

Key Management: The biggest issue in storage encryption

By Dore Rosenblum

Over the past several years, malicious attacks against computer systems and electronic thefts of private information have skyrocketed. And each data compromise or exposure leaves companies wondering if they will be next.

Over the past several years, malicious attacks against computer systems and electronic thefts of private information have skyrocketed. And each data compromise or exposure that lands in the headlines leaves companies wondering if they will be next, and how they can prevent such an event from happening in the first place.

To provide protection from these attacks, most companies have secured their systems and networks from outsiders, implementing perimeter-based security strategies with firewalls and virtual private networks (VPNs) to ensure that external users without proper authorization cannot access sensitive data. But according to the CSI/FBI 2005 Computer Crime and Security Survey, internal threats are nearly as prevalent as outside threats. Of the 453 respondents, 56 percent had at least one incident within the past 12 months from an internal source¹. The perimeter-based security solutions most companies depend on are powerless to stop these internal threats.

Acknowledging this gap – as well as the demands of increasing government and industry-driven² regulations concerning data retention and privacy – some companies are looking beyond traditional perimeter-based security methods to secure data. They are focusing instead on securing the data resident on the storage media within their organizations (data at rest) and the data moving between their systems on the network and storage devices (data in flight or data in transit). This is also known as “storage security.” With proper stor-

age security, a company can ensure data integrity as well as mitigate the damage compromised or stolen data can have on its long-term corporate image and financial standing.

Typically, storage security includes three components:

- Authentication
- Access control
- Encryption

Authentication ensures that users and systems are who they say they are. Several standards and protocols for authenticating users on a network are widely implemented in companies around the globe, including Remote Authentication Dial In User Service (RADIUS) and Challenge-Handshake Authentication Protocol (CHAP). New storage-specific methods and standards, such as Diffie-Hellman CHAP, are now emerging that enable organizations to add authentication to the storage infrastructure. In other words, they can require authentication of users or devices to occur before information can be stored.

Access control limits the ability of the user or system to access data. On a network, users can only view data allowed by router access control lists and directory services that control access. Within the storage infrastructure, which servers have access to what data is controlled by zoning and LUN (logical unit number) mapping.

Encryption is the third component of an effective storage security strategy. Encryption is the process of scrambling data to prevent unauthorized persons from reading it, and has two primary components: the encryption algorithm and the key. While encryption algorithms can be implemented using various standards, most sys-

1 A full copy of the report can be found on the US Department of Justice Website: http://i.cmpnet.com/gocsi/db_area/pdfs/fbi/FBI2005.pdf.

2 One example of an industry-driven initiative is the Payment Card Industry Data Security Standard (PCI DSS) in the financial industry. See the end of this article for information on PCI DSS.

tems use specific algorithms for specific operations, such as AES for encrypting data at rest.

Many encryption algorithms in use today were created by government agencies or standards bodies. The National Institute of Standards and Technology (NIST) selected the Advanced Encryption Standard (AES) based on an open request for proposals. Other cryptographic algorithms and standard test criteria have been established by NIST under the Federal Information Processing Standards (FIPS). FIPS is a set of requirements and recommended practices for securing data in US government agencies³. Encryption devices and key management systems are certified by NIST to ensure vendors have met best practices.

Once an encryption algorithm is selected, a key is generated or assigned based on the specific security requirements. In order to ensure that security is maintained for encryption operations, processes must be put into place that allow for complete control and security of the keys used to encrypt and decrypt the data. Key management is the process used to provide this control.

Key management systems

A key management system combines the devices, people and operations required to create, maintain and control keys. The system contains operational practices that must be implemented to make it work effectively. While the key management system is part of an overall security strategy, security plays a very important part of key management itself, in the form of access control and logging.

Access control within the key management system ensures who or what has access to which keys. The simplest mechanism is to allow all key administrators and all encryption devices access to all keys. The reality, however, is that not everyone or not every device needs access to the same keys. By limiting access to keys, the organization also limits its vulnerability to security risks. Thus, an effective key management system has role-based access control to ensure a single user doesn't have ubiquitous rights to all keys.

A secure audit log server should log every event on the key management system. Administrators should have limited access to this server, and it should not allow deletion of a log without first archiving it using encryption, authentication, and a digital signature for the encrypted file. Access to the server for viewing the logs should be limited to audit users only.

The operational aspect of any key management system is probably the most overlooked aspect of the system as a whole. Processes must be repeatable, replicable, and secure to meet the requirements of key management in today's organizations. No matter what key management system is used, every key has a "shelf life" that must be monitored, maintained and controlled. This is the role of the key management system. From the moment it is generated or entered until it is deleted, managing the life cycle of the key is imperative to ensure it is never exposed or used inappropriately. Organizations should take care to ensure the security of keys, even restricting them from inappropriate use by administrators or other authorized users. Important elements of a key management system include: key generation, key distribution, key archiving, key sharing, key backup, re-keying, key deletion, and key logging.

Key generation

Keys can be created using either manual or automatic generation. The prevailing wisdom, however, is that the less human intervention, the more secure the key. In addition, unique keys generated on a per-use basis (e.g., a unique key generated for each tape) provides greater security than a single key generated to encrypt data on all tapes in the enterprise. An automated key generator can be a stand-alone device, or included in a piece of cryptographic equipment. The one absolute requirement is that the generator must be contained in a secure hardware component, rather than in software running on an off-the-shelf system.

Key distribution

Once created, a key must be distributed to all systems that will encrypt and/or decrypt data. Again, there are several options for performing this action. The first, and preferred, method is electronic key distribution. The second method is manual distribution via smartcards. No matter which method is used in an ongoing manner, the initial sharing of a key or certificate is typically conducted manually, so that a secure communication can be initiated to begin sharing keys electronically.

When using manual key-exchange methods, the recommended practice for keys used for data or keys that protect other keys is to use "split knowledge systems." These systems, such as M of N (also referred to as K of N) systems, split the key into pieces among multiple individuals. Normal practices of split knowledge systems break the keys into component shares to be given to five different users, and then require a minimum of two of these users to be present to reestablish the key⁴. This is good practice for top-level key recovery in the event of disaster.

No matter how a key is distributed, it should be encrypted at least once using a strong method, or split into multiple shares using split knowledge trust.

Key archiving

When a key is distributed, best practices advise to send the key directly to an archive and, therefore, a backup facility. If the key user has the ability to forward it to the archive, he or she should do so before using the key to encrypt data. Key archiving provides the ability to quickly recover a key. Typically, the key archiving process is automated, but it can be done manually if required. Key archives are typically implemented within some form of tamper-proof hardware to ensure key security. Examples of hardware-based key archiving solutions are secure memory, the hardware security module (HSM), or a secure hardware appliance.

Key sharing

In some cases keys need to be shared outside of an enterprise with business partners. For example, an organization which sends an encrypted tape to a supplier requires a mechanism to share the encryption key to read the tape. Key management systems should be able to granularly share keys and support mechanisms for securely sharing these keys with outside partners.

3 More information on NIST and FIPS can be found at <http://csrc.nist.gov>.

4 A. Shamir, "How to Share a Secret," *Communications of ACM*, Volume 22, Number 11, 612-613.

Re-keying in a storage environment

Re-keying is the operation where a new key is used to encrypt and decrypt data. If the system re-key was a result of potential exposure of the key or data, the old key should be marked for deletion. Once the re-key operation is completed, the key should be deleted either automatically or as part of an operational process.

There are situations where re-keying data at rest must be planned. One such case is tape media, where re-keying can require a large amount of time. Re-keying tape media should be planned when media or equipment is rotated out due to age, in order to ensure recovery. Because tape can be kept for many years, a good archiving mechanism is imperative, to ensure the recoverability of the key when the medium is recovered, replaced, or expired.

A final consideration that can alleviate some of the concerns of constant re-key operations is to use granular keys, such that at minimum one key must exist for each medium, such as key per tape, key per LUN, or key per file.

Key recovery

Key recovery from an archive in a data-at-rest scenario is extremely important, particularly when encrypted data must be stored for several years due to regulatory or other requirements. An archive should be capable of retaining keys for long periods of time and providing those keys when needed. If the organization chooses to implement automated key recovery, the process should be tested at regular intervals to ensure that it meets the organization's needs, no matter in which type of archive the keys are stored.

Key deletion

The most challenging part of any key management system is ensuring that, once a key has been exposed or retired, or the data medium on which it was stored has been lost, stolen or replaced, it can be deleted so that it cannot be recovered by any malicious party. A good key management system will have both automated and manual processes, and will ensure that all copies of a key are deleted from all devices, archives and backups.

Key logging

A good key management system must track every key, logging which users have used it, and when and what actions those users conducted with the key. This is called key logging. From the time a key is generated until it is finally deleted, all events related to that key should be logged in one or more types of logs. Then, depending on the nature of the key, the data it protects, and who must be notified of a key event, one or more type of alert may be required.

Alerts based on events can be used to correlate potential misuse of keys or systems, or potentially malicious activities, as well as the occasional human error. Automating the alert process is important, simplifying the day-to-day operations of the key management system and ensuring that the appropriate individuals are notified in a timely fashion when an event occurs.

Recommended practices

There are different concerns for implementing key management at single versus multiple sites.

Single-site implementations – Particular attention must be paid to key backup and recovery. The organization must ensure that keys are

regularly backed up to an offsite location, such as a disaster recovery site. The organization should consider key escrow at a third-party facility, but not before evaluating whether the escrow service can meet the organization's security and operational requirements for data recovery.

Multiple-site implementations – On the other hand, multiple sites have the benefit of a remote site at which to replicate keys within the organization, as long as the appropriate security mechanisms are implemented. At a minimum, keys should be archived locally, and regular backups should be conducted remotely to provide full recovery capabilities. Logging should also be replicated between at least two sites for local as well as centralized secure audit logging. An effective key management system can automate sharing of keys between locations to facilitate information recovery at either location.

In a multi-site implementation, separation of duties such as administration versus security functions becomes more important, because information may be sensitive to the corporation or a specific department, so that not all sites in the organization should have or need access to the data.

Conclusion

Key management is a critical part of encryption, no matter what is being encrypted. The longer data must be maintained in an encrypted form, the more important key management becomes. And when encryption is part of a storage security solution, ensuring that keys can be managed, maintained and recovered can help an organization mitigate many of the risks that exist when encryption is used improperly.

Key management systems today must provide the appropriate access limitations to keys based on the requirements of the organization and the type of data being encrypted, e.g., data at rest or in flight. Regulatory data, intellectual property, financial data, and other types of sensitive information should be classified unless the encryption solution warrants encrypting all data in the environment.

While architecting a complete key management system can be time-consuming, companies should at least implement a key archive and backup policy, with appropriate access controls, to minimize risk. In addition, by performing a risk analysis for the data in question – prior to implementing an encryption solution – organizations can help ensure that the right data is protected by the right solution.

About the Author

Dore Rosenblum is VP of Marketing for NeoScale and holds responsibility for the development and implementation of the firm's global marketing strategy. Dore brings over 19 years of marketing and corporate development experience, with extensive expertise in the information security sector, from NeoScale, F5 Networks, uRoam, 3Com and IBM. Dore holds an MS in computer science from the University of North Carolina, Chapel Hill, and a BA in computer science from the University of Virginia.

References

For information on the Payment Card Industry Data Security Standard (PCI DSS):

American Express: http://www125.americanexpress.com/merchant/oam/ns/USEng/FrontServlet?request_type=navigate&page=dataSecurityRequirements

Diners Club: http://www.dinersclub.com/dce_content/merchants/fraudmanagement

Discover: http://www.discovernetwork.com/resources/data/data_security_overview.html

MasterCard: http://www.mastercard.com/us/merchant/security/what_can_do/index.html

Visa: http://www.usa.visa.com/business/accepting_visa/ops_risk_management/cisp.html?it=12%7C/business/accepting_visa/ops_risk_management/index.html%7CCardholder%20Information%20Security%20Program