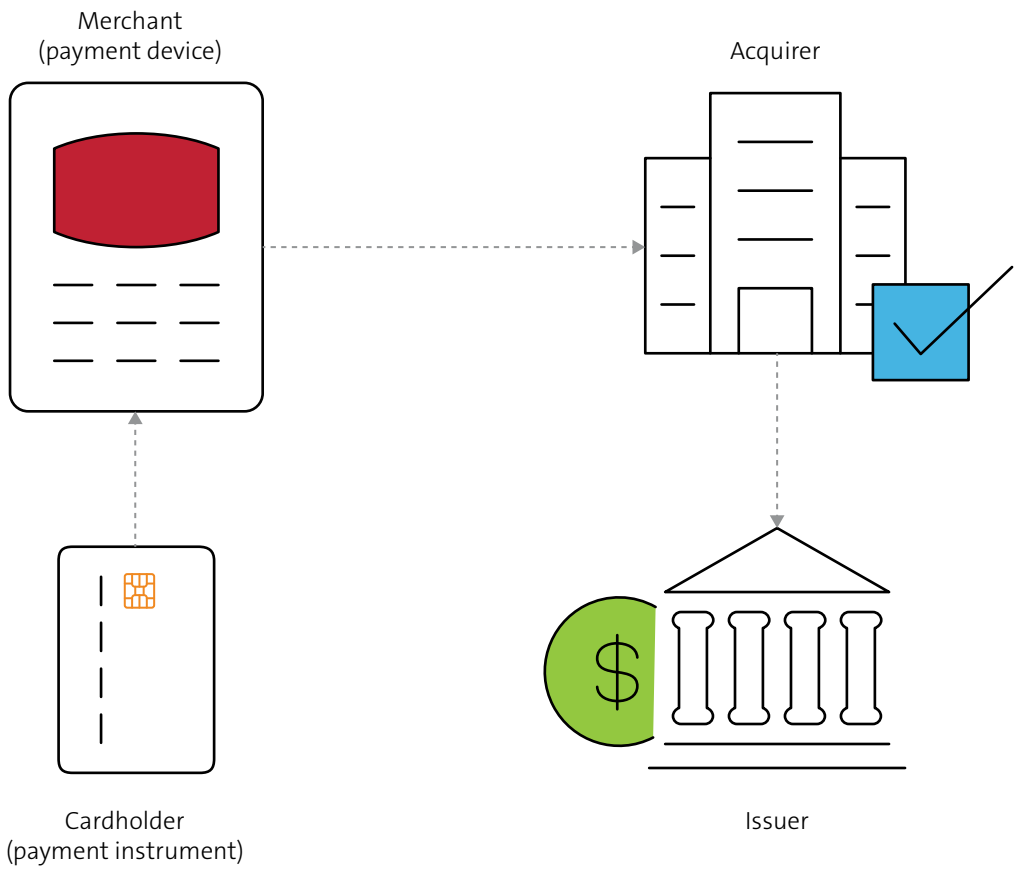
Card and Mobile Payment Threat Models

Empowering Trust®

Card and Mobile Payment Threat Models

Understand threat models facing mobile-based digital wallets, including a review of card payments, mobile architectures, fraud statistics, and mitigation techniques.

This paper discusses how card-based payments work and outlines the differences between conventional payment cards and mobile payment systems that are common today. Building on this information, UL mobile security experts describe threats that apply to all types of card-based payments, and how each threat applies to each type of payment implementation.



How card payments work

Electronic payment cards have been around for many decades, with the first automated teller machines (ATMs) using these cards for the instant issuance of cash in 1967.[1] Before and after the introduction and widespread use of the ATM, these cards have gone through many cycles of change – in form factor, in the method by which the card conveys data, and in the functionality and security inherent in the card itself. Since 1999[2], payment cards have been migrating from the use of physical media to convey data (printing, embossing, and magnetic stripes) to an electronic form using embedded processing elements — based on payment infrastructure interoperability specifications administered by EMVCo (called EMV after the founding members of Europay, Mastercard and Visa).

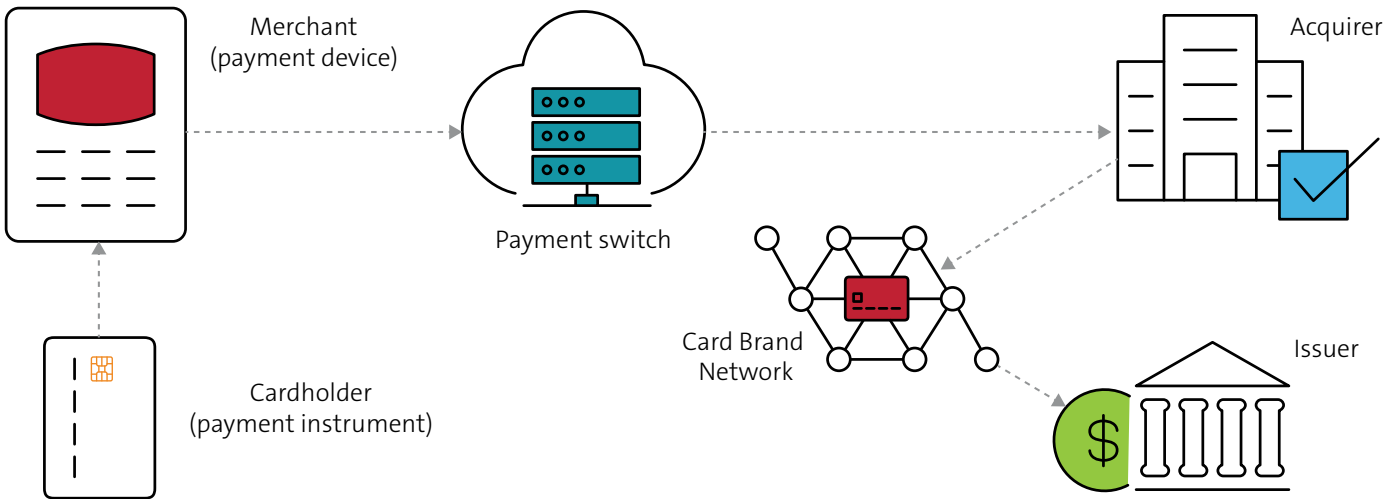
At its core, a payment card is a tool to convey data about a customer's financial account so funds may be transferred into or out of that account. A single value known as a Primary Account Number (PAN) carries this data. All other data on the card, the form factor of the card, the security features used in the card, and the functionality that allows for the authorization of the card's use are there to support the use of this PAN value during a payment.

Traditionally, in a card payment ecosystem, there are at least three and often four parties that must be involved, and the relationship between the parties is often called the four-corner model. These include:

1. The cardholder making the payment.
2. The merchant receiving the payment.
3. The financial institution where the merchant holds the financial account, called the acquirer.
4. The financial institution in which the customer has the account called the issuer.

In some scenarios, the acquirer and the issuer may be the same entity, reducing the group to three. However, many other entities are often involved, generally providing linkage between two or more of the entities (merchant to acquirer, acquirer to issuer, etc.). We show an expanded view of the four-corner model below.

The merchant or its payment processor configures the merchant payment device, so it knows where to send any transaction data, but how does the acquirer know who the card issuer is? This information is provided in the PAN, of which the first six to eight digits is a Bank Identification Number (BIN), which provides a unique ID for the card issuer. The remaining digits identify the customer account at that financial institution along with a check digit. Therefore, the PAN represents a Globally Unique Identifier (GUID) for any specific financial account (although more than one person may share a single account).



Authentication – The Missing Link

At least four things are required to complete a payment:

1. An entity making the payment
2. An entity receiving the payment
3. An amount for the payment
4. A method to transfer the payment

To avoid fraud, a method is required to authenticate or authorize the payment. This method includes authenticating the data of the transaction — amount, PAN, the card itself, etc. — as well as authenticating the intent of the transaction, confirming the account owner actually wants to make the payment.

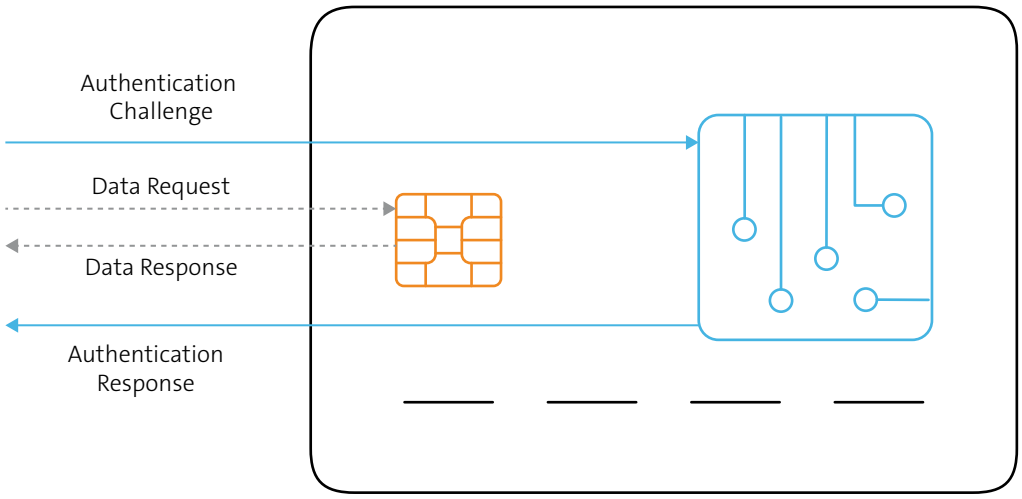
With traditional 'pre-EMV' cards, the card provides limited authentication and the system relied entirely upon payment acceptance devices to authenticate the transaction data. Authentication of customer intent was provided by handwritten signatures or use of a Personal Identification Number (PIN), which had to be transmitted through the payment network to the issuer for validation.

EMV payment cards, on the other hand, include two major authentication features.

- Validation of the customer, using offline PIN authentication, or other methods such as biometrics and
- Validation of the card and transaction data using stored cryptographic keys, which allow for an EMV compliant payment instrument to effectively 'sign' data used in the transaction, so the issuer can validate it.

Therefore, an EMV compliant card can both supply data to the payment acceptance device upon request and perform processing internally and produce responses based on secret data it never exposes externally. This functionality allows for the card to authenticate itself to the terminal and provide values that authenticate the transaction, called transaction cryptograms.

Part of the process that makes an EMV card work is how the data is transferred to, stored and protected on the card. If this authentication data — the secret and private keys used to generate responses to the authentication challenges — can be extracted or copied, then it is possible to reproduce a perfect replica of the card, which would allow for fraudulent payments to be made.



The Provisioning Process

All this data, both secret and accessible, must be loaded onto the card in some way. As the data is unique to each cardholder, this cannot be done during the mass manufacturing of the card itself. Instead, it is done before shipping the card to the cardholder in a process called provisioning or personalization.

The personalization process must be performed securely to ensure the data on the card is not compromised. This data could include not only the PAN but also the secret and private cryptographic keys used to authenticate the transactions, the customer PIN and other such sensitive data. Usually, this is done at a physically secure facility, often known as a personalization bureau, but this is only possible if the payment card is to pass through this facility before being sent to the customer.

What if the customer wants to install payment data onto something they already own?

Beyond the Card

Up to now, we have discussed the use of payment 'cards' – but a card is simply a form factor used to facilitate the conveyance of the data used for the payment process. The specific size and shape of payment cards are defined in ISO/IEC 7810[3], with the size and locations of embossing, magnetic strips or contacts for physical chip interfaces defined in ISO/IEC 7811-2[4], and ISO/IEC 7816-1[5]. With the advent of contactless EMV, which allows for communication between the payment card and the payment acceptance device without physical contact, maintaining a specific form factor for a payment 'card' was no longer necessary.

Contactless EMV allowed for the creation of new form factors, such as stickers, rings, watches, glasses and, of course, mobile phones and tablets. None of these systems can be inserted or swiped through a physical card reader interface, but they can integrate a contactless antenna and allow for conveyance across a standardized wireless interface (defined in ISO/IEC 14443-3:2011).

The departure from a conventional 'payment card' requires new terminology, so this has become the 'payment instrument'.

What Is a Payment Instrument?

Although the move from payment card to payment instrument may appear easy, it's not always that simple. In fact, when we take the term payment instrument and apply it retroactively to payment cards, we start to see that the definition of what a payment instrument is has been unclear for some time.

In the days of magnetic stripes, cards could have up to three tracks on the stripe. Track one and track two were commonly used for the payment data in different forms. The data on track two is less dense and, therefore, more easily read, so this is the most common track used in payments. Track one is a superset of track two, containing the same data but with additional information, such as the customer's name.

However, track three is not defined for international payments and has different purposes worldwide, from local payments to loyalty and closed-loop systems. This concept of different applications on a payment card was carried over to the EMV system, where each payment brand has its own application selected upon the initial powering of the card by an Application Identifier (AID).

The AID acts as an electronic method for selecting the payment 'type' within a card. Essentially, each type of payment method — Visa, Mastercard, local debit, etc. — has its own specific set of functional and security requirements. They're broadly similar, but there can be specific differences, especially when it comes to contactless transactions. To ensure the payment acceptance device can properly 'talk' with the payment card presented by the customer, the payment applications on that card are selectable using the AID.

The use of the AID is essential even if the card has only a single payment application installed, but it is more critical when there are multiple payment methods on a single card. Ultimately, there are many different applications[6], and there is no reason for the non-coexistence of a non-payment application on the same card as a Visa, Mastercard or other payment brand application.

For example, many payment cards are loaded with both a loyalty application and a payment application. Alternatively, there may be a transit application, or a separate security application for authentication purposes outside of card payments[10]. In some markets, multiple payment applications are present on a single card — an international credit brand along with a local domestic debit application, for instance.

We have previously discussed that a payment card has many different aspects to it — the plastic carrier, the chip, the OS and, of course, the applications. Some cards may have other elements, such as additional electronics to support dynamic security code displays, fingerprint readers, etc.

So, even in the traditional form factor, a payment card may not always be a card composed entirely of systems dedicated for payment use. This complexity is increased further when integrating payment instruments into devices primarily designed for other purposes — mobile phones, watches, tablets, etc. Here, the payment function is often ancillary to the other functions of the device. What is the definition of the boundary of the payment instrument in this case?

Mobile Payment Types Compared

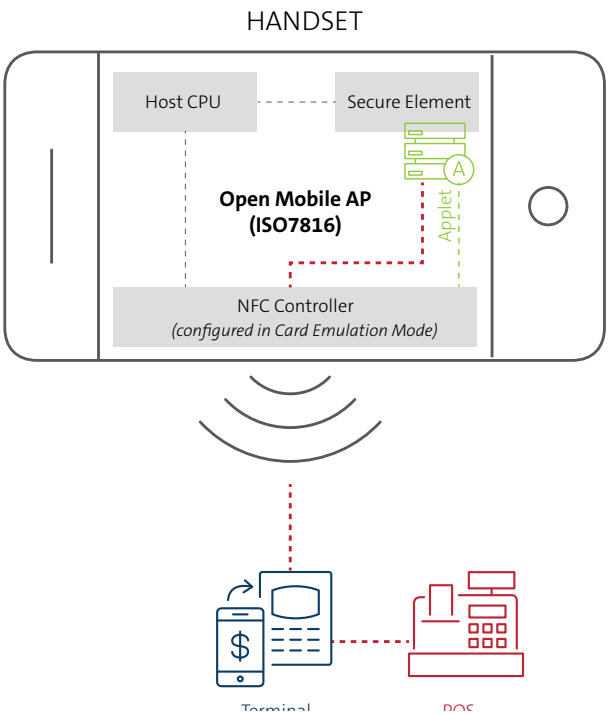
In most cases, when implementing payment instrument functionality in a general-purpose device, such as a smartphone, a payment app is required. This is not the same as the application, which is selected during a payment transaction using the AID, but is instead a concentration point for that code and payment processing — providing the user interface for the virtual card, where that would otherwise be provided by the physical card itself. AID selection is still required in a mobile payment app, the same way it is for a card.

The mobile payment app may be integrated into the operating system or come pre-bundled with it. Still, it remains an individual section of code that is dedicated to the payment operation. However, this app is not the only code involved in the payment — the app must integrate with other areas of the mobile system for storing data, keys, interfacing to the screen and receiving inputs from the user, as well as connecting to the outside world through the near-field communication (NFC) interface.

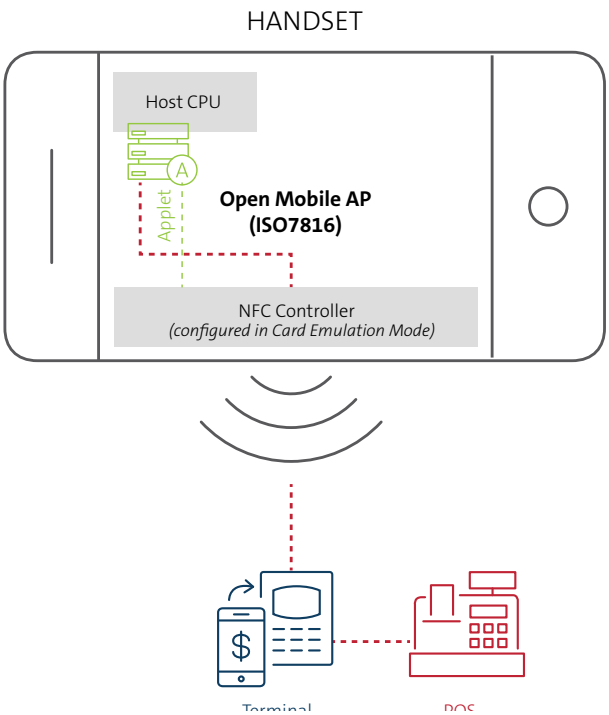
How the payment functions are integrated can vary. Some systems, such as Apple Pay, use an embedded Secure Element to contain much of the functionality and, therefore, are more similar to the traditional payment card. Others, including most implementations of Google Pay, store the payment application code within the payment app itself and sensitive data, such as cryptographic keys within secure storage provided by the platform, such as the Android Keystore. This type of payment instrument implementation is often called host-based card emulation (HCE), indicating that the card aspect of the instrument is emulated by another host — in this case, the mobile phone.

We illustrate these two main implementation types below.

Secure Element based mobile payment system



HCE based mobile payment system



The specifics of the implementation impact many different aspects of how the payment method works. For example, Apple Pay is limited to being personalized with a maximum of 12 cards on newer phones — the limit is eight cards on iPhone 7 and below[8]. Google Pay, however, has no such limitation when it is implemented entirely within application space (although other Android implementations that use a Secure Element, such as Samsung Pay, do have limits[9]).

What is the reason for the differentiation between these two types of payment implementation, and how does that affect the utility and security of the overall system? To answer this, we need to understand a little more about how mobile payment instruments are provisioned or provided with the card data they use to make payments.

Life Cycle of a Payment Instrument

All payment instruments have a life cycle, from inception through to destruction. This life cycle can be broken down broadly into the following steps:

1. Creation/manufacturing of an unprovisioned payment instrument or its environment
2. Shipping before provisioning or sale
3. Enrollment of account holder
4. Provisioning of payment instrument
5. Shipping to customer
6. Storage of payment instrument data
7. Use of payment instrument
8. Update/re-provisioning of payment instrument
9. Decommissioning of payment instrument

In this context, we use the term 'payment instrument or its environment' to cover the payment instrument's physical and logical/digital aspects. For a traditional payment card, this is the chip on the card, the operating system (OS) on the chip, the applications resident in the OS, and the plastic carrier on which the chip is mounted, etc. For mobile payments, it is the mobile phone, the mobile OS and the NFC interface, etc.

In this life cycle, we can start to see some significant differences between a Secure Element based payment instrument and HCE based payment instrument. For one, the environment of the payment instrument can be mostly constrained to the Secure Element itself, reducing the number of involved parties in almost all steps. However, this comes at a price, as it requires the cooperation or authorization of the Secure Element owner to provision new applications and/or keys onto that element. In this context, the owner of the Secure Element is not the consumer who owns the mobile device but instead the organization that has control over what applications can be loaded into the Secure Element.

For traditional payment cards, the supply chain for the payment instrument will generally involve the card issuer directly — the cardholder receives the card from the bank or its authorized agent. However, in mobile payments, the card issuer generally has no direct relationship with the mobile phone manufacturer, so provisioning new payment instruments onto a mobile phone can be more complex if the manufacturer must be involved.

Involvement of the phone manufacturer is not necessary with HCE based implementations. Once the card details are converted into a virtual card, any payment app loaded onto the device may interface to the NFC controller directly through provided APIs, which allow for sufficient functionality to implement payments. All that is needed is to obtain the card details required to create a virtual card on the mobile device. This step is referred to as provisioning, and there are some differences in how it is managed on a mobile device compared to a traditional payment card.

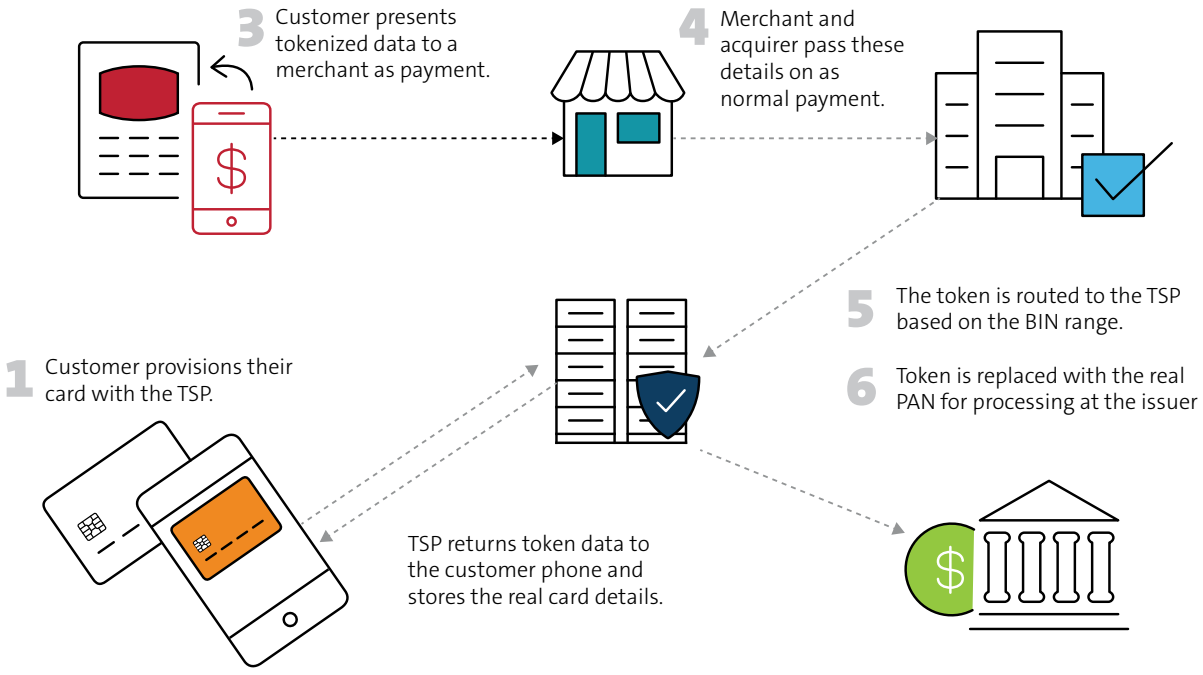
Provisioning of Payment Instruments

As previously noted, the payment instrument is primarily a mechanism for identifying the customer account — through the Primary Account Number in card-based payments. Over time, payment instruments have integrated other data to assist with the processing or security of the payment, from security codes stored on the magnetic strip to secret keys contained in an EMV compliant payment instrument.

This data is loaded onto any specific payment instrument in a process called provisioning. For traditional payment cards, this process is physical — the cards are provisioned in a secure facility by personalization bureaus. Mobile systems do not use bureaus; instead the personalization process is performed remotely, often through a third party known as a tokenization service provider (TSP). This term is used because, in mobile payments, the card data is not copied or cloned directly from the card to the mobile phone. Instead, the data required is 'tokenized' for deployment to that mobile device.

This tokenization process substitutes real or funding PAN on the customer card with a different tokenized PAN value. The cryptographic keys and other data required for an EMV system are, most often, also newly produced for the mobile instance at this point. During a payment, the BIN of the token PAN (tPAN) directs the transaction to the TSP, instead of the issuer, who can then forward the transaction to the actual issuer.

This helps ensure that even if the mobile payment instance is compromised, the funding PAN (fPAN) value is not. It also allows for instant re-issuance of a new tPAN in the case of such a compromise or allows for the rolling of the cryptographic keys — the tPAN is generally not changed to ensure consistency of this value across different purchases or uses, which is important for some use cases.



This process presents a significant benefit when compared to the use case for a physical card. If you find that your card has been compromised, the card will usually be blocked or disabled, and a new card produced and sent out. This can take days at best or up to several weeks in some cases. However, the real change that is occurring here is not the update of the physical card but the update of the payment data stored on that card. The card itself is just a physical carrier for that information.

In mobile payment implementations, the system can be much more agile in its response to compromise, as the reprovisioning process can be done remotely — essentially instantly. As soon as information indicates a payment instrument has been compromised, the data can be updated. This is not only more convenient for the cardholder, but it also helps reduce the shelf life of any compromised data, reducing or perhaps even preventing fraudulent transactions.

However, the new process also changes the threat landscape for the payment system somewhat, replacing the physical security of the 'personalization bureau' with the logical security of the remote TSP system. Previously, when payment instruments were limited to cards, the supply chain for the cards was easier to keep secure, from manufacturing to personalization to shipping to the customer. In the context of mobile payments, the cardholder effectively purchases the payment instrument first, so the supply chain for that product — the hardware, the software or the applications — is unknown or at least uncontrolled, from the point of view of the payment industry.

Understanding the threat landscape and how it changes is vital to developing methods to prevent or at least mitigate attacks. Most important is understanding how this landscape changes over time, ideally to develop a set of controls that will apply in any instance.

Threat Categories

EMV based physical payment cards have been readily available and used for many years. Significant experience has been gained in the threats facing these cards. Out of the multiple potential ways to group payment instrument frauds, listed below are some of the commonly used categories:[7]

- **Lost/Stolen –** fraud resulting from the loss or theft of an existing card, and a transaction has taken place without the cardholder's consent or authority.
- **Never Received –** fraud where a card has been intercepted (stolen) before delivery or use by the customer.
- **Fraudulent Application –** fraudulent applications are applications for card accounts using a fictitious identity, using someone else's identity or providing false information during the application process.
- **Counterfeit/Skimming –** the use of altered or illegally reproduced cards, including the replication/alteration of the account data and changes to the details on the face of the card with intent to defraud
- **Other**

Lost or stolen fraud currently forms the bulk of card-present fraud for payment cards. While a physical card can securely store cryptographic key materials, the card does not know if the operator is the genuine account owner. PIN entry can be used to authenticate the cardholder and prevent lost and stolen fraud. However, for usability purposes, PINs are used only for high-value transactions. Mobile platforms used as payment instruments often use fingerprint or face recognition to verify the operator for all value transactions. This feature lessens the risk from lost and stolen mobiles when compared to physical payment cards.

Never received is fraud type which applies to physical cards and is often perpetrated by the theft of mail containing a payment card. Electronically provisioned mobile-based payment instruments are not vulnerable to mail theft. The closest equivalent threat would be an attack on the provisioning process — either attacking the electronic communications or cardholder authentication, known as enrollment fraud. Modern cryptography limits the threat of eavesdropping, interception or modification of traffic. Enrollment fraud has occurred. However, issuers have added additional procedures to manage this threat.

Fraudulent applications can occur with both physical cards and mobile-based payment instruments. Online application and online provisioning, as used by mobile-based payment instruments, may be more attractive to fraudsters when compared to having to wait for physical cards to arrive

by post. However, the process of stealing an identity and applying for new accounts will be the same for both physical cards and mobile-based payment instruments.

Counterfeit or skimming attacks are predominantly a problem with magnetic stripe cards or systems that store MSR equivalent account data in the chip. EMV based physical cards are extensively tested to ensure cards are difficult to clone. The security testing program managed by EMVCo[11] includes laser fault injection, side-channel analysis, physical probing and review of test features. The effectiveness of this technology and testing program is evidenced by the reduction in counterfeit fraud in regions that have migrated from magnetic stripe to EMV[12]. Cloning a mobile-based payment instrument is arguably easier than cloning a physical EMVCo card. However, this may not be a real-world issue, as cloning attacks on non-MSR cards compromise a small component of payment fraud.

Other is an amorphous category covering attacks not included in the above groups. Australia has relatively low rates of other fraud at the current time[13, 14]. Mobile payment instruments typically require explicit authorization from the cardholder, e.g., fingerprint or face ID[15]. This may make mobile payment instruments less vulnerable to relay attacks than regular physical cards, where an attacker only needs to be near the target card.

Mitigations to Payment Threats

Protecting against threats to traditional payment cards generally involves ensuring there is sufficient oversight and protection across the life cycle of the payment instrument. This involves security validation of the processors used in the payment cards, the operating systems installed onto these processors and the payment applications themselves. The provisioning process must follow stringent physical and logical security guidelines, and shipping of the card to the customer is often performed using envelopes that don't clearly display their contents and are not provided at the same time as the customer PIN.

Not all these controls can be easily conveyed to mobile payment instruments. The use of the Secure Element can vary based on the implementation — some systems embed the payment application into the Secure Element, such as Apple Pay, while others like Samsung Pay and most Google Pay systems only use the Secure Element to store cryptographic keys and process operations using those keys.

All mobile payment systems rely on remote provisioning of the tokenized card details, and the use of changeable tokens here marks a significant change in the security posture of mobile systems vs traditional cards. Physical payment cards must be secure enough to be deployed with a set of static values (PAN, cryptographic keys, etc.) that are not changed throughout the card's life — generally at least three years. Compromise of that data can allow for the production of fake cards, which may be used without limitation until the card is canceled/blocked.

By using remote provisioning, mobile systems do not have this constraint — personalization data can be changed at any time. Updates to the underlying software are also possible from the operating system to the payment application itself, allowing for patching of potential vulnerabilities without a mass recall of physical cards. These controls are specific to mobile — they do not exist in respect of physical payment cards.

With the discussion of different types of payment instruments, it is essential to remember that any implementation of a payment instrument — be it as a plastic card, a mobile with an embedded Secure Element or an HCE system — remains inherently a software implementation. The system may implement hardware protections for cryptographic keys and processing and for isolating the processing of the payment functions. Still, those payment functions are always implemented in a software application that sits on top of a software-based operating system.

True hardware implementations do not exist in the context of payments.

Therefore, when comparing security, the question is not "hardware versus software" but more one of specific implementations. Implementations that allow for applications to interface directly to the NFC subsystems in the rich OS trade this increased utility for an increase in the attack surface of the execution environment in which the applications operate. However, does this materially increase the risk of fraud when considering payments?

Mobile Payment Fraud in the Wild

Detailed data on fraud performed by or on mobile payment instruments is hard to come by. Published articles[16, 17] indicate fraud in this space is typically performed within a short time of provisioning, implying that it is primarily enrollment or personalization fraud. Lost and stolen fraud is also possible on some mobile systems, where the payment may be made without user authentication. However, the ability to rapidly disable processing of any tPANs deployed to the mobile device, coupled with the speed by which most people notice the loss of a mobile device, make this less likely than lost and stolen fraud for traditional payment cards.

Additionally, to reduce the risks associated with frauds from a displaced or lost device, many mobile systems integrate a 'find my phone' function enabling remote location or even remote data wiping.

Initial implementations of mobile payment were known to suffer from enrollment fraud issues due to a lack of customer authentication during that process. Criminals could surreptitiously capture an image of a customer card or use data previously captured or stolen[18] to create a mobile instance that operated as a valid EMV contactless card. However, security protections were rapidly deployed into these systems, requiring customer authentication through banking apps, two-factor processes, or such features to prevent these attacks.

As a result, remote attacks on mobile payment instruments, although possible, appear uncommon. Malware that targets banking applications does exist[19] and continues to evolve[20]. However, malware that is targeted to exploit card payment data, rather than internet banking data, does not appear to be prevalent. There has been suspected malware used to attack a Google Pay instance[21], but this appears to be due to an issue in the backend transaction authentication, rather than anything specific to HCE or mobile payment instruments. Similar issues have occurred with regular EMV cards[22].

The tokenization and provisioning systems and processes appear to be the most open to an attack in the mobile payment model. Attacking of the system through the NFC interface itself is possible, but there does not appear to be any wide research, and the threat is mitigated by the close range required for these interfaces. Secure Element and HCE based implementations are both potentially vulnerable, either through vulnerabilities in the payment app or other apps running on the same host/SE processor.

Specific security issues have been reported in Apple Pay implementations, but these are primarily concerned with online payments or attacks on a jailbroken device[23] and have not been seen in the field.

Similarly, data leakage with Samsung Pay has been reported[24], including those implementations that use Secure Elements, but exploitation of this is not known, and the vulnerabilities were patched before disclosure.

Ongoing Evolution of Payments

In this document, we have looked at the various ways in which payment instruments can be implemented, from plastic cards to software apps on mobile phones. In each instance, we have discussed the threats that apply, finding a common set that applies to all payment instrument types. Overall, attacks applicable to the different mobile types have significant crossover, even though they use different technology stacks. A large part of the threat is based on the enrollment and provisioning process, which is similar between both Secure Element and HCE based payment models.

Review of publicly available information found no clear evidence of widespread exploitation of these attack methods on any platform. We found no indication of actual risk differential between the different types of mobile payment systems. Designs based on HCE or Secure Element, or open NFC or closed NFC, do not seem to make a difference to fraud rates or real-world attacks[25]. This may be because it is easier or more lucrative for criminals to target mobile banking apps and gain access to bank accounts directly rather than through intermediaries such as mobile payments, which often have their own fraud monitoring systems. However, as payments continue to evolve, it is vital to continue to consider the threat models and ensure they are kept up to date with the risks posed by the technologies used.

Learn more about our mobile payment security solutions at UL.com/services/mobile-payment-security.

References

1. Reuters Staff (2017, June 27). World's first ATM machine turns to gold on 50th birthday. Reuters. https://www.reuters.com/article/us-atm-anniversary-idUSKBN19I166
2. Overview. (2021, May 13). EMVCo. https://www.emvco.com/about/overview/
3. ISO/IEC 7810:2003. (2004, March 17). ISO. https://www.iso.org/standard/31432.html
4. ISO/IEC 7811–2:2018. (2018, August). ISO. https://www.iso.org/standard/73638.html
5. ISO/IEC 7816–1:2011. (2011, February). ISO. https://www.iso.org/standard/54089.html
6. Complete list of Application Identifiers (AID). (2020, November 4). EFTLab - Breakthrough Payment Technologies. https://www.eftlab.com/knowledge-base/211-emv-aid-rid-pix/
7. Jaracz, J. (2012, April 9). EMV can be more than payments. SecureIDNews. https://www.secureidnews.com/news-item/emv-can-be-more-than-payments/
8. Apple. (2021, July 9). Set up Apple Pay. Apple Support. https://support.apple.com/en-au/HT204506
9. Samsung. (n.d.). Samsung Pay. https://www.samsung.com/au/apps/samsungpay/
10. Australian Payments Network Limited. (2020, June 1). Payment Fraud Statistics (Revised April 2021) [Summary of results]. Australian Payments Network. https://www.auspaynet.com.au/sites/default/files/2021-05/PaymentFraudStatistics_Jul19-Jun20_RevisedApril21.pdf
11. EMVCo, LLC. (2016, June). EMVCo Security Evaluation Process (5.1). EMV Security Guidelines. https://www.emvco.com/wp-content/uploads/2017/04/EMVCo-SEWG-14-P02-V5-1_EMVCo_Security_Evaluation_Process_20160725082101992.pdf
12. UK Finance. (2019). Fraud the Facts 2019: The definitive overview of payment industry fraud [E-book]. https://www.ukfinance.org.uk/system/files/Fraud%20The%20Facts%202019%20-%20FINAL%20ONLINE.pdf
13. Drimer, S., & Murdoch, S. J. (2007, December). Relay attacks on card payment: vulnerabilities and defences. https://murdoch.is/talks/ccc07relayattacks.pdf
14. Chothia, T., Garcia, F. D., Thompson, M., de Ruiter, J., & van den Breekel, J. (n.d.). Protecting Contactless EMV cards from relay attacks. University of Birmingham. https://www.cs.bham.ac.uk/%7Etpc/Relay/
15. Google. (2021, May). Parliamentary Joint Committee on Corporations and Financial Services inquiry into Mobile payment and digital wallet financial services. https://www.aph.gov.au/DocumentStore.ashx?id=7bbe0b65-5ab4-4b07-b038-565ae91d07e3&subId=707289
16. Harrison, P. J. (2021, July 5). Fourthline Finds Digital Wallet Fraud is Thriving in the UK. The Fintech Times. https://thefintechtimes.com/fourthline-finds-digital-wallet-fraud-is-thriving-in-the-uk/
17. Fisher, D. (2017, September 8). Mobile Wallets Present New Opportunities for Fraud. Pindrop. https://www.pindrop.com/blog/mobile-wallets-present-new-opportunities-for-fraud/
18. Brewster, T. (2021, January 6). Millions Are Being Lost To Apple Pay Fraud—Will Apple Card Come To The Rescue? Forbes. https://www.forbes.com/sites/thomasbrewster/2019/03/27/millions-are-being-lost-to-apple-pay-fraudwill-apple-card-come-to-the-rescue/?sh=2f991607622f
19. Osborne, C. (2019, July 9). Anubis Android banking malware returns with extensive financial app hit list. ZDNet. https://www.zdnet.com/article/anubis-android-banking-malware-returns-with-a-bang/
20. EventBot: A new mobile banking trojan is born, Cybereason, https://www.cybereason.com/blog/eventbot-a-new-mobile-banking-trojan-is-born
21. Doffman, Z. (2021, January 8). Critical PayPal Security Hack: Multiple Thefts Now Reported—Check Your Settings. Forbes. https://www.forbes.com/sites/zakdoffman/2020/02/25/critical-paypal-security-hack-multiple-thefts-now-reported-check-your-settings/?sh=518cf7276e98
22. Chip Card ATM 'Shimmer' Found in Mexico. (2015, August 14). Krebs on Security. https://krebsonsecurity.com/2015/08/chip-card-atm-shimmer-found-in-mexico/
23. Yunusov, T. (2017, July). ApplePwn: The future of cardless fraud. Black Hat. https://www.blackhat.com/docs/us-17/thursday/us-17-Yunusov-The-Future-Of-Applepwn-How-To-Save-Your-Money.pdf
24. Android Phones: NFC Logs and Dumpsys Privileges. UL. https://www.ul.com/resources/android-phones-nfc-logs-and-dumpsys-privileges
25. Eyers, J. (2021, July 27). Commonwealth Bank chief Matt Comyn attacks Apple over its 'anti-competitive' payments system in iPhones. Australian Financial Review. https://www.afr.com/companies/financial-services/cba-s-comyn-attacks-apple-for-being-anti-competitive-20210727-p58d73

UL.com/cybersecurity

005.01.0921.EN.CYB
CS675435-0921