CHAPTER

11 Storage Security

The primary concern of network security is to protect assets that reside on the network. Naturally, the most significant of those assets is data. Data resides in storage, which is either controlled or unmanaged. Storage technologies have evolved over the past decade in complexity, capability, and capacity, and the effectiveness of storage security controls and technologies has advanced accordingly. Today's storage technologies can protect data natively in many ways; for example, many modern storage technologies include built-in encryption and access control to protect confidentiality and integrity, redundancy to protect availability, and onboard protection against malware.

In this chapter, we'll cover the ways in which the built-in security features of modern storage infrastructures can be leveraged to protect data. We'll also look at how to protect data on storage devices and platforms using additional technologies outside the native functionality of storage systems, to remediate residual risks to that data. And finally, we'll review best practices for building storage infrastructures to provide the best protection for data assets. Let's begin with a look at how storage security has changed in recent years.

Storage Security Evolution

When the first edition of this book was published almost ten years ago, 3.5-inch floppy disk drives were still included on some computers. Being portable storage devices, floppy disks were hard to secure. They were easily lost, or the data on them became corrupted. They could be used to propagate malware, either through files on the disk or through active code like the "girlfriend exploit" (as described in Chapter 2, named for the infamous practice of breaking into a network by giving a disk containing exploit software to a significant other who works there, and instructing her to run the program). The use of floppy disks was largely phased out by the late 2000s.

The next generation of storage devices, compact discs (CDs) and digital video discs (DVDs), posed a unique threat due to their longevity. Unlike other, more volatile storage media, these polycarbonate-encased metal optical data storage devices seem like they will last forever if handled properly. While optical discs are great for reliability and availability

of data, their longevity elicits concerns of its own. If you place private, confidential data on a CD or DVD and then misplace the disc, who knows how long it might stick around and who may discover it in the future. For this reason, optical storage devices were banned in many corporate environments, especially those required to comply with privacy regulations. Moreover, once the data is burned to the media, it can't be changed, so you can't retroactively apply protection to it.

Flash drives (USB sticks and the like) have exploded in popularity over the past few years. These devices have become so cheap and prevalent that they have practically supplanted optical storage devices. Who needs to burn when you can simply copy? Nevertheless, while not as durable as optical storage, flash drives are similar to the archaic floppy disks of the past in many ways. They are omnipresent—many organizations try to ban their use, but everybody has one—so policies prohibiting these devices are hard to enforce outside of controlling the USB ports on every computer in the environment. They are prone to both malware and girlfriend exploits, in the same way floppies were—even more so, in the age of "autorun" (automatic execution of any code that is on the device, immediately upon connecting it). Flash drives are a significant source of malware infections in many environments. In addition, they make data theft remarkably easy with their small size, portability, and compatibility with every major computing platform.

Portable hard drives, like flash drives, are cheap and plentiful. With their large storage capacities, they carry all the same threats. In fact, portable USB hard drives have so much capacity that they can be used to steal all the data in many organizations. Portable hard drives have made it so easy to bulk-download huge amounts of data—like fishing with a huge net—that data thieves are sure to find valuable intellectual property strewn among the files they collect. Even modern smartphones, cameras, and tablets contain large amounts of flash memory and are accessible via USB, allowing data thieves to copy files unobtrusively.

The newest form of portable storage is the solid-state drive (SSD). SSD devices combine the best features of flash drives and portable hard drives, and as their prices drop in relation to demand, we can expect them to become increasingly ubiquitous. And, like flash drives and portable hard drives, SSDs facilitate bulk data theft.

In addition to the previously mentioned dedicated storage devices, the security practitioner now also has to contend with smartphones and mobile devices, which have significant amounts of onboard storage. These devices pose a significant risk to an organization's data because they are less "obvious" than a hard drive or memory stick and because any stolen data hiding on them can be hard to detect. Chapter 25 contains some advice on how to deal with this problem in particular.

All of the storage devices mentioned thus far are considered to be *unmanaged*. The best protections for (and against) them are encryption and access control. Encrypting confidential data can stop, or discourage, data theft. Information rights management (covered in Chapter 9) can protect confidential documents such that, even if they are stolen, they can't be opened by unauthorized users. In addition, USB device control software can block access to the USB ports on computers where it's installed, and it can allow or block various activities such as copying to or from USB devices, based on the type of document.

Chapter 8 covers solutions for protecting unmanaged data on all the types of storage discussed in this section. Ultimately, unmanaged storage devices are hard to secure and hard to control. That's why organizations have turned to managed storage, which allows their data to be accessed in secure, controlled ways. With managed storage, organizations can block USB storage devices and drive users toward the managed storage instead.

Modern Storage Security

Modern storage solutions have moved away from the endpoint computers to the network. Network-attached storage (NAS) and storage area networks (SANs) consist of large hard drive arrays with a controller that serves up their contents on the network. NAS can be accessed by most computers and other devices on the network, while a SAN is typically used by servers.

These storage systems have many built-in security capabilities to choose from. Based on the security requirements of the environment, these security settings can be configured to meet the objectives of the security policy. Today's storage environments are complex. In fact, modern storage environments can be considered as separate IT infrastructures of their own. Many organizations are now dividing their IT organizations along the lines of networks, servers, and storage—acknowledging that storage merits a place alongside these long-venerated institutions.

Storage Infrastructure

Storage infrastructure can often be found on a dedicated LAN, with servers, arrays, and NAS appliances, as shown in Figure 11-1, with specialized operating systems to support the storage. Storage can also be located in multiple sites, including geographically diverse regional distributions, and even third-party and Internet locations. In securing these components, you must take into account three primary categories:

- Storage networks
- Arrays
- Servers

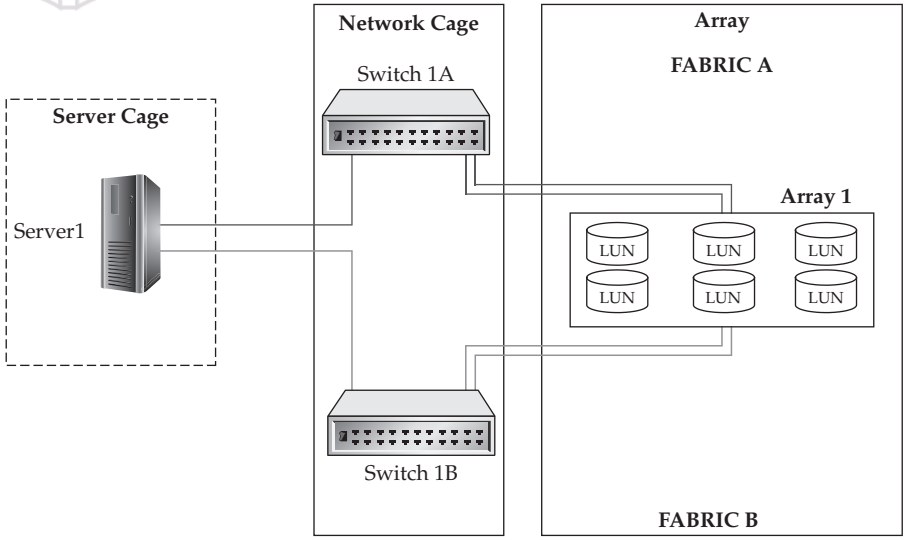

Figure 11-1 Fundamental storage infrastructure

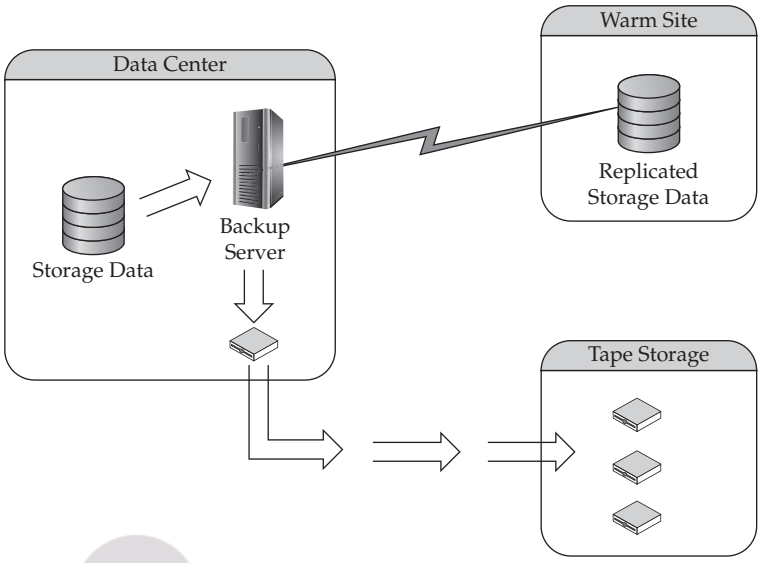

Figure 11-2 Offsite data movement

Primary storage is composed of a storage device such as a NAS appliance or a storage array. The contents of the storage components are managed and served via a server infrastructure, with an operating system that is compatible with servers and workstations in the end-user environment. The network connections between the primary storage and the storage servers should be independent of the corporate IP network, because the communications that take place on these local connections are internal and don't require access from the rest of the network—they are specialized in their functionality.

In the following sections, we consider the risks to the storage infrastructure, and controls and processes to mitigate those risks. We also consider the lifecycle of the data as it moves from its primary location to secondary storage as it is backed up or replicated, as depicted in Figure 11-2.

Storage Networks

Separation of duties should be applied within the storage infrastructure. Since all storage devices are connected physically, either over a network or through a storage connection protocol, separating access to the physical servers prevents a storage administrator from connecting a rogue server into the environment and then provisioning it access to restricted logical unit numbers (LUNs). A LUN is the mechanism an array uses to present its storage to a host operating system. Likewise, while someone may connect a server to the environment and configure it, methods of protecting the LUNs are applied so that the server cannot gain access to restricted LUNs.

Isolating data traffic between LUNs via the switch is accomplished through the use of *zoning*—comparable to virtual LANs (VLANs) in the network world. Zoning creates a protected zone where only identified devices within that zone are allowed to communicate with each other. This is illustrated in Figure 11-3.

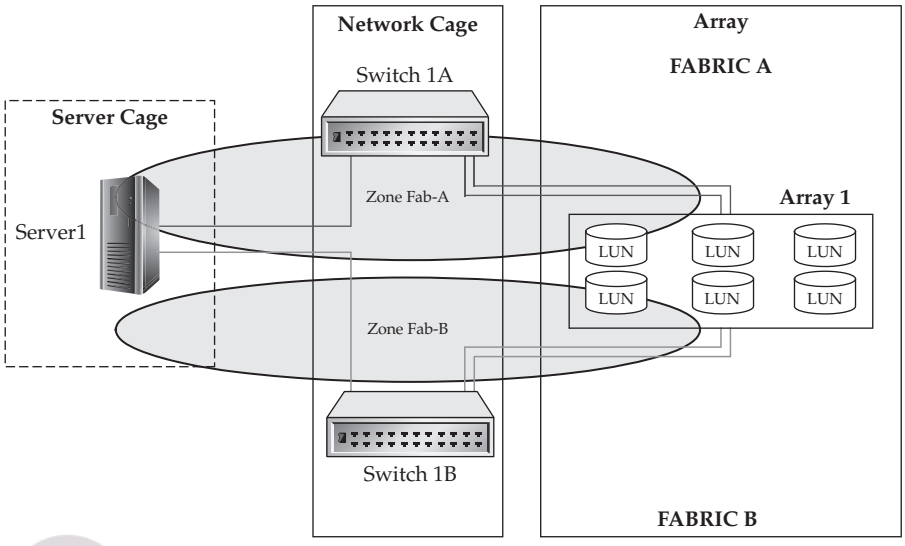

Figure 11-3 Security areas of zoning

In addition to providing security, zoning also protects against a faulty hardware device affecting other servers through excessive chatter. Zoning also provides the opportunity for redundancy, since there can be multiple device addresses within the zone that allow communication to continue between the remaining good interfaces.

When a storage administrator configures zoning for the infrastructure, there are two types of zoning to choose from: port zoning and World Wide Name (WWN) zoning. In fact, these two methods can be used interchangeably, though generally one or the other is used, to maintain consistency. Each zoning type has its own advantages and disadvantages.

Port Zoning The most notable characteristic of port zoning is that the accessibility of the host to the LUNs is defined by the switch port. The advantage to zoning in this manner is that an intruder cannot connect a host to the switch, enable spoofing of a good WWN, and access LUNs of another host. Since the protection is enforced on the port interface, the intruder would need to disconnect the good host interface and connect the intruding host into the defined port. All this would need to be done without any alerts being flagged by the host operating system, which is practically impossible.

The disadvantage of port zoning is that management requires extra work. Each time you re-cable a host to another port, you need to change the zoning for that host's connection to its storage resources to continue to function. Even though moving a host to different ports is not common, it may happen more often than you realize. For example, your SAN environment may grow, requiring an additional switch. Or perhaps you already have multiple switches but you need to distribute the workload across the SAN more efficiently. In either case, what otherwise would be a simple task consisting of unplugging a cable and connecting the new one requires an additional *zoneset reconfiguration* (change to

the data that contains all of the zones defined on the switch). Zoneset reconfigurations, though minimally intrusive, still cause some disruption. Therefore, though port zoning is more secure, you will find many SAN environments configured with WWN zoning because it is easier to manage.

WWN Zoning The alternative to port zoning, in which the zones are created relative to the ports the servers are connected to on the switch, is WWN zoning, which defines the individual zone based on the WWN ID of the host bus adapter (HBA). The WWN is very much like the MAC address of a network card. It is a 16-digit hexadecimal number that uniquely identifies the HBA within the SAN fabric. These numbers are assigned in much the same way as MAC addresses are assigned to OEM manufacturers, with the first eight digits assigned to specific manufacturers and the rest of the numbers assigned by the manufacturers.

Arrays

Another area of risk is the storage array itself, as highlighted in Figure 11-4. When LUNs are created, it is necessary for the array to provide a screen to prevent the data that resides on the array from being accessed by other hosts that are able to connect to the array. Storage arrays are therefore equipped with a mechanism that provides protection known as LUN masking. This allows multiple hosts to communicate with the array and only access LUNs that are assigned through the application that provides the LUN-masking protection.

Consider the differences in protection between zoning and LUN masking. We described zoning as being comparable to isolating traffic between hosts on a network utilizing VLANs. While zoning, like VLANs, isolates the traffic as it travels between the host and the storage array so that it is not intercepted, it provides no protection to the data once it is on the host.

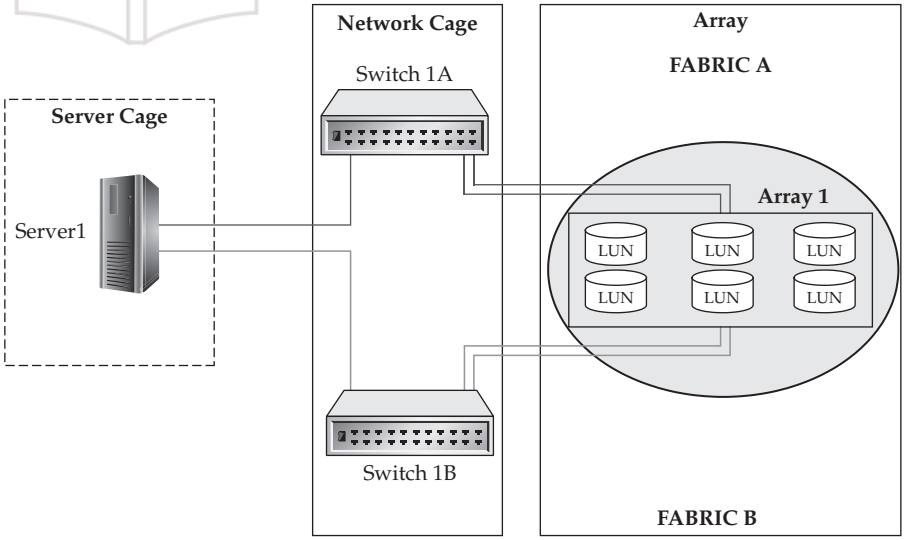

Figure 11-4 Security areas of arrays

Similarly, though a server may have data being sent to it from several hosts on different VLANs, once the data is put on the server, the potential still exists for that data to be accessed by other hosts on other networks. LUN masking adds a layer of protection to the data once that data resides on the storage array.

Servers

Finally, we need to consider the risks that reside on the host itself, as illustrated in Figure 11-5. Storage administrators often have limited control over what can or cannot be done on the host, as this administration is handled by the systems administrators. However, in many organizations, the systems administrator is also the storage administrator, which means that person has full access to both the storage and the systems that use it.

As long as the data "rests" on the server, the potential to access that data exists. Many options are available to protect that data while it is at rest on the server. The concern of the storage administrator is what happens if someone is able to access the data either locally or remotely. In the worst-case scenario, an attacker may obtain access to the server and escalate his authority to attempt to read the data. In order to keep the data secure in this scenario, it is necessary to implement data encryption.

Therefore, when securing data, a comprehensive solution is necessary. The operating system must be secured and patched, file permissions must be planned and applied to reduce access as much as possible, and monitoring needs to be performed. Finally, confidential data should also be encrypted to protect it from unwanted access.

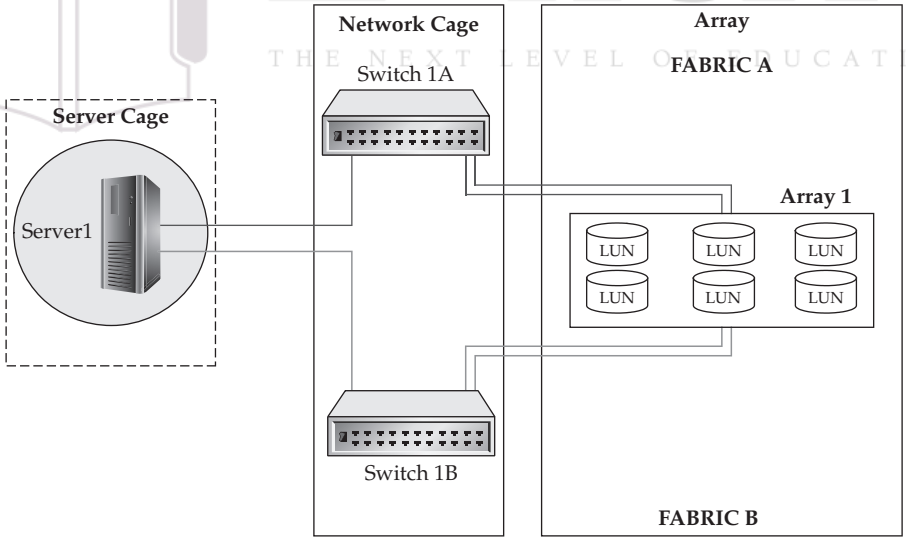

Figure 11-5 Security areas of servers

Administration Channel

Administration of the storage environment should be done through a network that is separate from the main corporate network. Malware, rogue administrators, and attackers all need to rely on a corporate network to gain unauthorized access to administration functions they can exploit to compromise infrastructure. It's not uncommon for an Internet-facing web server to be attacked, successfully compromised, and then used to attack other systems on the internal network. You don't want those compromised systems to be used to attack your storage infrastructure through the administration channel, so when designing your storage network, you should include a separate, access-controlled network segment just for the administration of the storage array.

Risks to Data

Earlier in this chapter, the "Storage Infrastructure" section outlined areas of risks in the individual components of the SAN/NAS storage environment. This section covers the specific risks to the data itself. There are two key areas of risk to data, and those are related to how the data is presented to the clients. The first risk involves data that can be accessed via an unauthorized system. The second risk is data access by unauthorized persons.

Access by an Unauthorized System

The potential for an unauthorized system to access protected data may seem unlikely at first glance. However, when you consider issues that may arise from either administrator error or intentional unauthorized access, the potential for data to become compromised begins to increase. How, then, can an unauthorized system obtain access to another system's data?

In this scenario, the data most likely will be presented in the form of a LUN. This LUN can be provided through either a Fibre Channel connection or an Internet Small Computer Systems Interface (iSCSI) connection. Both connection types present the same level of risk. Attacking the LUN would require the use of spoofing, which enables a computer's host bus adapter (HBA) to change the WWN that it presents to that of the target system.

This is not necessarily easy to accomplish, because Fibre Channel ports in general do not utilize port spanning, which is what an attacker attempts to exploit to intercept (sniff) traffic in order to learn which WWNs are transmitting data on the network. An attacker who wanted to spoof a WWN would need to have inside information about which host WWNs they should target. However, it is theoretically possible.

Despite the difficulty, the ability of a host to spoof a WWN is a potential risk—and once that WWN is spoofed, much of the protection that is in place within a storage environment is exposed. Theoretically, the spoofed WWN would then have access via the zones defined—if WWN zoning is used, which is often the case—and the LUN-masking provided by storage arrays is also usually configured based on WWNs. Having bypassed those two key security methods, the intruding host can gain access to all of the data on those LUNs.

Think of this in the context of an individual disk. Suppose you have removed a disk from a server and placed it on another server—what happens to the file protection that was put in place by the original system? The disk is now owned by the new OS, and, as administrator or root of this rogue system, you can now change permissions and access the data. And as long

as the attacker just reads from the volume and avoids writing to it, the original host may never become aware anything unusual has taken place.

Another best practice to prevent WWN spoofing and sniffing is to dedicate the switches used to connect the storage devices to service only the servers and storage, so that end-user devices and other systems are not allowed to share the switch hardware. This approach relies on the physical security of the switches to limit your exposure.

The other way that data can be exposed to risk from an unauthorized system is through deliberate or negligent configuration by a storage administrator. A storage administrator could deliberately or mistakenly assign a LUN to the wrong servers, or perhaps select the wrong LUN for a particular server. In either case, nothing would prevent the administrator from doing this, since the zone would exist and the server would be properly connected and zoned to the array. Because the server would be properly registered to the array, LUN masking would not prevent it either. You might wonder why storage arrays would be allowed to do this. For migration purposes, storage vendors provide LUN-sharing capability between servers in order to support server clusters. This is commonly seen with the prevalence of virtualized clusters. In order to move the virtual servers from one host to another, the LUNs must be shared between the hosts.

Recognizing the risks involved with presenting LUNs to your servers is thus important when deciding how to secure your storage.

Access by Unauthorized Person

Another risk to data at rest on a server is compromise of the server itself through the data-access mechanisms built into the server. All data that is controlled by a server is at risk of the authorization mechanisms of the system itself being compromised and thereby exposing the data to an attacker.

Once the server is under the control of an attacker, the attacker has the ability to change permissions on the file system; thus, the new OS owner can permit access to all data. An attacker who compromises a system does not necessarily need to begin making changes to the file systems in order to collect information. Perhaps the attacker is only interested in intercepting data being written to or read from storage. Just as there are tools that can sniff network traffic on wired and wireless networks, there are tools that can sniff traffic on a Fibre Channel network. Using a compromised system, or perhaps malware, an intruder could launch a sniffing tool and collect data from the system. In addition, by having access to this compromised system, the attacker has the option to launch repeated attacks to the storage infrastructure to gain access to data from other servers in addition to the server initially compromised.

Risk Remediation

This section categorizes the risks associated with data storage according to the classic CIA triad of Confidentiality, Integrity, and Availability (introduced in Chapter 4). For each identified risk, where possible, security controls consistent with the "three *D*s" of security (introduced in Chapter 1)—defense, detection, and deterrence—are applied in an effort to mitigate the risk using the principle of layered security (also known as defense-in-depth). What's left after those controls are applied to mitigate the risks is then identified as residual risks.

Confidentiality Risks

Confidentiality risks are associated with vulnerabilities and threats pertaining to the privacy and control of information, given that we want to make the information available in a controlled fashion to those who need it, without exposing it to unauthorized parties.

Data Leakage, Theft, Exposure, Forwarding

Data leakage is the risk of loss of information, such as confidential data and intellectual property, through intentional or unintentional means. There are four major threat vectors for data leakage: theft by outsiders, malicious sabotage by insiders (including unauthorized data printing, copying, or forwarding), inadvertent misuse by authorized users, and mistakes created by unclear policies.

- **Defense** Employ software controls to block inappropriate data access using a data loss prevention (DLP) solution and/or an information rights management (IRM) solution, as described in Chapters 8 and 9.
- **Detection** Use watermarking and data classification labeling along with monitoring software to track data flow.
- **Deterrence** Establish security policies that assign serious consequences to employees who leak data, and include clear language in contracts with service providers specifying how data privacy is to be protected and maintained, and what the penalties are for failure to protect and maintain it.
- **Residual risks** Data persistence within the storage environment can expose data long after it is no longer needed, especially if the storage is hosted on a vendor-provided service that dynamically moves data around in an untraceable manner. Administrative access that allows system administrators full access to all files, folders, and directories, as well as the underlying storage infrastructure itself, can expose private data to administrators.

Espionage, Packet Sniffing, Packet Replay

Espionage refers to the unauthorized interception of network traffic for the purpose of gaining information intentionally. Using tools to capture network packets is called *packet sniffing*, and using tools to reproduce traffic and data that was previously sent on a network is called *packet replay*.

- **Defense** Encrypt data at rest as well as in transit through the use of modern, robust encryption technologies for file encryption, as well as network encryption between servers and over the Internet.
- **Detection** An information rights management (IRM) solution can keep track of data access, which can provide the ability to detect inappropriate access attempts. In addition, an intrusion detection system (IDS) can help identify anomalous behavior on the network that may indicate unauthorized access.

- **Deterrence** In storage environments that are hosted by a third party, employ contract language that makes the service provider liable for damages resulting from unauthorized access.
- **Residual risk** Data can be stolen from the network through tools that take advantage of network topologies, network weaknesses, compromised servers and network equipment, and direct access to network devices.

Inappropriate Administrator Access

If users are given privilege levels usually reserved for system administrators, that provide full access to a system and all data that system has access to, they will be able to view data or make changes without being properly restricted through the system's authorization processes. Administrators have the authority to bypass all security controls, and this can be used to intentionally or mistakenly compromise private data.

- **Defense** Reduce the number of administrators for each function (servers, network, and storage) to as low a number as possible (definitely fewer than ten, and preferably fewer than five) and ensure that thorough background checks are used to screen personnel who have administrative access. A vendor security review should be performed to validate these practices before engaging any vendors.
- **Detection** Review the provider's administrative access logs for its internal infrastructure on a monthly or quarterly basis. Review the provider's list of administrators on a biannual basis.
- **Deterrence** Establish security policies especially for administrators, that assign serious consequences for inappropriate data access. In hosted environments, select only providers that have good system and network administration practices and make sure their practices are reviewed on a regular basis.
- **Residual risk** Because administrators have full control, they can abuse their access privileges either intentionally or accidentally, resulting in compromise of personal information or service availability.

Storage Persistence

Data remains on storage devices long after it is no longer needed, and even after it is deleted. Data that remains in storage after it is no longer needed, or that is deleted but not strongly overwritten, poses a risk of later discovery by unauthorized individuals.

- **Defense** Maintain a U.S. Department of Defense (DoD)-level program of disk wiping or file shredding when disks are decommissioned or replaced, and after old data is archived.
- **Detection** There isn't much that can be done to discover that your data persists on a disk that has been taken offline.
- **Deterrence** Establish data-wiping requirements before selecting a storage product and ensure that contract language clearly establishes these requirements.
- **Residual risk** Data can remain on physical media long after it is thought to have been deleted.

Storage Platform Attacks

Attacks against a SAN or storage infrastructure directly, including through the use of a storage system's management control, can provide access to private data, bypassing the controls built into an operating system because the operating system is out of the loop.

- **Defense** Ensure that strong compartmentalization and role-based access control (RBAC) are implemented on the storage system. Ensure that access to the management interface of the storage system is not accessible from the common network.
- **Detection** Implement an IDS on the storage network, as described in more detail in Chapter 18, and review storage system access control logs on a quarterly basis.
- **Deterrence** Employ strong legal representation and project a strong commitment to identifying and prosecuting attackers.
- **Residual risk** Data can be stolen directly from the SAN, and you may find out about it after the fact or not at all.

Misuse of Data

People who have authorized access to data can do things with the data that they are not supposed to do. Examples are employees who leak information to competitors, developers who perform testing with production data, and employees who take data out of the controlled environment of the organization's network into their unprotected home environment.

- **Defense** For employees, use security controls similar to those in private data networks, such as DLP, RBAC, and scrambling of test and development data. Block the ability to send e-mail attachments to external e-mail addresses.
- **Detection** Use watermarking and data classification labeling along with monitoring software to track data flow. IRM can be used to perform these functions.
- **Deterrence** Employ a strict security policy paired with an awareness program to deter people from extracting data from controlled environments and moving it to uncontrolled environments.
- **Residual risk** People can find ways around controls and transfer data into uncontrolled environments, where it can be stolen or misused.

Fraud

A person who illegally or deceptively gains access to information they are not authorized to access commits fraud. Fraud may be perpetrated by outsiders but is usually committed by trusted employees.

- **Defense** Use checks and balances along with separation of duties and approvals to reduce the dependence on single individuals for information access, so if somebody does perform a fraudulent action, it will be noticed. This can also be a deterrent action.

- **Detection** Perform regular audits on computing system access and data usage, giving special attention to unauthorized access.
- **Deterrence** Ensure that security policies include penalties for employees who access data they are not authorized for. In hosted environments, transfer risk to service providers using contractual language that holds the service provider responsible for fraud committed by a service provider employee.
- **Residual risk** Fraudulent data access can occur despite the controls that are designed to prevent it.

Hijacking

Hijacking in the context of computing refers to the exploitation of a valid computer session—sometimes also called a session key—to gain unauthorized access to information or services in a computer system. In particular, it's the theft of a magic cookie used to authenticate a user to a remote server. For example, the HTTP cookies used to maintain a session on many web sites can be stolen using an intermediary computer or with access to the saved cookies on the victim's computer. If an attacker is able to steal the authentication cookie, they can make requests themselves as if they were the genuine user, gaining access to privileged information or changing data. If this cookie is a persistent cookie, then the impersonation can continue for a considerable period of time. Any protocol in which state is maintained using a key passed between two parties is vulnerable, especially if it's not encrypted.

- **Defense** Look for solid identity management solutions that specifically address this risk using strong, difficult-to-guess session keys with encryption. Use good key management, key escrow, and key recovery practices as a customer so that employee departures do not result in the inability to manage your data.
- **Detection** Routinely monitor logs, looking for unexpected behavior.
- **Deterrence** Not much can be done to deter attackers from hijacking sessions, other than aggressive legal response.
- **Residual risk** Attackers can impersonate valid users or even use administrative credentials to lock you out or damage your infrastructure.

Phishing

Phishing is an attempt to trick a victim into disclosing personal information. The most common method of phishing is to send potential victims an e-mail message that appears to be from a legitimate organization and directs the recipients to log in and provide a username, password, credit card information, or other sensitive information.

- **Defense** Employ anti-phishing technologies to block rogue web sites and detect false URLs. Use multifactor authentication for customer-facing systems to ensure that users are aware when they are redirected to fake copies of your web site. Send periodic informational updates and educational materials to customers explaining how the system works and how to avoid phishing attempts. Never send e-mails that include or request personal details, including ID or passwords.

- **Detection** Use an application firewall to detect when remote web sites are trying to copy or emulate your web site.
- **Deterrence** Maintain educational and awareness programs for individuals who use and store personal information of employees or customers.
- **Residual risk** Employees can fall for phishing scams despite the best training and awareness programs, especially if those scams are sophisticated. This can result in data loss.

Integrity Risks

Integrity risks affect both the validity of information and the assurance that the information is correct. Some government regulations are particularly concerned with ensuring that data is accurate. If information can be changed without warning, authorization, or an audit trail, its integrity cannot be guaranteed.

Malfunctions

Computer and storage failures that corrupt data damage the integrity of that data.

- **Defense** Make sure the storage infrastructure you select has appropriate RAID redundancy built in and that archives of important data are part of the service.
- **Detection** Employ integrity verification software that uses checksums or other means of data verification.
- **Deterrence** Due to the nature of data, because there is no human element involved, there isn't much that can be done.
- **Residual risk** Technology failures that damage data may result in operational or compliance risk (especially relating to Sarbanes-Oxley requirements for publicly traded companies to ensure the integrity of their financial data).

Data Deletion and Data Loss

Data can be accidentally or intentionally destroyed due to computer system failures or mishandling. Such data may include financial, organizational, personal, and audit trail information.

- **Defense** Ensure that your critical data is redundantly stored and housed in more than one location.
- **Detection** Maintain and review audit logs of data deletion.
- **Deterrence** Maintain educational and awareness programs for individuals who access and manage data. Ensure that data owners are assigned that have authority and control over data and responsibility for its loss.
- **Residual risk** Once critical data is gone, if it can't be restored, it is gone forever.

Data Corruption and Data Tampering

Changes to data caused by malfunction in computer or storage systems, or by malicious individuals or malware, can damage the integrity of that data. Integrity can also be damaged by people who modify data with intent to defraud.

- **Defense** Utilize version control software to maintain archive copies of important data before it is modified. Ensure that all data is protected by antivirus software. Maintain role-based access control over all data based on least privilege principles, pursuant to job function and need to know.
- **Detection** Use integrity-checking software to monitor and report alterations to key data.
- **Deterrence** Maintain educational and awareness programs for individuals who access and manage data. Ensure that data owners are assigned that have authority and control over data and responsibility for its loss.
- **Residual risk** Corrupted or damaged data can cause significant issues because valid, reliable data is the cornerstone of any computing system.

Accidental Modification

Perhaps the most common cause of data integrity loss, accidental modification occurs either when a user intentionally makes changes to data but makes the changes to the wrong data or when a user inputs data incorrectly.

- **Defense** Utilize version control software to maintain archive copies of important data before it is modified. Maintain role-based access control over all data based on least privilege principles, pursuant to job function and need to know.
- **Detection** Use integrity-checking software to monitor and report alterations to key data.
- **Deterrence** Maintain educational and awareness programs for individuals who access and manage data. Ensure that data owners are assigned that have authority and control over data and responsibility for its loss.
- **Residual risk** Corrupted or damaged data can cause significant issues because valid, reliable data is the cornerstone of any computing system.

Availability Risks

Availability risks are associated with vulnerabilities and threats pertaining to the reliability of services, given that we want the services that we use to be reliable, to pose a low risk, and to have a low incidence of outage.

Denial of Service

A denial of service (DoS) attack or distributed DoS (DDoS) attack is an attempt to make a computer resource unavailable to its intended users. This type of attack commonly involves

saturating the target machine with too many communications requests, such that it cannot respond to legitimate traffic, or responds so slowly as to be rendered effectively unavailable.

- **Defense** Select a storage platform that has solid protection against network attacks. Implement firewalls, an IPS, and network filtering at the perimeter of the storage network to block attacks.
- **Detection** Monitor intrusion detection systems 24×7×365.
- **Deterrence** Work with your legal department to ensure that attackers are found and prosecuted.
- **Residual risk** Because most DoS and DDoS attacks make use of compromised systems across the globe, they can be hard to track, and because they flood system and network resources, they can get through an environment's defenses.

Outage

An outage is any unexpected downtime or unreachability of a computer system or network.

- **Defense** The primary defense against any service outage is redundancy. Ensure that individual systems, devices, and network links are clustered or set up to use high availability. Outages are expensive—calculate the cost of downtime and use that to justify investment in the additional equipment needed for redundancy. Additionally, employ a solid disaster recovery plan to ensure that you are ready for extended outages, so that storage environments can be automatically switched to a different location during an outage.
- **Detection** Employ monitoring tools to continuously monitor the availability and response time of the storage environment.
- **Deterrence** Because outages generally occur as a result of software problems, little can be done to stop them from happening.
- **Residual risk** Unforeseen outages can occur even when all devices and network paths are completely redundant, due to malfunctions or human error, so storage infrastructures may be down for as long as it takes to switch over to the disaster recovery environment.

Instability and Application Failure

Problems, such as bugs, in software or firmware can cause freezing, locking, or crashing of applications, making them unresponsive and resulting in loss of functionality or failure of an entire computer or network.

- **Defense** Ensure that all software updates are applied to the infrastructure on a frequent basis.
- **Detection** Implement service monitoring to detect and alert when an application does not respond correctly.

- **Deterrence** In contracts with storage suppliers, include clear language that specifies penalties and remuneration for instability issues.
- **Residual risk** Because instability in applications and infrastructure generally occurs as a result of software problems, little can be done to stop them from happening.

Slowness

When the response time of a computer or network is considered unacceptably slow, its availability is affected.

- **Defense** Using redundant storage system and network connections, set up the architecture so that application access will automatically switch to the fastest environment. Also ensure that you have implemented high-capacity services with demand-driven expansion of resources.
- **Detection** Monitor response time of applications on a continuous basis and ensure that alerts have an out-of-band path to support staff so that response problems don't stop alerts from being delivered.
- **Deterrence** Establish contract language with storage manufacturers that provides compensation for unacceptable response times.
- **Residual risk** Slowness can persist despite best efforts, resulting in loss of efficiency and effective downtime.

High Availability Failure

A service that is supposed to fail over in the event of a problem with one device to other, functioning devices may not actually fail over properly. This can happen, for example, when a primary device slows down to the point where it becomes effectively unresponsive, but the HA software doesn't actually consider it to be "down."

- **Defense** Monitor the health of secondary systems or all systems in an HA cluster.
- **Detection** Perform periodic failover testing.
- **Deterrence** Not much can be done to guarantee that systems will switch over when they are supposed to.
- **Residual risk** Sometimes, a primary device slows down to the point that it becomes unresponsive for all practical purposes, but because it's not officially "down" according to its software, the backup system doesn't take over.

Backup Failure

When you discover that those backups you were relying on aren't actually any good, either because the media is damaged or the backup data is corrupted or missing, data is lost.

- **Defense** Leverage storage elasticity to avoid the use of traditional offline (tape or optical) backups.
- **Detection** Frequently perform recovery testing to validate the resilience of data.

- **Deterrence** Establish a data-loss clause in the contract with the storage manufacturer so that they have incentive to help with unforeseen loss of data.
- **Residual risk** Backups fail, but multiple recovery paths can eliminate most of the risk. The practice of backing up data has been around for a long time and, consequently, is one of the most reliable security practices. As long as data is appropriately replicated, it can live forever, so the majority of residual risk in this case would be due to substandard data replication practices or lack of attention to this matter.

Best Practices

Given the risks to storage infrastructure and the data that resides on it, what can be done to design a robust architecture that is resistant to attack? The following practices provide the best available mitigation.

Zoning

Port-based zoning improves security through control of the connections between hosts and the storage array. This method of zoning provides increased protection against a WWN spoof attack. With port zoning, even if a host system is introduced into the environment with a spoofed WWN, the host would need to also be in the port defined by the switch in order for its traffic to transmit to the storage array, because the zones are configured based on ports. The switch provides the path, by way of the zone, from the server's HBA to the array's HBA. Without that zone, the spoofed WWN has no path to the array.

Arrays

Arrays have been developed over time to provide LUN masking as a form of protecting LUNs from access by unauthorized servers. The most likely cause of a LUN being accessed by an unauthorized system is accidental or intentional misconfiguration by a storage administrator. The best defense against this is to ensure that storage administrators are trustworthy and capable, and to control and limit the management of the storage array to a small number of highly trained, reliable administrators.

Servers

In order to fully secure a storage environment, you must ensure that the server environment itself is controlled and monitored. Securing the storage infrastructure itself is not enough. Access to any server can significantly expose that server and the storage environment to harmful activity. It is important that servers be configured securely, and that the equipment is located in a secure facility with access control and monitoring. Change management and activity monitoring, to track changes to the system and the activities of administrators on the server, should be done with the security of the storage environment in mind. These steps need to be taken not only on the servers that are hosting the data but also on the management servers used to manage the arrays and switches.

Staff

When hiring individuals to manage and secure the storage environment, the requisite skill set should include solid knowledge of storage security practices. Background and/or training in computer security methods should be considered an important requirement. Naturally, training and experience in managing storage arrays is also important, preferably with the product in use within your organization, rather than tasking an administrator of some other platform with managing the storage infrastructure. In addition, given the convergence of storage and networking that has resulted in the SAN, a background in networking can be very valuable.

Offsite Data Storage

Storing data offsite (securely) is a critical aspect of any organization's business continuity process. Many vendors will pick up backup tapes and move them to a secured facility. Regular audits of these facilities should be done to ensure accountability for all data sent offsite. To protect the data, it should be encrypted whether on disk or tape. Any form of online data backup should be performed with an end-to-end encryption method.

Summary

As the storage of data has evolved from individually carried media to a specialized infrastructure environment, storage now requires specific planning and implementation of security in order to protect the data. Avoid the false assumption that, because the SAN appears to servers as an extension of the local disk farm, a focus only on securing the operating system is sufficient. Fibre Channel networks can be built with inherent resistance to attack using certain design techniques and best practices, but this is not enough to completely avoid data compromise. This chapter has presented several options, techniques, and best practices to equip the storage administrator to make the best choices for the specific environment of the organization.

References

Chirillo, John, and Scott Blaul. *Storage Security: Protecting SANs, NAS and DAS*. Wiley, 2003.

Dwivedi, Himanshu. *Securing Storage: A Practical Guide to SAN and NAS Security*. Addison-Wesley, 2005.

EMC Education Services. *Information Storage and Management: Storing, Managing, and Protecting Digital Information*. Wiley, 2009.

Preston, W. Curtis. *Using SANs and NAS*. O'Reilly, 2002.

Yu, Ting, and Sushil Jajodia. *Secure Data Management in Decentralized Systems*. Springer, 2006.