SECURE PAYMENT TECHNOLOGIES DEMYSTIFIED

EMV Chip, Tokenization, Point to Point Encryption

PROLOGUE

The purpose of this paper is to illustrate the value proposition of technologies such as Tokenization and Point-to-Point Encryption (P2PE) and to provide guidance on how those technologies can supplement EMV Chip technology to provide a card-present merchant with a layered approach to reducing risk.

SUMMARY

Data breaches continue to make headlines as payment card data remains a valuable target for attackers. Even companies that have implemented strong security infrastructure have fallen victim to attackers who find weaknesses in the company's systems. Criminals are consistently expanding their skill sets and developing more sophisticated methods to access and compromise payment card data while at the same time the payment ecosystem continues to deploy ever-stronger security controls to prevent data breaches. In this race to secure data, technology must continue to evolve or be eclipsed by evolving attacks. Three specific security technologies work well in combination to assist organizations in staying ahead of the attackers: EMV Chip, P2PE, and Tokenization.

The goal of this paper is to illustrate the steps an attacker might take in conducting an attack, how each of the three security technologies can work in concert to reduce risk associated with the attack, and how an entity can consider moving forward to further safecard card data. Together the technologies protect sensitive data to reduce risk and minimize exposure. Likewise, these technologies, working together, protect the data from unauthorized access and reduce the value of the data if compromised, making the data both less attractive AND more difficult to obtain.

ANATOMY OF A BREACH

A company may be targeted or it may be a victim of a chance data breach. In crimes of opportunity, an attacker simply scans the internet for systems that appear weak. Attackers target two primary weaknesses to gain access to a company's network: they look for website coding flaws such as SQL Injection, or they probe the company's remote access tools for insecure configurations, such as a default user-id and password.

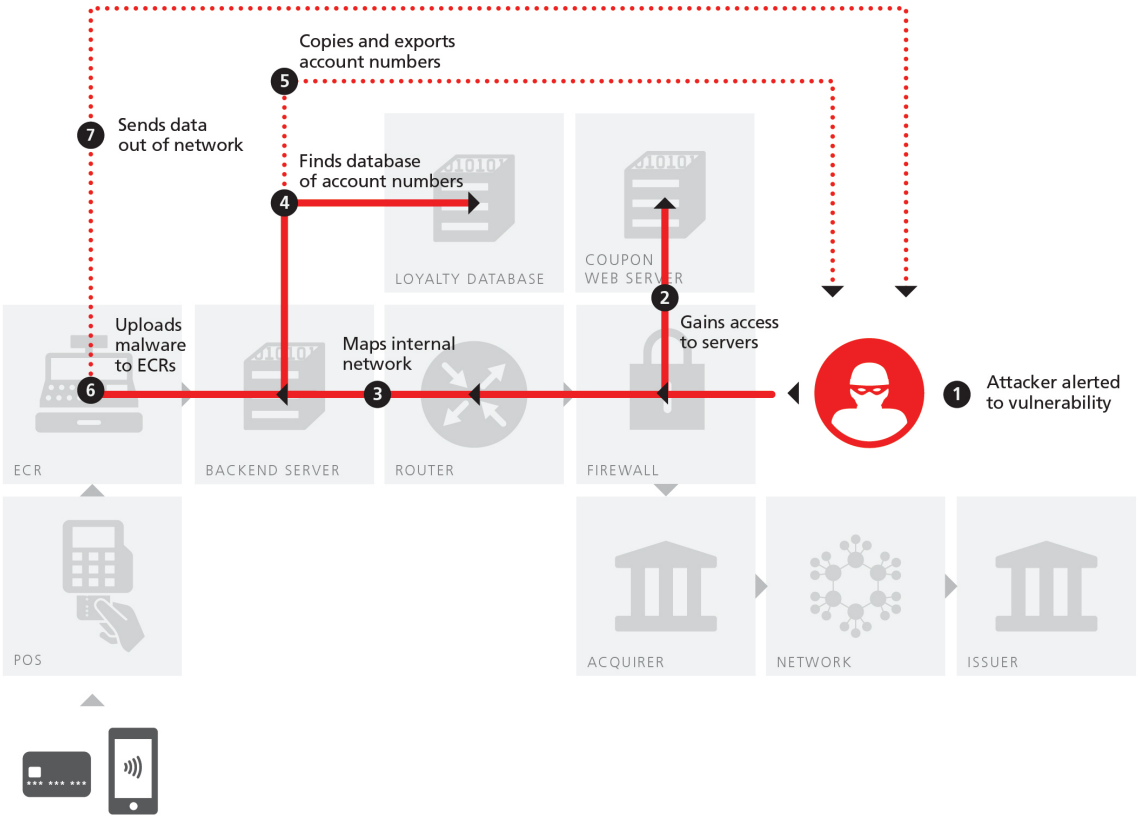
It's important to remember that an attacker will look for any path into a network, even if it's not the most direct means of entry. Here is an example of such an attack:

A brick-and-mortar merchant may have a seemingly innocuous system, such as a marketing website that hosts daily coupons. The merchant has no e-commerce activity, so it has not implemented detailed security controls (such as Payment Card Industry Data Security Standard) to protect the coupon delivery web servers. An attacker's automated scanning tool identifies the web servers as having a potential SQL Injection vulnerability and alerts the attacker. The attacker finds that they are able to access the coupon delivery servers, but doesn't find any valuable data. The attacker then uses the merchant's own web servers to map the merchant's internal network. The first thing the attacker finds is a loyalty database full of cardholder account numbers. The attacker copies the account numbers and exports them out of the network via the merchant's own internet connection, encrypting the card data on the way out. The attacker then finds that they are able to access a back-end payment application server that manages the Electronic Cash Registers (ECRs) at all of the merchant's locations. With that access, the attacker uploads memory-scraping malware to all of the ECRs. The malware captures all payment card data as it is passed from the card reader to the ECR. The malware then encrypts the card data and sends the encrypted data out of the network in small batches in order to avoid detection by internal security systems.

In addition to strong network security controls (such as those required by PCI DSS), EMV Chip, Point-to-Point Encryption, and Tokenization could greatly reduce the risk associated with this type of compromise.

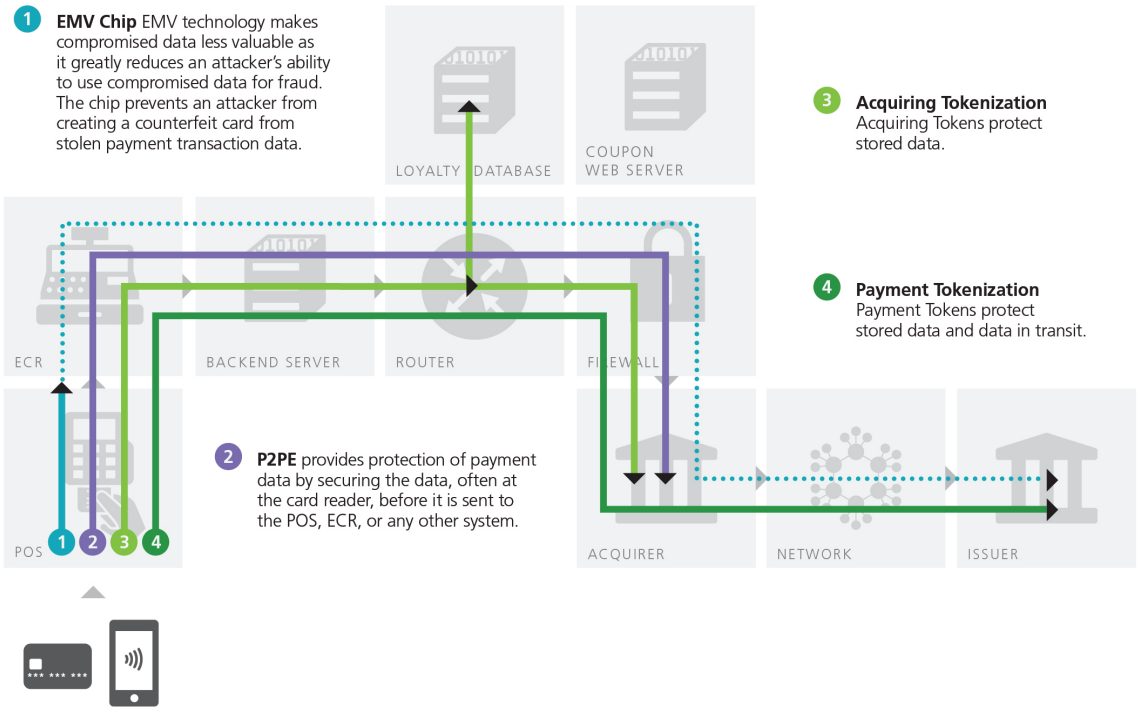
The Anatomy of a Breach

ATTACK



Reducing Risk of a Breach

PREVENTION



REDUCING RISK

EMV CHIP

Prevents card counterfeiting. EMV technology makes compromised data less valuable because it greatly reduces an attacker's ability to clone or copy the data and then reuse the compromised data to create a counterfeit card and commit fraud. The chip prevents an attacker from creating a counterfeit card from the stolen payment transaction data. Thus, the attacker can use the compromised card data for fraud only in the card not- present channels (e-commerce, mail order, or telephone order). In other words, use of EMV Chip technology reduces counterfeit fraud risk but it does not, by itself, eliminate all fraud risk or end a merchant's objective of securing payment card data. The value of EMV technology is that it significantly reduces the value and attractiveness of compromised data once in the hands of an attacker.

POINT TO POINT ENCRYPTION (P2PE)

Protects card data in transit. P2PE provides protection of payment data by securing the data, often at the card reader, before it is sent to the POS, ECR, or any other system. In the above example, if the merchant had implemented P2PE technology in its payment terminal, the attacker's malware would only have had access to encrypted account data. This technology does leave the payment data vulnerable at the point of decryption, such as at the merchant's back end systems or at its payment processor. However, encrypting data throughout the payment chain reduces the number of potential points of compromise that must be defended to prevent an attack. (Note: If software encryption is employed in lieu of hardware encryption, it may not protect against the attack scenario described above.)

TOKENIZATION

There are three classes of tokens: Acquiring Tokens (protects stored data), Payment Tokens (protects stored data and data in transit), and Issuer Tokens (protects stored data and data in transit).

Acquiring tokens replace card data with a substitute value and are created after a cardholder presents the card. There are many types of acquiring tokens that are effective in both brick and mortar and e-commerce channels. These tokens may be provided by acquirers, processors, gateways, terminal vendors, financial technology (fintech) companies, or may be generated directly by a merchant. An acquiring token is generally not a form of payment but is used for critical business functions where the merchant does not need to know the original PAN. Had the above merchant been using acquiring tokens for its loyalty system, the card data would not have been available to the attackers when they first accessed that database.

Payment tokens are used to make a payment. Unlike acquiring tokens, the payment token, is used in place of the regular PAN. These tokens allow for one-time-use dynamic cryptograms as well as domain controls to restrict or eliminate potential fraud. Payment tokens are also used for card-on-file transactions where a merchant may replace a database of recurring payment data with payment tokens. Payment tokens are designed to be of such a low value to criminals, that the tokens do not require PCI DSS protection when used with dynamic cryptograms and/or domain controls. If the merchant had an acceptance channel that utilized payment tokens, the attacker would likely prefer to focus his efforts on another channel or another target altogether.

Issuer tokens are issuer-created account number replacements, often deployed as one-time-account numbers, also called one-time use virtual cards. These are used in unique scenarios where it is desirable to limit an account number to a single use, a set dollar amount, or even a specific merchant. These types of tokens are generated by an issuer or on behalf of an issuer. These tokens are often used in the travel industry and the merchant is not always aware that they are receiving an issuing token as it works like a regular PAN today. Because of this inability to distinguish between PANs and issuer tokens, merchants should always treat these tokens as if they were regular unprotected card data. (Note: As Issuing tokens are a special use case and not in the merchant domain of control, they are not referenced in the illustrations above.)

WHAT TECHNOLOGY TO CONSIDER?

As EMV Chip, P2PE and tokenization each reduce risk in different ways, it may be challenging to identify the best way forward. Ideally, a merchant will implement all three technologies as the three address different risks and together offer the highest level of risk reduction.

Many merchants in the US are moving forward with EMV Chip technology through the implementation of new payment terminals. EMV Chip technology is meant to prevent the use of stolen card data being used to create counterfeit cards by providing the ability to authenticate the card. EMV Chip does not provide protection of the account number and other information associated with that card.

While merchants are migrating to EMV Chip technology, it is important that they consider how to quickly follow on with P2PE and Tokenization technologies. A merchant that is largely card present with little e-commerce activity may choose to first implement P2PE to maximize risk reduction efforts instead of tokenization. A merchant that is predominantly e-commerce based, or has a large database of stored account numbers, may want to focus first on tokenization technologies and follow on later with P2PE for protection of its payment terminals and ECRs.

If a merchant is only performing card-not-present transactions, then it is likely to focus on tokenization technologies exclusively. In this case, the merchant may investigate payment tokens and potentially payment token enabled e-wallets for its card-on-file systems. These merchants can also use payment tokens for loyalty and/or analytic systems and/or may wish to investigate acquiring tokens for this purpose. (Note that all eCommerce merchants already use channel encryption to protect browser to web server communications—this paper does not any suggest changes to this practice.)

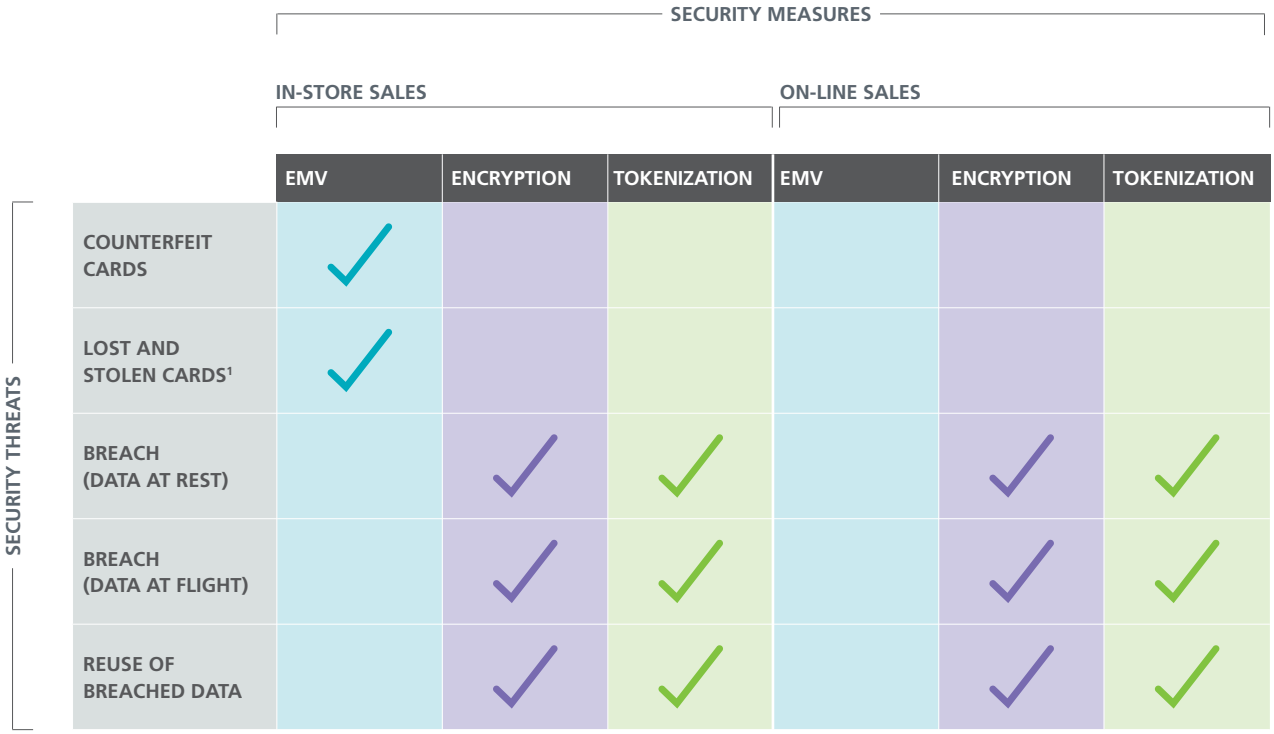
Non-merchants can also benefit from these technologies. Financial institutions, processors, and merchant service providers can use encryption and tokenization technologies to protect data in transit and to protect stored data.

All entities should ask themselves whether or not they truly need access to sensitive card data, or if a unique identifier of the payment data (a token) is adequate to meet business needs. If sensitive data is not needed, it should be securely deleted. If data is transmitted between entities, it must be transmitted using strong encryption, much the same way as a merchant would encrypt card data in its payment terminal. A merchant should also consider removal of legacy data when moving to secure payment technologies. For example: If a merchant tokenizes its loyalty database, it must ensure that the old card data is removed or otherwise protected per PCI DSS requirements.

In summary, a layered approach to payment security is best. Each technology has a very specific purpose and minimizes risk in a unique way. By implementing layers of security technology, one can ensure that they are maximizing risk-reduction efforts and minimizing the chance of becoming the next big name in breach headlines.

APPENDIX

The following illustrations include detailed use cases and are intended to foster conversation amongst technical staff, customers, etc.



1 When used with a PIN