Chip and PIN is Broken –  
a view to card payment infrastructure and security

Petri Aaltonen
The card payment infrastructure key players are card issuers, card holders, points of sales and acquirers. The EMV (Chip and PIN) was designed and marketed among other things as counter measure for most common types of frauds possible using the (pre)-existing card type - which utilizes a magnetic strip to hold the relevant card and card holder information.

EMV protocol defines among other things how a smart card with a chip interacts with the point of sale or cash terminal. The cardholder is identified usually by verifying a four-digit PIN code which is done inside the smart card chip vs. the magnetic strip where the merchant would for example compare the signature on the back of the card and the signature on a receipt, perhaps asking for additional identifying documentation to make sure that a given card belongs to the person trying purchase goods or services.

There are significant technical differences between these two methodologies as well as the changes in liability of a fraudulent transaction (liability shift).

It has been proposed that there are significant flaws in the EMV (Chip and PIN) protocol.

An attack exists where using a generally available hardware and common tools an attacker can mount a man-in-the-middle attack on the smart card and point-of-sale terminal so that it seems to the merchant that a PIN was used to verify the transaction when actually any four numbers will work. From the Issuers point of view it seems that the transaction is completely legit and it remains as the responsibility of the card holder to dispute these kind of transactions.

ACM Computing Classification System (CCS):

K.4.4 [Electronic Commerce],
K.6.5 [Security and Protection]
Content:

1  Introduction  1

2  Payment Infrastructure  3

3  EMV Protocol  5
   3.1 Card authentication................................................................. 6
   3.2 Cardholder verification........................................................... 6
   3.3 Transaction authorization...................................................... 6

4  Attack on Broken EMV  7
   4.1 Attack Demonstration........................................................... 8
   4.2 Causes and Solutions............................................................. 8

5  Conclusions  10

References  11
1 Introduction

The payment infrastructure consists of Card issuers, e.g. banks and credit institutions, Cardholders e.g. individual consumers, Payee's payment terminals e.g. a merchant's point of sales and Acquirers who gather the card transactions e.g. Luottokunta in Finland [FBA06].

Card frauds have existed for as long as payment cards have been in use and as in all payment related industry, there is an ongoing race between the card payment infrastructure stakeholders and those who wish to take advantage of the weaknesses in the system in order to gain criminal profits.

![Image of fraud statistics on UK issued cards]

[Figure 1: fraud statistics on UK issued cards (MDA10)]

In United Kingdom alone the losses from different kind of card frauds was estimated to be over 700 million pounds on year 2008 alone. The statistics show a steady rise of about 100 million pounds every year since 2005.

The payment industry key players introduced a new smart card based payment card solution which was widely adopted in Europe from 2005. This standard is called EMV according to the key players originally involved in the development, Europay, Mastercard and Visa.

This new card type based on an integrated circuit or a chip on a card is supposedly much more secure in many ways than the old magnetic stripe. For example, when using the magnetic stripe card the merchant would compare the signature on the card and the customers signature on the payment receipt. The EMV card can verify the PIN code stored inside the smart card against what was entered at the time of purchase – even if there is no online connection to the Issuers system.

However, the EMV chip cards are not without problems and there are ways to fool the payment terminals so that any PIN code may be entered. It seems that the transaction is legit even if an online point-of-sale (POS) terminal was used [MDA10]. This is especially problematic from cardholders point of view as along with the new EMV protocol, there was also a shift in liability. When using the EMV card the cardholder is responsible for keeping the PIN safe, and if the PIN is lost and then
criminally used, the card issuer can say that the cardholder was negligent and therefore responsible for the misuse of the card – and it remains for the responsibility for the cardholder to prove if this is not the case. Needless to say, this is worse from the cardholder (consumer) point of view, as with the old magnetic stripe cards the banks and merchants carried most of the risk regarding card misuse.

Currently in Finland there are 13,4 million payment cards issued which are used about one billion times in a year with a total worth of around 36 billion euros. The total amount of payment terminals in Finland alone is 176 thousand. [FFS10].
2 Payment Infrastructure

First we need to take a look at the payment infrastructure. In this seminar report we will not go into details about the finer points of the system, but it is important to understand where the man-in-the-middle attack discussed later happens in the big picture.

Also it is good to see how many different participants are in this eco-system and realize that there are many areas where the infrastructure may be weak – achieving total security over the whole system may be difficult and expensive.

Everything starts when a potential cardholder contacts the Issuer, who is marketing their card products for use. The card issuer receives the application and decides based on their own investigations and risk assessments if the applicant should be issued a card or not.

Just as a side note, this is where a successful identity theft could be used to obtain a card and PIN without the the knowledge of the individual who's identity is being used – and use the card to it's limit before the fraud is noticed.

After receiving the card and PIN code the Cardholder may use the issued Credit or Debit card in any point-of-sale or an ATM to purchase goods and services or to withdraw money. From the payment terminal, which may be purchased or leased by the merchant, the transaction is transferred to the Acquirer. This can happen every day, many times a day or maybe once a week if the merchant is not in a too much of a hurry to get the money from the goods they have already delivered. Once a day is usual. Because of the fact that any Visa card for example from anywhere in the world, issued by any bank with the appropriate licences may be accepted at the point-of-sale, an acquirer service is needed. The merchant does not know which Issuing bank for example to contact in order to get the
money from the service provided, so Acquirer is therefore needed to get all the card transactions from all the merchants and routes the transactions to the different issuing banks via direct connections or dedicated payment networks like the Visa-network.

Once the transaction is received by the bank who issued the card, the cardholder is then billed, usually the statements are generated once a month. The merchants usually receive their money sooner though, within days after the purchase has been made. The credit card cardholder pays the bill only maybe weeks from the purchase. If the purchase is done with a debit card, then the cardholder account is adjusted at the bank once the transaction arrives instead of via a monthly billing cycle.

In our paper we will next investigate what is the weak point for the man-in-the-middle attack. This part is illustrated in figure 3 on top-right corner, where the cardholders card and the merchants terminal interact.
3 EMV Protocol

The EMV protocol is both a protocol suite and a proprietary protocol framework. This means that from the merchants and terminal manufacturers points of view, they simply comply with the framework without exactly knowing how different options in the protocol are used. Depending on the card program and Issuer, different parameters, cryptographic algorithms, allowed authentication methodologies and so on may or may not be utilized.

In the same EMV chip there may be different programs (or applications) available for use. This makes it possible to put a Visa Credit card and Visa Debit card on a same chip. Technically it should be possible to put a Diners Club and American express there as well, but maybe there exists a conflict of interests preventing this. But all our credit and debit card needs could be put on a single EMV chip and the need to carry around many different plastics would not exist.

As said, in an application, the authentication methods may vary. Depending on the conditions under which the purchase is made, it is possible to force the use of online PIN verification, as is done with the ATM cash withdrawals. Or it is possible to allow the transaction without any verification at all, for example when we use our credit card at the entrance and then at the exit of a car park. Without going into too much details, there are many degrees between these two which are a) allowed and/or b) preferred authentication methods depending on where the card is used and under which conditions. These conditions include but are not limited to the place where the card is used, the terminal capabilities and the amount of the purchase.

In order to better understand the EMV protocol, we need to enumerate the three phases of the protocol, which are card authentication, cardholder verification and transaction authorization.

![Figure 4: The EMV protocol run phases (MDA10)]
3.1 Card authentication

As said before, the EMV smart card may contain many separate applications, commonly in modern cards Issued in Finland these are Credit and Debit applications of the same card scheme on the same chip. Each application can be with its individual cryptographic keys and other parameters.

First the point-of-sale terminal finds out which applications are supported by the card and after a selection of an application – like Visa Credit, proceeds into Get Processing Options -phase. After this the terminal reads card details with the Read Records -command which include the card number, RSA signatures, certificate chains and the card scheme root key.

As an interesting side note, in the UK all bank issued credit cards prior to 2009 were a subtype (static data authentication – SDA) where the card was not able to do any cryptographic operations, which lead into a situation where it was easy to use a stolen card to create a 'yes card' which works with any PIN code. These cards do not fortunately work well if the terminals are online. The later cards are capable of performing cryptographic operations dynamically (DDA) and are more safe to be used in an offline terminal. Both of these cards though are vulnerable to the man-in-the-middle attack discussed later, but this is mentioned here to emphasize the fact that the EMV has had it's problems in the past too.

3.2 Cardholder verification

After the application has been selected we now need to verify the cardholder. The terminal and the card negotiate this by iterating verification methods from Cardholder Verification Method (CVM) list. Here it is stated which verification methods, under which circumstances and in which order may be used to verify the cardholder. Depending on the selected verification method, there might be different outcomes in the fees the merchant pays for the Issuer or the liability of the transaction, for example, if a signature is accepted instead of PIN code, the liability for the transaction validity may be shifted back to the merchant even though an EMV card was used.

In most cases, the PIN verification is required and here the customer then enters the PIN code into a PIN pad or similar PIN entry device. The card receives the PIN code and internally verifies if the PIN matches the one store to card, and returns a code (0x9000) if the PIN is correct. If not, a failure code indicating how many PIN attempts remain before the card is locked is returned instead. This is called offline PIN verification and must not be confused with ATM transactions, as they use online PIN verification. In an online version of the PIN verification the ATM encrypts the PIN and sends it to the Issuer over the payment network and the Issuer then centrally verifies the PIN and gives the response back to the ATM. Therefore this man-in-the-middle attack will not work on an ATM.

3.3 Transaction authorization

Finally the terminal asks the card to generate transaction details which are eventually send to the Is-
suer. This data includes among other things type code, transaction identifier code, card generated data and a MAC calculated over the rest of the message including a description of the transaction using (typically) a shared symmetric key and 3DES.

The Issuer receives this information and then according to it's own analysis based on details like is there any money left in the credit bucket of this card to various risk assessments, black lists, where was this card topologically used and for how long time ago (is it possible to physically use the card now here as I saw it last time 10000 km away and that was only an hour ago) decides if the transaction is allowed or not and then returns the result code.

Now that the terminal knows that both the Card and the Issuer thinks that the transaction is valid, it asks the card to generate a transaction certificate which is then send back to the issuer and stored by the terminal, prints a copy to the cardholder with the 'verified by PIN' message. Offline terminals work differently, but this online version is more complex and therefore iterated here.

4 Attack on Broken EMV

Now that we have some idea about the infrastructure and how a typical protocol run works with an online point-of-sale (not to be confused online PIN verification), we are now able to see how it can be misused using a man-in-the-middle attack.

The flaw is between the card and the terminal (as said before), or more specifically in the PIN verification step. You see, the PIN verification is never authenticated – when the Terminal Verification Results are send to the Issuer, we do not send information about which verification method was actually used, only which are possible to be used and what was the result.

In the attack we simply put a device in between the terminal and the card which can intercept and modify the records passed to and from the card. We fool the card to believe that actually the terminal did not support PIN verification and a signature is used and fool the terminal to think that the PIN entered was valid. Since the response we get from the card which we send to the Issuer does not tell which method was used, only the result, everybody seems happy and the Issuer has no way of detecting any problems and at the point-of-sale the merchant is happy to see PIN OK message on their terminal. In an offline version there is even less possibilities to detect any problems as the issuer is not contacted at the time of the sale, the man-in-the-middle attack can actually substitute any messages – which will be of course evident once the terminal is online, but by now the purchased goods are far away.
4.1 Attack Demonstration

The man-in-the-middle attack discussed here can be demonstrated using using relatively low cost hardware and some python script which is running on a laptop. All other communication is here left unaltered, but once the terminal issues the Verify -command, the script stops this from going to the card and instead sends the terminal the PIN ACCEPTED -code (0x9000).

Although in this demonstration the hardware is quite large, a miniaturized version could be easily created with moderate effort [MDA10].

4.2 Causes and Solutions

The root cause of this problem is, that the cardholder authentication method used during the protocol run cannot be verified either by any party. Therefore EMV framework may be consider to be flawed. It is however possible for the issuing banks to implement countermeasures in the future to prevent this, as the EMV framework allows for the implementation of issuer specific proprietary schemes. This will have it's drawbacks as adding more complexity into the authorization systems will make it more difficult to ensure backward compatibility, therefore this option will be difficult and expensive.

When the EMV was designed, there were several security design related anti-patterns which can now be observed in order to understand why this kind of attack is now possible. For example, the design process was done in a closed environment and no external review of the architecture and protocols was done. Eventually the protocol documentation did 'leak' into the public domain as it was not possible to make sure that all implementing parties involved (20000 banks alone) would keep it a secret. But this happened so late, that the research community could not give timely feedback on the specification work. Additionally the fact that the specification itself is large and complex and poorly structured had it's hand in the reason how this kind of flaw may have been left undiscovered until re-
cently. The EMV protocol core documents are 707 pages, with 2126 pages of testing documentation, on top of which there is the card scheme specific documentation. In Visa case the public documents are 810 pages and it is not known how much non-public documentation is made available once the non-disclosure agreements are in place. Security related details are not gathered in one part of the document, but rather scattered across the whole bundle. Actually the EMV specification itself – even if followed to the letter including the optional recommendations does not produce a secure protocol implementation [MDA10].

There is no easy way to fix this problem in one go. There needs to be a method where either the card or the issuer can determine which cardholder verification method was actually used, instead of just a list of possible verification methods. Then the inconsistency of what was thought to have been used and what was actually used could be detected. This would mean that the Issuer who takes this measure would need to re-issue the whole of their card base before the attack can be effectively countered. And it would mean that the Issuer would generally accept that there is a significant flaw, which is something that the industry is reluctant to admit – as we know, if the trust of the general public has on the payment systems is gone, the costs for fixing the system and returning the trust can be quite significant.

Even if this one problem is somehow fixed, it is likely that more problems are found and exploited. The card fraud statistics show that since the EMV was taken into use, the fraud has not actually disappeared, but is generally on a steady rise. There could be many reasons for this, for example the amount of card transactions rise every year, so cumulative losses rise even if the relative losses remain the same. The monetary value probably goes up just because of inflation alone.

In any case, the next version of the EMV needs to be designed on a more open forum so that the thread model, security policies and protocol specifications can be reviewed in an open domain.

It should be noted, that once this man-in-the-middle attack was published, it did face criticism, some more valid than other. One such response from EMVCo states that this attack can already be detected, is very limited to only a subset of transactions and proposes high risk of getting caught for anyone attempting to exploit it [EMV10].
5 Conclusions

The purpose if this report was to introduce the current EMV smart card based payment infrastructure as it is widely adopted and continues to replace the existing magnetic strip based payment cards. Additionally the purpose was to understand and underline that card frauds have not gone anywhere with the EMV smart cards – some could justifiably argue that the frauds are increasing.

If this is directly related to the EMV standard or not cannot be said.

In this paper we refer to a relatively new and easy to mount man-in-the-middle attack as one example where the protocol weaknesses may be exploited by compromising the data traffic between the card and the terminal. We discuss the underlying root causes for this weakness and iterate some potential solutions as outlined in [MDA10].

From security point of view, it is important to understand that a payment ecosystem such as is in use with the EMV protocol has many potential weak points. In order to understand these different parts which work on very different domains from computer science standpoints a very broad understanding is needed from network protocols to cryptographic algorithms, threat and security models, programming languages and so on. Total security is not easy to achieve but given an open enough design processes for the future payment systems a reasonable level where the costs meet the benefits in most efficient way may be achieved.

It should also be understood, that change is difficult to achieve in the said payment ecosystem. There are no reasons for the major stakeholders to change the current implementations. Due to – among other – the successful liability shift towards the consumer, costs and image reasons. The consumers are in worse situation that with the magnetic strip cards and only once the consumers join forces and demand a change to better anything will happen.
References


