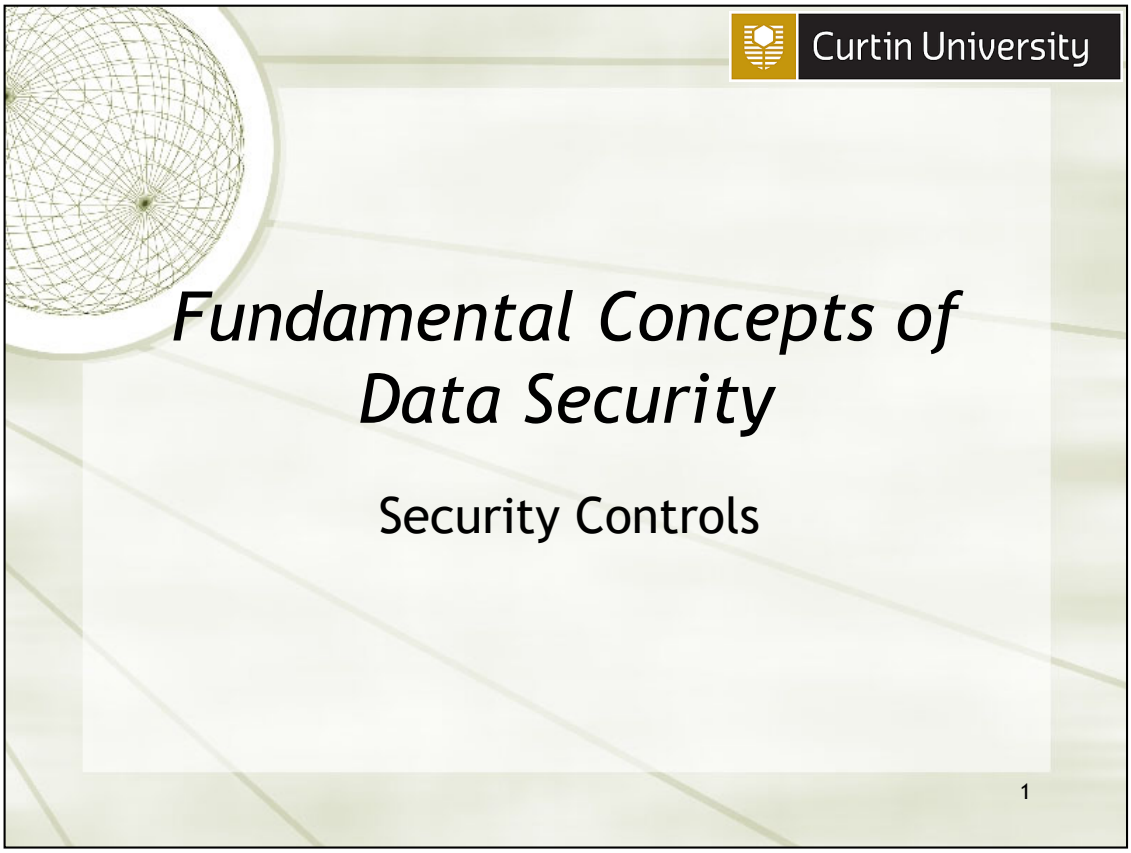
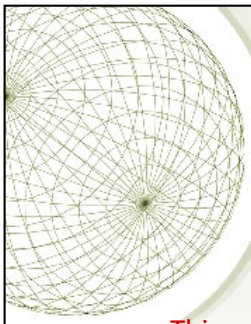

Curtin University
Fundamental Concepts of Data Security
Security Controls
1



Access controls are security features that control how users and systems communicate and interact with other systems and resources. They protect the systems and resources from unauthorized access and can be components that participate in determining the level of authorization after an authentication procedure has successfully completed. Access control is a broad term that covers several different types of mechanisms that enforce access control features on computer systems, networks, and information. Access control is extremely important because it is one of the first lines of defense in battling unauthorized access to systems and network resources.

Access Control Review

The following is a review of the basic concepts in access control:

- Identification
- Subjects supplying identification information
- Username, user ID, account number
- Authentication
- Verifying the identification information
- Passphrase, PIN value, biometric, one-time password, password
- Authorization
- Using criteria to make a determination of operations that subjects can

carry out on objects

• “I know who you are, now what am I going to allow you to do?”

• Accountability

• Audit logs and monitoring to track subject activities with objects

Identity

Identity is a complicated concept with many varied nuances, ranging from the philosophical to the practical. A person can have multiple digital identities. Creating or issuing secure identities should include three key aspects: uniqueness, nondescriptive, and issuance. The first, uniqueness, refers to the identifiers that are specific to an individual, meaning every user must have a unique ID for accountability. Things like fingerprints and retina scans can be considered unique elements in determining identity. Nondescriptive means that neither piece of the credential set should indicate the purpose of that account. For example, a user ID should not be “administrator,” “backup_operator,” or “CEO.” The third key aspect in determining identity is issuance. These elements are the ones that have been provided by another authority as a means of proving identity. ID cards are a kind of security element that would be considered an issuance form of identification.

Identification Component Requirements: When issuing identification values to users, the following should be in place:

• Each value should be unique, for user accountability.

• A standard naming scheme should be followed.

• The value should be non-descriptive of the user’s position or tasks.

• The value should not be shared between users.

Identification and Authentication

Identification describes a method of ensuring that a subject (user, program, or process) is the entity it claims to be. Identification can be provided with the use of a username or account number. Once a person has been identified through the user ID or a similar value, she must be ***authenticated***, which means she must prove she is who she says she is. Three general factors can be used for authentication: ***something a person knows, something a person has,*** and ***something a person is***. They are also commonly called authentication by knowledge, authentication by ownership, and authentication by characteristic. ***Strong authentication*** contains two out of these three methods: something a person knows, has, or is. Strong authentication is also sometimes referred to as ***multi-authentication***, which just means that more than one authentication method is used. ***Three-factor authentication*** is possible, which includes all authentication approaches.

Authorization

Once the subject provides its credentials and is properly identified, the system it is trying to access needs to determine if this subject has been given the necessary rights and privileges to carry out the requested actions. The system will look at some type of access control matrix or compare security labels to verify that this subject may indeed access the requested resource and perform the actions it is attempting. If the system determines that the subject may access the resource, it ***authorizes*** the subject.

Identity Management

Identity management is a broad and loaded term that encompasses the use of different products to identify, authenticate, and authorize users through automated means. The following are many of the common questions enterprises deal with today in controlling access to assets:

- What should each user have access to?
- Who approves and allows access?
- How do the access decisions map to policies?
- Do former employees still have access?
- How do we keep up with our dynamic and ever-changing environment?
- What is the process of revoking access?
- How is access controlled and monitored centrally?
- Why do employees have eight passwords to remember?

Accountability

Auditing capabilities ensure users are accountable for their actions, verify that the security policies are enforced, and can be used as investigation tools. There are several reasons why network administrators and security professionals want to make sure accountability mechanisms are in place and configured properly: to be able to track bad deeds back to individuals, detect intrusions, reconstruct events and system conditions, provide legal recourse material, and produce problem reports. Audit documentation and log files hold a mountain of information—the trick is usually deciphering it and presenting it in a useful and understandable format.

Accountability is tracked by recording user, system, and application activities. This recording is done through auditing functions and mechanisms within an operating system or application. Audit trails contain information about operating system activities, application events, and user actions. Audit trails can be used to verify the health of a system by checking performance information or certain types of errors and conditions. After a system crashes, a network administrator often will review audit logs to try and piece together the status of the system and attempt to understand what events could be attributed to the disruption.

It is a good idea to keep the following in mind when dealing with auditing:

• Store the audits securely.

• The right audit tools will keep the size of the logs under control.

• The logs must be protected from any unauthorized changes in order to safeguard data.

• Train the right people to review the data in the right manner.

• Make sure the ability to delete logs is only available to administrators.

• Logs should contain activities of all high-privileged accounts (root, administrator).

Password Management

Different types of password management technologies have been developed to get these pesky users off the backs of IT and the help desk by providing a more secure and automated password management system. The most common password management approaches are listed next:

• **Password Synchronization** Reduces the complexity of keeping up with different passwords for different systems.

• **Self-Service Password Reset** Reduces help-desk call volumes by allowing users to reset their own passwords.

• **Assisted Password Reset** Reduces the resolution process for password issues for the help desk. This may include authentication with other types of authentication mechanisms (biometrics, tokens).

Security Controls are a recommended set of actions for cyber defense that provide specific and actionable ways to stop today's most pervasive and dangerous attacks. A principle benefit of the Controls is that they prioritize and focus a smaller number of actions with high pay-off results. The Controls are effective because they are derived from the most common attack patterns highlighted in the leading threat reports and vetted across a very broad community of government and industry practitioners. They were created by the people who know how attacks work - NSA Red and Blue teams, the US Department of Energy nuclear energy labs, law enforcement organizations and some of the nation's top forensics and incident response organizations - to answer the question, "what do we need to do to stop known attacks." That group of experts reached consensus and today we have the most current Controls. The key to the continued value is that the Controls are updated based on new attacks that are identified and analyzed by groups from Verizon to Symantec so the Controls can stop or mitigate those attacks.

https://www.sans.org/critical-security-controls

Inventory of Authorized and Unauthorized Devices

Inventory of Authorized and Unauthorized Software

Secure Configurations for Hardware and Software on Mobile Device

Laptops, Workstations, and Servers

Continuous Vulnerability Assessment and Remediation

Controlled Use of Administrative Privileges

Maintenance, Monitoring, and Analysis of Audit Logs

Email and Web Browser Protections

Malware Defenses

Limitation and Control of Network Ports, Protocols, and Services

Data Recovery Capability

Secure Configurations for Network Devices such as Firewall Routers, and Switches

Boundary Defense

Data Protection

Controlled Access Based on the Need to Know

Wireless Access Control

Account Monitoring and Control

Security Skills Assessment and Appropriate Training to Fill Gaps

Application Software Security

Incident Response and Management

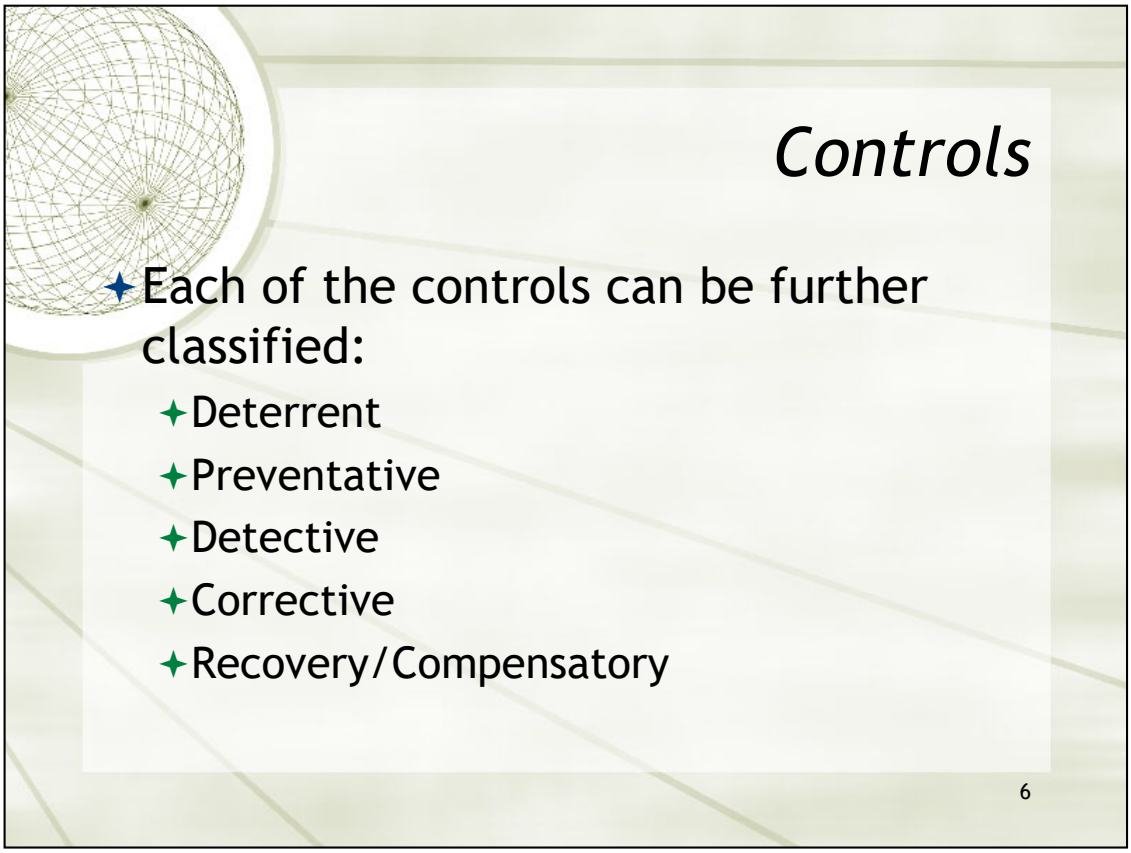
Penetration Tests and Red Team Exercises

The following controls should be utilized to achieve management's security directives:

Administrative controls: These include the developing and publishing of policies, standards, procedures, and guidelines; risk management; the screening of personnel; conducting security-awareness training; and implementing change control procedures.

Technical controls (also called logical controls): These consist of implementing and maintaining access control mechanisms, password and resource management, identification and authentication methods, security devices, and the configuration of the infrastructure.

Physical controls: These entail controlling individual access into the facility and different departments, locking systems and removing unnecessary floppy or CD-ROM drives, protecting the perimeter of the facility, monitoring for intrusion, and environmental controls.



Deterrent: controls to discourage attacks at the first place, e.g warning, banner, logon message,

Preventive: controls that make it hard for attacks to succeed, e.g. firewall, encryption

Detective: controls that detect if an attack has occurred, e.g. checksum, intrusion detection system, rotation of duties, security audits

Corrective: controls that reverse the damage, e.g. version control, incident handling procedures, fire extinguishers, undo, recycle bin

Recovery: controls that bring the system back after a major disaster, e.g. disaster recovery plan, hot/cold/warm sites, backup power

According to the Government Accountability Office (GAO), "The control environment sets the tone of an organization, influencing the control consciousness of its people. It is the foundation for all other components of internal control, providing discipline and structure. Control environment factors include the integrity, ethical values, and competence of the entity's people; management's philosophy and operating style; and the way management assigns authority and organizes and develops its people."

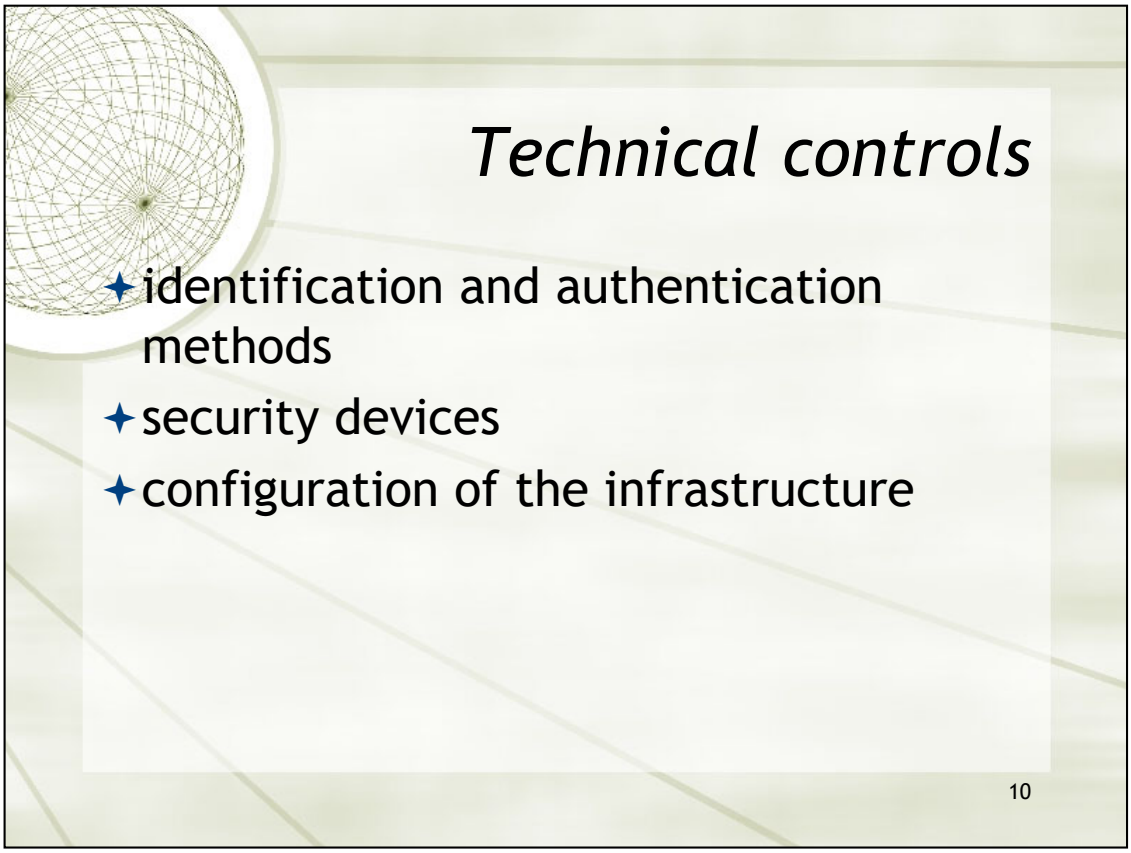
From this we can derive that some controls are the actions that people take, we call these administrative controls. Administrative controls are the process of developing and ensuring compliance with policy and procedures. They tend to be things that employees may do, or must always do, or cannot do.

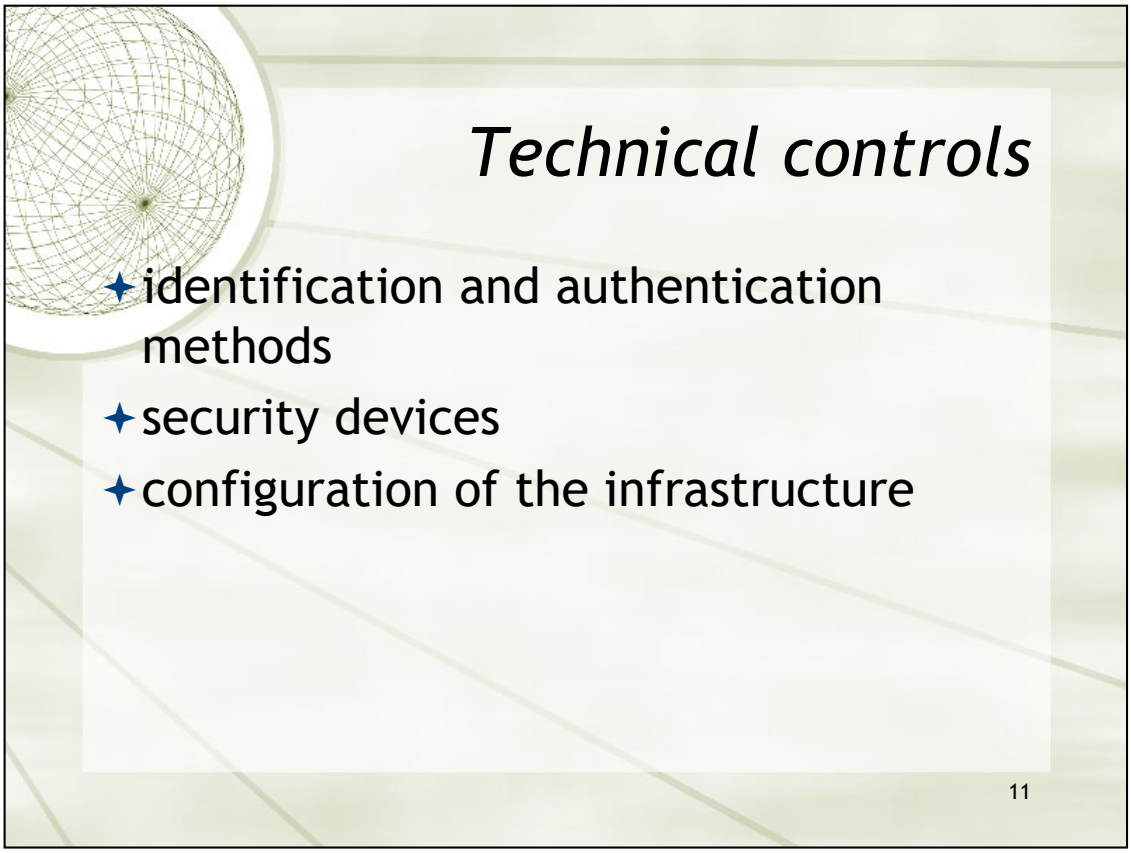
http://www.sans.edu/research/security-laboratory/article/security-controls

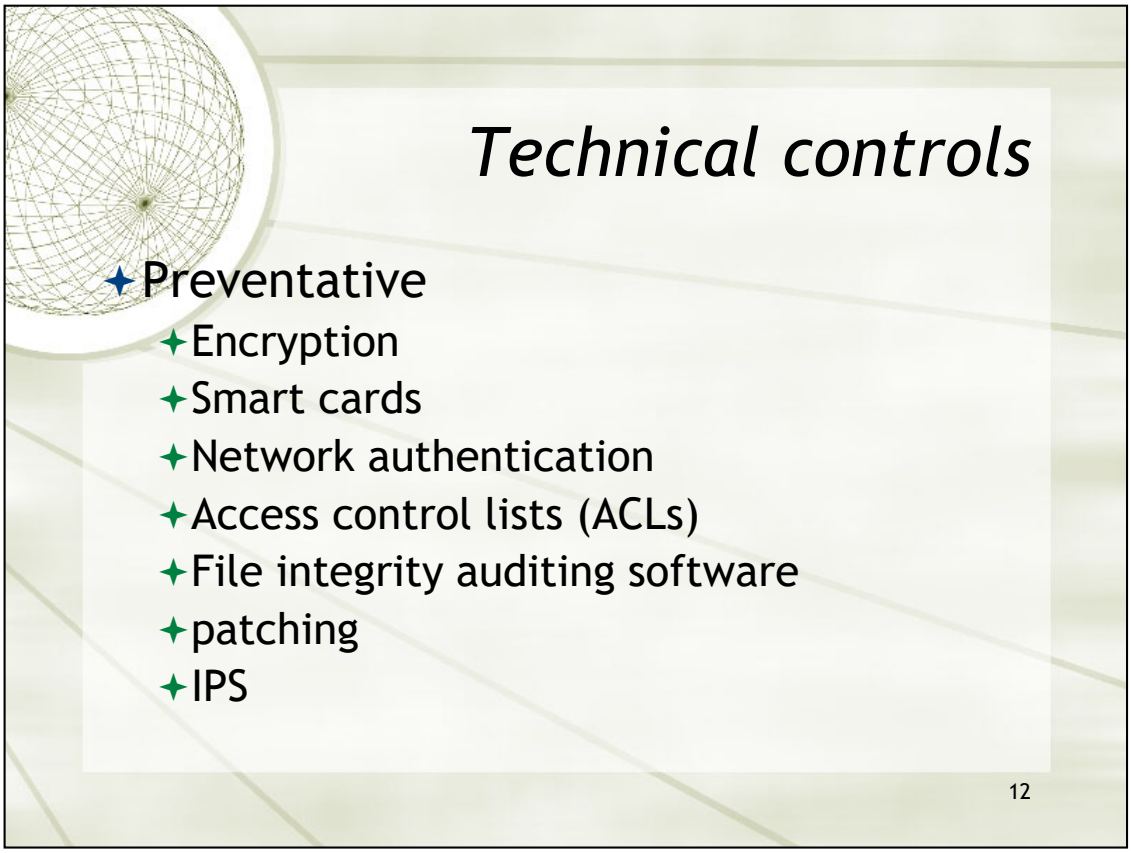

Administrative controls
risk management
screening of personnel
security-awareness training
change control procedures
8

Another class of controls in security that are carried out or managed by computer systems, these are technical controls.

http://www.sans.edu/research/security-laboratory/article/security-controls


Technical controls
identification and authentication methods
security devices
configuration of the infrastructure
10


Technical controls
identification and authentication methods
security devices
configuration of the infrastructure
11



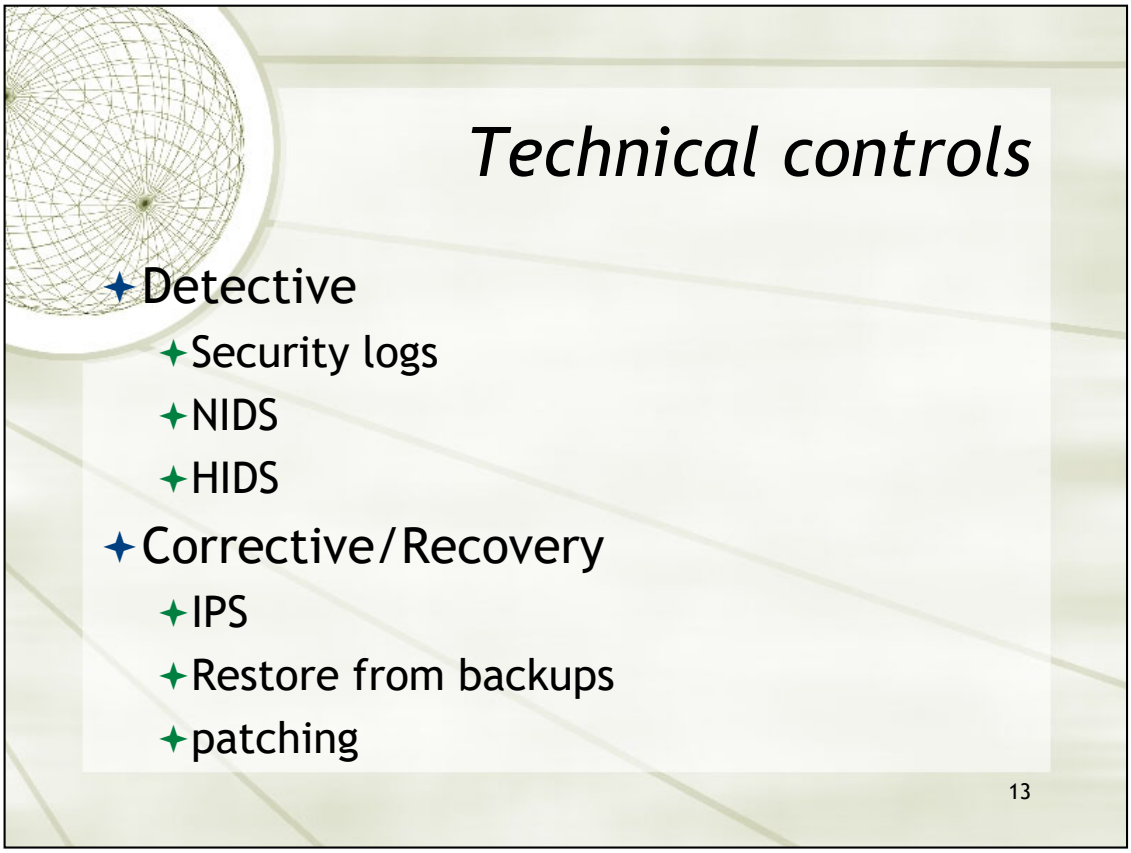
Encryption

Smart cards

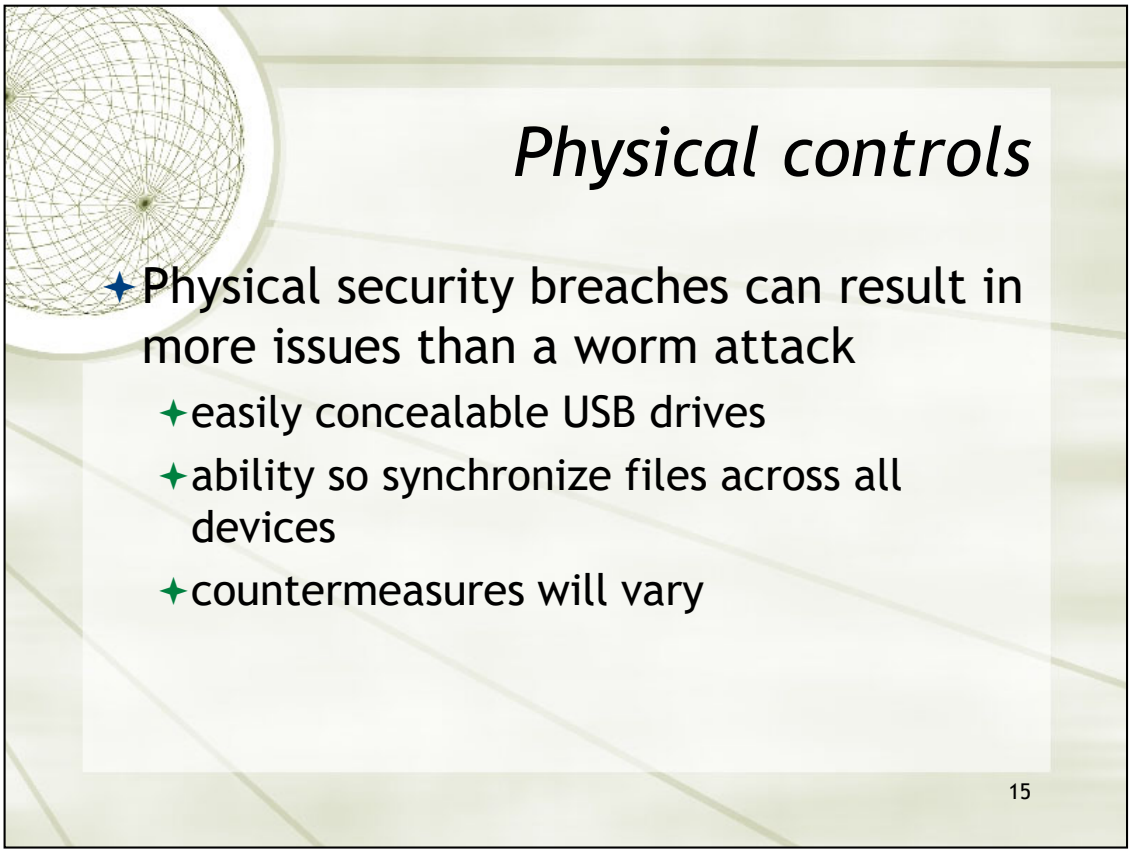
Network authentication

Access control lists (ACLs)

File integrity auditing software


Technical controls
Detective
Security logs
NIDS
HIDS
Corrective/Recovery
IPS
Restore from backups
patching
13


Physical controls
controlling individual access into the facility and different departments
locking systems and removing unnecessary drives/peripheral devices
protecting the perimeter of the facility
monitoring for intrusion
environmental controls
14



Physical security breaches can result in more issues for an organization than a worm attack. Loss of data, temporary loss of availability by shutting systems down, or longer term loss of availability by bomb or arson are all things to consider when implementing physical security. This is a survey article, for more in-depth information please consult the references, they are in the order they are used.

With the advent of easily concealable USB drives, or iPods for that matter, the issue of physical security is becoming more important than it was in the past. "Pod Slurping" is a significant threat to data. If you query a search engine for "steal data USB" you will find a number of approaches.

The protection of laptops and desktops is often overlooked; laptops in particular. According to Statistica, laptop usage compared to desktop has been increasing since 2010 and their 2019 projection is 121 million desktops compared to 170.4 million laptops. They also project tablet use to continue to decrease after the tablets will replace PCs hysteria of 2013 when more tablets were sold than laptops. Not only are these mobile devices subject to theft, but Android, Windows and Mac also have the ability so synchronize files across all devices: PC, laptop, tablet, smartphone. If one of them is lost, it is a potential portal into all of them.

Depending on the organization physical security countermeasures will

vary. A government agency such as the Department of Defense may have armed guards at the door of the building. Many organizations are not in the position of breaching national security so armed guards are not a necessity. In many cases a receptionist greets any new visitors and makes the appropriate arrangements for an on-site visit. Let's review some physical security countermeasures for the server room, as well as laptops and desktops.

Physical controls

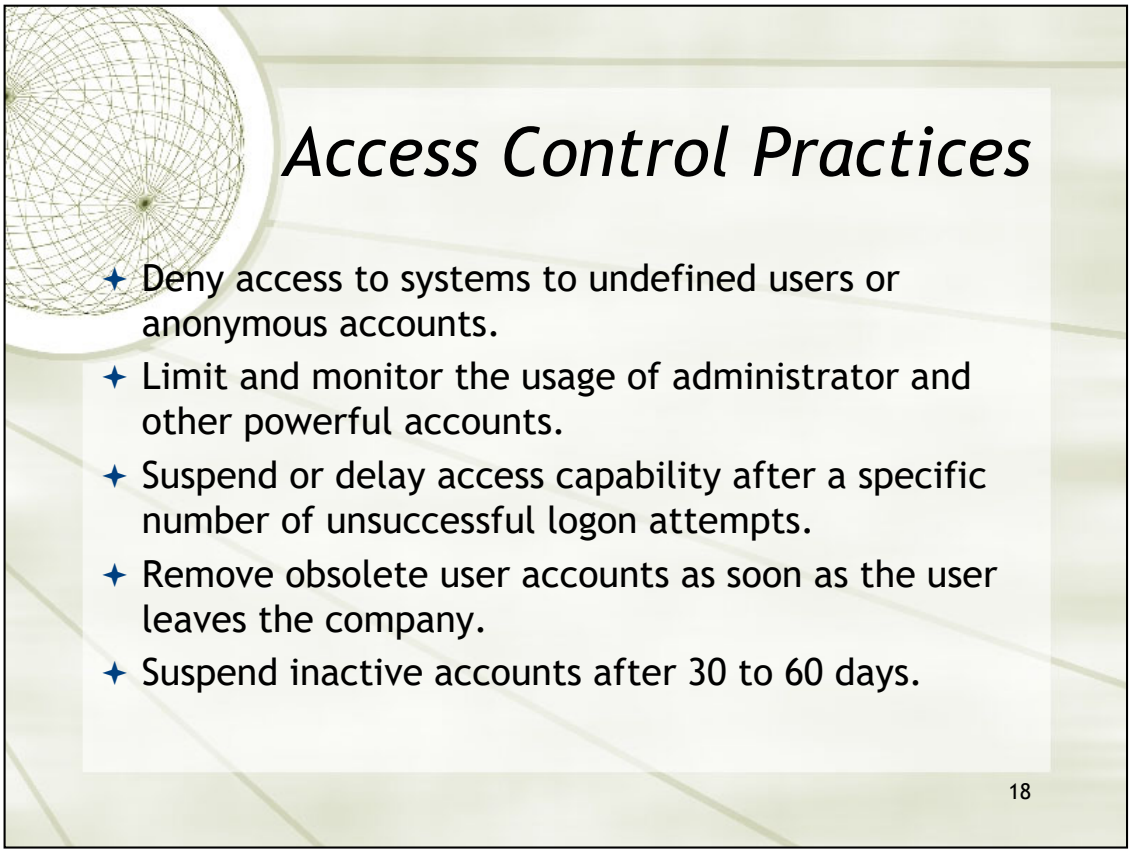
- Automated barriers & bollards
- Building management systems like Heating, HVAC, lifts/elevators control, etc.
- CCTV- Closed Circuit TV
- Electronic article surveillance - EAS
- Fire detection
- GIS mapping systems
- Intercom & IP phone
- Lighting control system
- Perimeter intrusion detection system
- Radar based detection & Perimeter surveillance radar
- Security alarm
- Video wall
- Power monitoring system
- Laptop Locks

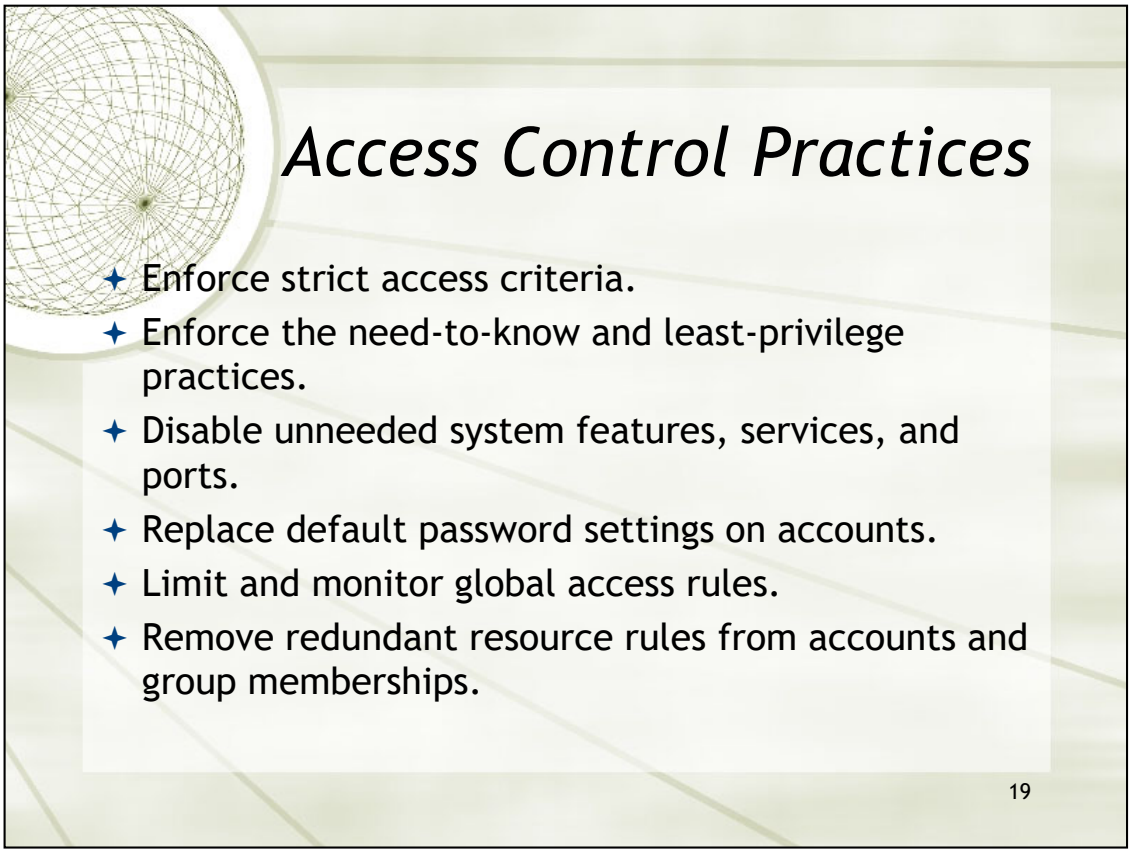
16

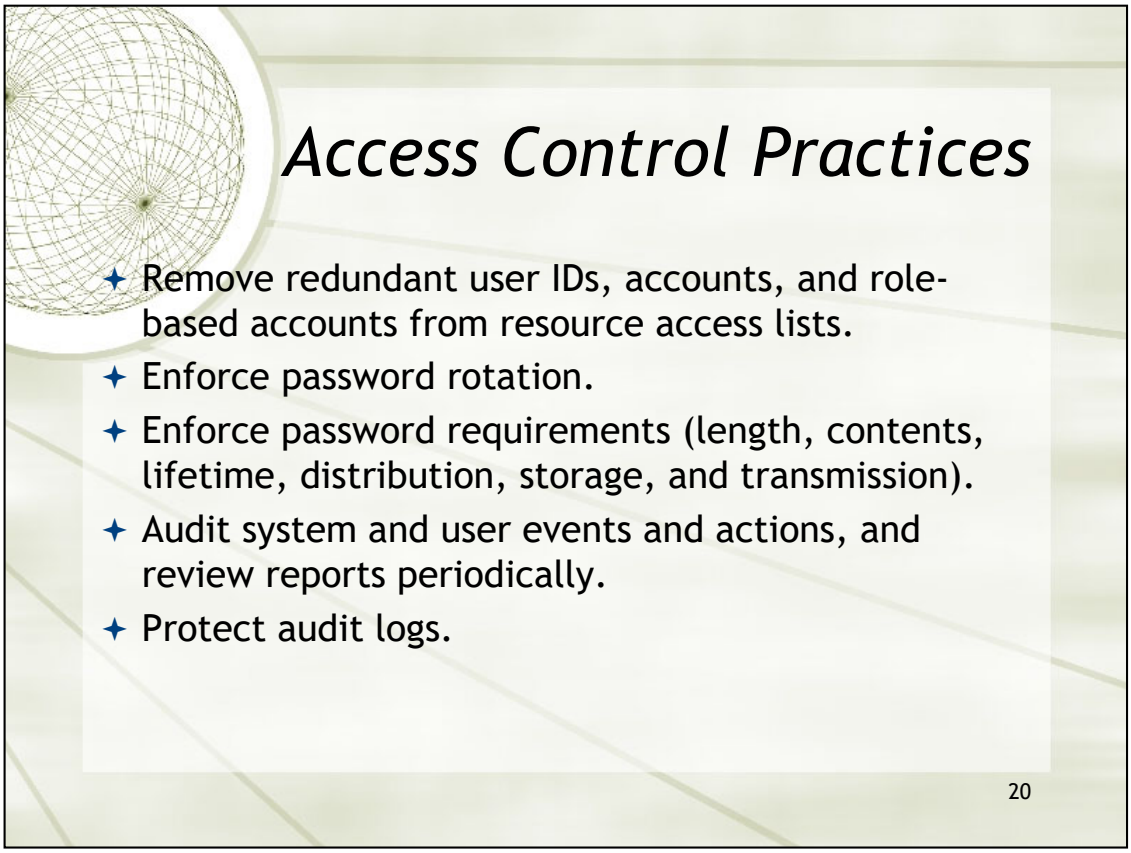
Controls

	DETERRENT	PREVENTIVE	DETECTIVE	CORRECTIVE	RECOVERY/COMPENSATORY
Administrative	Penalty & termination policy Publication of previous incidents	Security awareness & training Separation of duties Password policy ICT guidelines Recruitment checks Supervision User registration to access data/resources Change control procedure	Security reviews Performance evaluations Required vacations Background investigations Rotation of duties	Incident handling procedures	Disaster recovery and contingency plans
Technical	Pop-up window Log-on screen Welcome message Display deterrent information on websites	Access control software Library control systems System configuration Antivirus software Passwords Smartcards Biometrics Encryption Firewall (packet filtering) Network architecture Software patching OS hardening	Intrusion detection system Honeypot Firewall (application proxy) Antivirus software Audit trails Penetration testing software Check-sum Signature (MD5, hashes) Integrity validation Task/process manager Advanced CPU features	Recycle bin Undo feature Version control Error correction methods RAID arrays File recovery software Safe-mode booting	Redundant server Recovery technologies
Physical	Warning signs Lights/flashing strobes	Fences Barriers & bollards Locks & keys Double door systems Site selection HVAC Security guards Badge system	Motion detectors Smoke and fire detectors CCTV cameras Security alarms & sensors (heat, moisture, etc.)	Fire extinguishers	Hot/cold/warm sites Backup power/generator

17


Access Control Practices
Deny access to systems to undefined users or anonymous accounts.
Limit and monitor the usage of administrator and other powerful accounts.
Suspend or delay access capability after a specific number of unsuccessful logon attempts.
Remove obsolete user accounts as soon as the user leaves the company.
Suspend inactive accounts after 30 to 60 days.
18


Access Control Practices
Enforce strict access criteria.
Enforce the need-to-know and least-privilege practices.
Disable unneeded system features, services, and ports.
Replace default password settings on accounts.
Limit and monitor global access rules.
Remove redundant resource rules from accounts and group memberships.
19


Access Control Practices
Remove redundant user IDs, accounts, and role-based accounts from resource access lists.
Enforce password rotation.
Enforce password requirements (length, contents, lifetime, distribution, storage, and transmission).
Audit system and user events and actions, and review reports periodically.
Protect audit logs.
20

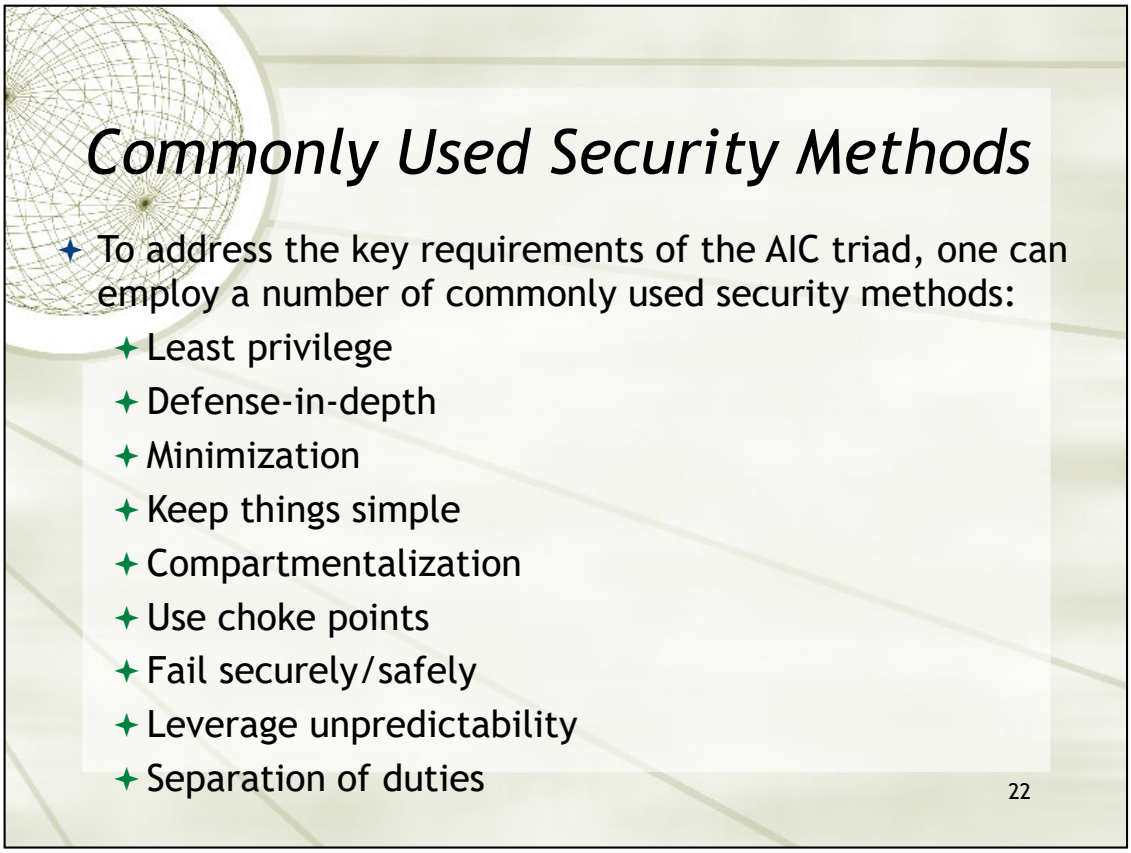
Application whitelisting of permitted/trusted programs, to prevent execution of malicious or unapproved programs including .DLL files, scripts and installers.

Patch applications e.g. Java, PDF viewer, Flash, web browsers and Microsoft Office. Patch/mitigate systems with "extreme risk" vulnerabilities within two days. Use the latest version of applications.

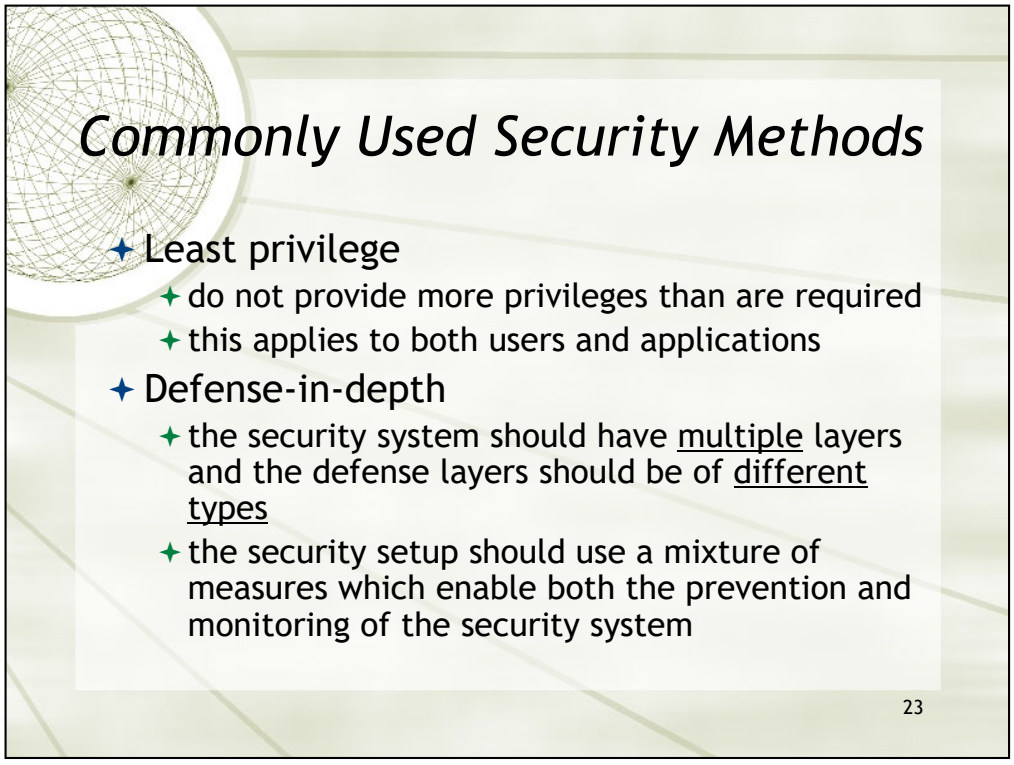
Patch operating system vulnerabilities. Patch/mitigate systems with "extreme risk" vulnerabilities within two days. Use the latest suitable operating system version. Avoid Microsoft Windows XP.

Essential

Restrict administrative privileges to operating systems and applications based on user duties. Such users should use a separate unprivileged account for email and web browsing.



Now that we have covered the fundamental concepts of information security, let's consider some of the universal security principles/methods, such as principles of least privilege, minimization, and compartmentalization. They are known as control methodologies – different ways to apply controls.



Least Privilege

The principle of least privilege stipulates, "Do not give any more privileges than absolutely necessary to do the required job." This principle applies not only to privileges of users and applications on a computer system, but also to other noninformation systems privileges of an organization's staff. The principle of least privilege is a preventive control, because it reduces the number of privileges that may be potentially abused and therefore limits the potential damage. Like most good principles, the principle of least privilege is applicable in all information systems environments. Some examples of application of this principle include the following:

- Giving users only read access to shared files if that's what they need, and making sure write access is disabled
- Not allowing help desk staff to create or delete user accounts if all that they may have to do is to reset a password
- Not allowing software developers to move software from development servers to production servers

Defense in Depth

The principle of defense in depth is about having more than one layer or type of defense. The reasoning behind this principle is that any one layer or type of defense may be breached, no matter how strong and reliable you think it is, but two or more layers are much more difficult to breach. Defense in depth works best when you combine two or more different types of defense mechanisms—such as using a firewall between the Internet and your LAN, plus the IP Security Architecture (IPSEC) to encrypt all sensitive traffic on the LAN. In this scenario, even if your firewall is compromised, the attackers still have to break IP Security to get to your data flowing across the LAN.

Generally, different types of controls should be used together: first, preventive controls should be in place to try and prevent security incidents from happening at all; second, detective controls are necessary so that you can know whether preventive controls are working or have failed; and third, corrective controls are needed to help you respond effectively to security incidents and contain damage. However, the defense in depth principle does not mean that you should indiscriminately apply all the controls and security measures you can get your hands on: balance has to be found between security provided by the defense in depth approach and the financial, human, and organizational resources you are willing to expend following it. This balance is addressed by the cost-benefit analysis.

How is file access protection provided in a layered approach?

If an administrator puts all users in specific groups and dictates what those groups can and cannot do with the company's files, this is only one layer in the approach.

To properly protect file access, the administrator must do the following:

1) Configure application, file, and Registry access control lists (ACLs) to provide more granularity to users and groups's file permissions.

2) Configure the system default user rights (in a Windows environment) to give certain types of users certain types of rights.

3) Consider the physical security of the environment and the computers, and apply restraints where required.

4) Place users into groups that have implicit permissions necessary to perform their duties and no more.

5) Draft and enforce a strict logon credential policy so that not all users are logging on as the same user.

6) Implement monitoring and auditing of file access and actions to identify any suspicious activity.

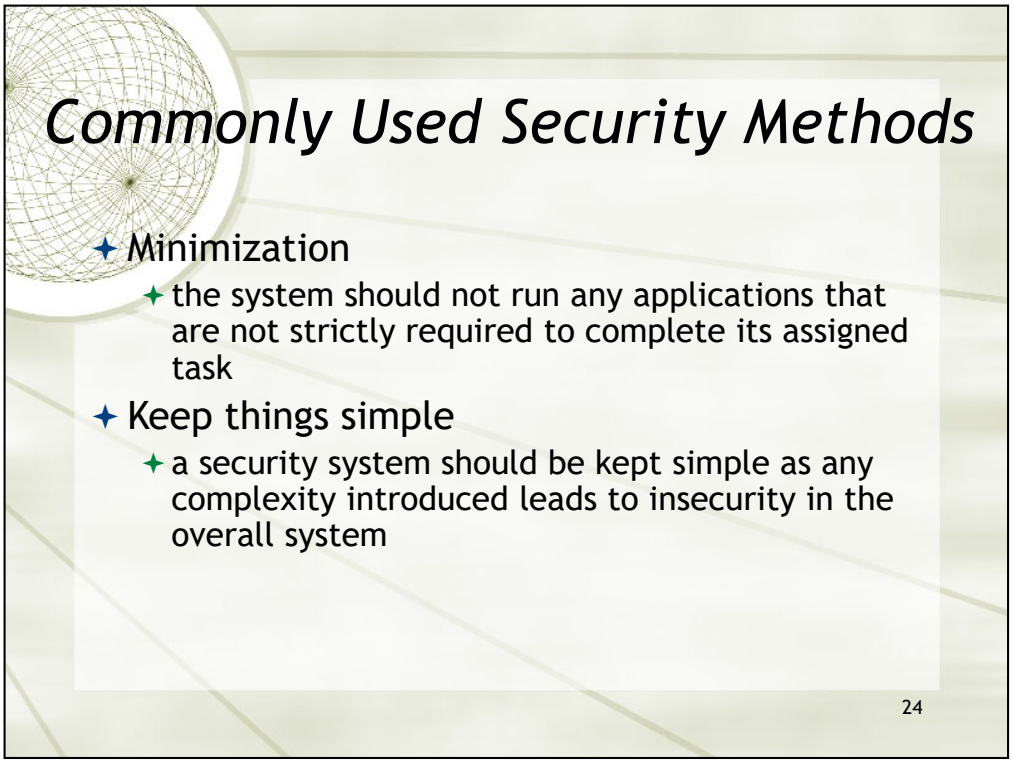
Sound like overkill? It really isn't. If an administrator makes all users log in using different accounts, applies file and Registry ACLs, configures groups, and

monitors audit logs but

does not consider physical security, a user could use a USB drive with a simple program to get around all other security barriers. All of these components must work in a synergistic manner to provide a blanket of security that individual security mechanisms could not fulfill on their own.

A network that has a firewall with packet filtering, a proxy server with content filtering, its public and private DNS records clearly separated, SSL for Internet users, IPSec for VPN connections, and public key infrastructure (PKI), as well as restricted service and port configuration, may seem like a fortified environment, and a network administrator most likely implemented these mechanisms with the best intentions. However, one problem is that it is fortified only for a moment in time.

Without a scanning device that probes the environment on a scheduled basis or an IDS that looks out for suspicious activity, the environment could be vulnerable even after the company has spent thousands of dollars to protect it. Technology and business drivers continually change, and so do networks and environments. When you configure a new application, apply a patch, or install a device, the change to the environment could have unpredictable con- sequences (not to mention the new ways hackers have found to circumvent the original security mechanisms).



Minimization

The minimization principle is the cousin of the least privilege principle and mostly applies to system configuration. The minimization principle says “do not run any software, applications, or services that are not strictly required to do the entrusted job.” To illustrate, a computer whose only function is to serve as an e-mail server should have only e-mail server software installed and enabled. All other services and protocols should either be disabled or not installed at all to eliminate any possibility of compromise or misuse. Adherence to the minimization principle not only increases security but usually also improves performance, saves storage space, and is a good system administration practice in general.

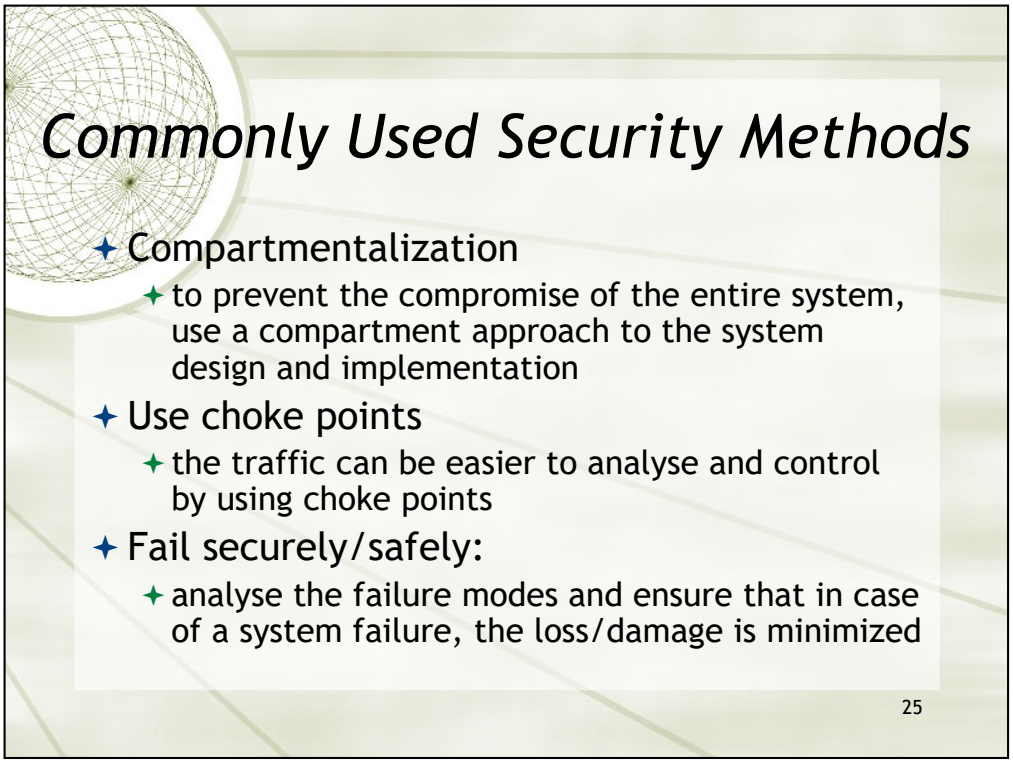
Cost-Benefit Analysis

Although not strictly a principle, the cost-benefit analysis is a must when considering implementation of any security measure. It says that the overall benefits received from a particular security control or mechanism should clearly exceed its total costs; otherwise, implementing it would make no sense. Cost-benefit analysis directly affects return on investment (ROI). This may sound like simple common

sense, and it probably is; nevertheless, this is an important and often overlooked concern. When doing cost-benefit analysis, one should consider all costs and all benefits over a period of time, for example from one to five years, to have a complete picture.

Keep Things Simple

Complexity is the worst enemy of security. Complex systems are inherently more insecure because they are difficult to design, implement, test, and secure. The more complex a system, the less assurance we may have that it will function as expected. Although complexity of information systems and processes is bound to increase with our increasing expectations of functionality, we should be very careful to draw a line between avoidable and unavoidable complexity and not sacrifice security for bells and whistles, only to regret it later. When you have to choose between a complex system that does much and a simple system that does a bit less but enough, choose the simple one.



Compartmentalization

Compartmentalization, or the use of compartments (also known as zones, jails, sandboxes, and virtual areas), is a principle that limits the damage and protects other compartments when software in one compartment is malfunctioning or compromised. It can be best compared to compartments on ships and submarines, where a disaster in one compartment does not necessarily mean that the entire ship or submarine is lost. Compartmentalization in the information security context means that applications run in different compartments are isolated from each other. In such a setup, the compromise of web server software, for example, does not take down or affect e-mail server software running on the same system but in a separate compartment. Zones in Solaris 10 implement the compartmentalization principle and are powerful security mechanisms.

Use Choke Points

Security is very much about control, and control is so much more effective and efficient when you know all ways in and out of your systems or networks. Choke points are logical “narrow channels” that can be easily monitored and controlled. An example of a choke point is

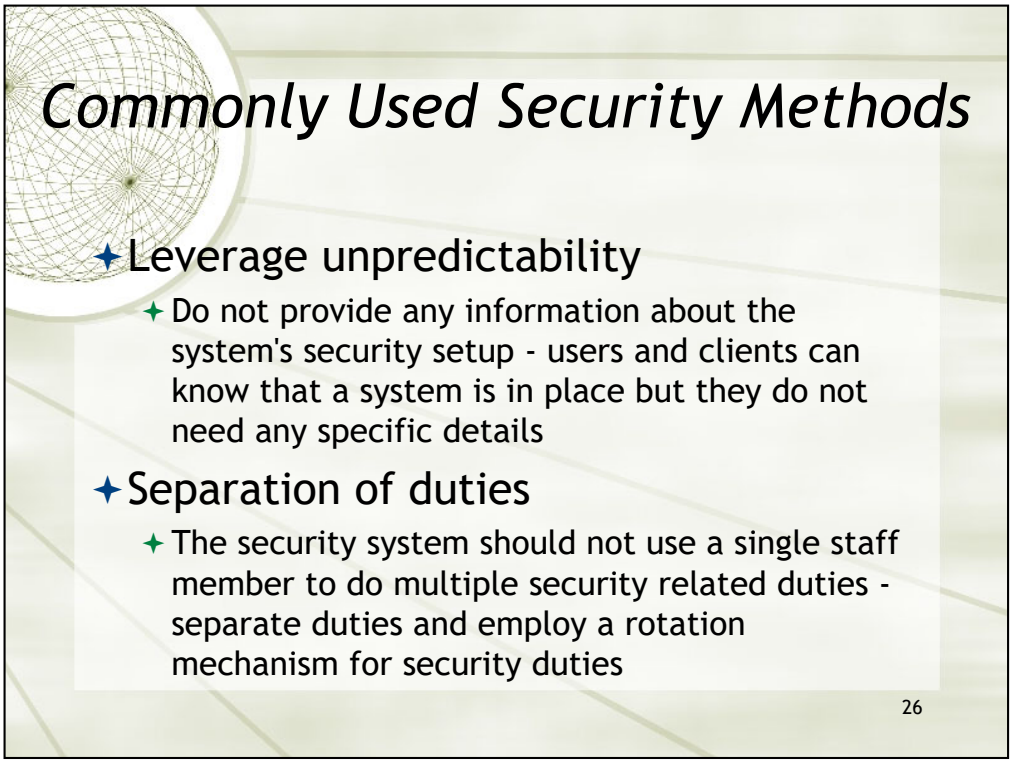
a firewall—unless traffic can travel only via the firewall, the firewall's utility is reduced to zero. Consider the example of controlled entrances to buildings or facilities of high importance, such as perimeter fencing and guard posts.

Fail Securely

Although fail securely may sound like an oxymoron, it isn't. Failing securely means that if a security measure or control has failed for whatever reason, the system is not rendered to an insecure state. For example, when a firewall fails, it should default to a "deny all" rule, not a "permit all." However, fail securely does not mean "close everything" in all cases; if we are talking about a computer-controlled building access control system, for example, in case of a fire the system should default to "open doors" if humans are trapped in the building. In this case, human life takes priority over the risk of unauthorized access, which may be dealt with using some other form of control that does not endanger the lives of people during emergency situations.

Secure the Weakest Link

To people new to information security, many information security principles and approaches may sound like little more than common sense. Although that may well be the case, it doesn't help us much, because very often we still fail to act with common sense. The principle of securing the weakest link is one such case: look around and you will likely see a situation in which instead of securing the weakest link, whatever it may be, resources are spent on reinforcing already adequate defenses. For example, there are technological solutions already employed to protect the system but no training on how to handle attachments in email messages.



Leverage Unpredictability

Just as states don't publicize the specifics of their armaments, exact locations, or numbers of armed forces, you should not publicize the details of your security measures and defenses. This principle should not be seen as contradicting deterrent security controls—controls that basically notify everyone that security mechanisms are in place and that violations will be resisted, detected, and acted upon. The important difference here is that deterrent controls don't provide details of the defenses but merely announce their existence so as to deter potential attackers without giving them detailed information that later may be used against the defenders. In practical terms, this means you can, for example, announce that you are using a firewall that, in particular, logs all traffic to and from your network, and these logs are reviewed by the organization—there is no need to disclose the type, vendor, or version number of the firewall; where it is located; how often logs are reviewed; and whether any backup firewalls or network intrusion detection systems are in place.

Segregation of Duties

The purpose of the segregation (or separation) of duties is to avoid the

possibility of a single person being responsible for different functions within an organization, which when combined may result in a security violation that may go undetected. Segregation of duties can prevent or discourage security violations and should be practiced when possible. Although the actual job titles and organizational hierarchies may differ greatly, the idea behind the principle of separation of duties stays the same: no single person should be able to violate security and get away with it. Rotation of duties is a similar control that is intended to detect abuse of privileges or fraud and is a practice to help your organization avoid becoming overly dependent on a single member of the staff. By rotating staff, the organization has more chances of discovering violations or fraud.