

Exploring Different Approaches to Increasing Data Security Using Tokenization and End-to-End Encryption

Data Breaches: An Ongoing Threat

A rise in massive, high profile credit card breaches in recent years has underscored the need for merchants, point-of-sale (POS) and property management system (PMS) providers, credit card processors and other third party organizations to do everything they can to secure sensitive payment data. Despite the many measures being taken – the billions of dollars spent to secure customer data, to harden and fortify payment systems, and to create policies to prevent unwanted intrusion or leakage of that sensitive data – those who seek to compromise and profit from it continue to find new ways to infiltrate security systems.

Adopting a New Mindset for Securing Data

Bob Russo, General Manager of PCI Security Standard Council, boiled it down to: “There needs to be a mind shift from just compliance to security [since] compliance is a byproduct of good security.” And when it comes to PCI DSS, Russo added “PCI DSS is the baseline.”¹

John Sheets from Visa made it clear for merchants that protecting cardholder data cannot be viewed as merely a fire drill. Instead, PCI DSS assessment should be seen as a key step to achieving security. Sheets said “Everyone needs to move away from a validation and it’s done approach. Instead, it is an ongoing process.”¹

PCI DSS then, should be used as a starting point in the evolving efforts to thwart attackers and prevent them from achieving their goal. PGP Corporation and Ponemon Institute report that data breaches from malicious attacks doubled in 2009 – from 12 percent to 24 percent – and cost substantially more than those caused by human negligence or IT system glitches. They noted that “organizations should strongly consider a holistic approach to protecting data wherever it is – at rest, in motion and in use.”²

This paper explores the use of two technologies to protect merchant POS/PMS systems and network infrastructures – **tokenization**, which is principally used to secure “at rest” data, and **end-to-end encryption**, which is being used to protect “in-flight” data.

Securing Data at Rest: Tokenization

Tokenization provides two clear advantages that build on strong POS/PMS system security practices:

- It reduces the instances of sensitive data in an organization, thus reducing the scope of a PCI DSS audit.
- If a merchant suffers a hack, there is no stored card data for thieves to steal.

With tokenization, a token or replacement value is returned and stored in place of the original data. The token refers to the actual data, which can be stored locally or in a “hosted” data vault but the sensitive data cannot be derived from that token.

When the token is created in the same format as the sensitive data it can be safely used by any application, database, or backup medium within the organization. The token minimizes the risk of

¹ RSA Conference Panel, March 18, 2009, “Protecting Vulnerable Data in Payment Systems – Are We There Yet?”

² 2009 Annual Study: Cost of a Data Breach - Understanding Financial Impact, Customer Turnover, and Preventative Solutions (US), www.pgp.com/insight/research.reports/index.html, January 25, 2010, p. 3 and p. 6

exposing the actual sensitive data and allows operational and analytical applications to work with little or no modification.

Tokenization solutions such as Merchant Link's TransactionVault™ have been successful in removing sensitive cardholder data from merchant systems and have greatly reduced the risk of data breaches. To date, TransactionVault has been installed in more than 15,000 locations across North America. Customers include IHOP, Carlson Restaurants Worldwide (TGI Friday's), Ruth's Chris, Perkin's, and Friendly's, as well as a major retailer.

Securing Data In-Flight: End-To-End Encryption

Despite the advantages for organizations that adopt some form of tokenization and its capability to secure sensitive data at rest, merchants must also safely transport cardholder data to the payment processing banks and subsequently to the card issuers. In order to achieve a truly secure solution, some methodology must be implemented in addition to tokenization to protect the data in-flight – that is, the data that is transported to the payment processing banks and to the card issuers.

Current PCI DSS standards state that SSL encryption of connections being made over public networks is sufficient for protecting data in-flight. However, vulnerabilities can be exploited in the way data is passed between applications, databases, and files from the point where it is entered at the end user interface to another systems or servers within a merchant's network infrastructure.

Vulnerabilities Still Exist

A recent security alert release from *Visa Business News* spelled out some very real concerns over vulnerabilities that may still exist within organizations and how those weaknesses are currently being exploited.

According to Visa's computer forensic investigations, hackers are gaining unauthorized access to POS/PMS environments as a result of insecure remote desktop solutions or poor network configuration. A memory-parsing vulnerability previously identified in the *October 2008, Visa Data Security Bulletin*, is being actively targeted and exploited within the hospitality industry. This vulnerability can be exploited by hackers when they install debugging or "sniffing" software on POS/PMS systems in order to extract magnetic-stripe data from volatile memory. The increased use of debugging tools that pull sensitive data from volatile memory suggests that attackers have successfully modified their techniques to obtain payment data that has not been tokenized.

In order to remove the risks posed by exposure of sensitive data in-flight and as it is stored in volatile memory, many providers, including Merchant Link, offer clients an end-to-end encryption solution, in which card information is strongly encrypted at – or as near as possible to – the point where the card is swiped or entered into the POS/PMS system. The aim is to leave the data in that encrypted form as it passes through the POS/PMS system and only decrypt and manipulate the sensitive data in highly-secure hosted data storage and routing facilities, such as those provided by gateway or network providers, or at the processors themselves.

Encryption Methodology Requires Coordinated Components

Achieving a solid and strong encryption methodology calls for the coordination of several important components:

- The encryption scheme itself – such as 3DES, AES, and others.
- The management of encryption keys, e.g., Public Key Infrastructure (PKI), Derived Unique Key per Transaction (DUKPT), Identity-Based Key Management, etc.
- The securing of the location or devices that hold the encryption keys to prevent exposure to attackers.
- The ability to change or rotate the keys.

All of these components must be tightly managed and synchronized to ensure creation of the expected data set that can then be decrypted for use “down stream” in the payment processing data flow.

Additionally, for a solution to truly be considered encrypted “end to end,” it must encompass not only the POS/PMS and its local environment, but also the gateways used to route the information, the processors that handle the information for the merchant, and the card issuers.

Along this path there are numerous systems, applications, databases, and networks over which the data will traverse. Therefore, a more feasible approach and accurate description of current solutions being developed in the industry are “point to point” solutions that cover the POS/PMS system, its local network, and the transit that must be made to more highly secured PCI DSS compliant organizations like gateway providers or the payment processors. Solutions involve one or more of these approaches:

- **Encrypting software at the POS/PMS**
- **Encryption from the point of swipe**
- **Integrated terminal encryption**

APPROACH 1: Encrypting Software at the POS/PMS

This solution entails the use of software to intercept the swiped sensitive data as it passes to the POS/PMS by the card reader. The software encrypts the data and passes it to the integrated POS/PMS software in encrypted form. It remains in encrypted form as it passes through the POS/PMS system and for the journey to the gateway, where the sensitive data is decrypted and routed to the payment processor. The tokenization process then returns a token with the authorization response, which does not contain card data in any form.

APPROACH 1: Encrypting Software at the POS/PMS (continued)

Advantages of this solution

- This solution may be easier to implement than hardware-oriented solutions.
- This solution is consistent with implementations generally already in place, rendering the issue of manually-entered card numbers much less complicated.

Drawbacks to this solution

- Payment card data is still in its raw form as it is passed from the magnetic card stripe reader (MSR) to the encrypting software, providing a small window of opportunity for extracting the sensitive data.

APPROACH 2: Encryption from the Point of Swipe

This solution entails the use of a magnetic card stripe reader that has the capability to strongly encrypt swiped data and pass it to the integrated POS/PMS software in encrypted form. It remains in the encrypted form as it passes through the POS/PMS system and for the journey to the gateway. There, the sensitive data is decrypted and routed to the payment processor. The tokenization process then returns a token with the authorization response, which does not contain card data in any form.

Advantages of this solution

- The data itself is encrypted within the MSR hardware and doesn't exist in its raw form anywhere on the POS/PMS or in transit to the gateway provider or processor.
- The MSR is typically a tamper-proof peripheral and the window of opportunity for compromise of the data is very, very small.

Drawbacks to this solution

- The encrypting MSR has to be an integral part of the POS/PMS system and its encrypting functionality has to be activated, usually at the point of installation into the POS/PMS or at some point later, once the merchant begins to process transactions.
- Typically, once the encrypting functionality has been activated it can't be de-activated, making maintenance and "swapping" of POS/PMS hardware more complicated.
- Some number of cards must be entered into the POS/PMS manually due to damage to the magnetic stripe on the card itself, and that path of card number entry doesn't include the MSR, which contains the encrypting function. Manually entered cards would not be encrypted in this solution.

APPROACH 3: Integrated Terminal Encryption Solution

The aim of this solution is to remove the POS/PMS from the scope of PA-DSS entirely by using a separate piece of terminal hardware to manage the swipe of the card, the encryption of the sensitive data and the transport of that data to the gateway provider. The terminal is also responsible for accepting the pertinent sale information from the POS/PMS and then formatting it and sending it to the gateway. After receipt of the response from the gateway provider, the terminal sends pertinent information – such as the approval or error code and the token – to the POS/PMS system.

Advantages of this solution

- Sensitive cardholder data never resides on the POS/PMS in raw form, greatly reducing audit costs for the merchant.
- The terminal hardware is locked down or hardened, meaning even the users themselves cannot access the device. This takes some of the onus of hardening the POS/PMS off of the POS/PMS provider and the merchant.

Drawbacks to this solution

- It represents a fairly significant change from the way POS/PMS systems currently handle payment processing.
- The solution entails the implementation of an additional piece of hardware for each point where end users swipe card data.
- It calls for development by the POS/PMS providers to have their system work with this device during the tendering workflow.

Conclusion:

The ongoing threat of credit card breaches has underscored the need for companies to do everything they can to secure sensitive payment data. This means they must utilize solutions to protect both data at rest and data in-flight.

Essentially, companies must seek out solutions that ensure data is protected “end to end.” Three common approaches in the market today are:

- Encrypting software at the POS/PMS
- Encryption from the point of swipe
- Integrated terminal encryption

The approach that appears to be the most effective at removing data from merchants’ systems and reducing the scope of a PCI DSS audit is the integrated terminal encryption approach.

Still, Merchant Link recognizes that every merchant has different needs. Some may find that one of the other approaches is better suited to their requirements, while others may prefer a hybrid approach. As a forward-thinking payments security provider, Merchant Link supports all of these approaches and offers customers the flexibility to integrate with almost any encryption software or device.

Want to learn more about Merchant Link’s E2EE solution?

Contact us at mlesales@merchantlink.com or 1-866-853-3845.

About Merchant Link

Merchant Link is a leading payments gateway company, providing PCI compliance, secure solutions, data transport services and comprehensive technology to merchants, software providers and credit card processors. Its premier product, TransactionVault™, features the next generation of tokenization by replacing each card number with unique keys. Merchant Link currently supports more than 150,000 hotels, restaurants, ballparks, and other venues, and maintains connectivity to the major US payment card processors. Founded in 1993 and headquartered in Silver Spring, Md., Merchant Link handles more than 3 billion transactions for some of the world's best-known merchants. Further information is available at www.merchantlink.com.

Merchant  Link *Relax. We got it.*

8401 Colesville Road, Suite 900
Silver Spring, MD 20910
301.562.5000
866.853.3845

merchantlink.com