TDDD17 Project, Spring 2008

Magnetic Card Fraud – Can you do it?

David Eriksson

Supervisor: Viiveke Fåk

TDDD17

Magnetic Card Fraud – Can you do it?

David Eriksson
Email: david.k.eriksson@gmail.com
Supervisor: Viiveke Fåk
Project Report for Information Security Course
Linköpings universitet Sweden

Abstract

Every year more and more purchases are made by bank card transactions. At the same time the reports about card fraud are flooding the news. This paper first tries to describe the current situation of magnetic card fraud and what different types of fraud exist today. The aim of the paper is then to observe if everyone can perform card forgery by studying the tools and knowledge needed.

1. Introduction

Magnetic cards have been used in a wide range of areas (i.e. entry systems, cash machines) since it was developed some 50 years ago. However, it soon was clear that the security concerns were many.

This paper attempts to address the fraud impact from magnetic cards on society and organizations, and also identify what these attacks can be. But what do you need to acquire this necessary information, and can everyone achieve this? The last section of the paper investigates what information Internet can provide for this.

2. Research Questions

This chapter clarifies the research questions together with their delimitations and methodology. Each question is then addressed in its own chapter (chapter 3, 4 and 5) and then jointly in the conclusion chapter from the author (chapter 6).

2.1 How high is the estimated cost caused by magnetic card forgery for society and companies?

The question serves to answer how frequent and common card forgery is. Not by giving exact cost estimation, but rather pinpointing the current situation as a society problem. The subject will be addressed with a literature study, covering news articles to achieve an updated understanding of the current situation.

2.2 What are the different attacks of magnetic cards?

This question will focus on different types of magnetic card related fraud. Card forgery in E-commerce will be studied at a higher level since many skimming techniques are used for obtaining data for Internet use.

2.3 How difficult is it to obtain equipment for magnetic card forgery and what do you need?

This question tries to clarify what it takes for a normal individual to obtain both knowledge and tools for skimming. A field study of internet forums will be performed.

3. Magnetic Card Forgery – impact in daily life?

The use of debit and credit cards are becoming more and more frequent for shopping. At the age of 13 some banks offer you to get your own debit card. And almost every single one at an age of 18 uses his Visa or MasterCard credit card for shopping. At the same time the problems of skimming and fraud related to the magnetic cards are more frequent in the press. But how frequent is the forgery and how much money do we as normal citizens and organizations loose on this?

The trade in Sweden is estimated to around 420.000 billion of SEK per year, where as much as 57-58 % of all transactions are made with different kinds of bank cards. This makes the potential card forgery a very profitable industry even in a small country like Sweden [1].

Dick Malmlund, chief of security at Svensk Handel (Swedish Trade Association), states that they consider three types of card forgery; someone steel you physical card, internet hacking of card details and skimming.

According to Dick Malmlund a new case of skimming is reported every third day in Sweden. He also believes that the non-reported cases are many, especially since the banks are not interested in reporting more than necessary not to worry their clients [2]. This can be one of the reasons why it is so hard to get exact figures about bank card fraud. Another point is that the essence of fraud is to not be revealed, so therefore it is difficult to know the real sum since it hasn't been detected. According to VISA's own figures, the total amount of card forgery in Europe was 46 million Euro in 2007 [3]. This corresponds to an estimate from Dick Malmlund of 500 million SEK [4].

With increase of Internet transaction sites in Sweden one can buy everything from bus tickets to cars and DVDs [5]. Therefore the card details have been more useful for fraudsters. With just the card number and often, but not always, the CVV2 code (see chapter 5.3), you can buy whatever things directly from Internet without showing your face to a single surveillance camera or personnel. So the trend seems to be obvious: the card fraud is increasing together with the increase of E-commerce [6]. Back in 1996 in the United Kingdom, 62% of all fraud transactions were made with a stolen/lost card and only 7% were done where the card was not present in the purchase situation. Ten years later the situation is the opposite, 50% of the fraud transactions are made without the card and only 16% with a stolen card [7]. This view is also shared by VISA's deputy CEO Steve Perry, who says that the forgery in direct sales (using the card) is decreasing meanwhile Internet fraud with card details are increasing heavily [8].

As a user of different types of magnetic bank cards the future might look a bit brighter due to the increase of smart cards and use of PIN for authorization. In the United Kingdom all cash machines already have been upgraded from magnetic to chip readers, resulting in a decrease of cash machine fraud with 6% from 2004 to 2006 [9]. In Sweden the chip shall have replaced the current magnetic cards at the end of 2008. In 2010 all European countries shall have implemented the chip and also the PIN, which will be used for authentication instead of written signatures [10]. Today around 68% of Europe's total 359.000 ATMs are equipped with 'chip n pin' [11]. However, according to Superintendent Geir Hogstad at the fraud unit of Gothenburg Police Department, the change in Sweden goes slowly [12]. In the US they still haven't decided if they will implement the chip solution or not [13].

A recent problem related to card fraud is hacking of big databases containing millions of card credentials (i.e. banks and credit card companies). One year ago a problem like this was identified in Sweden, where a security hole was detected between the shops' terminals and the banks' transfer systems. Estimations show that hackers by this got their hands on tens of thousands of credit card numbers. When this was detected all affected customers got new cards from the banks [14]. This type of internet fraud pinpoints an old saying: a chain is never stronger than the weakest link. It doesn't matter if you replace the magnetic cards with smart cards and PIN, as long as you cannot guarantee the security of the databases containing these credentials.

4. Magnetic Card Attacks – what types are they?

There are many ways of getting hold of card information for fraudsters. In this area some of the most common terminology is explained.

4.1 Skimming

Skimming is a type of card fraud where you steel information used in an otherwise legitimate transaction [15]. A very common example is when you take out money from an ATM and someone reads your credentials without your knowledge.

Skimming is becoming more and more common as bank card transactions are replacing cash payments [16]. According to Marcus Qvennerstedt, coordinator of Financial Fraud at the Swedish Police Department, there are three main types of skimming.

4.1.1 Traditional skimming

By traditional skimming is meant that someone reads and copies your card in a purchase situation, i.e. in a taxi or at a restaurant. With a card writer device (see chapter 5) the fraudster then creates a copy of your card.

4.1.1.1 Cash machine skimming

A small card reader is placed on the cash machine in front of the real reader. When entering your card, the fake card reader extracts your information and stores it. If the fraudsters also want to obtain your PIN code, they often place a camera nearby to spy when you enter your digits. A more sophisticated way of obtaining the PIN is to install a fake keypad that registers what keys you are pressing.

Cash machine skimming is the most frequent type of skimming in Sweden [17]. Figure 1 and 2 shows a normal ATM and a manipulated one that was detected in Sweden earlier this year.

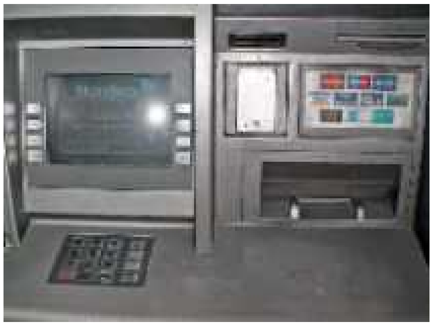

Figure 1: Normal ATM

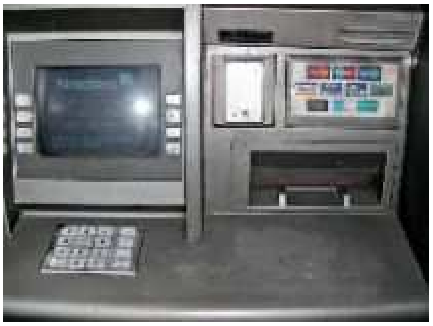

Figure 2 – Manipulated ATM (fake card reader and key pad)

4.1.2 In store skimming

By in store skimming it is meant that the salesman use your card twice without your notice. Some cases have also been identified where thieves have installed own card readers without the salesman's notice.

4.2 Phishing

Phishing is more related to obtaining secret information and is not necessarily related to card fraud. The idea is to trick the victim to enter his card credentials. This can be achieved by sending him a URL similar to his normal Internet bank but it is only a duplicate and the fraudsters receive all the information instead of the bank [18].

4.3 Carding

Carding is a term used for verifying the validity of stolen cards. The fraudsters enter the card information on a site which has real-time transaction processing. If the card is processed successfully, that confirms that the card is still good.

In the past these terms also covered the possibility of using "generators" of credit card numbers and then test them to see which were good. With the launch of CVV2 codes, this possibility was heavily reduced. Today carding is typically used for checking that the card credentials you have obtained by skimming or phishing are correct. [19]

5. Magnetic Card Fraud – Can you do it?

After seeing that there is a big market for potential magnetic card fraud and clarifying the terminology for these fraud cases, we have now reached our last question: Can you do it?

Let us go trough what equipment you need and what knowledge is available.

5.1 The equipment

The first thing you need is the tool to read the magnetic card data; a card reader.

First choice for searching after this information is of course Internet. When entering "*magnetic card readers*" I immediately get more than half a million hits. First hit after the sponsored ones is a page called "www.hackershomepage.com", which of course triggers my interest for this essay. Today they have a special offer for a "must have" card reader/writer which reads all three tracks. Included in the price you also get some computer software to encode/decode all information on the different tracks. It is described how to use it; one swipe to read the card, all information will be shown on your screen and a final swipe to copy it to a new card. For 499,99 USD this reader will be mine and I will also get ten blank cards included. Blank cards can also be bought on several sites at a price of around 3 USD/unit for 3 track cards with signature panel.

Figure 3 – Magnetic card reader/writer (MSR206)

Getting hold of a card reader doesn't take more than a week and can be ordered from a huge amount of different Internet sites. For just a reader the price seems to be around some 500 SEK, and to also get the writer capabilities you need to pay around 1000 SEK or more. After just some hours of googling I can without doubt confirm that the supply is big.

However, it isn't necessarily needed to buy from Internet. According to Svenska Dagbladet many supermarkets are selling card readers/writers today, which is not appreciated by the Swedish Police. They say that the purpose in many cases is clearly criminal. Today all you need in order to buy a card reader/writer in a shop is to show your organization number [20].

Even though it looks easy to obtain the right equipment it is however not completely without risk. If you have software together with you reader that can be used for illegal actions you can be arrested by the Swedish Police for preparation of fraud, according to Stig Sandgren at the Swedish Police fraud unit in Stockholm [21].

To obtain a standard card reader/writer looks doable but what about readers that are sophisticated enough to be used for ATM skimming? From my field study I have found a couple of readers that I believe would be possible to use. One example is the MSR41, which is a portable reader that can store up to 3.000 records and with a rechargeable battery that lasts up to 55.000 swipes. It has a USB interface to transfer the information to a computer. It also stores a timestamp for every swipe which is useful in skimming attacks since you can synchronize it with a keypad or camera for relating the card with the introduced PIN. These portable readers tend to be a bit more expensive than the standard ones. The MSR41 costs 199 USD. However, I believe that rigging an ATM would be difficult without some modifications of the readers. Many banks are now also trying to protect themselves from skimming by putting spikes around the real card reader to make it more difficult to rig the fake reader. But according to Kaj Hahne at Swedish Police fraud unit in Stockholm, new tools are detected constantly. Lately very thin readers, only some millimeters thick, have been detected by the Swedish Police [22].

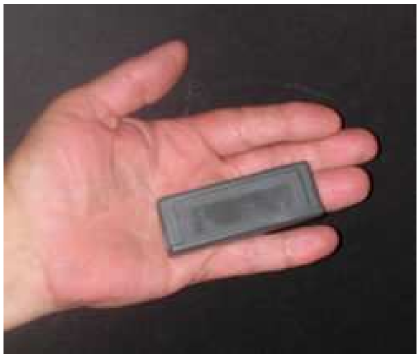

Figure 4 - MSR41 portable card reader

If you want to use your copied card in public, you can also buy plastic card printers to personalize your cards. These can be a bit more expensive since most of them are for business use and not for individuals. The price for this kind of printer is about 10.000 SEK. Even so, many bank cards are personalized in a way that will not be very easy to copy. One must not forget that the real personalization of the card also has its anti-fraud protection, i.e. holograms as the one on the VISA card below.

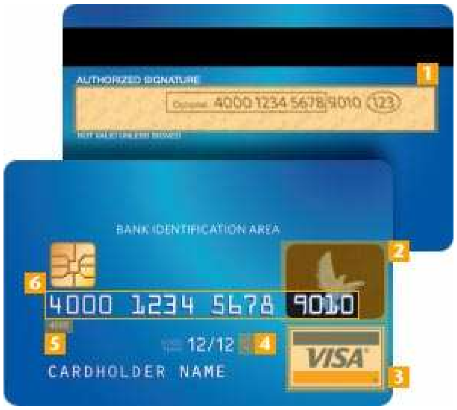

Figure 5 - Personalized bank card from VISA

5.2 The knowledge

Once the equipment arrives, your next step will be to learn how to perform this forgery. In this section the author only presents what you will have to learn and if it is easy to achieve this knowledge. No instructions will be given since it could encourage people of trying this, which is considered illegal.

Stig Sandgren states that after buying the reader, there are no difficulties to download excellent skimming guidelines from Internet [23]. However, from my field study of different Internet sites I can conclude that it is not as easy as expected. There are many forums with discussions about skimming but real guidelines are harder to obtain.

An essential knowledge before you launch your attack is to know what information you are likely to catch when reading the card. Especially one interesting item is if the printed card number also exists on the magnetic stripe. Obviously there is no real need for having it included on the magnetic stripe since the banks can use a different number internally (compare the account number that is linked to a debit card). But it might just be there anyway. With the increase of Internet attacks of card information this issue is becoming very important. If the printed card number doesn't exist on the magnetic stripe, the possibility of combing skimming and Internet related fraud is limited. From a skimming attack you will then never get what is printed on the card, which is vital for e-commerce. The same logic applies on phishing attacks were you most likely will get the printed number but not the magnetic stripe information. Hence you will not be able to create any fake cards.

In this paper it has not been possible to confirm whether the printed number also is written on the magnetic stripe. A field study of some Internet forums gives no clear answers about it and only a few threads address this.

5.3 The attack

Once you have the equipment and knowledge needed, next step is to get your magnetic card for copying. As we have seen in chapter 4 there are different possibilities for this, other than just steeling a wallet.

The easiest type of skimming is most likely the traditional way, where you just need to get the card from its host for some seconds in order to swipe it through your reader [24]. Setting up cash machine skimming equipment would be more expensive and time consuming. From chapter 5.1 it was also stated that it is not very easy to get a reader ready to be installed on an ATM. Nevertheless, if you can do the set up for a skimming attack, you are more likely to collect the PIN then through traditional skimming where the victim often just validate with a signature.

In order to create a usable copy of the card, you often need the CVV2 number (Card verification value). This is not printed on the magnetic stripe so you will not capture it by reading it. This feature is meant to decrease the fraud where the card is not present in the purchase situation (i.e. E-commerce). So if you don't manage to capture the CVV2 you will most likely have problems using the card on Internet. However, both phishing where you trick the card owner to give away his CVV2, and hacking merchant databases, have reduced the CVV2 as an anti-fraud feature [25].

It is often enough if you collect the card information in order to get some share of the money. There are several sites on Internet where you can sell the card data to the highest bidder [26]. A big Internet auction site was recently detected where one could sell and buy stolen card credentials to the highest bidder. For a complete set of card credentials the price was 38 USD but if you bought bigger quantities you were given discount! [27]

6. Conclusions and reflections

As we have seen in this paper there is a big market for magnetic card forgery in Sweden today with new cases of skimming reported every third day. However, it looks like it will decrease during the upcoming years with the introduction of smart cards. On the other hand it will take a long time before the whole world will have the smart card and its readers in place. Even when it is implemented in Sweden or even EU, you could probably just cross the border to many other countries that will still use the magnetic stripe. Since this paper focus on magnetic cards rather than smart cards, it is difficult to predict the evolution of whole bank card forgery. Nevertheless the increasing numbers of card transactions and e-commerce will probably continue to attract fraudsters to card forgery.

We saw that there are plenty of ways to get the necessary card reader/writer of magnetic cards from Internet and that you can even buy it in Swedish supermarkets. If an organizational number is all you need and no extra check is made, you can have the equipment the same day you decide to buy it. It might be a bit harder to actually rig an ATM for a skimming attack since tailor made readers probably are needed. The banks often also use spikes to prevent fake readers from being installed. One must not forget that it is considered preparation of a crime if you are caught with a reader and suspicious software for cloning cards.

A very interesting concern applying not only to magnetic cards but also to all kind of cards is the hacking of merchant databases. This tends to connect Internet/network securities with card security. Magnetic cards have been criticized for their lack of security. However, improving card security meanwhile your card credentials are being hacked while you still have the card in your pocket really shows the difficulties in securing end-to-end processes. As stated in chapter 5.2, this paper couldn't confirm if the printed number also exist on the magnetic stripe. By separating the printed number from the one at the magnetic stripe, you would easily reduce possibilities of making false cards from database hacking.

If you really want to commit card fraud we have seen that the tools and knowledge are available for almost everyone. However, one has to answer one question before starting:
Would you dare to buy the card reader on Internet with your own credit card?!

References

[1] SVT Nyheter – Skimning oroar Svensk Handel
Published: 2006-05-26
http://svt.se/svt/jsp/Crosslink.jsp?d=53277&a=598209&lid=senasteNytt_611539&lpos=rubrik_598209

[2] Aftonbladet – Löning, då slår det till;
Published: 2006-02-27
http://www.aftonbladet.se/nyheter/article356881.ab

[3] E24 – E-handel ökar kortbedrägerier
Published: 2008-01-29
http://www.e24.se/pengar24/dinarattigheter/konsumentratt/artikel_219595.e24

[4] SVT Nyheter – Skimning oroar Svensk Handel
Published: 2006-05-26
http://svt.se/svt/jsp/Crosslink.jsp?d=53277&a=598209&lid=senasteNytt_611539&lpos=rubrik_598209

[5] Dagens Nyheter – Dyrare varor köps på nätet
Published: 2007-09-05
http://www.dn.se/DNet/jsp/polopoly.jsp?d=678&a=688859

[6] E24 – E-handel ökar kortbedrägerier
Published: 2008-01-29
http://www.e24.se/pengar24/dinarattigheter/konsumentratt/artikel_219595.e24

[7] APACS – Fraud, the facts 2007

[8] E24 – E-handel ökar kortbedrägerier
Published: 2008-01-29
http://www.e24.se/pengar24/dinarattigheter/konsumentratt/artikel_219595.e24

[9] APACS – Fraud, the facts 2007

[10] E24 – Bästa skyddet mot skimning
Published: 2008-02-28
http://www.e24.se/pengar24/dinarattigheter/konsumentratt/artikel_290251.e24

[11] Banknet - ATM fraud losses down 55% in Europe due to EMV adoption
http://www.banknetindia.com/banking/71124.htm

[12] Dagens Industri – Poliskritik mot bankerna
Published: 2008-02-27
http://di.se/Nyheter/?page=/Avdelningar/Artikel.aspx%3FO%3DRSS%26ArticleId%3D2008%255c02%255c27%255c272523

[13] E24 – Bästa skyddet mot skimning
Published: 2008-02-28
http://www.e24.se/pengar24/dinarattigheter/konsumentratt/artikel_290251.e24

[14] Dagens Nyheter – Tiotusentals kontokort byts ut
Published: 2007-05-09
http://www.dn.se/DNet/jsp/polopoly.jsp?d=678&a=648229

[15] Wikipedia - Skimming
http://en.wikipedia.org/wiki/Skimming_%28credit_card_fraud%29#Skimming

[16] Svenska Dagbladet - Bedragare slår till mot tankomater på bensinstationer
Published: 2008-03-24
http://www.svd.se/nyheter/inrikes/artikel_1010909.svd

[17] Svenska Dagbladet - Bedragare slår till mot tankomater på bensinstationer
Published: 2008-03-24
http://www.svd.se/nyheter/inrikes/artikel_1010909.svd

[18] APACS – Fraud Fact Pack

[19] Wikipedia - Carding
http://en.wikipedia.org/wiki/Credit_card_fraud#Carding

[20] DagensPS – Kriminella köper utrustning till skimning – på varuhus!
Published: 2008-03-06
http://www.dagensps.se/article.aspx?articleID=37669 &categID=193

[21] DagensPS – Kriminella köper utrustning till skimning – på varuhus!
Published: 2008-03-06
http://www.dagensps.se/article.aspx?articleID= 37669 &categID=193

[22] Svenska Dagbladet - Bedragare slår till mot tankomater på bensinstationer
Published: 2008-03-24
http://www.svd.se/nyheter/inrikes/artikel_1010909.svd

[23] DagensPS – Kriminella köper utrustning till skimning – på varuhus!
Published: 2008-03-06
http://www.dagensps.se/article.aspx?articleID= 37669 &categID=193

[24] Aftonbladet – Löning, då slår det till;
Published: 2006-02-27
http://www.aftonbladet.se/nyheter/article356881.ab

[25] Wikipedia – Card Security Code
http://en.wikipedia.org/wiki/Cvv2

[26] Dagens Industri – Poliskritik mot bankerna;
Published: 2008-02-27
http://di.se/Nyheter/?page=/Avdelningar/Artikel.aspx%3FO%3DRSS%26ArticleId%3D2008%255c02%255c27%255c272523

[27] IDG – Nätgalleria med stulna kortuppgifter avslöjad
Published: 2008-03-27
http://www.idg.se/2.1085/1.152592