

A Strategic Approach to Preventing Data Breaches

By Derek Tumulak

Proven technologies are now available which allow administrators to encrypt data on the desktop or laptop at the application, database, file, or storage level.

As the financial impact and reported number of information security breaches continue to increase and regulatory compliance becomes mandatory, many corporations are focusing their security efforts and investments on data encryption. Proven technologies are now available which allow administrators to encrypt data at the application, database, file, or storage level, and on laptops as well as on storage media such as disks, tape, optical or other electronic media.

Regardless of which of the above techniques is implemented, cryptographic keys are the essential foundation of any encryption solution. If private keys fall into the wrong hands – whether through negligence or a malicious internal or external attack – the security of your encrypted data is permanently compromised. In addition, if the wrong person is provided authentication or access, the safeguard of encryption can be easily bypassed. A number of advanced authentication and access control mechanisms can be used to ensure that only authorized users are permitted to encrypt and decrypt sensitive data.

Given the complexities of encryption, organizations should adopt a strategic approach to preventing data breaches and protecting their data that takes into consideration processes for backup and replication, and look at solutions that provide access to essential information and meet *all* industry legislation and compliance requirements.

Types of encryption

Depending on where an organization stores its sensitive data, decisions need to be made regarding where and how information is encrypted. The basic types of encryption are the following:

- **Application:** protects data as soon as it enters the enterprise

- **Database:** often used to protect payment card industry (PCI) related data like credit card numbers, as well as employee and customer information, and social security numbers
- **File:** includes sensitive data such as corporate plans and intellectual property residing in files
- **Storage:** includes in-line encryption, and encrypting all information that is stored in NAS/SAN environments
- **Tape:** typically used for off-site storage of archived information
- **Laptop/device:** often implemented as a precaution against physical theft

Different types encryption can be used together as part of a strategic plan against data breaches; however, not all encryption is equal, so security professionals should consider the types of encryption as well as where they encrypt.

Native encryption solutions

A number of vendors have introduced native encryption into their products. While this provides a rudimentary level of security through encryption, it can still leave an enterprise vulnerable to data breaches if not used in conjunction with an effective overall security strategy.

There are a number of potential vulnerabilities and performance disadvantages inherent with a stand-alone native encryption solution compared with using a comprehensive encryption solution. Specific issues arise regarding key management, support of heterogeneous environments, batch processing, and granular access control and auditing.

With database and storage encryption, native solutions typically use the precaution of encrypting database specific keys with a master key. Nonetheless, the master key is stored on

the database where it is vulnerable to attack. Since all cryptography is performed on the database server, the table-specific keys exist in memory, allowing a hacker to gain access to the key in the clear. Ideally, encryption keys should be stored on an external appliance and thereby secured against application layer attacks and malicious administrators. FIPS 140-2 validated appliances for tamper-resistant hardware requirements, and not allowing keys to exist in memory on the database server, provide a much higher level of security

The advantage of an external encryption appliance is the ability to optimize encryption processing, which when done on a native encryption product often impairs other processes. The off-loading of cryptography to an appliance for batch processing provides much higher processing power and speed and consumes fewer resources than cryptography in software. Off-loading batch processing is especially beneficial with granular access control and auditing, where every cryptographic function is logged, and real-time reporting allows for immediate detection of any potentially dangerous activity.

A strategic security plan

Developing an encryption strategy will often mean balancing a number of different and sometimes apparently contradictory requirements. In general, all of the following criteria must be considered:

- **Security:** Administrators, users, partners, and customers need to know they can trust that their data and identities are safe at all times.
- **Performance:** The system must function in a manner that is transparent to legitimate data users and business processes, and it must scale easily.
- **Flexibility:** The system must be adaptable to a range of environments and be capable of integration, through standard interfaces, with all types of data encryption systems from a range of vendors. Interoperability and adherence to industry standards is also an important consideration.
- **Manageability:** Key and policy management must be simple and intuitive so that administrators fully understand – and granularly control – system status at all times. There must also be capabilities for logging and auditing all administrator and user actions.
- **Availability:** The system must be able to recover in the event of one or more network or equipment failures, or even a widespread disaster.
- **Scalability:** The solution may need to support not only data center applications, but also remote sites such as retail point of sale (POS) and branch offices, so the system must scale easily to accommodate future requirements for business growth or additional redundancy requirements. The infrastructure must also support open APIs, and integrate seamlessly with the existing information and security management

To effectively manage keys within an enterprise, security teams need a single solution that can be integrated with multiple key management and security products from a range of vendors.

systems that are part of the enterprise infrastructure. This includes PKI, identity management, logging, and information life cycle management (ILM) solutions.

Enterprise key management

One of the most important aspects of implementing an encryption strategy, and often the weakness that leads to a security breach, is key management. Key management comprises all of the processes that are used to create, store, distribute, rotate, archive, and delete keys. To ensure encryption meets its objectives, all of these phases must be conducted in a manner that is secure, reliable, and auditable.

Further, to effectively manage keys within an enterprise, security teams need a single solution that can be integrated with multiple key management and security products from a range of vendors. For example, in an enterprise that has implemented database, application, and storage encryption technologies, the cost and management overhead of implementing a vendor-specific key management solution for each product could be prohibitively high. Multiple different resources would need to be trained and managed. Auditing and record keeping would be extremely complex. Overall, there would be increased risk of either not meeting compliance requirements or not being able to recover data because of misplaced keys.

Centralized management

The first step in ensuring security is to deploy a key management solution that enables administrators to manage keys from a single central authority. A good key management system should also let you know what other devices have copies of a key. Ideally, it would be able to set limits on how long those other devices can keep copies of a given key, although this requires some trust that the other device will actually delete the copy. The central authority may decide to delegate authority to other parts of the organization, but should have the ability to take back control in the event of system abuse or failure. Centralized logging and auditing is also enabled so that all user and administrator actions can be tracked.

Secure key management must also enforce separation of duties. This is required in order to prevent an administrator from having sufficient permissions to carry out an internal attack. For example, one administrator might only be given access to network configuration functions, while another might only be given access to certificate management con-

trols. An enterprise should also be able to use multi-credential techniques to protect against malicious administrators who might attempt to grant themselves unauthorized access to create or delete keys. This level of granular access control enables organizations to control and closely monitor administration operations, and significantly reduce the risk and exposure from internal attacks.

Key storage

The system should also provide a location for key storage that is separate from the location that holds the encrypted data. As mentioned above, storing keys on the same application or database servers that hold sensitive data presents significant security risks when compared to storing keys on security appliances. When cryptographic keys are stored on unsecured platforms, attackers can gain access to them very quickly. While a system that stores keys and data in the same location may still be compliant with some security standards, clearly encryption is worthless if such a location has been compromised.

There are primarily three ways for securely creating and storing keys:

- A hardware security module, or HSM, is the most secure method. An HSM is typically a PCI card specifically designed for securely generating and storing keys. Physical security is the fundamental difference between an HSM and other methods. In the event of physical theft or tampering, keys stored on an HSM are destroyed.
- Using a hardened security appliance is another method for providing secure key generation and storage. Hardening is the process of securing a system against attackers, which often includes removal of unnecessary accounts and services, encrypting the file system, removing root access, and marking highly sensitive files as read-only. Often an HSM is integrated with the security appliance to provide physical security.
- The last method is software-based key management. With this method keys are often encrypted using a hard-coded master key and/or split apart with each piece stored in a different area of the system. Often software-based key management solutions run on systems that have not been hardened, thus making them more susceptible to application layer attacks and malicious administrators. One example is that an administrator could easily attach a debugger to the key management solution, allowing himself to easily extract the key(s) undetected. Further, particularly in a large enterprise environment where the application and database servers often number in the hundreds, it becomes increasingly difficult to manage the cryptographic keys residing on these servers. In addition, as the complexity of key management increases, the risk of not backing up a key, or exposing a key, increases

exponentially. Software solutions also do not protect against physical attacks.

Key rotation

The ability to rotate keys is an important security feature. Key rotation can occur on a regularly scheduled basis or may be required as part of the reaction to a breach. In both cases, it is important for the system to remain online as new keys are introduced. Historical information, such as information stored offline on tape, can be encrypted in addition to online data if there is reason to believe the keys have been compromised.

Open cryptographic standards

To support security best practices and eliminate the exposure of weaker or older encryption algorithms, key management must support keys for the most advanced open cryptographic standards available, including RSA 2048 and AES 256. It is important to implement industry standard cryptography algorithms, as they have been thoroughly tested by government agencies and standards bodies such as NIST to ensure high levels of security.

There also needs to be the option to protect data and keys in transit using SSL or another secure transport technology.

Backup and replication

Enterprise key management needs to be able to provide service even in the event of a sharp increase in demand or in the event of one or more network or equipment failures. A complete approach to ensuring availability requires the implementation of replication, load-balancing, and recovery capabilities.

Take for example a company with two data centers: one in San Francisco and another in New York.

All of the key management appliances for this company have been configured for replication. All of the appliances automatically share the same configuration for keys, groups, users, and authentication policies. This gives each of the appliances sufficient information to backup any of the others.

Load balancing is a client-side feature that enables a client to balance its load, typically in round-robin fashion, between multiple appliances. In this case, each of the two data centers shares its load between the appliances that are in the same geographic location. Each of these groups is configured as a load balancing group.

To provide recovery in the event of a network or system failure, a system administrator configures a second load balancing group as a backup tier that can take over in the event that the primary load balancing group (or tier) is disabled. Health-checking is used to continually monitor the status of all appliances in the system to determine when recovery is required. This example shows just two tiers, a primary in San Francisco and a secondary in New York; however there should be the capability of setting up a tertiary tier if desired.

Having capabilities for replication, load-balancing, and recovery provides the ability to configure a fault-tolerant architecture that ensures service will continue, even in the event of multiple network or equipment failures.

Authentication, authorization and auditing

Along with key management, authentication, authorization and auditing is also extremely important. Below are the key areas of what you should look for when evaluating a solution.

Authentication

It is important to require mutual authentication between an encryption solution and systems requesting keys. Without mutual authentication it is possible for an attacker to execute a man-in-the-middle attack. One way to address this is to require a password and username *and* a certificate. For additional security, the key management solution can access the client user name from the certificate. That user name can be compared against the user name provided in the authentication request. If the user names match up and the password provided is correct, the user is authenticated. In addition to traditional methods, solutions can also offer ways to restrict access to keys based on the IP address that originated the request.

To facilitate integration into existing environments, the encryption solution should have the ability to use an LDAP server for authentication. In addition, it is an added convenience and cost saving if the key management solution is able to operate as a certificate authority. This eliminates the cost of working with a third-party certificate authority.

In order to ensure that administrators are promptly advised of any suspicious activity, automatic alerts, such as industry-standard SNMP traps, should be triggered if security thresholds are exceeded.

Auditing and logging

Lastly, a comprehensive system of auditing and logging is required in order for administrators to spot any significant usage trends or to establish a forensic trail. There should be the ability to track every administrator, user, or system action. Some examples of information that should be audited and logged include the following:

- Key and policy generation, edits, deletion, etc.
- Device configuration including name, network, logging, etc.
- System events for monitoring threshold boundaries and sending alerts
- Encryption and signature requests

Encryption solutions should provide logs that are cryptographically protected against malicious modification. For example, a software solution running on the same host that is using the keys and logging to a plain file would allow an at-

tacker who can compromise the box to not only get keys but also modify the logs to cover his tracks

Conclusion

In response to security threats and regulatory mandates, enterprises have adopted a range of encryption technologies. Because sensitive data can exist in many locations and forms, enterprises should realize that single point or native solutions may not provide sufficient protection or performance. A strategic approach is recommended that looks at an enterprise's total requirement for data protection. In addition, encryption needs to be part of a comprehensive solution that also takes into consideration performance, backup and replication, authentication and authorization, and auditing and enterprise key management. One of the reasons data breaches occur is because organizations see encryption as a one-shot solution, not a process. Companies fail to realize that once enterprise-wide encryption is in place, continual monitoring of not only the encryption processes but of personnel management is essential.

To summarize the information and best practices included in this article, below is a basic list of recommended best practices gathered from previous encryption strategy implementation experiences of many Fortune 500 companies.

- Ensure the enterprise's business and security objectives are well understood before choosing and deploying key management.
- Plan for all aspects of the key management life cycle and for future scalability in terms of both system size and diversity.
- Ensure access controls are implemented with as much granularity as practical.
- Never transmit or store keys in an unencrypted format.
- Use standard cryptographic algorithms and utilities.
- Back up keys on a regular interval to a separate dedicated hardware device.
- Continually monitor or audit all automated and manual actions.
- Ensure procedures are in place to ensure the integrity and security of logs.
- Authenticate and sign logs for non-repudiation.
- Restrict access to audit logs to prevent tampering or deletion.

About the Author

Derek Tumulak is Vice President of product management at In-grian Networks and has over 12 years of product management and engineering experience in the technology industry. He has an extensive background in enterprise security, payment systems, and Internet messaging. You may reach him at derek@ingrian.com.