

Decrypting Retail Card Data Security

Retailer environments are just too complex to completely and constantly lock down against all intruders. Encrypting cardholder data from end-to-end may be the only way to meet current security requirements. But not all encryption solutions can fully meet the task.

Executive Summary

Getting a driver's license doesn't mean you can't be sideswiped or get a speeding ticket. Similarly, being assessed as compliant with the PCI Data Security Standard one day doesn't necessarily insulate you from a data breach in the future.

It's a fact of life that the retailer's environment is just too complex to completely and constantly lock down against all intruders. An organization may have hundreds or thousands of distributed store and distribution center locations, tens of thousands of employees, and multiple connected devices, systems and networks. Maintaining constant vigilance over every access point and every place where data is stored or transported is a challenge that will likely never be fully met. Many retail organizations are understandably frustrated that the millions of dollars invested in becoming PCI compliant does not protect them from the threat and the liability of a data breach.

Retailers aren't in the business of security, nor can they be expected to be experts in payments technologies—their primary focus is on understanding customer needs and delivering the right goods at the right time in the right location. PCI requirements follow a two-year update cycle, so by the time a retailer gets up to speed on current mandates, it's going to be time to learn the next set. Meanwhile, security challenges are constantly evolving as criminals—some with insider access—seek to leapfrog electronic protection schemes.

Thus, many are increasingly convinced the only way to protect data is to encrypt it from end-to-end so that any data that is intercepted is unusable. The challenge is how to decide which emerging encryption solution can best meet your needs with minimal disruption to your existing infrastructure. This white paper provides information to help make that evaluation.

The End-to-End Challenge

The current and evolving PCI DSS standards reflect a perpetual cold war with cyber criminals, with each side trying to better the other's capabilities. As long as retailers need to accept, transmit and store credit and debit card information, organized crime will attempt to breach the retail enterprise to obtain this information.

Many retailers say that basic compliance is like trying to hit a rapidly moving target. "The PCI guidelines are onerous, confusing, and are constantly changing," said Dave Hogan, senior vice president and CIO for the National Retail Federation, during testimony to a Congressional panel reviewing the issue of whether PCI DSS improves security. Reflecting growing retailer frustration, Hogan charged that, "PCI is little more than an elaborate patch."

Shielding retailers from the liability of security breaches requires that they rid their systems of credit and debit cardholder data. But because that data must transit from the point of sale through internal and external servers and networks to a processor in order to complete a transaction, the retailer needs a way to handle the data without possibility of compromise. No retailer can afford to ban card payments and no retailer can be completely sure that all of its computer systems and points of entry are completely secure from intrusion or internal misappropriation.

The only realistic way to deal with cardholder data, then, is to ensure that it is completely unusable. Encryption, utilizing the strongest, government sanctioned levels of cryptography, provides the potential answer. But nothing dealing with retail security is that simple. PCI DSS requires the protection and encryption of the primary account number (PAN) and other card data wherever it is stored, processed, or transmitted. The difficulty with implementing this essential and common-sense security measure is that encrypted data, by definition, cannot be read by other systems without first being decrypted (or "normalized").

The conventional process for normalizing encrypted data so that local POS systems can use the data requires a non-trivial upgrade, retrofit, or replacement of the existing POS/ECR application software as well as major increases in throughput capacity to deal with the overhead of encrypted data transport. This is a major new cost for brick-and-mortar merchants, and one that creates a substantial obstacle for widespread

merchant accommodation of the PCI Standard for encryption. Perhaps more importantly, the conventional approach of enabling local decryption so that card data can be used locally (e.g., for authorization) defeats the primary purpose of encrypting card data in the first place. If card data resides anywhere in the local system in an open format, it can be compromised. Further, the endless cycle of encrypt-decrypt-encrypt that is required to support conventional encryption creates additional layers or pockets of security vulnerability and puts a significant strain on throughput capacities of the merchant host system.

Under the Hood

There are a variety of encryption techniques that have been offered or proposed for the retail industry. Each offer well-documented strengths, but also feature key limitations that inhibit their ability to provide a complete solution.

Database Encryption is widely used in the computer industry to protect records. Various methods and tools exist to encrypt fields, records or an entire database. Databases can be encrypted on a single server or on distributed servers, and there are both software- and hardware-based products and solutions available.

This form of encryption does not, however, protect data from end-to-end. The infrastructure of most retailers typically reflects a hodge-podge of servers, applications and networks. Many, or all, of these systems may require access to the database information. Even if data is quickly decrypted and subsequently re-encrypted, that moment of passage in an unencrypted format may be all that is needed for a network sniffer program or hidden Trojan Horse to capture the information and route it outside of the corporation's firewalls. In larger operations, the situation may be complicated by the fact that there may be many disparate databases to protect, and in all likelihood some legacy systems that represent a complicated integration task.

As recent news stories have detailed, even well-protected military databases are frequently under assault from sophisticated hackers who frequently are able to gain entry despite security precautions, and leave behind small, hidden software programs for nefarious purposes.

Tokenization Schemes replace cardholder information (usually the PAN) with a numeric, randomly generated token. This type of security is

relatively inexpensive and provides a means for a retailer to store information that does not violate PCI DSS restrictions. Actual cardholder data is typically held by an outside service provider, while the retailer can store the token and utilize it later as a means to track chargeback and other subsequent activities.

While this after-the-fact storage may be relatively hacker proof, the tokenization doesn't occur until after the authorization of the transaction. Somewhere along the line, the cardholder data is being encrypted/decrypted and passed along networks between servers. Another inherent weakness is that token cipher keys are likely stored somewhere within the retailer/service provider infrastructure where hackers may have an opportunity to sneak in and obtain them.

Secure Sockets Layer (SSL) is a widely deployed technology that enjoys broad support across multiple industries. This is a communications protocol that allows computers to safely communicate with each other over a network without fear that the conversation can be eavesdropped. Based on public key cryptography, this method of security bears little or no cost for use and has become the standard of choice for conducting commerce over the Internet.

The inherent limitation of SSL is that data is only encrypted while in transmission on the network. The sending and receiving servers must encrypt and decrypt, respectively, the cardholder data, creating potential exposures on either end. Many payment terminals cannot support SSL and the communications protocol imposes a processing burden that may hamper older POS systems.

Software-based Encryption Schemes are usually implemented independently by POS vendors, typically by exchanging keys with an upstream application.

Who holds the keys? That's a question anyone considering software-based encryption should be asking. A significant vulnerability of software encryption is the storage and location of the encryption keys. For example, in the wake of one large retailer breach, the company disclosed in an SEC filing that, "...the intruder had access to the decryption tool for the encryption software [we] utilized..." If a hacker can gain access and has the wherewithal to root around a company's systems, stored encryption keys can provide a bounty. Some vendors may implement the same key across all systems, making any retailer using such systems vulnerable to the trading of passwords and keys that is endemic across

the Internet. Such systems may also require changes at the POS system or on host applications.

Hardware-based Encryption Schemes are built around a secure tamper resistant hardware module that generally sits at a central location on a corporate network, providing strong key management and secure key storage. Hardware-based encryption is widely held to be superior to software-based encryption.

However, these hardware solutions can be very expensive to deploy at store locations, where the need for encryption is as great, if not more so, than at corporate headquarters. These systems will require changes to the POS in order to accommodate encrypted card information, and still leave exposed the passage of cardholder data from the payment terminal to the POS system.

Encompassing the Whole Problem

The major limitation to the approaches just described is that they generally address just part of the problem, and leave out one or more critical components that could prove to be the point of vulnerability in a breach situation.

VeriFone firmly believes that a total systems solution approach to the problem must encompass the following:

- End-to-end encryption means encrypting card holder information at the exact instant of acceptance inside a secure, trusted device and keeping it encrypted throughout your enterprise.
- Key management per industry standards including secure transport, tamper-resistant security module (*TRSM*) storage and secure key generation in a facility certified with proper controls and procedures.
- A monitoring component to provide 100% device and transaction encryption compliance and instant notification of potential issues.

Key factors to consider in evaluating end-to-end encryption solutions include:

Hardware Based Encryption in a *TRSM*, essentially a mini-Host Security Module (HSM) that can be easily deployed across large numbers of points of service. These devices are tamper resistant, and offer detection and shut-down protections in the event of tampering. It is critical that the device be able to thwart breach efforts by automatically destroying stored keys in the event of a tampering effort.

Last Mile Coverage ensures the solution encrypts the cardholder data at every point in the enterprise. Criminal elements will always seek out the weakest link in the security chain, so it is most beneficial when end-to-end encryption starts at the card acceptance and ends at the acquirer.

Encrypt – Decrypt – Encrypt Cycles can pose multiple points of exposure, while also adding processing overhead to POS systems and other retail payment applications. Every time that information is decrypted it is vulnerable to attack. As one large processor acknowledged following a widely publicized breach, “We have industry-leading encryption, but the data has to be unencrypted to request the information. The sniffer was able to grab that authorization data at that point.” True end to end encryption schemes should not require the data to be decrypted until it reaches its final destination.

Data Formats – most encryption schemes produce encrypted data that features a longer character string than the original data, contains characters that may not be valid to the POS system, and may not pass normal data validation schemes. Without some means of format-preserving encryption, existing POS and application software will require costly updates to adapt to the scheme.

Encryption Cipher Schemes are crucial to end-to-end encryption. Because of the diversity of the retail environment, it is tempting for vendors to adopt non-standard encryption schemes that have not been vetted by the encryption community and may not meet the requirements of Triple-DES or AES-level security. Some proprietary encryption schemes may in fact be exploited by sophisticated hackers and may not work with debit transactions if the PIN block is not properly encrypted.

Encryption Key Management -- Software and Database based encryption schemes often lack basic encryption key management security controls. A truly secure key management solution has the ability to securely synchronize local data encryption keys with back-end decryption systems. End-to-end encryption keys should be generated on a per-terminal basis in a secure facility.

Encryption Key Storage – As demonstrated in one large retailer breach, encryption keys can prove to be a treasure trove to criminals if they are stored in an accessible location. Keys should only be generated within a Host Security Module and inside a secure room. A true end-to-end solution ensures that keys are never transmitted in the clear and are never stored in memory or on disk that is subject to compromise.

Compliance Monitoring - The security cycle consists of three components, protection, detection and remediation. Encryption covers the protection component, but a good security system also needs the ability to detect attempted breaches and mitigate the damage from detected breaches.

VeriShield Protect

Responding to industry needs for a solutions-approach to end-to-end encryption, VeriFone developed *VeriShield Protect*—a payment card security solution that ensures no cardholder data can be compromised even in the event of a breach. VeriShield Protect was designed to be implemented without requiring changes to most existing POS and enterprise applications. VeriShield Protect shields credit and debit account information from the moment a card is accepted until the data is received at a secure decryption appliance located in a retailer's secure data center, at an off-site service provider, or at an acquirer or processor organization.

It's a fact of life that retailers are loath to implement new technologies that require major changes to their infrastructure. The cost and time involved to upgrade POS systems across all stores is a major impediment to implementing new protection schemes; in addition, many retailers fear this is just the beginning and that additional changes will be required in the future to support changes to the encryption scheme. VeriShield Protect provides end-to-end encryption without imposing on

retailers the burden of managing an encrypt-decrypt-encrypt cycle, which is prohibitively expensive and disruptive.

Based on AES encryption, VeriShield Protect utilizes a format preserving encryption technology called *VeriShield Hidden Encryption™* (VHE) that is compatible with existing retail application infrastructure and will not require POS application changes. This is possible because once the card information has been encrypted, patented algorithms convert the data string back into the format that the POS application expects, allowing the transaction to be processed normally. To the retail POS application, data encrypted with VHE looks like normal card data; the encrypted card data will pass all standard checks at the POS level such as MOD 10 or LRC. The VeriShield Protect solution retains the ISO prefix in first six digits of the card number in unencrypted fashion for BIN range processing and the last four digits for receipt processing purposes. Other encryption schemes change and extend the character string in a manner that is not compatible and can increase network bandwidth requirements by 37% to over 100% if multiple messages are required. The network Decryption Appliance determines if the card data needs to be decrypted by Merchant ID, Terminal ID and the BIN range of the PAN.

VeriShield Protect is deployed by installing the encryption application into VeriFone MX800 Series and Vx Solutions payment devices to encrypt the card information; a decryption appliance is installed at the host processor, retailer's switch or on VeriFone's managed gateway to decrypt the card number for subsequent processing.

The AES based cipher has been vetted by the encryption community and the VeriShield Protect solution is designed to utilize industry standard key management schemes. Because the encryption is processed within the tamper resistant security modules of VeriFone's existing PCI PED approved payment systems, card data is never in an unprotected state whether stored in memory or in transit over networks until it is decrypted by the decryption appliance. Even if hackers are able to breach a retailer's systems and gain access to data, anything encrypted with VeriShield Protect would be unusable by them.

Another component of VeriShield Protect is the *VeriShield Secure Device Management Service*. This is a real-time, always on, and continuous compliance monitoring and fraud identification solution that provides security status data on a device and per-transaction basis via an alert messaging and dashboard system, so if a breach were attempted or occurred the retailer or acquirer would be immediately

alerted. In addition, data encryption keys can be managed remotely as part of the device management service.

Data Protection Effectiveness

As you evaluate encryption option for your operation, we offer the following checklist to assist in selecting the most effective and most feasible solution.

- A strong encryption cipher scheme to prevent compromises
- Secure encryption key storage to prevent theft of the encryption keys
- Industry standard and certified encryption key management
- A solution that does not require POS & application software changes
- A solution that does not increase processing overhead
- A solution that does not burden network bandwidth
- A real time monitoring component to ensure 100% encryption compliance

No retailer wants to be vulnerable to a security breach. But complying with security requirements imposed by card brands can be confusing and potentially costly. Because these requirements are constantly evolving, many retailers are hesitant to invest now at the risk that future mandates will require yet another retooling. An end-to-end solution using the format preserving encryption technology optimized in VeriShield Protect meets today's challenges and provides the flexibility to adapt without impacting the POS infrastructure.

For more information, email verishield@verifone.com or visit www.verifone.com/definitivesecurity

Security Glossary

AES – Advanced Encryption Standard – accepted by the US Government for encryption purposes – uses 128-bit ciphers

Cypher – an algorithm for encrypting and decrypting data

DES – Data Encryption Standard – older, 56-bit encryption standard no longer considered suitable for withstanding ‘brute force’ attacks from commercially available computers. Triple DES is a commercially viable method of encryption that utilizes three DES keys to produce a stronger cypher of up to 168 bits

FPE –Format preserving encryption - a method of encrypting data where the result looks like the original unencrypted value in terms of length, characters used and error checking supported

HSM -- Host Security Module, a tamper-resistant device that provides the cryptographic facilities necessary for securing transactions in financial networks

SSL – Secure Sockets Layer, an industry-standard encryption protocol for securing communications over the web; typically used to secure online credit card transactions

TRSM -- Tamper-Resistant Security Module, a device intended to make intrusion difficult, to make such efforts visible to physical inspection, and to disable the functionality of a device in the event of intrusion

Copyright © 2009 VeriFone and Semtek Innovative Solutions Corporation. All rights reserved. No portion of this document may be reproduced or distributed in any form or by any means without the prior written permission of said companies. All trademarks are the property of their respective owners.