



Efficient SAN-Based Tape Encryption

Efficient SAN-Based Tape Encryption

By W. Curtis Preston and Doug Anderson

© 2008 TechTarget

BIOS

W. Curtis Preston is the Vice President of Data Protection Services at GlassHouse Technologies. He wrote *Using SAN and NAS*, *Unix Backup and Recovery*, and *The Storage Security Handbook*. He has been designing and implementing data protection systems for over 12 years and now consults on data protection with end users from Fortune 100 and Fortune 500 companies, as well as with vendors around the world. Preston is a sought-after speaker for technical and CXO-level audiences. He can speak the languages of business and technology to any level of audience, using humor to keep the presentation enjoyable. Preston speaks at several storage, security, disaster-recovery, and business-continuity-oriented industry events.

Doug Anderson is the MDS Software Product Manager with Cisco. He is the Cisco product-line manager for Storage Media Encryption and Cisco Fabric Manager software for the MDS 9000 family. Anderson has been managing SAN-related software products for the past eight years and has been involved with large-scale computer I/O subsystem design and architecture for over 20 years.

This *IT Briefing* is based on a Cisco Systems/TechTarget Webcast, “Efficient SAN-Based Tape Encryption.”

This TechTarget *IT Briefing* covers the following topics:

• Introduction	1
• Routes to the Backup Data	1
• The Backup Server	1
• The SAN	1
• Employees	1
• The Backup Administrator	1
• The Backup Tapes	1
• Responding to the Threats	2
• Encryption	3
• The Cisco Solution	3
• MDS 9000 Product Family	3
• Cisco SME	4
• Conclusion	5
• Common Questions	6

Copyright © 2008 Cisco Systems and W. Curtis Preston. All Rights Reserved. Reproduction, adaptation, or translation without prior written permission is prohibited, except as allowed under the copyright laws.

About TechTarget *IT Briefings*

TechTarget *IT Briefings* provide the pertinent information that senior-level IT executives and managers need to make educated purchasing decisions. Originating from our industry-leading Vendor Connection and Expert Webcasts, TechTarget-produced *IT Briefings* turn Webcasts into easy-to-follow technical briefs, similar to white papers.

Design Copyright © 2004–2008 TechTarget. All Rights Reserved.

For inquiries and additional information, contact:

Dennis Shiao

Director of Product Management, Webcasts

dshiao@techtarget.com

Efficient SAN-Based Tape Encryption

Introduction

This document discusses the protection of stored data, particularly the data that resides on backup tapes. Many enterprises vigilantly protect the data that resides on their servers, but they forget that their backup data has a security hole in it.

Routes to the Backup Data

An enterprise's backup data takes one of five routes:

- The backup server
- The SAN
- Employees
- The backup administrator
- The backup tapes

The Backup Server

The backup server is all-powerful by design. In order for it to function, it must be able to read and write every file in the environment and it also must be able to execute a script before or after a backup. The problem is that the script-running functionality can be turned on or off—and it is generally on all the time.

Any backup package must run as Root or Administrator to do its job. Combining the ability to run a script with administrator-level access means that the backup server can perform many actions, such as system inventories, changing the root/administrator password, making a copy of the data, or starting a remote xterm session on a Unix machine.

The SAN

It is possible to hack a SAN, though it is a somewhat unlikely route. Most enterprises use worldwide names (WWN) as their authentication method. WWN are easy to fake or guess and a means is built into the driver to change the WWN. In addition, the management port of the corporate LAN is generally managed by plain-text protocols. The tape library, disc devices, VTL, and other key items are attached to the corpo-

rate LAN. If a “black hat” can control the management port, this individual could get into any portion of the LAN, including the backup data.

Prevention includes simple methods, such as changing passwords and not using plain-text protocols.

Employees

Employees can be one of the security threats. As shown in Figure 1, the costs can be enormous.

Roger Duronio, on the right, worked at Paine-Webber, which was acquired by UBS. He was expecting a \$30,000 bonus. When he did not get his bonus, he created a script that deleted data on 2,000 servers. The cost of restoring the data was about \$3 million and the company is still not sure whether they ever fully recovered all the data. Duronio was found guilty and sentenced to eight years in prison.

On the left is Marie Cooley. This is something relatively recent. She worked in an architectural firm and she saw an ad for what appeared to be her job in the newspaper; the ad contained her boss's last name. She deleted all the company's data: \$2.5 million of architectural drawings. There was no backup. The ad was actually for her boss's wife's company, not her own.

The Backup Administrator

The backup administrator is quite often a junior member of the staff. It is a very common entry-level position in IT, because it is the job that nobody wants. This means that they are junior members, usually with lower salaries and less education about security. This makes them susceptible to social engineering and bribery. Yet, this junior employee is running the most powerful system in the data center. This is an important consideration.

The Backup Tapes

Companies make backup tapes and hand them over to someone who is, for all intents and purposes, a stranger. To send those tapes to an off-site company without encrypting them is foolish and may not be in

Your Own People



- Marie Cooley
- Deleted \$2.5M of architectural drawings after seeing ad she thought was for her job
- There was no backup!
- The ad was for boss' wife



- Roger Duronio
- Script deleted data on 2000 Paine-Webber/UBS servers after not getting a \$30K bonus
- Cost UBS \$3.1M
- Found guilty, sentenced to 8 yrs

 **GLASSHOUSE**

© 2004 GlassHouse Technologies, Inc.

This material may not be reprinted or redistributed without the express written consent of GlassHouse Technologies, Inc.

Figure 1

compliance with various data protection laws, such as the Data Protection Act in the European Union or SB 1386 in California. If those unencrypted tapes contain any personal customer data and any tapes go missing—which translates to losing control of that data—it is a security breach. Customers must be notified. If the company does not notify all the affected customers within the legal period of time, the company must then notify the media. This means public exposure of the company's failing.

How realistic is the threat? All plain-text backup tapes are readable by anyone who wants to read them. Even backups produced by specific backup packages that give the impression that the data cannot be read without that package can be read. A commercial index engine can read tapes produced by a number of backup packages, including TSM, NetBackup, NetWorker, ARCserve, and Backup Exec. At least eight documented incidents of stolen backup tapes have occurred since 2001.

Responding to the Threats

The backup server should be the most hardened server in the data center. The backup server is the most powerful server in the data center, and typically

all the administrators have the password to that server. Access should be limited to essential personnel; if possible, it should be limited to the backup administrator only, with the password stored at some other location for emergencies. Plain-text access should be turned off. One way to do this is to put the backup server behind a VPN.

In addition, enterprises should use a separation of duties. For instance, one group of people might make the backups while a separate group handles the physical tapes. Neither group is allowed to do the other's job.

In terms of the tape SAN, again, plain-text access should be turned off. The company should change the default password; companies commonly fail to do this. Separate management of the SAN can also reduce threats.

At a minimum, companies should perform background checks on IT personnel. Roger Duronio, for instance, was hired by a company after he was indicted but before he was convicted. The hiring company found out about his indictment entirely by accident—not because they did a background check.

Companies need to show respect for their employees, trying to maintain morale and not create disgruntled employees. Watch for signs of stress and malice. Also, educate employees about social engineering; showing them the movie “Sneakers” can be helpful. Also educate employees about security.

When discarding used media, companies should know that many types of modern media cannot be degaussed and reused. Operations that buy used media and claim they degauss them are probably not able to do it successfully. It is better to use secure media-shredding services for disposal. However, if a company wants to sell the tapes for reuse, encrypting the data is key to security.

Encryption

Backup tapes with personal data on them should be encrypted. For small amounts of data, the company should encrypt at the source or using backup software. Doing this with large amounts of data could impact the performance of applications and the system, so companies should encrypt with some kind of hardware, such as in the SAN, the library, or the drive.

The SAN contains network devices that encrypt data. Because they are doing this in hardware, they can do it at line speed. They can also solve the compression problem, because they compress the data and then deliver the compressed data to the encryption system. Encryption can also happen in the tape library or the tape drive.

The three rules of encryption are: key management, key management, and key management. If a company loses their keys, they lose their data. A company must protect their keys from loss, whether accidental or intentional.

One of the things to consider is data classification and deciding what to encrypt. Key types of data that should be encrypted include:

- Personal information
- Intellectual property
- Operational information

If a company can exclude one or more types of data from encryption, they can save capital and operating expenses.

Encrypt in the least expensive, simplest way possible. Key management should be a major focus. Backup tapes especially will need long-term retention plans for the keys, because the company may need to comply with retention requirements. Otherwise, a company may end up with a backup tape they cannot read.

Getting professional help for encryption and security is highly recommended.

The Cisco Solution

Any tape encryption solution must meet a number of requirements:

- Support existing backup applications
- Encrypt using required tape-device types
- Use same quantity of tape media
- Provide secure key management
- Meet backup window with encryption
- Deploy without disrupting production systems
- Apply encryption easily and consistently

The Cisco solution delivers encryption as a SAN service, shown in Figure 2.

MDS 9000 Product Family

The Cisco MDS 9000 product family—the 9200 and 9500 series, in particular—offers a variety of products from the smallest single RU phone-backup fixed-switch up to the largest directors. These products can incorporate hardware that provides service units to use for encryption. By introducing one or more modules via the multiprotocol service, the module becomes a hybrid switching module with 80 Fibre Channel ports that can perform SAP, iSCSI, and other services such as encryption. The idea is to introduce enough encryption engines into the system to handle the system’s encryption throughput. Once the company introduces encryption units, they must determine which ones to actually use for encryption.

The Cisco solution is not a device that just does encryption: it offers services in the SAN. Cisco provides a logical definition of what needs to be encrypted; in other words, traffic from a specific media server to a particular, user-defined tape drive. No physical association mandates that everything on

key manager takes key material from multiple sources and provides a common repository, high availability, and a common place of reporting. SME provides KMC for this functionality, or a company can incorporate this with third-party key managers for long-term retention of keys. SME also enables compression with encryption of data.

Cisco SME is also highly scalable; a company can grow the solution by adding modules to the system without impacting the rest of the network. By adding another module, a company adds another service unit. The process becomes a simple definition of the new encryption needs. Automatic failover to the best available service unit provides broad coverage in the event of a failure.

The solution can be provisioned quickly using Cisco Fabric Manager wizards. This extends the web client, using secured communication. The wizard basically asks which service unit is required, and then which encryption policy to apply.

Conclusion

The benefits of encrypting in the SAN include centralization and heterogeneity. Most organizations have a variety of existing tape drives, even drives that are considered obsolete, because tape drives have long lifespans. A heterogeneous solution that can perform encryption across all existing drives is very compelling.

SME is simple and nondisruptive, not requiring reconfiguration of hardware or rewiring of the SAN. In addition, the encryption engines are embedded into the Fibre Channel fabric, which eliminates the need for new cables, switch boards, and external appliances. SME performs automatic load balancing and failover, reducing the cost and complexity of the solution. The solution can be managed simply, with a minimum of tools.

Cisco is not offering a specific device that only performs encryption. Cisco offers services in the network: a service-oriented SAN architecture that contains storage-media encryption functionality.

Common Questions

Question: What is the weekly management of switches, since introducing another device adds more management?

Answer: There is no weekly management. Once encryption policy is defined, the encryption takes care of itself on a regular basis.

One possible issue is, if the process is writing to a VTL and the deduplication is being done there, encryption should not be done ahead of that process, because that would prevent deduplication. Instead, take the information that is stored in the VTL and encrypt it during the process of transferring it to removable media.

Question: Which enterprise key managers are supported by Cisco Storage Media Encryption?

Answer: The RSA key manager for the data center is supported. Cisco is currently working on additional initiatives. Once the IEEE standards are in place, especially the standard for key management, Cisco hopes to support many more key managers.

Question: Does encryption at the source or with the backup software make deduplication counterproductive?

Answer: If the data is encrypted, you don't need deduplication. Encryption works by getting rid of patterns; deduplication works by looking for patterns. Deduplication and disk-space backup can be very important, however. Cisco recommends that, if a company plans on making tapes and then encrypting those tapes prior to sending them off-site, they should encrypt in the SAN or in the device itself.

Question: What type of overhead and utilization do customers typically have using Cisco SME?

Answer: One thing that works in favor of Cisco SME is compression. Cisco SME uses a very strong algorithm for both compression and encryption. By examining patterns, it reduces the overhead significantly. Degradation percentages are within the 1–10%

range. Cisco SME is able to compress as much or more than a tape drive and therefore does not take significantly longer to run jobs and does not extend the backup window.

Question: Is being able to run root from backup a huge security vulnerability?

Answer: Yes, but this is common to every backup software program. For the backup software to do its job, it must be able to access every file. In order to access every file, it needs to be root or something just like root—in other words, a user ID that is privileged and able to read every file on the system. Also by design, a backup system needs to be able to execute script, because it needs to perform tasks such as shutting down databases, putting databases in backup mode, or taking snapshots. Accessing all files and executing script together create a huge security risk.

Because it is such a huge security risk, the people who will use the backup system must be carefully reviewed and limited as much as possible. This is often the opposite of what companies do. Everyone gives backups to the newest employee and everyone tends to have the administrator password to the backup systems. Neither of these things should be true for maximum security.

Question: Can this solution also be host space to help prevent administrators from corrupting the data on primary storage?

Answer: No, this particular solution only addresses tape; it does not deal with disk-space storage.

Question: How is BCP to another site handled? For example, what if a company needs to restore data from a remote site to a site 1,400 miles away that has another Cisco SME?

Answer: The media must be transported to the primary site and then the administrator accesses replicated keys from the remote site. The company would

have a link in the key management between the remote site and the primary site.

Question: What are worldwide names?

Answer: A worldwide name is the Fibre Channel equivalent to a MAC address. Most users create a zone in Fibre Channel by specifying the members of the zone using the worldwide names of those members. Fibre Channel HBA can be thought of as the equivalent of the nick. Let us say that a company has Fibre Channel HBAs on some servers that need to access storage on the other side of the SAN. The administrator can specify the worldwide names of all of those ports in order create a zone to allow them to access that storage. It is also possible to specify the physical ports that they are plugged into, which is the more difficult way because the administrator has to know what all those ports are, and then the changes actually take more steps.

However, it is important to understand that worldwide names are easily faked. Not only are they easily faked, but the means to fake them is built into the drivers. The ability to create worldwide-name-based zones was developed because doing port-based zoning was problematic from a management perspective. An administrator can swap out one of the HBAs to make it easy for the customer to not have to redo their zone because of a failed HBA. The vendors built an ability into the drivers to change the worldwide name of the HBA, so that the zone would not have to be changed when they replaced it.

Well, the problem with that is built right into the driver—it says that it is server A when really it is server B. What this means is that the administrator must have complete control over the servers and their identities and must be right on the ball to make sure that each HBA is reading correctly. This is not always an easy thing to do. Organizations that use worldwide-name-based zoning must consider everything that is plugged into the SAN at the same security level. Typically, a company has more hardened

servers than nonhardened servers. If they are all plugged into the same SAN and are using worldwide-name-based zoning, however, they all must be hardened servers, because if a user hacks one of them, they could use the same techniques to hack another server's data.

Question: Is documentation available on the Cisco SOA from a SAN perspective?

Answer: No paper on this topic is available at this time, but we have documentation on the particular features that utilize this architecture. Also available are data sheets for a data mobility manager product and for storage media encryption.

Question: Can a company use both application-level backup with TSM and SAN-based encryption?

Answer: Yes. Cisco SME will encrypt whatever it is asked to encrypt. SME is fully compatible with TSM and a variety of other products. Some companies consider encrypting data within the backup software, because they are concerned about the data in transit in their data centers. This is not necessarily a major consideration. However, sometimes the backup software can encrypt data for the transit, then unencrypt it on hand-over to the backup server to assist in deduplication. The hardware encryption would then encrypt the data on the tape drive. SME can do authentication of who connects to the switch and link-level encryption on the modules offered.

Question: Does Cisco also make Ethernet switches?

Answer: Yes.

Question: What types of tape devices are supported by Cisco SME?

Answer: Cisco SME supports commonly used tape drives, including LTO-2 and LTO-3 IBM enterprise drives, a number of STK drives, and Super DLT. It supports the most popular drive types.



About TechTarget

We deliver the information IT pros need to be successful.

TechTarget publishes targeted media that address your need for information and resources. Our network of technology-specific Web sites gives enterprise IT professionals access to experts and peers, original content, and links to relevant information from across the Internet. Our events give you access to vendor-neutral, expert commentary and advice on the issues and challenges you face daily. Our magazines give you in-depth analysis and guidance on the critical IT decisions you face. Practical technical advice and expert insights are distributed via specialized e-Newsletters, video TechTalks, podcasts, blogs, and wikis. Our Webcasts allow IT pros to ask questions of technical experts.

What makes TechTarget unique?

TechTarget is squarely focused on the enterprise IT space. Our team of editors and network of industry experts provide the richest, most relevant content to IT professionals. We leverage the immediacy of the Web, the networking and face-to-face opportunities of events, the expert interaction of Webcasts, the laser-targeting of e-Newsletters, and the richness and depth of our print media to create compelling and actionable information for enterprise IT professionals.

Cisco_12_2008_0002