Providing Security to Debit Cards Using Message Authentication

Moshina Priyadharshini[1], Arokiaraj Jovith.A[2]

[1]*Department of IT- Information Security and Computer Forensics, SRM University, Kattankulathur, Chennai, T.N., INDIA*
[2]*Department of Information and Technology, SRM University, Kattankulathur, Chennai, T.N., INDIA*

Abstract- **Authentication require two or more factors: "something only the user knows", "something only the user has" and "something only the user is". The factors must be validated by the other party for validation to occur. In debit cards authentication mechanisms which can be easily cracked using different mechanisms. According to US attorney report at least 7,000 fake identities are used to obtain more than 25,000 credit cards and documented $200 million in losses, but the figure could rise. The present authentication mechanisms use mechanism where we enter our PIN in pos (point of sale) devices where it is vulnerable in case if we have any skimmer devices installed in any one of the component. Sometimes we have to enter OTP (one time password) in card reader, but it's vulnerable in case of lost or theft of both mobile and card together. In proposed method, GSM mobile service is used provide the security. When the Debit card is used, Server will request user to enter a password in his/her mobile phone. If the password valid, Server proceeds the transaction, if not so, denies it. The proposed solution effectively prevents clone cards and relay attacks on Debit cards using mobile phone authentication through the flash message service. The proposed solution effectively prevents clone cards and relay attacks on Debit cards using mobile phone authentication through the flash message service. This methodology can be implemented with the current system.**

Keywords: **Flash SMS ,Clone cards, Payment Gateway, Card Skimming Attack, Relay Attack**

I .INTRODUCTION

Existing system - For some debit cards, we do not have any security mechanisms, we just swipe those cards and make the transaction. This system is highly vulnerable for all attacks, now a days security is added to these cards that we have to enter the PIN in card reader, but its vulnerable to relay attack which makes duplicate transactions and may leads the cards to be skimmed when they are swiped on malicious, For few other cards , we have to enter OTP in card reader, but it's vulnerable in case of lost or theft of both mobile and card together.

Proposed system - In proposed method, flash message mobile service is used provide the security. When the Debit card is swiped at terminal, the transaction information send to visa server through acquirer bank and with an authentication normal procedures. Visa server will request user to enter a password in his/her mobile phone through the mobile network. If the password is valid, Server proceed the transaction towards the card holder bank and checks availability of required amount then flow of the transaction is as usual, if the password is not valid, server denies the transaction and lets the merchant and user to know that the transaction is denied. So this method can resolve three drawbacks in existing system first case if a card is cloned and swiped at some terminal, anyway the request for password to original owner of the card, he/she can know this transaction is not done by them and they can decline the transaction. Second case, if relay attack happens in a transaction, the user will be requested for password to perform a parallel transaction also, so he/she can avoid duplicate transaction. In third case, if the mobile phone and card are lost together, no one can make any transaction because the password is not known to any one other than original user

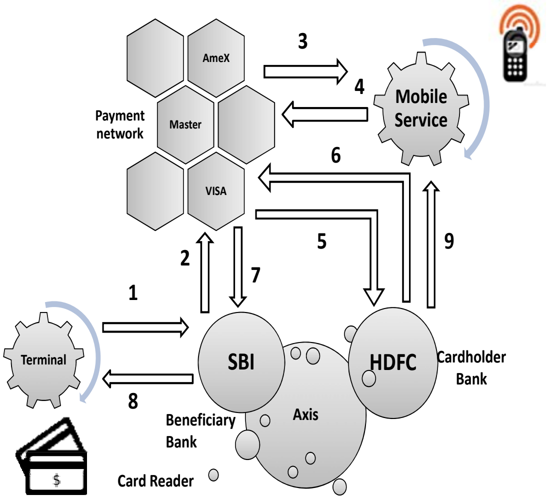


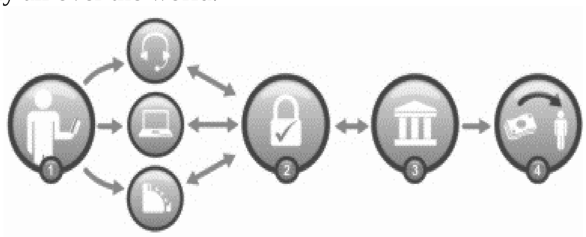
Fig 1: Proposed system architecture

Flash SMS

The SMS has to be displayed and we can use Proximity Flash SMS[1] makes a regular text message appear on the recipient's mobile phone instead of being delivered in the inbox. Flash SMS is a normal SMS text message that pops up in mobile phone screens and it is not stored in the mobile SMS inbox. Flash SMS is a simple application that displays incoming SMS as soon as they are received, in a non-interactive way, even on lock screen (unless stock lock screen is being used). Unlike SMS popup, we can touch through the displayed SMS and continue interaction with the screen. So we do not need to stop what we thee doing to read the SMS. SMS is formatted and notified as a transparent view on the fly, we can set the number of seconds sensor to dismiss SMS Flash[1] on first touch of Proximity sensor (SMS Flash is dismissed within next 1 second after touching the sensor). We can extend the display time when we need more to finish reading by touching and holding. We can go to reply box when Proximity sensor is touched twice.

II PAYMENT PROCESSING

Credit and debit card processing systems operate the same way all over the world.



This description lays out the basics of payment processing. It also helps to appreciate the charges and risks involved in accepting payments[2].

1. Collecting payment data: Payment details are entered into the payment device. They could be entered by a call center operator, read by a card-reader or entered directly into an internet page.
2. Authentication: Details of the purchase, details from the card and the PIN are sent. We identify the relevant card scheme (Visa, MasterCard etc.)[4]. And send the details through them to the bank or other institution that issued the card. If the details can't be verified, the payment is normally declined and the shopper or payee is asked to use another type of payment.
3. Authorization: The issuing bank checks the cardholder's identity, that the account has sufficient funds and that the card hasn't been reported lost or stolen. If everything is OK, the issuing bank authorize the amount requested and reserve those funds. Once the payment transaction is complete, we send a follow-up instruction to the bank to debit the funds.
4. Settlement of funds: The World Pay merchant account is credited with the value of the card transaction within four working days (depending on the card issuing bank and the agreement with us). Every month, we'll send the merchant statement which details the transactions processed, and how much we've paid for each transaction.

The Debit Card

The 16-digit[3] number on the front of the debit card is crucial to the process[3]. Typically, the 16 digits are comprised of a six-digit bank identification number, the customer's bank account number called check digit that's generated by the Luhn test algorithm and is used to verify that the account number is legitimate. The back of the card contains the magnetic strip, a security code and signature panel. Sometimes, the issuer puts a hold on the consumer's funds when the transaction is authorized and adjusts the amount when the transaction settles.

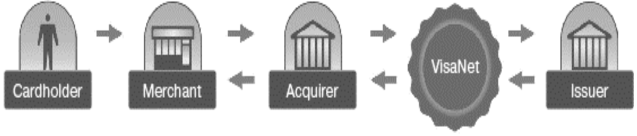
Signature or PIN

Visa[4] and MasterCard tend to process signature-based transactions, which typically use a so-called two-message process in which authorization and settlement are performed separately. The smaller networks usually handle PIN-based purchases, which occur via a single message that incorporates both authorization and settlement. Merchants take MasterCard and Visa[4] all around the world. PIN we'll find mostly at supermarkets, gas stations and major retailers. “The line between the two technologies is blurring now that some merchants accept debit card transactions where the card user doesn't have to sign or use a PIN. “Those used to be distinct, but now we have signature (transactions) that don't have any signature, and we're starting to see PIN transactions that don't have a PIN”. "The preference for most merchants as well as cardholders is swipe and go.

The typical Visa transaction involves four parties:

The merchant is any entity, a store, restaurant, physician, utility company, online retailer, hotel or airline that accepts Visa as payment. The acquirer is a financial institution that initiates and maintains contractual agreements with merchants for the purpose of accepting and processing Visa card transactions and enables Visa card payments from customers. The issuer is a financial institution that provides Visa-branded cards or Visa-branded payment products to consumers and businesses. When a Visa-branded credit card is used the issuer “lends” the consumer the funds to complete the transaction. If it is a debit or prepaid card transaction, the funds are automatically withdrawn from the account and transferred to the acquirer. The cardholder is any consumer or business using a Visa card or other Visa-branded product to make payments.

The Transaction Journey

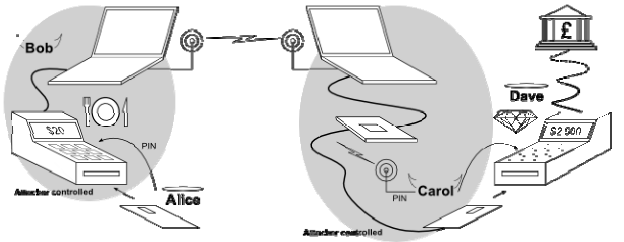


A Visa transaction is a structured process[4] When a Visa account holder uses a Visa card to buy a pair of shoes, it’s actually the acquirer, the merchant’s bank that reimburses the merchant for the shoes. Then the account holder’s bank reimburses the acquirer usually within 24 to 48 hours. Lastly, the issuer collects from the account holder by withdrawing funds from the account holder’s bank account if a debit account is used, or through billing if a credit account is used. VISA classifies the banks as either Issuers or Acquirers. Issuers issue cards to the cardholders, whereas the Acquirers manage the relationship with the merchants. When a cardholder presents a card for payment to a merchant the payment request is forwarded to the acquirer. The acquirer contacts the issuer through the VISA network. The issuer shares the information on whether sufficient balance is available to carry out the transaction[4]. The information is then routed to the merchant. In case sufficient balance is available, the payment is accepted otherwise it’s rejected. The issuer bills the cardholder on a monthly basis. The cardholder pays those bills then. The actual process involves separate loops for Authorization and Clearing & Settlement. VISA also offers several value-added services such as risk management, debit issuer processing, loyalty services, dispute management and value-added information services.

Payment gateway

A payment gateway[5] is an e-commerce application service provider service that authorizes credit card payments for e-businesses, online retailers, bricks and clicks or traditional brick and mortar. It is the equivalent of a physical point of sale terminal located in most retail outlets. Payment gateways protect credit card details by encrypting sensitive information, such as credit card numbers, to ensure that information is passed securely between the customer and the merchant and also between merchant and the payment processor. A payment gateway[5] facilitates the transfer of information between a payment portal (such as a website, mobile phone or interactive voice response service) and the Front End Processor or acquiring bank

III. Card Skimming Attack



'Skimming': Skimming[6] is an act of using a skimmer to illegally collect data from the magnetic stripe of a credit, debit or ATM card[7].

Skimming can occur easily in a restaurant because the card is taken away when the bill is being settled. If the server is a skimming identity thief, he or she will, before giving the card back to we, scan the credit card with a hand-held electronic device, which takes only seconds. The electronically captured information is then used to by the thief or sold to other criminals. This information, copied onto another blank card's magnetic stripe is then used by an identity thief to make purchases or withdraw cash in the name of the actual account holder. Skimming works by replacing a card reader like an ATM with a camouflaged counterfeit card reader. The counterfeit reader records all of the data on a credit, debit or ATM card[7] as it passes through the skimmer. In addition to ATMs, other locations where card skimming happens include restaurants, taxis or other businesses where an employee will take the card from the actual account holder in order to run the charge. In these instances the thief has fitted the card reader with a skimmer or uses a hand-held skimmer hidden in a pocket.

ATM Skimming

It occurs when an ATM[7] is compromised by a skimming device, a card reader which can be disguised to look like a part of the machine. The card reader saves the users' card number and pin code which is then replicated into a counterfeit copy for theft.

IV. How Clone Card Works

In this scam, crooks work together with the people who are serving. It has been reported that there are two ways criminals clone[10] the debit card.

1. They insert a thin card reader inside the device, right underneath the keypad. We can't see it, so it's hard to avoid. The card reader looks like a film strip and records the pressed keys.
2. The other one comes as a reader as well, but is attached to the PIN pad. We can see this one if we pay attention to the device which is now a little bigger than usual.

How to avoid

Criminals do not take the money from the account right away. Police reports indicate they usually leave a few months in between just so we record hundreds of other transactions on the bank statement. This makes it almost impossible for investigators to track the exact store where the card was defrauded. We can avoid this if we change the PIN number very often. It's inconvenient but doesn't cost us anything “better safe than sorry”. On the other hand for the alternative scams, always cover the PIN number when we type it in as well as check the PIN pad for any unusual attachments.

V. Relay Attacks

A Relay attack[8] is a type of hacking technique related to man-in-the-middle and replay attacks in which an attacker relays verbatim a message from the sender to a valid receiver of the message. The sender may or may not be aware of even sending the message to the attacker; if the sender is aware it is likely under the impression that the attacker is the intended receiver of the message.

Why does this attack work?

Customers insert their card into a terminal without any way to verify that it has not been tampered with. They depend on the integrity of the terminal to:

- Display the correct value of the transaction
- Keep the PIN secret
- Use the card only for transactions approved by the customer

Merchants accept customer's cards without verifying that they are genuine. In some cases they may even not handle the card and they are encouraged look away while the PIN is being entered. They depend on the security of EMV to detect unauthorised transactions although EMV does not prevent relay attacks such as the one described above.

How can the attack be prevented?

Merchants can try to identify fake cards by taking them from customers, checking the counterfeit detection features (such as the hologram and embossing) then inserting them into the card reader themselves. This will require the relay card be wireless rather than the wired prototype we have developed. A further protection is for the merchant before handing over the goods to confirm that the account number on the receipt matches the one on the card. This would require the attacker know in advance, the account number of the customer whose card they are about to exploit making it substantially harder to perpetrate. Banks could deploy measures to detect such relay attacks. Distance bounding protocol is one example of a secure positioning system, it requires the terminal measure of time it takes to communicate with the card, the maximum distance between the card and terminal can be calculated. By carefully designing the communication method cards use the estimate can be made very accurate and ensure that relay attacks over even short distances (around 10m for our prototype) are detected. This will require modifications to both the cards and terminals and will only be feasible for the longer term. Banks or third parties could release a device so that the customer avoids entering their PIN into a merchant terminal. If the customer enters their PIN into a keypad they control, a malicious terminal could not record it. Similarly, such a device could also show the value of the transaction and so allow the customers to detect if they are being charged for more than expected. Such device would transfer the trust from the merchant's terminal to a personal device that the customers bring themselves into the transaction. Banks could deploy terminals which allow customers to detect if they have been tampered. Currently there are hundreds of different designs for EMV terminals and customers cannot tell the difference between legitimate or fake ones, or if a real terminal has been tampered. Visible tamper-resistant seals may allow a merchant to detect such tampering if properly trained. However it is unlikely that customers would have the time, skills or patience needed to reliably check a terminal before each use.

Chip & PIN (EMV) relay attacks:

EMV (named after its founders Euro pay, MasterCard and Visa) is the standard on how smartcards used for payment communicate with the terminal in shops. In the UK, the system based around EMV is known as Chip &PIN[9]. Chip& PIN is intended to reduce fraud by requiring the genuine card and matching PIN be presented for a successful transaction. The process starts by the terminal sending the card a random number, known as a challenge. The customer then enters their PIN into the terminal and it is sent to the card. The card computes a cryptographic response, which incorporates the challenge, whether the PIN was entered correctly, and a secret known only to the card and the bank which issued it (the terminal does not know this secret). The purpose of including the challenge is so that the terminal can detect whether an old response is being replayed. This response is sent back to the terminal which then goes on-line and sends the challenge and response to the bank, who will verify them. Let us consider some potential scenarios of fraud which Chip & PIN[9] is intended to protect against stolen card. Without the correct PIN being entered the card will not produce the correct response and it cannot be used in an on-line Chip &PIN transaction. Without the card, a fraudster who knows the PIN will find it difficult to produce a fake card which will compute the correct response. When stolen card and its PIN are observed the fraudster can use the card and PIN to produce a valid response and use it as though he is the rightful owner. The account holder, however will eventually notice the fraudulent transactions and promptly contact his bank to block his card.

Observed response: If the fraudster knows the PIN (or persuades the customer to enter it) and gets temporary access to the card the card will produce correct responses. These responses, however, cannot be used later as the challenges from legitimate terminals are meant to be unpredictable. Despite these protections, vulnerabilities remain. For example, when customers pay with a Chip and PIN card, they have no choice but to trust the terminal when it displays the amount of the transaction. The terminal, however, could be replaced with a malicious one without showing any outward traces. When the customer pays for a low-value product and enters the PIN into the terminal, the challenge from a different shop selling a far more expensive product could be relayed to the card. The PIN and response from the card could likewise be relayed back to the other shop, which will accept the transaction.

VI. Conclusion

. When the Debit card is swiped at terminal, the transaction information send to visa server through acquirer bank and with an authentication normal procedures. Visa server will request user to enter a password in his/her mobile phone through the mobile network. If the password is valid, Server proceed the transaction towards the card holder bank and checks availability of required amount then flow of the transaction is as usual, if the password is not valid, server denies the transaction and lets the merchant and user to know that the transaction is denied. So this method can resolve three drawbacks in existing system first case if a card is cloned and swiped at some terminal, anyway the request for password to original owner of the card, he/she can know this transaction is not done by them and they can decline the transaction. Second case, if relay attack happens in a transaction, the user will be requested for password to perform a parallel transaction also, so he/she can avoid duplicate transaction. In third case, if the mobile phone and card are lost together, no one can make any transaction because the password is not known to anyone other than original user. Even though there are many security mechanisms for debit cards still we don’t have any proper authentication mechanism so we provide authentication by entering the pin in user mobile phone and hence we can prevent clone cards and relay attack through message authentication service.

References

[1]. (http://www.nawras.om/Personal/Talk/Extras/MessagingCallManagement/FlashSMS.aspx)

[2]. (http://www.worldpay.com/products/index.php?page=how)

[3]. http://www.bankrate.com/finance/banking/how-do-debit-cards-work.aspx)

[4]. (http://bmimatters.com/2012/03/19/understanding-visa-business-model/)

[5]. (http://en.wikipedia.org/wiki/Payment_gateway)

[6]. (http://www.webopedia.com/TERM/C/card_skimming.html)

[7]. (http://www.businessdictionary.com/definition/ATM-skimming.html)

[8]. (http://en.wikipedia.org/wiki/Relay_attack)

[9]. (https://www.cl.cam.ac.uk/research/security/banking/relay/)

[10]. (http://scam-detector.com/face-to-face-scams/pin-pad-cloned-debit-cards)