PUBLIC PERCEPTION OF CARD SECURITY

Rajeshkumar Sundaram *{rajsu674@student.liu.se}*
Supervisor: Viiveke Fåk, {*viiveke@isy.liu.se*}
Project Report for Information Security Course
Linköpings universitetet, Sweden

Abstract

The report examines the public awareness of security risks associated with both magnetic stripe and smart cards. Both types of cards have been affected by similar as well as a few different kinds of threats. The report describes the different risks and defines the loss or effects to the users and shop keepers. The report includes a theoretical part about public awareness of card security, and a survey has been made to present a clear view of the situation. It ends with a final discussion compiled from the theoretical study and the survey results and presents the pubic views of each risk.

1. Introduction

In the current world credit cards are the primary means to buy all necessities in life like goods, services, etc. People think that this is a simple way to keep our assets safe. Magnetic stripes have been used in the credit cards to store and modify data [2]. But cards with a integrated circuit chip also called smart cards are popular and effectively used for processing data. Smart cards transfer information using the microprocessor rather than the magnetic stripe [1]. Smart cards can be reprogrammed to edit existing data according to our needs. Both kinds are mainly used for authorization, so security is a very important concern to be taken [1]. Smart card access is secured and controlled by a personal key. This is the key that is required when the card is being used for purchasing or other transactions. If the security of the card is the impossible to maintain, loss will be extreme. For example if the credit card is stolen and misused then the users would lose all their assets that they earned. Security issues for both types of cards, magnetic stripe and smart cars, are different [1]. User and shop keepers awareness to the issues are very important. Even though credit cards are important to day life, due to the security problems some shop keepers and users avoid using it. But we cannot say they are aware of all security issues. The best way to protect the card from fraud is public awareness. Increasing usage is also the reason for the increase of smart cards fraud which affects both the card holders and shop keepers. Understanding the security problem is the effective way of controlling this fraud rather than developing technical solutions. Even if we make a technical solution, in order to prevent complete frauds understanding public perception is essential. The user perception will be differing according to people and their business and their usage of cards. This report is mainly intended for understanding public views and for knowledge of card securities and awareness of the risks.

2. Background

In general when we talk about authorization the most important word is security. Likewise card security should be the primary issue to the card users. If the security fails then the entire usage of the cards should be reconsidered. Major attack to the magnetic card is skimming [6] where the card details are stolen and duplicated when it is swiped across the equipment. Once the PIN is copied, then entire card access can be controlled. It can be done using external equipment which copies the card information [7]. Money from the original credit card can be stolen using this clone card. So it is not suitable to have sensitive data. Smart cards are very hard to get attacked since all the processing is carried out by microprocessor itself. When a computer communicates the card, the microprocessor accesses all the data to send and retrieve information [2]. Smart cards are more reliable and allow storing large number of information.

3. Method

This section presents the methodology to be used for the report. The method is divided into a theoretical and a practical part. The theory is based on information gathering qualitative in nature, while the practical information based on the collection of quantitative nature and the results were compared and presented in the alaysis.

3.1 Theoretical Methods

First method of the report is literature study of the topic card security. Here complete knowledge of the authentication, list of risks involved with the card and their impacts are discussed by read different articles and online sources.

3.2 Practical Methods

In order to get quantitative data online survey has been conducted. Survey has the questionnaires presented to the card users and shopkeepers. The responses would be gathered and merged to find out user knowledge and awareness on card security. This is the best way to examine card security issues in width.

4. Risks associated with card

Several security issues are associated with the card. In 1998, Cryptography Research Inc. researchers announced that the attacks on the smart cards are called Simple Power Analysis (SPA) and Differential Power Analysis (DPA) [3]. SPA is one kind of attack that is used to observe a secret key by examining the power usage of the card. Power variation depends on different operations of the card [3]. After few readings, the power trace can be measure from the obtained data. DPA is a technique which extracts the secret key by statistically analysing their different power consumptions during encryption and decryption of the data. Skimming is the severe kind of attack to the smart card users same like magnetic stripe attack. The new device has been attached at top of the slot for ATM card swiping machine. Whenever the user swipes their card, the new device saves the card details. They capture the PIN number with the help of hidden cameras and then send alerts to the criminals [11]. These details are used to manufacture new card with the stolen details of the card. Money can be taken without the knowledge of the card owner with the help of the clone card. Online purchase is one of the popular ways of buy things where individual fraud on the internet is a severe problem for the online purchasers. Hacking the personal account is the expertise way of attacking individual account [5]. Biometrics technology is one kind of security method introduced to the cards. It takes a person physical features like finger print, voice recognition or facial image as a personal identification [12]. It was considered as one of the safest and convenient methods of purchase using credit cards. Timing attack is another kind of attack which affects cryptography to gain the secret key of the card. It attempts to analyse the time taken for cryptographic algorithms in order to penetrate the card cryptosystem [13]. Every operation takes some time to execute and it differs based on input and operations. Attackers attempt to measure this time to commit the attack.

In day-to-day life, it is very hard to identify DPA attack even it is processed by the algorithms RSA, DES, DSA, Diffie-Hellman. DPA bias contains two parts signal which contains the key information and noise [4]. In order to perform successful DPA attack, the attacker has to detect the signal of the card over the noise [3]. Here the attackers need to find the single signal from large amount of bias signals. The reduction of the noise energy is important to reveal the analysis of signals. It can be easy for attackers to make most of the attacks successfully. Skimming is new kind of attack that comes to know all recent card users. Public awareness is considered as important aspect to escape from attacks. During skimming, the card information is copied from card's magnetic stripe which is used to produce the clone card. Skimmer takes the advantage from the magnetic card because this is passive [10]. Magnetic stripes are not designed to secure this kind of attacks. In recent days, well secured active cards have been implemented by the advanced encryption techniques that cannot be skimmed. New anti-skimming techniques and devices have been introduced to protect the card from this kind of attack. Online security to protect hacking is still lacking in all the places. As soon as the new security schemes are introduced, the attackers find an efficient way to penetrate it by using latest technologies. The main problem about the hacking is there is no information that will help to find the criminals after the attack has been made online. When the biometrics was introduced, it was believed to be the enhanced and safe way to protect cards from attacks. But later, the disadvantages of biometric methods have been realized. If attackers hack the database, they can take over the biometric information and account number [12]. In the same way, the image of the person would be captured by using modern devices (mobile cameras or digital cameras) and the finger prints can be taken under many circumstances. These ways help the attacker to get access to the card. During timing attack, measurement of the time is used to leak the information based on different variables such as design of the system, algorithm, processor execution, timing attack attempt and its accuracy. Timing attack generally depends on implementation of the system, so the design phase is aimed for this attack [13]. This seems timing attacks are considered to be one of the effective ways of identifying secret key of the card to get illegal access.

5. Public awareness on card security

Cards became very essential for an individual to fulfil everyday needs. At the same time, they have to be aware of the risks involved on the cards. The bank cannot give assurance for 100% security to the card. So self-awareness is key point to escape from frauds. In the recent innovative world, for every new technology each security issues arise by advanced technology. So people cannot believe on technical solutions in order to prevent all attacks. People don't really distinguish passive cards and active cards, with little information security knowledge in mind, people turn to ignore the warnings and alerts from their card providers and thus they are exposed to the risks [2]. However, cards users do care about the risks once they are told about the details and they would like to take necessary steps to prevent hazards from happening. For example as we discussed skimming is the kind of attack get access to the card by fixing the external device on the card readers. Initially it happened in most of the restaurants, bars and some shops. But now many ATM centres are affected by this. In Sweden, skimming attack happened in gas stations especially where cards are rarely used. So people have to know about this and monitor very carefully while they pay. But few attacks cannot be prevented even though we are alert. Some shop keepers are not using the credit card payment due to such kind of attacks.

6. Survey

The survey focus on different kinds of people based on occupation, age, educational level, gender and how frequently they are using smart card type of credit cards. Due to the restriction of human resource and time, survey is mainly conducted towards shop keepers and consumers in towns along the journey as well as friends and relatives of the writers. The survey has conducted to the 8 people including 4 shop keepers and 4 users.

The questionnaire is in the draft as follow:

1. How many cards to you hold as a tool of verification and identification?

2. How many cards to you hold as a tool of verification and identification?

3. What are the card issuers?

4. Do you know the difference between a positive and negative card?

5. How many magnetic cards do you know you hold?

6. How many smart cards do you use?

7. Do you know that you are under threats using your cards?

8. What kinds of threat do you aware of using your cards? Please illustrate.

9. Where do you get the security information?

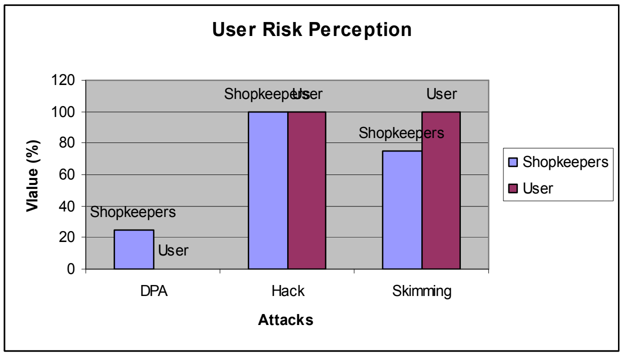
10. Have you/your friends ever get attacked in using your card?

11. After being told about some basic threats and risks, will you change your card using habit?

12. After being told about some basic threats and risks, will you reduce the number of your cards in hand?

7. Results

This survey results reflected that people were not completely aware of risks to the card and none of them had been affected by any attack. They mostly heard about the attacks from the news. In the survey, many people aware of the e-commerce risk, but at the same time they believe the security measures of the bank. From the shopkeepers' point of view, 25% of people know about the threat DPA. Others never heard about this kind of threat. Since hacking (e-commerce) is popular risk, 100% of the people have the basic knowledge about it. Skimming attack is done by the shopkeepers in many places. So 75% of the people has the knowledge about it even they didn't have any experience in losing money by skimming. When we look at the credit card users' point of view, none of them has the knowledge about the DPA attack. The ratio of hacking knowledge to the users are same like shop keepers. More than shopkeepers, users need to have more awareness of it because the risks are more to the users. 100% of users in the survey have the knowledge about skimming attack and they are aware of this attack, but only few people are cautious when they are paying bill in shops or restaurants. The people are not willing to change the number of holding credit cards even after they hear about the risks. Probably all the payment cards has both magnetic as well as smart cart chip. This is the results which obtained from the survey.



Pic 1

Pic 1 shows a graph that describes the results of the survey. Here the X-axis represents the three risks, first is DPA, second is e-commerce attacks, and third is skimming attack. The Y-axis represents the people awareness value for each risk. In the graph, each risk is plotted with two categories are shopkeepers and users plotted with columns that differentiated with colours.

8. Analysis

Many risks to the cards have been discussed and few have been taken to the survey. Public awareness of the card security is less than expected level. Most of the people do not care about the card security because they trust the card provider like banks. The results show that the skimming is the popular attack known to both shopkeepers and credit card users. This attack cannot be prevented by technical solutions. Hence public awareness is the only way to prevent the major part of the attack. The shopkeepers do not worry about this attack till they use their card users in other shops. But skimming in ATM machine is unpreventable even though we have knowledge about this attack. Because it looks like ordinary ATM machine till take to checking. DPA is very severe and innovative attack that the users can never predict. But 25% of the shopkeepers have the knowledge of DPA attack. Most popular attack to the users which gives 100% awareness is online fraud like hacking the card. Because it's not only happens to the card almost in on authentication areas. So people have more awareness when they use cards for online transactions and purchase. Most of the people delete the browser history after they have done their job and they keep the easy predictable passwords like first name, email address. They believe this is enough to prevent attacks and thinking this is the maximum level that they can do. The people knowledge of the difference between active and passive cards are the technology and how to use. They don't have any idea about the difference between cards risks. Recently smart cards are mostly provided by all the banks and many of them have the magnetic stripe too. Magnetic stripe cards can be sometimes damaged by external magnetic fields also it is not in a format that humans can read. Even though smart cards are more secure than magnetic stripe, high capacity and volatile memory to edit many shopkeepers avoid accepting it. First reason is that still it has the security problem that is not been completely resolved yet. Second reason is that many people don't trust these cards due to security issues. For example skimming attack is mostly done in many shops and public places. Next important reason is that the smart cards are cheaper but the card reader is expensive. So shopkeepers keep these reasons in mind along with the security issues and take decision to accept the cards. Some of the users don't want to use credit cards due to this security issues. As per the survey results, only a small ratio of people think like this. But the main reason for avoiding card usage is if the card cash details deleted by memory failure then who is liable: the bank or the person? In case the details are not recorded in to the database, then what would happen to the user? These questions are always comes to the people mind.

9. Discussion and Conclusion

The card security is the popular controversy in the recent days because of increasing usage of cards. The new developing technologies help to introduce new risks to the cards. Magnetic cards have been severely affected by skimming and more popular algorithms have also been attacked. Smart card has replaced the magnetic stripe card due to the cost and security reasons. But the smart cards also has few security issues hence the people cannot trust it fully. Smart cards have few popular attacks like Public perception to the cards security has got by survey. The survey has taken from 8 people with different categories including shopkeepers and card users. The survey concludes that the public awareness of the risk is less than average. Around 25% of people only have the knowledge about the different kinds of risks that affect the smart card security. Remaining people have the idea about only few of these risks. Surprisingly, the survey participants had never been attacked by any kind of threats as well as their friends too. The risks to the shopkeepers are less than the card users. For example skimming is all about how the user card is attacked while shopping. Also, they don't have the knowledge of security differences between active and passive cards, but technical difference is reached to many people. When we analyse the risks associated with the cards, every security method has its own disadvantages in some cases. They are not completely protecting the cards and we can say the cards are not 100% protected. Public awareness is the best way to mitigate the attacks. In order to increase public awareness, banks can help the customers to get to know the risks associated with the both type of credit cards.

References

[1] Thomas S. Messerges, Ezzat A. Dabbish and Robert H. Sloan, "Examining Smart-Card Security Under the Threat of Power Analysis Attacks", IEEE Transaction, May 2002.

[2] Umesh Shankar and Miriam Walker, "A Survey of Security in Online Credit Card Payments", May, 2001.

[3] Paul kocher, Joshua Jaffe and Benjamin jun, "Introduction to Differential Power Analysis and Related Attacks", Cryptographic research, 1998.

[4] Marijke De Soete, Sylvie Lacroix and Olivier Delos, “Study of user identification methods in card payments, mobile payments and e-payments – WP3 Comparison with previous 2003 study”.

[5] Thomas S. Messerges Ezzy A. Dabbish Robert H. Sloan, “Investigations of Power Analysis Attacks on Smartcards”, USENIX Workshop on Smartcard Technology, Chicago, Illinois, USA, May 10–11, 1999

[6] Mike Hendry, “Smart Card Security and Applications”, Second edition, 2001

[7] http://www.hightechaid.com/tech/card/what_ms.htm

[8] http://cobweb.ecn.purdue.edu/~tanchoco/MHE/ADC-is/Magnetic/main.shtml

[9] http://www.textboxdesign.com/ITSite/dwalsh/smartcards.html

[10] Harshil Kotecha, ”Using Smart Card Technology For Deploying Secure Information Management Framework”.

[11] http://www.icma.com/info/hypercom7801.htm

[12] http://www.creditcards.com/credit-card-news/credit-card-biometric-technology-1273.php

[13] http://en.wikipedia.org/wiki/Timing_attack