VORMETRIC WHITE PAPER

Protecting Credit Card Data at the Point of Sale

Deploying CoreGuard to Protect Data on Remote Point of Sale Applications

VORMETRIC

In light of recent high-profile credit card data thefts, protection of customer data should be a top priority for any company that processes credit cards. Protection of data stored in point-of-sale applications should not be overlooked. Most Point of Sale applications store credit card account numbers locally in clear text, putting this data at risk of being comprised.

Exposing Credit Card Data at Point of Sale

The storage of customer credit card information locally at the point of sale opens your company to the following risks:

Physical Theft

Data stored in point-of-sale applications are highly vulnerable to physical theft, because they are outside the physical security of your IT environment. At your headquarters, sensitive data is stored behind locked doors, but Point of Sale applications located in public places are exposed to customers and any other individual in the vicinity. In addition, this Point of Sale equipment is accessible to employees, cleaning staff and anyone else who has access to the hardware after hours.

People with malicious intent could easily tap into the Point of Sale hardware and copy sensitive files. Handheld storage devices, such as USB flash drives, make quick and inconspicuous data theft easier than ever. Even if the Point of Sale hardware has no alternate IO ports, like a USB port, the disks themselves are subject to physical theft. Someone could literally pick up the hardware and carry it away. The only protection against this threat is to make the data unreadable to unauthorized users through encryption.

Stored Data

Although you may be under the impression that your customers' account numbers are only stored for a short time, while the credit card transaction is in progress, and are deleted once the transaction has been authorized and completed, you may not realize that many Point of Sale applications store numbers longer than just a few seconds. These applications use credit card numbers for purposes other than transactions.

For example, some Point of Sale applications may store an entire day's worth of transactions locally – including the credit card account number – and then upload and delete the file at end of day. While this additional transaction log can be useful for reconciling disputed transactions, it also exposes your customers' credit card data for extended periods. Point of Sale applications may also store data locally for other reporting functions. Another common Point of Sale feature is to cache "bad" credit card account numbers locally, so that a potential transaction with a known bad account can be rejected immediately.

In addition, due to network reliability and performance constraints, some Point of Sale applications allow for operation in an "offline" mode. In this case, transactions and credit card data may be stored locally while the network is unavailable. For any of these reasons, your Point of Sale hardware may be holding unprotected credit card account information at any time.

One of the problems lies with the third-party Point of Sale vendors. Literally hundreds of companies develop Point of Sale solutions and there is no uniformity with regard to how credit card data is stored. In

reality, you do not know what a Point of Sale application is doing with your customers' credit card numbers, or the many places this data is being stored. Point of Sale application vendors take no responsibility for the protection of your customers' data, leaving you powerless against these threats. In your customer's opinion, protection of this data is your responsibility. Again, the only solution is encryption of data at the point of sale.

Compliance

In addition to the risk of data theft, the accessibility of credit card data at the point of sale poses another problem — non-compliance with Payment Card Industry (PCI) standards. PCI, an industry-wide adoption of Visa's CISP (Cardholder Information Security Program), is the credit card industry's standard for securing cardholder data. Compliance is mandatory for any business that stores, processes, or transmits this data. Protection of stored credit card data is one of the foundations of the PCI guidelines. The only way to meet this requirement, and protect stored data on a system that is accessible to the public, is with encryption.

Protecting Point of Sale Data with CoreGuard™

Vormetric is a leading provider of solutions for protecting enterprise information from unauthorized access or theft. Vormetric's CoreGuard system is a single, scalable and manageable system for data privacy and protection that enables businesses to encrypt cardholder data and control access to sensitive information. CoreGuard has been deployed successfully on Point of Sale systems to protect cardholder information and to ensure compliance with PCI requirements.

Using industry standard AES algorithms, CoreGuard employs policy-based encryption to ensure only authorized applications and users are able to read the data. CoreGuard's five-factor system – based on who, what, when, where and how –requires each access attempt to be validated by your own policies. Any attempt at data access that is not authorized according to these well-defined pre-set parameters will be blocked by CoreGuard. The advantage of CoreGuard is the combination of access control with encryption, ensuring that only an authorized user running an intended unmodified application can decrypt cardholder data and other sensitive information.

Meeting the Challenges of Point of Sale Data Encryption

Protecting credit card data at the point of sale is challenging. In most cases, retailers cannot encrypt the sensitive data files themselves without hindering the operation of the Point of Sale application. The following challenges to encryption of Point of Sale data are outlined to demonstrate how CoreGuard solves them.

Performance

Challenge: Point of Sale applications run on a wide range of hardware. Some of the equipment may be several years old with modest CPUs and limited memory. Since you may need to protect data on hundreds or thousands of Point of Sale stations, however, upgrading the hardware is not feasible. Your

encryption solution must not add an insupportable processing burden to these machines. The problem is that trusted, standard encryption algorithms such as AES are calculation intensive, and adding encryption to the Point of Sale application can slow performance, especially on older hardware. Even adding just a few seconds to each transaction may be unacceptable if you have customers waiting in line. Consequently, any encryption solution must have an imperceptible impact on performance.

CoreGuard Solution: CoreGuard provides high-performance file encryption for data at rest. Vormetric encryption technology is optimized to efficiently utilize all available hardware resources on a host, delivering powerful parallel processing, working right above the file system, as the data is being read or written. In addition, policies determine which specific data files need to be encrypted, so the system only encrypts the sensitive data and does not consume overhead encrypting data that does not require protection.

Transparency

Challenge: Adding encryption to a Point of Sale application should not change the behavior of the Point of Sale system in any way, and it should not require any modifications to the Point of Sale application. The end user's interaction should not be impacted either, as this might add support and training costs. Even requiring an additional password to facilitate encryption could add support costs and downtime if users forget their passwords.

CoreGuard Solution: CoreGuard is totally transparent to your system and users, working right above the file system. CoreGuard integrates seamlessly with your systems, and no modification of the Point of Sale application is required. With appropriately configured security policies, authorized users will experience no changes in Point of Sale application operation.

Access Control

Challenge: While most end-users will only interact with data through the Point of Sale application interface, some managers and support personnel may have access to the file system. To truly protect the sensitive data, it must only be decrypted by the Point of Sale application – or by some other program that has been authorized by a security administrator.

CoreGuard Solution: CoreGuard policies, which are centrally defined and managed, are applied to the Point of Sale system to control which authenticated processes have access to files, and whether or not the data should be encrypted or decrypted. Even an end-user with a local system administrator login could not view the data unless your policies defined in CoreGuard specifically allow it.

Key Management

Challenge: Encryption algorithms use a key to protect data, so the Point of Sale application must have access to the key to encrypt the data when it is written to disk, and decrypt the data when it is read. The keys must be stored centrally in a physically secure environment where they can be managed by an authorized security administrator. But distributing the keys to all of the Point of Sale systems, and yet keeping them secure is a significant challenge. Not only must the key be protected when it is delivered to a client over the Internet, it must not be accessible in the event that someone steals the Point of Sale hardware.

CoreGuard Solution: CoreGuard's architecture provides automatic key management. Encryption keys are stored centrally on the CoreGuard Security Server, a hardware appliance that is in a protected environment and communicates with the CoreGuard software on the Point of Sale system to securely deliver the encryption keys. The keys are protected on the Point of Sale client, and can be configured to be completely offline so that no network connectivity is required for encryption or decryption.

Deployment

Challenge: An encryption solution should have minimal impact on how new Point of Sale systems are deployed and supported. If disk imaging techniques, also called cloning, are used to deploy the Point of Sale application, the encryption system must be compatible with those methods without exposing a security risk. For example, decryption keys should not be accessible in the disk image.

CoreGuard Solution: CoreGuard software is fast and easy to install on a new Point of Sale system, or you can use disk imaging to clone an existing Point of Sale system with CoreGuard. Then you can register the new Point of Sale installation with the CoreGuard Security Server so policies and encryption keys can be delivered to it. Meanwhile, keys and policies are created and maintained centrally on the CoreGuard Security Server.

Affordability

Challenge: You may have hundreds, thousands or more Point of Sale systems to maintain. Your encryption solution must not require additional expensive hardware for each system or the cost would quickly become prohibitive. In addition, the encryption solution must not involve expensive modifications to the Point of Sale software, or add costly support procedures.

CoreGuard Solution: CoreGuard is a scalable solution that can be economically deployed to thousands of Point of Sale stations. The only additional hardware required is the central CoreGuard Security Server to securely store keys and policies. All other functionality is carried out by software which is easily deployed to the Point of Sale systems at low cost. Centralized management further reduces the complexity and cost of the solution.

Leveraging Vormetric Across the Enterprise

The encryption and access control technology that make CoreGuard an ideal solution for protecting data at Point of Sale applications also enables CoreGuard to protect data stored anywhere within your organization. The same centralized CoreGuard Security Server that enables security administrators to enforce security policies at remote Point of Sale applications, can be used to enforce security policies for your application, database, and file servers, as well as individual workstations. Each of these policies can be defined by you according to your unique needs. So when thinking about implementing CoreGuard to protect POS applications, you should also consider maximizing your investment in CoreGuard to encrypt data and provide access control across your enterprise.

CoreGuard has been proven in real-world installations at many leading corporations in a variety of vertical industries that require protection for sensitive data. Vormetric is the technology leader in the data protection arena, holding 13 patents and FIPS validation on all products. The company is the winner of

industry acclamation such as ComputerWorld's 2004 Innovative Technology Award, and serves as a respected partner of industry giants such as IBM, Sun and Oracle.

Conclusion: Protect Your Customers with Point of Sale Encryption

Vormetric's CoreGuard is an ideal solution for protecting sensitive data at Point of Sale applications. The system's architecture allows CoreGuard to transparently work seamlessly with any Point of Sale application without requiring any modifications to software or hardware. CoreGuard's high-performance encryption combined with access control ensures that private data cannot be decrypted if the disk is stolen or if users with administrative rights try to access the data files outside of the Point of Sale application. Key management is secure, automatic and centralized, enabling fast deployment and ease of operation. CoreGuard is a vital tool to protect your customers and assure compliance with PCI standards.

For more information:

Vormetric Inc
3131 Jay Street
Santa Clara, CA 95054
www.vormetric.com
+1 408 961 6100
Email: sales@vormetric.com


VORMETRIC