Journal of Information

journal homepage: http://www.pakinsight.com/?ic=journal&journal=104

SECURITY ISSUES WITH CONTACTLESS BANK CARDS

Brendan McBride[1] --- Nigel McKelvey[2] --- Kevin Curran[3]

[1,2] School of Computing, Letterkenny Institute of Technology, Letterkenny, Co. Donegal, Ireland

[3]School of Computing and Intelligent Systems, Faculty of Computing and Engineering, University of Ulster, Londonderry, Northern Ireland, BT48 7JL

ABSTRACT

Contactless bank cards have been issued steadily to banking customers over the past four years and this trend has continued to grow rapidly more recently. We want to highlight a list of security issues as well as privacy threats to be concerned with when using such contactless bank cards. Further advances in smartphone technology applications can lead to new threats in relation to contactless bank cards. This paper highlights data protection issues in Ireland as a major push by authorities to a cashless banking society which could potentially lead to further data protection problems in Ireland.

1. INTRODUCTION

Near Field Communication (NFC) is based on Radio Frequency Identification (RFID) that uses a frequency to connect two devices within a short range. The ISO standard for this is ISO/IEC 14443 meaning the two devices will only communicate at a distance less than 10 centimetres [1]. An NFC device can be embedded into a bank card and this will enable it to communicate with other contactless smart card standards. NFC has been reinvented by Sony and Philips around 2002 and in recent years the technology has moved to contactless bank cards where customers can pay for their goods without having to enter a security pin [2]. Contactless bank cards are embedded with a small chip and antenna, this lets customers place their bank card near a reader and the transaction is complete in seconds. Gartner who are a marketing research company expects contactless bank card users to excide 450 million users worldwide by 2017 [3].

Contactless bank cards are seen to be a convenient way of paying for goods. Examples of this would be time spent queuing for the payment of good's, this would be significantly reduced as this

payment transaction is much quicker than current chip and pin methods. Contactless bank cards will also help banks and governments to continue onwards with a cashless society. This will help prevent tax evasion, fraud and also reduce the number of customers having to use their local banks possibly resulting in more profits as these could close [3]. Figure 1.1 illustrates a basic contactless bank card transaction. Although consumer would have a right to be cautious about using contactless bank cards, it's a relatively new technology and with new technologies comes security concerns and these bank cards are no different. This method of payment is convenient there are questions as to how secure consumers banking details and personal data really are. Cloning contactless bank cards can be relatively easy [3]. It has also been reported that with the correct equipment eavesdropping can potentially pick up signals being transmitted from contactless bank cards [4]. This is almost certainly a threat to consumer's data protection and also a security threat to the bank involved. Should this information be true, are companies like Visa and MasterCard investing enough in this sector to combat these issues and make it secure, it remains to be seen whether they will or not**.**

Personal data is being collected by companies all over the world and then been sold to large companies where they can target the consumer with advertisements of items they may have been looking at online. Why can't consumers be able to surf online without almost every website they visit been tracked, the main reason consumers are been tracked is sales. Business rely on gathering as much data from online users as possible so they can push advertisements to consumers PC's. This again raises the question, should consumers not have a say in all of this. People would prefer their governments to take a stronger stance by implementing legislation to stop this tracking, but it could be possible they are quietly gathering this data for their own use also.

Figure-1.1. Basic RFID Transaction [3]

2. SECURITY ISSUES WITH CONTACTLESS BANK CARDS

The introduction of wireless technology, could potentially lead to the possibility of security and person data risks to users. The banking sectors and other industries involved with this technology are also a security risk with these technologies. This section will look closely at the security and person data threats involved when using a contactless bank card to pay for goods at the checkout. There are many ways to intercept a signal being emitted from these bank cards, one being eavesdropping. These contactless bank cards are fitted with a wireless RFID tag and are usually a unique identifier. During a transaction, there is a risk that the communication between the tag and reader could be eavesdropped. This can happen when an attacker intercepts data using basic equipment like an oscilloscope while a legitimate transaction is transmitted. Since almost all RFID systems use clear text communication, cause of tag memory capacity or costs, eavesdropping is a very effective way for an attacker to obtain the required information from these RFID tags. The apparent information collected during this kind of attack could have serious consequences for the card owner and the banks who the customer deals with. The data collected from eavesdropping can be saved for further analysis and could be used for cloning tags in the future.

A. Cloning

There are other methods where an attacker could potentially collect sensitive information from these cards. Cloning been one, as previously mentioned eavesdropping could be useful as the attacker can store the data and use it later to clone a legitimate RFID tag. Cloning is referred to copying data from a legitimate tag to a new tag owned by the attacker.

B. Spoofing

Spoofing is another form an attacker can use to copy tag data. Although similar to cloning it is different as spoofing is defined as duplicating tag data and transmitting it to a reader. A very simple form of spoofing would be to replace a price sticker with a cheaper one in your local. The information collected from the legitimate tag is transmitted to the reader from an alternative tag that is not the original RFID tag.

C. Jamming

Jamming being another method an attacker could use to obtain personal data. Jamming refers to deliberately disturbing the air interface between a tag and reader which in theory is attacking the communication between both the devices. This attack can occur by using powerful transmitters which paralyses the communication of the RFID tag and generating a frequency noise the same as the system been used [4].

D. Wireless Copying

Wireless copying being the most recent development with contactless bank card security and should be a warning to the consumer. The attacker with a modified smart phone is able to collect personal data by just standing next the victim. Details obtained are the account name, account number expiry date as well as the last ten transactions can all be viewed using these modified smart phones. The attacker does this by placing the smart phone within a short range of the victims pocket and retrieves the data with-out the victim even knowing they were targeted. The modifications to the smart phone can be bought online for as little as £30 with the risk to millions of bank card owners having their private data read by these phones, [5].

E. Contactless Bank Cards

Having the convenience of using a contactless bank card to pay for items is a major advancement in NFC technology. But with new technologies come risks and risks to sensitive banking detailed information been leaked. The public will certainly want a closer examination off these cards to make them more secure. It is clear there are communication risks when using these cards and using wireless communication systems only add to this. The threats highlighted so far could frustrate consumers more and could potentially find it difficult to trust this technology.

3. PERSONAL DATA

When Franklin Benjamin discovered over 200 years that electricity could in fact move through the air, he would never have predicted how it has evolved modern technologies in this era [6]. This technology is better known today as wireless communication. The advances this technology has seen in recent years are incredible. From having a wireless connection to the internet, wireless printing, to now being able to pay for goods using wireless technology built into bank cards. But as this technology has evolved the issues surrounding security never seemed to grab the headlines as wireless was fast, convenient and worked. But security issues surrounding contactless bank cards have been around for several years and it's not going away. Banks are issuing their customers with these cards and the consumers are using them. Britons have made 5.4 million contactless transactions per month in 2013. Consumers deserve to know exactly what information could potentially be stolen when an attacker tries to exploit these bank cards. The possibility of bank account details, expiry date, account number being transmitted during these attacks would be worrying to individuals. Many reports have highlighted some of these issues and have been forwarded to the relevant authorities for analysing [5].

A. Smart Card Alliance

While security remains an issue with these cards the smart card alliance web site does not provide comfortable reading to consumers either in relation to personal data protection. When reading through the heading "How do smart cards help to protect privacy?" the word "can" appears very frequent. For example the following has been quoted from the smart card alliance web site "*Smart cards offer a number of features that can be used to provide or enhance privacy protection in systems. The following is a brief description of some of these features and how they can be used to protect privacy*" it makes one think personal data protection on these cards is not a requirement and just an option [7].

B. Personal Data Protection

Stated in the guide to your data protection in Ireland, when you give your personal details to an organisation in Ireland they have a duty to keep these details private and safe. Organisations that hold personal details are called "data controllers" this for example would be a banking organisation. No one would be able to hold a bank account unless they give their information to these banks for them to obtain a bank account. Under data protection laws in Ireland individuals have rights regarding the use of these details and data controllers have responsibilities in how this information is handled. Data controllers who hold information about someone states they must: "get and use the information fairly", "keep the information safe" [8]. These points highlight just some questions the consumers will be asking their banks should their details be obtained from the list of threats previously mentioned in this paper when using contactless bank cards.

C. Cashless Society

The government and major banks are currently willing people to join businesses in Ireland and have them move to a cashless society although many consumers would have reservations about personal data protection. Data is been collected from consumers almost on a daily basis now and technology is helping to add to this stock pile of data. It's difficult to predict how a cashless society would work on such a large scale, consumers could be exposing themselves to further data protection issues which is always very likely in the early stages of any new technology. Currently a cashless society is been deployed between the government and businesses. Dubbed "e-Day" as of September 19th 2014 in Ireland the Government will no longer write cheques to businesses and will no longer accepts cheques from businesses [7]; [8]. In addition, The Central Bank of Ireland are launching a €1m campaign for their consumers and businesses to stop using cash and move to a more favourable method of electronic transactions, stating the move would "*save the economy €1bn per year*" [6]. A cashless society being adopted in Ireland could be a possibility and with the government and the central bank leading the drive, it remains to be seen whether it be adopted or not.

4. CONCLUSION

This paper has discussed many different security concerns, consumers should be aware of when inevitable they will be issued with one of these contactless bank cards from their respective bank. The conveniences of using these cards make it easier for criminals collect sensitive information without the consumer being aware. The security threats mentioned in this paper need further investigations by major bank card authorities like Visa and Master Card. The current regulations have several issues, but in the short term more security could be easily implemented by having the card physically make contact with the reader until the transaction is complete. This would result in the RFID tag only making communication through touching a reader, which possibly could reduce the changes of eavesdropping. There's also a better the chance that an enhanced smartphone would not collect sensitive data. What needs to be implemented are better security measures by both banking sectors and governments as safety should be of the most importance from a social aspect.

REFERENCES

[1] Atmel, "Understanding the requirements of ISO/IEC 14443 for type B proximity contactless identification cards." Available: http://www.atmel.com/images/doc2056.pdf, 2005.

[2] A. Alqhtani, H. Elmiligi, F. Gebali, and M. S. Yasein, "NFC security analysis and vulnerabilities in healthcare applications," presented at the Communications, Computers and Signal Processing (PACRIM), 2013 IEEE Pacific Rim Conference, 2013.

[3] C. Stamford, "Gartner says worldwide mobile payment transaction value to surpass $235 billion in 2013." Available http://www.gartner.com/newsroom/id/2504915, 2013.

[4] G. Kulkarni, R. Shelke, R. Sutar, and S. Mohite, "RFID security issues & challenges," *Electronics and Communication Systems ICECS*, pp. 1-4, 2014.

[5] B. Ellery, "How 30million 'wi-fi' credit cards can be plundered by cyber identity thieves exploiting contactless payment technology read more," *Mail*, 2013.

[6] R. Burke, "Central bank kicks off €1m campaign for cashless society, Independent," 2014.

[7] Department of Finance, "Launch of media campaign for e-day by minister of state at the department of finance Mr. Simon Harris, T.D." Available: http://www.finance.gov.ie/news-centre/press-releases/launch-media-campaign-e-day-minister-state-department-finance-mr-simon, 2014.

[8] Data Protection Commissioner, "A guide to your rights." Available: http://www.dataprotection.ie/docs/a-guide-to-your-rights-plain-english-version/858.htm, 2013.