitations, first the technology used in this system is too slow it takes around 1-2 seconds to process one card[1], the method of authentication and authorization process used takes too long to make decision, and in last, they don't support small amount transactions.

To overcome these shortcomings new payment system known as micropayment system is proposed. This document provides a brief overview of micropayment system technology (RFID). Its basic requirements, components, working, and main issues related to its operation and security. This report begins with a brief introduction to micropayment systems in section 2. Followed by discussion on micropayment technology, its main characteristics, components and basic working, and advantages it provides over other current technologies used in payment systems in Section 3. Last section 4, of this report talks about the issues RFID faces in operations and security & privacy, and the suggested counter measures to overcome these issues.

[1] http://www.card-reader.com/idscan_magnetic.htm

2 Micropayment Systems

Micropayment systems are means for transferring very small amounts of money, in situations where collecting such small amounts of money with the usual payment systems is impractical, or very expensive, in terms of the amount of money being collected. In the non-digital world, micropayments themselves are not new of course. People have been paying cash for small purchases for hundreds of years. What is relatively new though is using non-cash or other electronic methods to make these payments (Williams L Amy, 2007). The electronic versions of micropayments have become important due to two main reasons, first, the handling of cash is very expensive as it needs to be collected, counted, stored, handled and redistributed, and secondly time to process a transaction. Authorities want to find a way to cut those costs and increase efficiency. As over the years, technologies have been invented to address society's problems or to fulfill its growing desire for speed and convenience. Development of micropayment systems is also a step towards this goal.

Kniberg, 2002 in his work on micropayment systems, revealed the main characteristics that system should posses to be successful in micropayments. Following should be taken in account by authorities while designing micropayment system.

Important characteristics

- Ease of joining
- Ease of use
- Pervasiveness
- Fixed transaction cost
- Transaction speed
- Security (Of Information)

Less important characteristics

- Security (Of Amount)
- Relative transaction cost

3 Micropayment Technology (RFID)

3.1 Introduction[2]

RFID as name implies is a wireless technology, which works on Radio Frequency. In RFID systems an active or passive RFID tag is attached to, or embedded in, an item which communicates its identity to an RFID reader using radio frequency wave. The RFID tag provides the reader with a sequence of data that encodes a unique identity for that object. In the case of passive RFID tags, the radio frequency waves power the tags to enable it to communicate, when it is within the reading-range of the RFID reader. RFID systems do not require line-of-sight and work contactless. Figure 1 [3]shows the basic structure of RFID system.

3.2 Basic components of RFID system

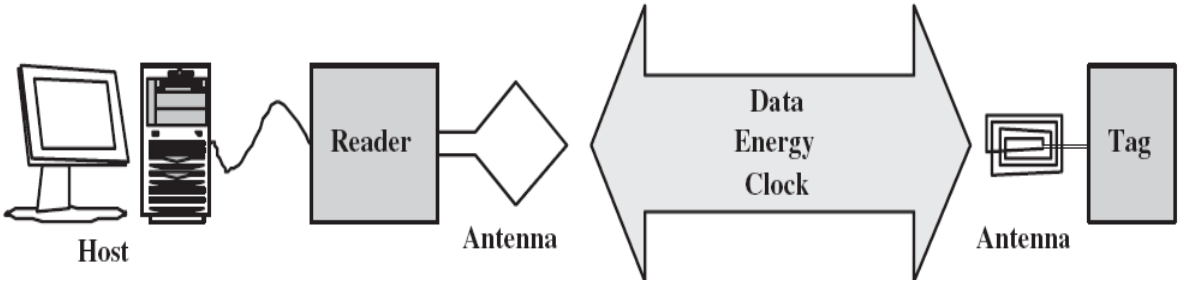

Figure 1 Structure of an RFID System

3.2.1 Tag

Radio Frequency Identification Tags consists of an antenna and integrated circuit. Antenna is used for transmitting and receiving signals and integrated circuit is for storing and processing information, modulating and demodulating a radio frequency signal. Some of the RFID tags known as chip tags consist of a microchip in addition to integrated circuit and antenna, there are the smart cards based on RFID technology. Most tags are only activated when they are within the interrogation zone of the interrogator; outside they “sleep”. Chip tags can be both read-only or, at higher complexity and cost, read-write, or both. Chip tags contain memory. The size of the

[2] This section summarizes the information from these sources (Curtin, Kauffman, and Riggins1q, 2007) (Feldhofer, Dominikus, and Wolkerstorfer, 2004)

[3] Figure obtained from Cryptographic Hardware and Embedded Systems - CHES 2004 [e-book]

tag depends on the size of the antenna, which increases with range of tag and decreases with frequency.

Passive tags which draw power from the reader are cheaper and smaller than active tags, these types of tags are mainly used and proposed for use in payment systems.
Semi-passive tags use an internal battery to ensure data integrity, however the signal sent from the reader generates the power to transmit the signal from the tag.
Active tags typically have internal read and write capability, their own batteries, and can transmit their signals over a longer distance.

3.2.2 Interrogator/Reader

Interrogators/readers are the devices which are connected to server. They read the whenever it comes in its interrogation zone/reading range and pass that information to the server connected. Depending on the application and technology used, some interrogators not only read, but also remotely write to, the tags. For the majority of low cost tags (tags without batteries), the power to activate the tag microchip is supplied by the reader through the tag antenna when the tag is in the interrogation zone of the reader, as is the timing pulse – these are known as passive tags.

3.2.3 Middleware

Middleware is the interface needed between the interrogator and the existing company databases and information management software.

3.3 Advantages

Contactless technology provides an edge to RFID cards over other cards currently in use. First, these cards do not require a contact pad for communications and power, implies there is less wear and tear as well. These cards can transmit data at far higher speeds than their analogues, since it has a serial communications line that runs fast, it doesn't have to be in proximity for very long (Callas, 2008), lastly since these device needs merely to be close enough to a terminal to work, they are easy to use.

Realization of the benefits of the RFID in the business community is fostering explosive growth in RFID-enabled systems in different applications at a tremendous rate. Number of these system have been deployed in number of industries such as logistics, supply chain management, library item tracking, medical implants, road tolling, building access control, transportation and payment systems. Few examples of deployment of RFID-based payment systems around the world are, "Speedpass," allow drivers to purchase gas and convenience store goods from ExxonMobil stations. "E-tags" to collect toll tax on highways, with the advent of around the world (Federal Trade Commission, 2005). It is also used in public transport network in number of countries for example, in Singapore EZ-Link cards, Oyster cards in UK, and Octopus Cards in Hong Kong.

4 Issues with RIFD

We RFID tags and RFID readers communicate using radio waves, and use of radio-frequency as a transmissions channel raises number of concerned when deployed/used in practice.

4.1 Operational Issues

4.1.1 Interoperability

In every payment system there are definite set of standards and rules that are to be followed to make it universally acceptable and successful. In case of RFID, as RFID systems are implemented in different ways by different manufactures, interoperability becomes a serious issue. The ISO/IEC 14443 standard for use of RFID technology is for proximity card, which is used in some payment systems. There is no dedicated standard for use in payment systems. In addition to it, the use of various types of encryption techniques and other security features, by different vendors doesn't support interoperability (Ahson, and Ilyas, 2008).

4.1.2 RFID Systems Can Be Easily Disrupted

Since RFID systems make use of the electromagnetic spectrum, they are relatively easy to jam using energy at the right frequency (Ahson, and Ilyas, 2008). a serious threat to payment system RFID system vulnerable to such attacks could become a serious organizational weakness.

4.1.3 RFID Reader Collision

Reader collision occurs in RFID systems when the coverage area of one RFID reader overlaps with that of another reader. This causes two different problems. Signal interference, the RF fields of two or more readers may overlap and interfere. This can be solved by having the readers programmed to read at fractionally different times. This technique (called time division multiple access - TDMA) can still result in the same tag being read twice. Multiple reads of the same tag, the problem here is that the same tag is read one time by each of the overlapping readers. The only solution is to program the RFID system to make sure that a given tag (with its unique ID number) is read only once in a session (Ahson, and Ilyas, 2008).

4.1.4 RFID Tag Collision

Tag collision in RFID systems happens when multiple tags are energized by the RFID tag reader simultaneously, and reflect their respective signals back to the reader at the same time. This problem is often seen whenever a large volume of tags must be read together in the same RF field. The reader is unable to differentiate these signals; tag collision confuses the reader. Different systems have been invented to isolate individual tags; the system used may vary by vendor. For example, when the reader recognizes that tag collision has taken place, it sends a special signal (a "gap pulse"). Upon receiving this signal, each tag consults a random number counter to determine the interval to wait before sending its data. Since each tag gets a unique number interval, the tags send their data at different times (Ahson, and Ilyas, 2008).

4.1.5 Unauthorized Tag Disabling

This is a form of Denial-of-Service (DoS) attack in which an attacker causes RFID tags to assume a state from which they can no longer function properly. This results in the tags becoming either temporarily or permanently incapacitated. Such attacks are often exacerbated by the mobile nature of the tags, allowing them to be manipulated at a distance by covert readers. Active RFID tags (those that use a battery to increase the range of the system) are more subject to these types of attacks as on being repeatedly interrogated wear the battery down, disrupting the system (Ahson, and Ilyas, 2008).

4.2 Privacy & Security Issues

Since, publicly available radio frequency is used as transmission channel between RFID cards and readers, it is harder to secure than wires or cables. The factors (Tien, 2005) which make RFID tags especially dangerous to privacy, In short, RFID tags are designed for convenience of reading, but that convenience comes with a high cost to privacy and a high risk of identity theft.

- RFID tags are promiscuous: They are generally designed to be activated, and their transmissions receivable, by any compatible reader/sensor device.
- RFID tags are stealthy: When RFID tags are being read, the people carrying the tags don't know that it's happening.
- RFID tags are remotely readable, and can be read through many common substances (cloth, leather, paper).

4.2.1 Unauthorized Disclosure Of Personal or Sensitive Information

RFID tags also present security issues, such as "cloning" or duplication and card forgery. Since RFID cards become active when in vicinity of card reader, and start communicating, the attacker can exploit this feature to obtain the information use this without the holder's knowledge or consent. Any compatible reader within range of the RFID tag could read the stored data. Read range varies depending on the radio frequency being used, the power of the reading device, and many environmental factors.
This could easily occur in "walk-through" application when the card is read from one's wallet, pocket or purse. Cloning the RFID tag alone might suffice for an illegitimate purpose (Ahson and Ilyas, 2008, Chapter 26, and Tien, 2005).

4.2.2 Unauthorized Tracking

An RFID card also enables others to secretly monitor its holder's whereabouts and possibly his or her actions. As the number of RFID readers in the social environment increases, the easier it will be to track RFID tags. Importantly, the tracking threat exists even if the RFID tag contains no name or other personal information. What matters is that the RFID tag contains a static unique number or pattern that is or can be persistently associated with a person's identity. So

long as the RFID tag or chip broadcasts this information, the person carrying that tag can be distinguished from any other person carrying a different RFID tag. It is a serious threat to privacy. (Ahson and Ilyas, 2008, Chapter 26, and Tien, 2005)

4.2.3 The Unique ID Number Problem

Any unique ID number on the card may be a "key" to personal information stored in a database somewhere. Our society often uses unique ID numbers to index or organize personal information in databases, or as a linking or matching identifier across multiple databases. The worst-case scenario would be a commonly used unique number like a Social Security number, phone number, or a driver's license number, which is already used to index and link personal data (Tien, 2005).

4.2.4 Eavesdropping

Eavesdropping attacks are a well known risk for RFID devices and there are several claims about the possibility of these attacks on RFID tokens. It is another type of information disclosure threat. In eavesdropping, the attacker does not read the information directly from the RFID tag or card; instead, the attacker listens to the transmission between the RFID tag and an authorized RFID reader. The eavesdropping threat is the main reason why merely shielding RFID devices is inadequate to protect privacy, because the RFID card must be exposed in all legitimate transactions. No physical contact needs to be made with the reader, which simplifies operation and increases overall transaction speeds. A growing security concern with RFID devices is the possible release of the user's personal information, or location, to unauthorized parties (Tien, 2005). The suggested solution for it was better encryption and shielding (Kelter, 2006).

4.2.5 Forward Security

Since RFID cards are proposed to be used in payment systems, they may be used to store the information related to all the recent transactions. As these devices are highly vulnerable to number of attacks, there shouldn't be any information stored related to previous transactions. Forward-security is important to guarantee the privacy of past transactions if the long-term key or current session key is compromised. (Le, Mike, Medeiros, 2007).

4.2.6 Relay Attack

It is a type of attack related to man-in-the-middle attacks, in which an attacker relays verbatim a message to a card reader. The card may not be aware of this communication. Since a contactless card communicate with other devices without any physical connection, the security of the payment system is based on a key feature of RFID-based systems that card works in very short range typical to operate at a range of 10cm. But it has been demonstrated by (Kfir and Wool, 2005) that contactless card technology is vulnerable to relay attacks. A setup was built that could remotely use a victim's contactless smartcard, without his knowledge. The suggested counter measures were to shield the contactless card against malicious attackers, and to activate the card only when the card owner wants to take some action.

4.2.7 Side Channel Attacks

This is an attack which is launched on the basis of information gained from the physical implementation of an equipment, rather than brute force or theoretical weaknesses. In these attacks the timing information, power consumption, electromagnetic leaks or even sound produced is exploited. Oren and Shamir, 2007 have successfully launched this attack against RFID system. In which they demonstrated that power analysis can be carried out even if both the tag and the attacker are passive and transmit no data, making the attack very hard to detect and suggested that in order to achieve strong security in practice, research is needed into either making RFID hardware more resistant to such attacks, or developing obfuscating techniques for cryptographic computations.

5 Conclusion

Despite the very advantages and benefits, RFID create security issues unique to it. These shortcomings prevent it from becoming the one-stop solution for payment systems. A lot of vulnerabilities have been discovered and patched. Since security is a continual evolving process; there can't be any exact solution to it. New vulnerabilities will arise time to time; authorities need to

take care of them before being exploited. Currently RFID is going through a research and development phase as all the other technologies has gone through before being accepted as a standard. RFID has lot of potential to deliver to various applications, but further research and development is required before being deploying at large scale.

Acknowledgments
I would like to thank Dr. Josef Pieprzyk for his enormous support and guidance.

References

Ahson S., Ilyas M., 2008. RFID Handbook. North West, North America: CRC Press

Burmester Mike, Medeiros D. Breno, 2007. RFID Security: Attacks, Countermeasures and Challenges
Available at:
http://www.cs.fsu.edu/~burmeste/133.pdf
[Accessed 10 April 2009]

Callas J., 2008. Position Statement in RFID S&P Panel: Contactless Smart Cards [e-book] Heidelberg: Springer Berlin
Available at: University library/databases/computing/springer/
http://www.springerlink.com.simsrad.net.ocs.mq.edu.au/content/t0w725224686664k/fulltext.pdf
[Accessed 1 April 2009]

Curtin J., Kauffman R. J., and Riggins F. J., 2007. Making the 'MOST' out of RFID technology. Information Technology and Management. Volume 8, Number 2. pp 87-110

Federal Trade Commission, 2005. Report on RFID
Available at:
http://www.ftc.gov/os/2005/03/050308rfidrpt.pdf
[Accessed 19 May 2009]

Feldhofer M., Dominikus S., and Wolkerstorfer J., 2004. Cryptographic Hardware and Embedded Systems - CHES 2004 [e-book] Heidelberg: Springer Berlin
Available at: University library/databases/computing/springer/
http://www.springerlink.com.simsrad.net.ocs.mq.edu.au/content/26tmfjfcju58upb2/?p=246ed1cfc14b49048c8a154d311082f0&pi=7
[Accessed 10 April 2009]

Kelter Harald, 2006. Security threats around RFID
Available at:
http://www.rfidconsultation.eu/docs/ficheiros/Kelter.pdf
[Accessed 20 May 2009]

Kniberg Henrik, 2002. What Makes a Micropayment Solution Succeed [Internet]
Available at:
http://www.kniberg.com/henrik/thesis/pdf/What-makes-a-micropayment-solution-succeed.pdf
[Accessed 25 March 2009]

Jari Kytojoki, Vesa Karpijoki, 2000. Micropayments - Requirements and Solutions
Available at: http://users.tkk.fi/vkarpijo/netsec99/
[Accessed 20 March 2009]

Kfir Ziv and Wool Avishai, 2005. Picking Virtual Pockets using Relay Attacks on Contactless Smartcard Systems
Available at: http://eprint.iacr.org/2005/052.pdf
[Accessed 10 April 2009]

Le V Tri, Mike Burmester, Medeiros D. Breno, 2007. Universally Composable and Forward-secure RFID Authentication and Authenticated Key Exchange
Available at:
http://www.cs.fsu.edu/~burmeste/130.pdf
[Accessed 10 April 2009]

Oren Yossef and Shamir Adi, 2007. Remote Password Extraction from RFID Tags
Available at:
http://iss.oy.ne.ro/RemotePasswordExtractionFromRFIDTags.pdf
[Accessed 20 April 2009]

Steve Halliday, 1997. Identification Cards - Just the Ticket?
Available at:
http://www.hightechaid.com/tech/card/id_cards.htm
[Accessed 10 April 2009]

Tien Lee, 2005. Testimony in support of the Identity Information Protection Act (S.B. 682)
Available at:
http://w2.eff.org/Privacy/Surveillance/RFID/tien_testimony_sb_682.pdf
[Accessed 10 May 2009]

Williams L Amy, 2007. Developments in Micropayment Systems
Available at:
http://www.dww.com/?page_id=1158
[Accessed 18 May 2009]