The Future of Electronic Money Transactions

Computer Security - Comp 116

Author: Alex Schaefer
alexander.schaefer@tufts.edu
Mentor: Ming Chow

Contents

Abstract

Every year, hundreds of billions of credit and debit card transactions are made. With the enormous volume of transactions comes fraud and theft. Billions of dollars are lost from retailers and consumers as credit and debit card details can be stolen, copied, or even forged. Credit card technology has progressed at a slow rate, but recently the field has seen an increase in security measures and practices that aim to reduce the amount of fraud.

This paper will look at two of the these new methods of securely making credit or debit card transactions, Apple's new implementation, Apple Pay, as well as the EMV standard of chip based cards. These new implementations aim to alleviate the most common credit card fraud practices, such as skimming a card number when a card is presented, as well as how account information is handled if credit card data is compromised. The strengths and weaknesses of each implementation will be discussed. Finally, this paper will look to draw conclusions on the current best practices for credit card transaction security, and provide insight as to whether practices used in the security of credit card transactions can be applied to broader security and authentication applications.

Introduction

It is unquestionable that financial transactions are moving away from the old paper world and into the digital world. One has to look no further than the number and magnitude of transactions of each kind of payment to see that checks and cash have been taken over in size by electronic payments. But as the world has moved away from paper money and checks, and towards electronic payments such as credit and debit card purchases, there have been large security problems that have arisen. For this paper, the scope will be twofold, the storing of credit and debit card account details, and the authorization of use of the card. Put in more general terms: making sure the account details stay private and proving whoever is using the card is allowed to.

The old way of authorizing credit cards and debit cards (for the remainder of this paper, I will just refer to the combination of credit card and debit card transactions as just credit card transactions) is insecure. The current credit card transaction goes much like this: if the transaction is being made in person, a Card Present transaction, a customer swipes a card containing a magnetic strip on it, a card reader reads the unencrypted magnetic strip, a merchant submits a request to an acquirer, the acquirer sends a request to the card issuer (the bank backing the credit card), which then returns an authorization code if there are sufficient funds, and the transaction is approved (CreditCards.com, 2013). To prove the person presenting the card is actually the cardholder, the signature on the back of the card is matched with the signature the user must provide after authorization. The same process is used in Card Not Present transactions, such as those made online or over the phone, but without the final signature check step.

The weakest part of the above process is the combination of the first and the last step; when a cardholder claims to be an authorized user of the card by having physical access to it, and then later confirmed to be the authorized user by the comparison of a signature. The insecure, plain-text storage of all necessary credit card information in a magnetic strip, combined with only the need for a signature to authenticate a transaction (or in the case of a Card Not Present transaction, no further authentication), makes it easy for a credit card to be copied or stolen, and then used by an attacker pretending to be the authorized user of the credit card.

There is little security in place in the current system to prevent unauthorized use of a credit card in the Authorization phase of a transaction. Compromise starts with either the theft of a physical credit card, or through the acquisition of the credit card account details. Once an attacker has the card, they can use it to make unauthorized purchases, and will have access to the account until the issuing bank closes the account. While the account holder of the card may not be directly liable for the fraud, they end up indirectly paying for it in increased credit card processing rates which merchants pass on to customers.

In this paper, the recent developments in Authorization security, as well as securely protecting account information while not in use, will be focused on. As mobile computing starts to encompass more and more of peoples daily computing, using a credit card stored on a smartphone seems like the way forward. In the past couple of years, Apple has put forward their attempt at securing credit card transactions. Credit card companies such as Visa and MasterCard have also put forward a EMV standard for chip based cards. This paper will delve into the specifics of those two implementations, how they increase the security of transactions, as well as their potential downsides. Finally, a conclusion will be drawn about the current state of credit

card security, as well as possibly applications of these technologies towards the broader security and authentication field.

To the Community

Credit card security is important to everyone. Around $190 billion is lost by retailers each year, with banks and consumers losing around $15 billion in total (LexisNexis, 2014). While consumers may not directly be responsible for fraud committed using their account, they feel the effects of fraud in terms of higher credit card interchange fees, which are passed on from retailers to consumers. A consumer having their credit card account compromised can lead to a hold on their account while the fraud is investigated, as well as the inconvenience of getting a new credit card number. Making credit card account details harder to compromise benefits everyone.

The topic of credit card security is important due to the amount of importance that is placed on keeping financial information secure. For normal people, their credit card information and financial information is some of their most sensitive pieces of information they must keep private. So in a broader security sense, how credit card information is kept private provides a lens on how all private and personal information should be kept and transmitted over the internet. What applies to credit card account numbers could easily equally apply to a user's password used to login to a website. If an attacker gains access to a users password, they can pass themselves off as the user, much like they can when making a fraudulent credit card purchase.

The importance here is how personal information is kept private, and when it is used as authorization across the internet, how a user can verify themselves so only they are authorized to transmit their information.

Applications

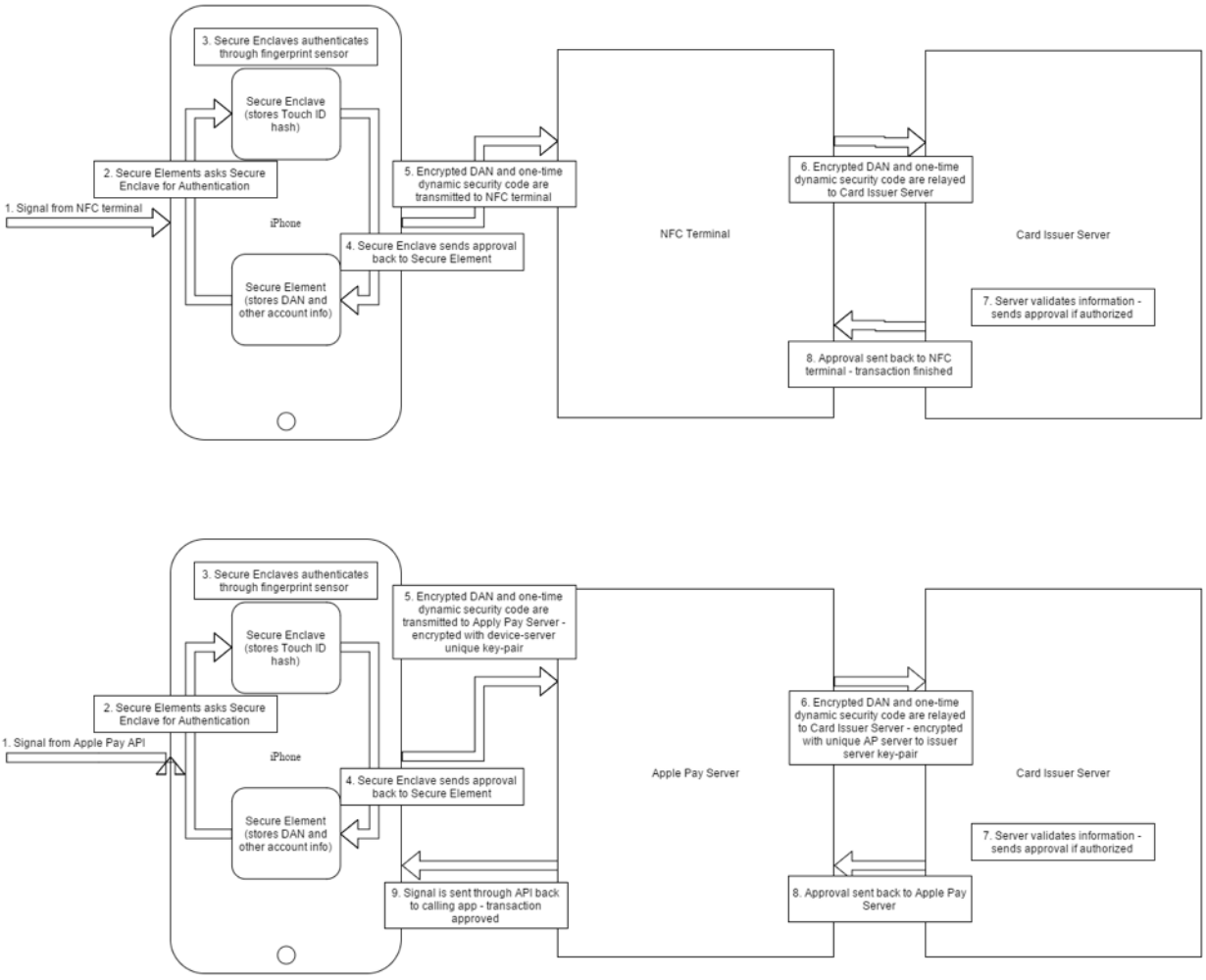
This paper will now highlight two recent implementations that look to improve credit card security. Both do so on the Authorization level of the transaction process. The first implementation is Apple Pay, which allows users that have a supported iPhone to make in-person purchases using NFC, as well as make purchases online. Apple Pay's implementation will then be compared to the implementation that is slowly being adopted known as EMV.

Apple Pay is a NFC, tokenization based payment implantation by Apple that is available on the iPhone. There are multiple security measures put in place to ensure that only the authorized user of the credit card enrolled in Apple Pay can use it. A credit card is first provisioned by gathering regular credit card information, such as account number, expiration date, card security code, and other information. This information is then encrypted on device with a key only known by the card issuer, and account details are sent to the card issuer to be verified. This is the only time while using Apple Pay that the credit card account number is transmitted. Once the card issuer has verified that the card belongs to the iPhone user attempting to add the card, they send back a unique Device Account Number (DAN), that is unique for each card enrolled in Apple Pay and to each device. This DAN is then stored in the iPhone's Secure Element. The Secure Element is a separate chip in the iPhone, and information stored on it is not accessible to apps installed on the phone, or even the filesystem if the operating system were to be compromised. The DAN is only stored on the Secure Element.

When a user initiates an Apple Pay transaction, the iPhone first checks to authenticate the user. This is done through either Touch ID, their proprietary fingerprint sensor, or through a fallback passcode. Touch ID data about a user's fingerprints are stored as hashes of their

fingerprint in another secure element, called the Secure Enclave. Because only the hash of the fingerprint is stored, if a user's phone was to be compromised, and an attempt was made to recover the fingerprint data, an attacker would not be able to recreate a user's fingerprint from only the hash data stored on device. In order to access the DAN stored on the Secure Element, proper user authentication must take place. "The encryption and authentication of the communication is based on AES, with cryptographic nonces used by both sides to protect against replay attacks. The pairing key is generated inside the Secure Enclave from its UID key and the Secure Element's unique identifier. The pairing key is then securely transferred from the Secure Enclave to a hardware security module (HSM) in the factory, which has the key material required to then inject the pairing key into the Secure Element." (Apple Inc, 2015) This implementation ensures that an attacker will not be able to access the DAN without proper authentication, and attempts to authenticate based on prior sessions are rejected.

Once user authentication has been approved, a "transcription-specific dynamic security code" is created. (Apple Inc, 2015) This is a one-time only use code that is based on a random seed that is only known to the card issuer and is stored in the Secure Element. The one time dynamic security code also incorporates a counter that increments for each transaction made. This ensures that for each transaction, there is a different dynamic security code that verifies each transaction. This dynamic security code, along with the encrypted DAN, are sent to the card issuer for each transaction that is made. Because the DAN is device specific, card issuers can insure that the transaction originates only from an iPhone, as opposed to at a physical terminal or over the internet.



Apple Pay Systems Diagram - NFC on top, in-app on bottom

Apple Pay solves many of the security related problems that come with credit card transactions. It solves the problem of using the same account number for every transaction by using a Device Account Number that is unique to each device that is enrolled for a given account. It adds a dynamic security code, meaning that an attacker would have to know the secret seed, as well as the number of transactions that have been made in order to validate with the card issuer. Even with all of these security measures, if an attacker was somehow able to extract the DAN and get the seed and transaction counter information off of a device, they still would have

trouble utilizing it. Card issuers would deny transactions that originated from non Apple Pay iPhones, such as those coming from a forged magnetic strip on a credit card.

Apple Pay works the same way over the internet or in an app. Instead of communicated via an encrypted NFC session, the encrypted DAN and dynamic security code are sent to Apple Pay servers from the iPhone using device-specific keys, and then forwarded to the card issuer using issuer-specific keys. Even if data is compromised in either of these steps, the dynamic security code will be invalid next time an attempt is made to use it, and transactions will be denied that do not originate from an Apple Pay iPhone.

Either in-person through NFC or online Apply Pay has solutions to the two areas of focus for this paper. It secures account details when not in use using the Secure Element, a chip not accessible by the phone OS, and ensures authentication by requiring biometric identification through fingerprints.

Although not as new of technology as Apple Pay, EMV cards which can use chip-and-pin or chip-and-signature technology have similar transaction mechanisms. Each issued card has a micro controller on it. This micro controller securely stores credit card account information, and "performs cryptographic processing for validating the integrity of the card number and certain static and dynamic data used in the transaction."[4] As with Apple Pay, a one-time dynamic security code is created each time a transaction takes place. Credit card account information is not stored unencrypted on a magnetic strip, it is stored in an encrypted state, and only the micro controller can unencrypted the account information. This solves a major problem of skimming credit cards. Skimming entails using a small device that stores the information contained in a magnetic strip of a credit card when swiped.

While EMV provides the benefit of encrypted account information and a dynamic security code, there are still drawbacks to the technology compared to Apple Pay. The significant type of EMV technology that has started to take hold in the United States, chip-and-signature, is less secure than chip-and-pin (Krebs, 2014). In the former case, a pin is not needed to authorize the account owner and the old traditional method of signature comparison is used. There is still little authentication in the Authorization part of the transaction. Whereas Apple Pay requires either biometric data (a fingerprint), or a 6-digital passcode. EMV also falls short for Card Not Present transactions. Here, EMV cards are no different than credit cards with a magnetic strip on the back. In order to make a purchase online or over the phone, the account number must be transmitted over, along with a static security code. If this information was to be obtained by an attacker, the entire account would be compromised, and the attacker would have everything he needs to make fraudulent purchases using the account. In European countries who have already mostly switched to chip cards, fraud has moved from in-person to online as it becomes harder to fake a chip card (Rosenber, 2015). For almost all purposes, the authentication, token based system that Apple Pay implements provides a higher level of security that current credit card options, including the magnetic strip and chip cards.

Broader Applications

Credit card security is an area that most consumers take seriously. Looking at new ways to implement credit card security can provide a lens at looking at new ways to more broadly implement security of personal information. A credit card transaction is nothing more than passing information that identifies and authorizes you, your credit card details, to another entity that then verifies the information and sends a response to accept or deny. Similar

implementations to those that have been shown above for credit cards can just as easily be applied to passwords.

Instead of having a user type in a password, a password that a user will likely remember in their head and is the same password used for every login account they have, keep a unique strong identifying key stored in a secure chip in a device they will always have with them, such as a smartphone. 45% of Americans have admitted to using the same password across sites (Anderson, 2015). Not requiring the user to remember their password allows for complex passwords that are hard to brute force, and will make user passwords more secure.

The tokenization methods also only allows access to the unique identifying key with proper authentication; this can be done through biometric identification, such as a fingerprint confirmation, or through a complex passcode. When a user authenticates with their unique key, have a dynamically generated one-time code be passed along as well, a code that changes every time and is based on a seed that only the device holding the keys and the authenticating server know. This will ensure that even if the unique key and one-time code are compromised, the attacker will not know what code will next authenticate the user. An attacker would have to retrieve the seed the code is based on either from the user device, which can have built in tamper protection, or from the server. This method has its flaws as well, but it is multiple times more secure than having a user authenticate with a password that is probably repeated and weak.

Conclusion

Over the past couple of years, there have been great strides towards greater credit card security. EMV, even with its limited usefulness has removed some of the easiest ways for credit card fraud to happen. But Apple Pay and similar tokenization implementations offer one of the

greatest advancements in credit card security yet. The requirement of biometric identification, combined with encrypted device specific identifies and one-time dynamic security codes, make a credit card transaction must less prone to attack. More importantly, the credit card tokenization scheme described above can be abstracted to be useful to the greater security field. Applying it to other secure information, such as passwords and other personal information, would provide a more user-friendly and more sophisticated security implementation.

References

Anderson, G. (2015). Identity Theft: Who's At Risk? - AARP. [online] AARP. Available at: <http://www.aarp.org/research/topics/economics/info-2014/identity-theft-incidence-risk-behaviors.html> [Accessed 15 Dec. 2015].

Apple Inc., (2015). iOS Security - iOS 9.0 and later. [online] Available at: https://www.apple.com/business/docs/iOS_Security_Guide.pdf [Accessed 15 Dec. 2015].

Berg, G. (2014). Fundamentals of EMV. [online] smartcardalliance.org. Available at: <http://www.smartcardalliance.org/resources/media/scap13_preconference/02.pdf> [Accessed 15 Dec. 2015].

CreditCards.com, (2013). How a credit card is processed. [online] Available at: <http://www.creditcards.com/credit-card-news/assets/HowACreditCardIsProcessed.pdf> [Accessed 15 Dec. 2015].

Krebs, B. (2014). Chip & PIN vs. Chip & Signature — Krebs on Security. [online] Krebsonsecurity.com. Available at: <http://krebsonsecurity.com/2014/10/chip-pin-vs-chip-signature/> [Accessed 15 Dec. 2015].

LexisNexis, (2014). 2014 LexisNexis True Cost of Fraud Study. [online] Available at: <http://www.lexisnexis.com/risk/downloads/assets/true-cost-fraud-2014.pdf> [Accessed 15 Dec. 2015].

Rosenberg, J. (2015). Expect more online fraud as new credit cards arrive. [online] Phys.org. Available at: <http://phys.org/news/2015-10-online-fraud-credit-cards.html> [Accessed 15 Dec. 2015].