Security Leadership White Paper

Securing Trust in the Payment Industry

Electronic payment is built on trust—trust between the consumer and the retailer, and just as important, among the various parties involved in supporting payment solutions. In an increasingly uncertain environment, the key to maintaining this trust is highly sophisticated security measures.

VeriFone

Contents

Executive Summary

Staying a step ahead of growing computing power

It's not a coincidence that the personal computer and electronic payment were introduced at approximately the same time, a little more than two decades ago. The ability to put significant processing power onto computer microchips opened the door to a series of technological breakthroughs that have changed the way people live and work.

But while personal computing was instrumental in the development of electronic payment, the rapid and relentless growth of processing power has also posed one of the biggest risks for payment. That's because this rise in processing power has put tremendous computing capabilities into the hands of individual users, a few of which have tried to use this power to defraud service providers and consumers.

Fortunately, fraud has been a relatively manageable problem for most of the two decades that electronic payment has been in existence. The reason for this is the emphasis that the payment industry has placed on comprehensive and sophisticated security. These security measures have established and maintained fundamental trust among consumers, retailers, and service providers that is necessary for electronic payment to function.

Today, the value of payments worldwide continues to soar, making the potential for losses huge. At the same time, fraud is becoming increasingly sophisticated and difficult to counteract. The concentration of supercomputing power on desktops and in homes has given resourceful criminals an even better opportunity to unlock respected security algorithms such as DES, and to devise clever schemes for card skimming and identity forgery.

To address this, payment security is undergoing significant changes. An enhanced encryption standard called Triple DES (3DES or TDES) has been created that would require more than a lifetime of processing with current computing power to break. This is being combined with key-management methods such as Master Key/Session Key—commonly known as Master/Session—and Derived Unique Key Per Transaction, or DUKPT.

As the leader in the electronic payment industry since it began in the 1980s, VeriFone has taken an active role in developing, promoting, and implementing many of the most sophisticated security protections. The company participates on national and international committees that have been responsible for many of the standards, including the consortium of industry leaders that wrote the 3DES

draft key management specifications. VeriFone will continue to work to provide the highest level of confidence for its customers around the world.

This white paper will review the current trends in payment system security, explain some of the alternatives that are available, and examine the latest advances in encryption, key management, and file authentication—which promise to further enhance the protections upon which consumers, retailers, and service providers rely.

Introduction

An age-old problem with a modern twist

For centuries, wherever currency has been exchanged for goods and services, there have been some that try to acquire wealth dishonestly. In this regard, electronic payment is no different from any other form of payment. As electronic payment has increased in transaction volume and dollar value over the past two decades, it has become the target of rising fraudulent activity by individuals and sophisticated gangs who would like to take advantage of any gaps in security.

Card skimming is one of the most common types of fraud. Skimming involves making a copy of a card's mag-stripe data, then using that "skimmed" data to create a bogus card and charge hundreds or thousands of dollars to that cardholder's account, before he or she receives the next statement. A common location for card skimming is in a restaurant, where a dishonest server could use a pocket device to read and capture the card data before returning it to the cardholder. There have even been cases where retail POS terminals have been tampered with—reprogrammed to capture card information and forward it to a third party.

But skimming is just the beginning today. There's a wide range of physical and logical schemes designed to capture magnetic stripe data, falsify a cardholder's identity, steal PINs, or break encryption codes. Among these are:

- "Shoulder surfing"—Looking over a cardholder's shoulder when he or she is entering a PIN at an ATM or POS terminal.
- Video cameras—Would-be thieves sometimes get very creative in devising schemes to steal PINs—watching through telescopes from nearby hillsides as customers use keypads at petro stations, or taking advantage of mirrors or video cameras mounted in ceilings to observe customers as they use terminals.
- Wireless transmitters—These can be attached to send data to unauthorized individuals with receivers in the near vicinity.
- Modifying or replacing hardware with altered devices—As mentioned above, terminals have been electronically modified or swapped with devices that can capture and store PINs until the thieves can access them.
- False prompting for PINs—One of the most common attacks using computer logic is to design a software patch that prompts the customer for a

PIN or other identification information, which is then captured in clear text rather than encrypted form for improper usage.

- PIN or key exhaustion—Taking advantage of the significant computing power that now exists on affordable PC workstations, the criminal element has designed programs that will automatically try for hours or days at a time to discover PIN combinations or security keys used to protect critical data.

The risk of losses is substantial, and growing larger each year. *The Nilson Report* estimates that card-based payment in the U.S. alone will reach $2.7 trillion by 2005. With that much money being processed at the POS and switched across payment networks, it has attracted the interest of some of very savvy criminals—all focused on finding any weakness that would make it possible to intercept some of those dollars.

The magnitude of risk has gotten the attention of not only the retailers and acquirers, but also the many governments, regulatory agencies and solution providers such as VeriFone, which work closely together to limit fraud. These well-known agencies include:

- International Standards Organization (ISO)
- American National Standards Institute (ANSI)
- EMVCo (the organization that now watches over the global EMV specifications for smart card transactions)
- National Institute of Standards and Technology (NIST), which has recently published the Advanced Encryption Standards (AES)—highly sophisticated guidelines and specifications that will be widely used by government and commercial organizations to protect sensitive data.

Security Trends

Better methods for identifying customers and authenticating transactions

The primary challenge to securing electronic payment is the difficulty posed by lack of face-to-face contact. Transactions do not take place in front of a bank officer who can vouch for a customer or verify that he or she has adequate balances to cover the payments. Instead, these purchases often occur hundreds or thousands of miles away from the acquiring institution, with transactions distilled to bursts of electronic data that often provide no verifiable proof that legitimate cardholders are interacting with the retailer or service provider.

As a result, most security measures have focused on positively identifying the various parties, authenticating transactions, and protecting the financial data that's sent or received. These security measures can be implemented in several ways:

- Hardware-based, software-based, or a combination of the two (best)
- At the point of sale, back-end host, or both (again, best)
- On the chip that's embedded in a smart card (*very* difficult to steal)
- Through increasingly sophisticated encryption and key-management schemes to withstand the most powerful attacks

One of the key trends in improving the identification and authentication process is the use of personal identification numbers (PINs). An increasing number of POS card-based transactions use online verification of PINs, including debit and electronic benefits transfer (EBT). Some countries with high fraud rates have made PIN entry a core element of the EMV specifications for the use of smart cards.

Smart card transactions can be controlled through the use of software on the embedded chip. PINs can be verified offline, matching them to data that is stored on the chip. This offers significant savings in regions of the world such as Europe and South America, where communications costs are relatively high. PINs can also be used together with online authorization, for an exceptionally high level of protection.

Not every country or region of the world is on the same page with the various trends in security. But around the globe, every retailer, acquirer, and service provider shares the same concerns: how to make transactions safer and financial data more secure. All are focusing on a common set of solutions as the means to achieve these goals.

Encryption and Key Management

The need for more sophisticated encryption techniques

POS transaction data has long been protected by encryption techniques. These techniques use mathematical algorithms, or problem-solving procedures, and cryptographic keys to scramble personal cardholder information and financial data from "clear text" into cipher text. For most of the past 20 years, the international standard encryption scheme used to protect POS transactions has been the Data Encryption Standard (DES).

Cryptographic algorithms alone are never sufficient to ensure reasonable levels of security. In fact, most cryptographic algorithms are not kept secret, but rather are published so that they gain widespread usage. To achieve the necessary security the encryption key must be kept secret. To assist in ensuring that the encryption key remains secret, sophisticated key-management methods are used to frequently change or vary the key or keys used to encrypt/decrypt the data. When a transaction takes place a key, securely stored in a PINpad or POS terminal, is used to encrypt the consumer's PIN information and, in some countries compute a code that is used to determine if the transaction message has been tampered with. In the case of DES, the host must have access to the same cryptographic keys in order to determine if the message has been tampered with and/or validate the consumers PIN.

For payment transactions to remain secure, it must take longer to discover a key by unauthorized methods than the useful life of the information that the key is protecting or cost more than the value of the information obtained. Several of the most common key-management methods are Master/Session and DUKPT, which will be explored in more detail below.

With symmetric algorithms such as DES, the same key is used to both encrypt and decrypt the transaction data. For this reason, the key must be carefully protected at all times—from the moment it is first loaded, or injected, into the PINpad or terminal at a secure site, until it is changed. Asymmetric algorithms such as those used in EMV use one key to encrypt data and another to decrypt it. Typically, one of the keys—known as the public key (used to encrypt) —is published, while the other—the private key (used to decrypt)—is kept secret so that unauthorized individuals can't gain access to protected data.

Until recently, breaking the single DES algorithm or stealing the 64bit key used with the encryption method was considered, if not impossible, at least relatively impractical. Exhaustive attacks, where a potential thief uses a

computer to try every combination of numbers until the key is discovered and the code is broken, were limited by the amount of processing power that was available.

Then, as computing power on the desktop and in the home advanced exponentially throughout the 1990s, the unthinkable began to enter the realm of possibility. That created the need for an even more sophisticated encryption standard, and Triple DES (3DES) was born.

3DES requires longer keys

The 3DES algorithm increases the difficulty of breaking the cryptographic keys by extending the number of DES operations and the number of keys used. Data that is to be protected is encrypted and then decrypted several times using multiple keys. The result is that these "key bundles" have stretched the compute time needed to break the code using today's computer processing power from 15 to 20 years to more than a million years. Refer to the ANSI X9.52-1998 standard for more details.

The 3DES algorithm is rapidly being adopted by the card payments industry as a proactive measure against potential attacks to break single DES keys. Although no major security breach under DES has ever been publicly reported, it has been demonstrated that it is feasible to do so, making a more secure encryption method a requirement.

Visa has announced that all newly deployed POS PIN acceptance devices (PINpads and terminals) must support 3DES as of January 2004. MasterCard has been requiring all newly installed merchant POS terminals and PINpads to support 3DES with a minimum of double-length keys since April 2002, with processor host systems expected to be 3DES compliant in April 2003.

The key to secure key management

As previously discussed, secure key management is at the heart of reliable data security. Keys *must* be kept secret to ensure the integrity of the encryption process. Key management is the method used to securely inject, change, and protect the identity of these keys.

The two leading key-management methods are Master/Session and DUKPT:

- Master/Session—In simplest terms, a "master key" is injected into the PINpad or terminal at a secure facility. This key is not used for encrypting or decrypting PINs. Instead, it is only used to decrypt a "session," or working, key—which has been encrypted by the host using the same master key, then sent over a network to the POS terminal.

This session key is the key that will be used to protect PINs and data as transactions take place. The term "session" refers to the length of time that the key will be valid. Session keys can be changed daily or more frequently—once every eight hours, or every four hours, or every hour, for instance.

It would even be possible to change the key after each transaction, by sending a new session key to the terminal the instant the previous transaction had been processed. This would greatly increase the security of the system, as even if the session key were discovered, it would only be useful for obtaining information regarding the one transaction for which it was used. The downside of changing the session key for each transaction is that it would greatly increase the processing and communications workload and costs for both the host system and terminals.

- DUKPT— Derived Unique Key Per Transaction is, as the name implies, an alternative key management scheme, which was developed to provide a new cryptographic key to be used for each transaction without the processing and communications cost penalties discussed above. In very simplified terms, DUKPT creates a new key following every transaction. But rather than transporting these keys from the host to the terminals, each successive key is *derived* by both the terminal and host based on elements contained in the previous transaction and a base derivation key. A series of up to one million unique keys can be generated within a typical PINpad or terminal. This scheme has the distinct advantage of not appreciably slowing transaction throughput at the POS, while significantly enhancing data security.

Both Master/Session and DUKPT key-management methods have had to evolve to keep pace with the enhancements of the 3DES algorithm. Don't settle for a shortcut. In the current payment landscape, some vendors have attempted to implement 3DES Master/Session encryption using older, single DES key management protocols. ANSI X9, the standards committee responsible for the financial industry standards in the US, has issued a specific warning regarding the misapplication of single DES techniques to 3DES Master/Session key management. Make sure the terminals you select comply with all ANSI standards and guidelines. VeriFone is committed to supporting the new 3DES specifications to the fullest extent to provide the maximum protection for our customers. In fact, VeriFone has played an active role in the development of 3DES, as one of six members of the ANSI committee developing the standard. VeriFone is also working to clearly define the 3DES implementation process, and has created a detailed set of draft guidelines for full 3DES support.

Other Security Protections

Additional security protections from card associations and VeriFone

Beyond encryption and key management, other security protections help to guard against unauthorized access or use of personal cardholder and financial data.

Visa PED specifications

Visa has published security specifications for PIN entry devices (PED), and effective January 2004, all new PINpads or POS terminals with internal PINpads must have passed PED specification testing by a Visa recognized laboratory to receive approval from the card association.

VeriFone's VeriShield security architecture

VeriFone has also created its own security architecture that incorporates sophisticated file authentication techniques using state-of-the-art Public Key Infrastructure (PKI) technology. In addition, VeriShield includes a number of security protections designed to thwart physical and logical attacks.

VeriShield has a number of components:

- VeriShield file authentication uses digital file signing techniques to verify the authenticity of a given file *before* it can be executed on a terminal or PINpad. For a file to be authenticated, it must be digitally "signed" by an authorized party, proving that the file is an original that has not been changed from the date it was approved. This is done by comparing the signature in a file against a copy of the signature, using public/private key verification. The actual file signing takes place with the help of a smart card-based file signing tool, which is securely supplied by VeriFone. VeriFone also operates a Certificate Authority that issues and maintains records of all digital certificates that are in use as part of VeriShield.
- Co-processor functionality can remove the burden of processing cryptographic operations from a terminal's main processor, which is responsible for sending transaction data and receiving approval from the service provider or acquirer. This can greatly improve the performance of the terminal. VeriShield's co-processor function is accomplished with the help of a powerful security chip that supports RSA asymmetric encryption.

- The architecture's *physical security* capabilities include special tamper-detection measures, which can render a terminal inoperative by erasing the encryption keys if it is attacked. Tamper-resistant features also make it infeasible for unauthorized third parties to obtain personal cardholder information or financial data by attempting to access the internal electronic components of terminals or PINpads.

VeriFone's VeriShield security operates as part of the Verix environment on many Omni POS terminals and SC family of Smart PIN Pads.. Visit www.visa.com/pin for a listing of PED-approved devices.

VeriFone Terminals and PINpads

The most comprehensive security protection in the payment industry

VeriFone has consistently been a leader in providing security for POS transactions. We have integrated a comprehensive suite of security protections—including the latest 3DES encryption and key management methods, Visa PED specifications, support for EMV-based smart card transactions (on models with smart card readers), and VeriShield file authentication—into a number of terminal families and PINpads:

- Omni 3700 family
- Omni 7000 terminals
- Omni 3600 wireless terminals
- Omni 3210 SE terminals (3DES only)
- Everest*Plus* terminals
- SC 5000, SC 5xx smart card devices
- PINpad 1000 SE

VeriFone also offers its SecureKit tool for secure key injection and the VeriShield File Signing Tool to efficiently and effectively support VeriShield file authentication.

VeriFone is actively rolling out full support for 3DES encryption with DUKPT and Master/Session key-management methods designed for the new standards.

VeriFone also understands the importance of secure transactions traveling over open IP-enabled public networks. Therefore, it has incorporated Secure Socket Layer (SSL) technology into its solutions supporting both IP wired (dial to ISP, Ethernet) and wireless (CDMA, GPRS) technologies. This provides the security necessary to further protect the integrity of the financial transaction messages.

Summary

Building a more secure future

The payment industry will continue to see efforts by unauthorized individuals to gain improper access to information and financial data. These efforts will grow more sophisticated with the never-ending expansion of computer power.

For acquirers, processors, and merchants, sophisticated new security methods and procedures will help in a number of ways. Reduced fraud rates will lower operating costs, putting money back into the pockets of everyone. New customers will be attracted to innovative forms of electronic payment and card-based, value-added applications as they feel more secure about the level of protection provided. In addition, existing customers will also enjoy increased confidence in the industry's ability to protect personal information and safeguard funds—leading to greater customer satisfaction and long-term retention.

VeriFone is continuing to take a leadership role in helping to drive the development and implementation of new security standards, and by being first to market with fully compliant 3DES products. The company offers an exceptionally broad line of products that incorporate the latest technology and support widely accepted security standards. Further, VeriFone is committed to building modular flexibility into a number of our terminal and PINpad families to stay ahead of change in both physical and logical security.

Electronic payment transactions among geographically separated parties demand the ultimate in trust. As the payments industry leader since 1981, no company offers a higher level of trust than VeriFone.

www.verifone.com

1-800-VeriFone