





Day 2

Welcome to the Chapter 2 in the SSCP curriculum!

In this chapter we will start to examine the basic steps that we need to put into place to develop a security culture within the organization. We will examine policies and how they should be written and used to enforce the security requirements. We will then move on to the actual business of controlling how our systems, services, resources and data can be accessed safely and only by those authorized to do so. We will discuss access control models (MAC, DAC, RBAC etc.) and conclude with an examination of both LAN and WAN identity management.

Chapter 2: Understand Risk Management Options and the use of Access Controls to protect Assets

Chapter 2 Agenda

Chapter 2 Agenda		
<i>Module</i>	<i>Domain Name</i>	<i>Domain Icon</i>
Document, Implement, and Maintain Functional Security Controls	Domain 2: Security Operations and Administration	
Implement Access Controls	Domain 1: Access Controls	
Participate in the Identity Management Lifecycle	Domain 1: Access Controls	
Implement and Maintain Authentication Methods-Identify and Access	Domain 1: Access Controls	

Chapter Objectives

After completing this chapter, the participant will be able to:

1. Discuss security strategies.
2. Evaluate policies through standards and baselines.
3. Evaluate controls.
4. Differentiate types of controls.
5. Describe the reference monitor.
6. Describe the information management model (IMM).
7. Explain access control models.
8. Choose which access control model best suits your organization.
9. Explain separation of duties.
10. Discuss identity management.
11. Compare identity management components.
12. Evaluate authentication methods.
13. Explain the authorization phase.
14. Discuss accounting.
15. Explain identity as a service (IDaaS)
16. Use single sign-on (SSO).
17. Describe trust models.
18. Compare wide area network (WAN) based authentication options.
19. Discuss access control standards and protocols.

Module 1: Document, Implement, and Maintain Functional Security Controls

Module Objectives

After completing this module, the participant will be able to:

1. Discuss security strategies.
2. Evaluate policies through standards and baselines.
3. Evaluate controls.
4. Differentiate types of controls.

Overview

In this module we are going to start looking at the pieces that make up a security program. Now that we have examined the process of risk management, we have the information needed to justify the controls and other actions taken to secure and protect the assets of the organization.

The core principle of information security must be remembered: security exists solely for the purpose of supporting and enabling the business mission. Our goal as security practitioners is not just to be secure but rather to secure the business. Our organizations do not hire us because they are really interested in security; they hire us because management realizes that security is necessary in order for the business to survive. But when the security practitioner forgets this principle then the business quickly begins to isolate and cut back on the security budget and the influence of the security team.

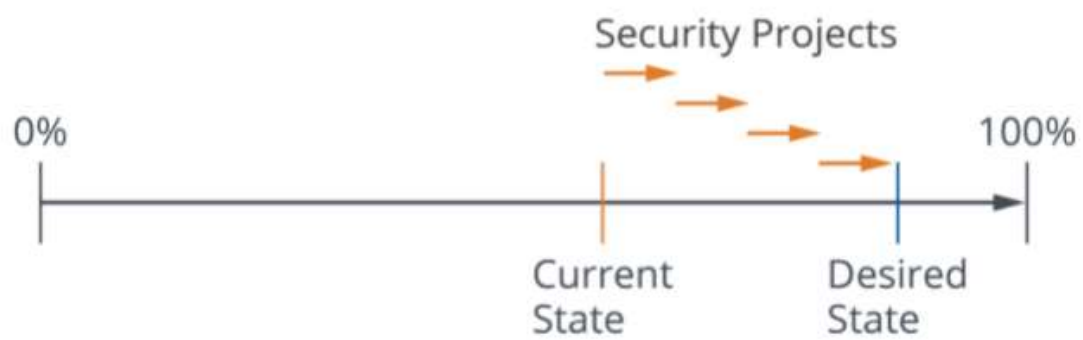
Security by its very nature has often been reactive, following along weeks or months later to try to secure technologies or business processes that have already been implemented. Security is often late to respond to emerging threats and new technology, and is speechless when asked by management for an opinion on how to secure a new business process or technology.

Security Strategy

We need security strategy, not just security operations. We need a plan that has a vision for the future and has an eye on how to protect the world as it will be in a few years – not just to react to what is happening now, or has already happened. But that strategy must be aligned with the strategy of the business. Security must not be aiming in one direction while the business is headed along a different road. If that happens, we will witness that security becomes more and more distant from the business and will be seen by management as irrelevant. Instead, our goal is to understand the business, listen to management, watch for changes in business and technology and demonstrate to management the value we bring. By so doing we may “have a seat at the table” and be much more effective and working with management to integrate and weave security into business processes.

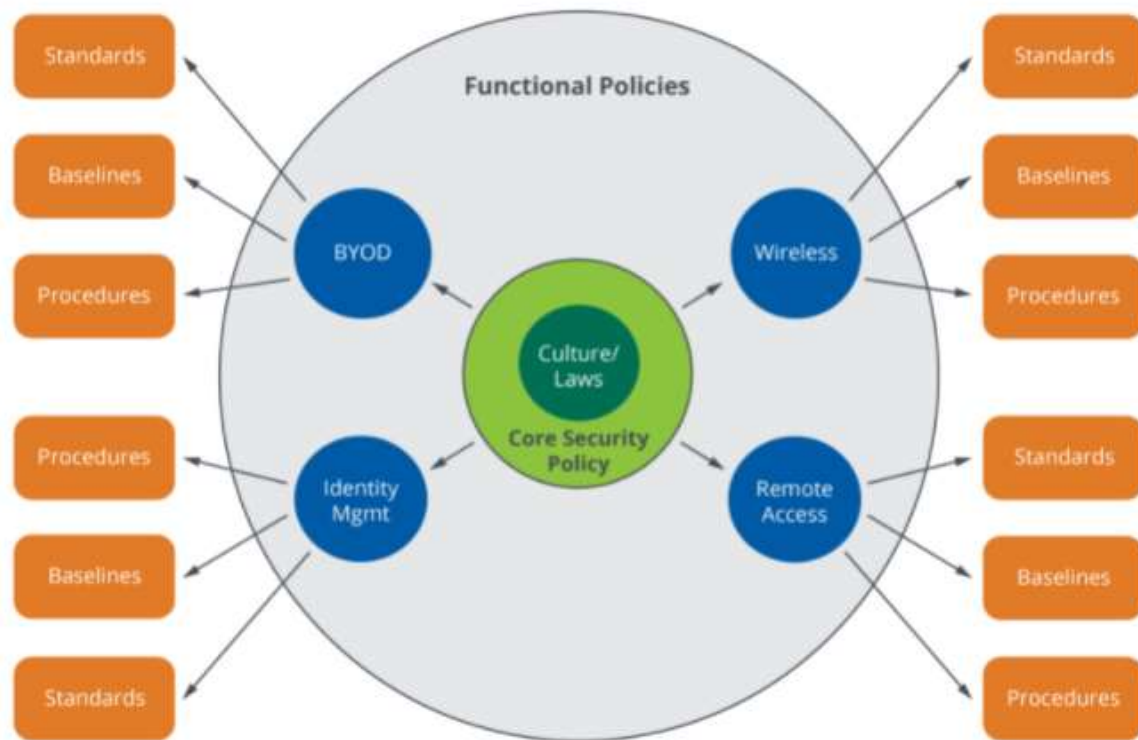
So, the first step in security is to have a strategy – a plan for the future. But a strategy is only words unless it leads to actions. A strategy should result in a security plan, which is the roadmap to implement the goals of the strategy. For most organizations there is a large gap between their current security state and where they want/need to be (the desired state). As such, the security plan will comprise several projects that work together to reach the desired state.

State is defined as the condition an entity is in at a point in time. Therefore, desired state is the desired condition, and state changes as the organization moves from one state to another as it progresses towards the desired state.



As can be seen in figure 2.1, the security program matures as various security projects move the organization from its current security state to its desired state. We see that the programs often work together and integrate the pieces of the security program into an enterprise security solution. We can also see that the desired state of security is not usually going to be 100% security. Depending on management, there may be a determination of what is an adequate level of security for this organization.

Policies



The above figure shows the relationship between many parts of an information security program. At the core of any security program are the laws and regulations that direct the behavior of the organization. The next factor in the development of policy is the culture of the organization – the ethics; the attitude of management toward employees, customers, regulations, suppliers and risk. This culture should be reflected and supported through the policies that the organization adopts.

Policies are what are called “directive” controls. They direct, or mandate, the behavior of the employees of the organization. Policies are signed by management and are the statement of what management intends and proclaims as the core principles of the organization.

Policy is the heart of an information security program. Policy itself is defined as the “Aggregate of directives, regulations, and rules that prescribe how an organization manages, protects, and distributes information.”

As seen in the above figure, policies are often a collection of documents. At the core should be a high-level policy that sets out the primary direction for the security strategy. This document should reflect management’s attitude towards security and demonstrate the commitment of management to sound security practices.



Discussion: Characteristics of Policies

What are the characteristics of good policies?



Discussion Review: Characteristics of Policies

Creation and approval of a high-level information security policy may take a period of months. Therefore, you do not want this policy to have to change often. It should be short and visionary, but not technical since technology changes frequently and the policy should not have to be updated every time technology changes.

Subject-Specific Security Policies

Subject-specific security policies typically address a limited area of risk related to a particular class of assets, type of technology, or business function.

Examples of specific security policies include:

- Email and internet usage policies
- Antivirus policy
- Remote access policy
- Information classification policy
- Encryption policies
- Policy document format

You should understand the basic elements of an information security policy that define and enforce the organization's security practices.

Typical Policy Elements

Objective: This statement provides the policy's context. It gives background information and states the purpose for writing the policy, including the risk or threats the policy addresses and the benefits to be achieved by policy adherence.

- **Policy statement:** A succinct statement of management's expectations for what must be done to meet policy objectives.
- **Applicability:** This lists the positions to whom the policy applies, the situations in which it applies, and any specific conditions under which the policy is to be in effect
- **Enforcement:** How compliance with the policy will be enforced using technical and administrative means. This includes consequences for noncompliance.
- **Roles and responsibilities:** States who is responsible for reviewing and approving, monitoring compliance, enforcing, and adhering to the policy.
- **Review:** Specifies a frequency of review or the next review date on which the policy will be assessed for currency and updated if needed.

To be effective, security policies must be endorsed by senior management, communicated to all affected parties, and enforced throughout the organization. When policy violations occur, disciplinary action commensurate with the nature of the offense must be taken quickly and consistently.

Policy Lifecycle

Security policies are living documents that communicate management expectations for behavior. Policy development begins with determining the need. The need for a policy may arise due to a regulatory obligation, in response to an operational risk, or a desire to enforce a particular set of behaviors that facilitate a safe, productive work environment. The parties that are affected, such as human resources, legal, audit, and business line management, should be identified so that they can participate throughout the development process.

Components of a Security Policy

Once the need is determined and the team assembled, address the following:

- **State the objective.** A clear statement of policy objectives answers the question, "Why are we developing this policy?" The statement of objective will guide development of the specific points in the policy statement and will help keep team discussions in scope and focused.
- **Draft the policy specifics.** The policy statement should be drafted in simple, clear language that will be easily understood by those who must comply with the policy. Avoid vague statements that could be open to multiple interpretations, and be sure to define all technical terms used in the policy document.
- **Identify methods for measurement and enforcement.** Policy enforcement mechanisms may include technical controls, such as access management systems, content blocking, and other preventive measures, as well as administrative controls, such as management oversight and supervision.
- **Compliance with policy expectations can be measured through audit trails, automated monitoring systems, random or routine audits, or management supervision.** The means of monitoring or measuring compliance should be clearly understood, as well as the logistics of enforcement. The logistics of taking and documenting disciplinary action should be established at this time to ensure that the organization is willing and able to enforce policy and prepared to apply corrective action quickly and consistently.
- **Communication.** The timing, frequency, and mechanism by which the policy will be communicated to employees and others should be established before final policy approval. Expectations must be clearly communicated and regularly enforced so that everyone remains apprised of what the appropriate conduct is considered to be. Whenever disciplinary action may be taken in response to policy violations, it is especially important that management make every effort to ensure that employees are made aware of the policy and what they must do to comply. Some organizations require employees to sign a form acknowledging their receipt and understanding of key policies and agreeing to comply with expectations.
- **Periodic review.** Policies should be reviewed at least annually to ensure that they continue to reflect management's expectations, current legal and regulatory obligations, and any changes to the organization's operations. Policy violations that have occurred since the last review should be analyzed to determine whether adjustments to policy or associated procedures, or enhancements to communication and enforcement mechanisms may be needed.

Functional Policies

Functional policies are the technical side of the policy framework. Since the high-level policy is not technical, an organization needs policies to address specific areas of technology or specific business processes. Functional policies are targeted and specific, and easier to change or replace than a high-level, general policy. Examples of functional policies would be policies regarding remote access, acceptable use of the Internet, Bring Your Own Device (BYOD), portable media and incident handling policies. Policies are words, but words should be followed up with action. Policy should direct actions and those actions will be written in procedures, standards and baselines.

Procedures

Procedures are the step-by-step actions taken to accomplish a defined task. For example, every organization should have a change control procedure to oversee the implementation of changes to systems, projects and networks. The advantage of having a defined procedure is that it ensures that a task is consistently completed in the same manner. Any deviation from the procedure could be noticed and lead to an investigation. If a procedure is documented then it allows other personnel to fill in for an absent co-worker.

Standards

There are two different ways to look at standards:

- International Standards such as ISO/IEC 27001
- Standards related to software or hardware implementation

ISO/IEC 27001 is titled Information technology – Security techniques – Information security management systems – Requirements. This is an excellent standard that can be used by an organization to help them establish a credible information security program. Many organizations struggle with the challenge of how to build a good security program. Using the ISO27001 as a framework for their security program can ensure that the organization bases their program on globally recognized best practices. It also ensures that all the main areas of information security are addressed and that nothing was missed. Another advantage of using the ISO27001 is that the organization can now be certified by a third party as compliant with the standard, thereby providing assurance to their clients, shareholders and vendors that they are meeting internationally recognized industry best practices in information security.

ISO27001 mandates the practices that an organization must follow to be compliant with its requirements. Therefore, it uses language like “shall” when it describes what an organization must do. However, most standards are not prescriptive enough – they tell what must be done, but not how to do it. The requirements can often be interpreted in different ways, which means that there is an element of subjectivity in how the standards are applied.

To help an organization to set up a strong security program that would be in compliance with ISO27001, a separate, supporting document was created named ISO/IEC 27002. This document helps an organization to build the security framework mandated in ISO27001. This can be seen through the naming of ISO27002 as: Information technology – Security techniques – Code of practice for information security controls. As the name indicates, this is only a guideline rather than a requirement. The language used in the ISO27002 standard also differs in that it uses the term “should” instead of the more prescriptive “shall.” ISO27002 lists the controls that an organization should consider in building, implementing and improving its information security program.

There are many other standards available that an organization could use as the standard for their security program. These may be national standards (such as NIST or BSI standards), or industry standards (such as the Payment Card Industry – Data Security Standard [PCI-DSS]).

The other use of the term “standards” can refer to the adoption of hardware or software standards that an organization selects. The adoption, for example, of a standard operating system or the choice to purchase equipment from one vendor (e.g., Dell, IBM, Lenovo, etc.) can provide significant advantages to the organization. If an organization only has to support one product, that can ensure greater consistency in the configuration and security of the organization’s systems, as well as reducing the cost of training and support. Standards also can result in better cost control through bulk purchasing and licensing. On the other hand, standards can pose a risk to the organization through having “all your eggs in one basket” where a flaw in the product would now affect the entire organization. Another risk with enforcing a standard is the problem of a lack of flexibility: the standard product may not be the best for all departments, and the vendor may increase prices and maintenance costs that are difficult to avoid without a complete change of standard.

Baseline

It is common to see situations where an organization has purchased an excellent product (device) that can provide a wide range of services (benefits), but the product is not configured correctly and is only providing minimal benefit. This can be a result of a lack of a defined baseline configuration for the device. A sound security practice is to define a minimal security baseline (configuration) for a product so that when the product is deployed in multiple locations it will be properly configured and secured. This baseline may include the hardening of the device (turning off services and functionality that are not required), setting of security controls, enabling security functions, or other configurable items that would ensure the device is adequately protected.

By setting a security baseline the organization can conduct security compliance scans to ensure that all devices on the network, for example, are configured correctly in accordance with the baseline. A baseline often represents the minimum acceptable configuration, in other words, no device may be connected that does not meet this minimum standard at the very least. However, it does not restrict a department from implementing an even more secure configuration where needed. In other words, everything on the network is secure to at least a minimum acceptable level – but some devices may be even more secure.

Important Tips from this Section

The foundation for a security strategy is the development of, and approval of, policy. Policy is that high-level document that states management's commitment to the information security program and mandates the behavior of the employees. The high-level policy is often supported through functional policies that address individual areas of technology. All policies are supported through standards, procedures and baseline to ensure that the intent of the policies is carried out in action.



Activity: Functional Policies

INSTRUCTIONS

Answer the following questions:

1. What is a procedure?
2. How does a baseline differ from a standard?



Activity Answers: Functional Policies

Answers

1. What is a procedure?

Procedures are the step-by-step actions taken to accomplish a defined task

2. How does a baseline differ from a standard?

The baseline represents the minimum set of security configurations. A standard is an agreed upon set of methods, technologies etc. within an organization that feeds into the baseline security requirements.

Controls

The selection of controls must be done with prudence and awareness of the impact of the control. A control may impact performance or productivity, it may be expensive to maintain, and it may introduce new vulnerabilities if the control itself can be attacked.

We know that there are usually three types of controls:

- Managerial controls (sometimes called administrative)
- Technical controls (sometimes called logical)
- Physical (environmental) controls (sometimes called operational)

Each type of control is important as all three types work together. For example, a technical control requires physical infrastructure and physical security in order to operate, and the support of managerial controls to manage and monitor its effectiveness.

Managerial Controls

Management Controls address security topics that can be characterized as managerial. They are techniques and concerns that are normally addressed by management in the organization's computer security program. In general, they focus on the management of the computer security program and the management of risk within the organization.

Physical (Operational) Controls

Operational Control policies address process-based security controls implemented and executed by people. These controls rely on management controls to identify the appropriate processes or actions, and often rely on the technical controls for enforcement.

We can further subdivide all three of these types of controls in sub-categories. Each sub-category provides a specific benefit.

Directive Controls: Controls that direct or mandate operational procedures or behavior. Examples of directive controls include:

- Managerial – policy
- Technical – warning window about a potentially dangerous website
- Physical – “Do Not Enter” sign

Deterrent Controls: Controls that discourage a person from committing an improper act. Examples of deterrent controls include:

- Managerial – disciplinary policy
- Technical – Warning banner regarding prosecution for entering prohibited systems
- Physical – “Beware of Dog” sign

Preventive Controls: Controls that try to stop improper behavior. Examples of preventive controls include:

- Managerial – separation of duties
- Technical – password
- Physical – fence

All of the above controls are precautionary controls that proactively try to stop bad events from happening, therefore we often hear proactive controls referred to as safeguards in that they attempt to safeguard an asset from attack. However, we need to move on to reactive controls – controls that come into effect once an undesirable event has taken place. These controls are often called countermeasures since they “counter,” or respond directly to, an attack.

Reactive Controls

Examples of reactive controls include the following.

Detective Controls: A detective control is one that would identify an attack and alert administrators. The problem in many cases today is that organizations have been attacked and compromised, but they are not even aware of the attack. This leads to a failure to respond to, contain, and eradicate the attack. Examples of detective controls include:

- Managerial – balancing reports
- Technical – intrusion detection system
- Physical – motion sensor

Corrective Controls: Corrective controls attempt to regain control over the incident. In many cases this does not resolve the incident; rather, it contains and identifies the nature and scope of the incident. Examples of corrective controls include:

- Managerial – removal of a suspect from the area
- Technical – isolate a system
- Physical – fire suppression system

Recovery Controls: Recovery controls restore the affected area to normal, whatever “normal” is. In some cases, normal may be a completely replaced system, or a new building in case of fire. For example: an organization attempts to protect its building and equipment through a managerial directive control that prohibits smoking near an area where explosive materials are stored. It enforces that policy through a managerial deterrent that states that a violation of the policy could lead to a fine or disciplinary action. It attempts to prevent fire through the managerial preventive control of monitoring and physical preventive control of removal of fire-causing materials. However, since a fire could still start, the organization installs physical detective controls such as smoke detectors to detect a fire. The organization then has the physical corrective control of a fire suppression system to put out the fire and stop further damage. Now the organization has an area that has been damaged by both the fire and the fire suppression system, and it needs recovery controls. Examples of recovery controls include:

- Managerial – training of new employees
- Technical – recovery from backups
- Physical – rebuilding the damaged area

From this example you can see how controls often work in layers. One control provides a layer of protection at a given level, but that control is supported by other controls. This is an example of defense in depth, or layered defense, a concept that will be examined in more detail in the networking section. Defense in depth is commonly used in networking to provide multiple obstacles to an attacker attempting to gain unauthorized access to assets of the organization.

One common control that was not used as an example above is closed-circuit television (CCTV). That is because CCTV is an excellent example of a control that fits into numerous control categories. While CCTV is a physical control (supported by the managerial control of monitoring and technical controls of passwords and secure communications), it can be seen as:

- A deterrent – the very presence of a camera may discourage crime
- A detective control – it can observe unauthorized behavior
- A corrective control – it can identify the type and scope of the incident to facilitate better response.
- A recovery control – it can record the previous state of the systems to enable rebuilding

Compensating Controls

There is one more category of control that should be reviewed: compensating controls.

Compensating controls are additional controls that attempt to compensate for, or address, a vulnerability that is not effectively addressed through other controls. For example, a user is usually prevented from doing administrative functions on their desktop. This prevents the user from installing unauthorized software or deleting system critical files. However, that control would not work for privileged users such as system administrators who need privileged access in order to do their jobs. They cannot be prevented from performing administrator functions on the system. Therefore, normal preventive controls would not work. So, management deploys additional controls

to compensate for that vulnerability through the use of additional controls. In this case, compensating controls could include “dual control” where separation of duties is enforced through the managerial and technical controls are requiring two people to work together to complete a task. The organization also may require additional supervision or monitoring of activity by privileged users. All actions taken by privileged users may be written off to an external system that cannot be overwritten or deleted by the administrator. Compensating controls are additional layers of control of all types and categories used to protect vulnerable assets of the organization that may not be adequately protected by other controls.

Discussion: Examples of Controls

Provide an example of each of the following without using the examples listed:

- Managerial deterrent control
- Technical corrective control
- Physical directive control

What type of control is an identity management system?

Implementation/Assessment

When an organization designs and implements a control, it does so with careful consideration. It wants to deploy controls that are not just effective, but also cost effective. The most expensive control is not always the best fit for the organization. It can be assumed that most controls are designed and implemented with the best of intentions, but not everything works out according to plan. Once deployed, a control may not be as effective as originally thought, and over time the control may lose some of its effectiveness over time so that it eventually no longer provides the expected benefits.

When controls are designed, they should be designed to facilitate monitoring and testing. The controls need to facilitate access, generate logs, and have testing capability to allow management, auditors and regulators the ability to examine and assess whether the control is working correctly.

When controls are implemented, they should conform to the security and operational baselines mandated for the control. For example, if a firewall is implemented in a remote location, it still should be implemented according to the configuration required by the central IT management or security department.

When testing a control, the assessor should test all the aspects of the control, including management of the control (training of users, monitoring, change control, etc.), the technical operations of the control (it is working correctly), and the physical controls supporting the control (power, physical security, etc.).

The results of testing and monitoring should be provided to management so that management will be aware of any problems with the control environment and take corrective action when required. This corrective action may include replacing a control, enhancing a control, or implementing additional layers of control.

Security Operations Review

The development of policies, standards, and processes is a daily occurrence for the security practitioner. Policies should be created with high-level organizational support and be written to last for years if possible. They should direct users to standards and procedures.

Standards and procedures should be written as specifically as possible and reference their parent policy when necessary. The individual tasked with keeping the standards and procedures updated must ensure the updates remain consistent with the policy and the technology environment of the organization.



Activity: Password Policies

Consider the following example:

Your organization has no consistent password methodology, approach, or standard configuration. As the security practitioner, you researched best practices and discovered that the best password strategy for the organization is a complex passphrase of 16 to 32 characters with at least two numbers, one special character, and one uppercase letter.

INSTRUCTIONS

Now, working with a partner, create the following policies to address the requirements outlined in the example:

- A policy explaining the organization's position on passwords.
- A standard explaining the minimum specifications for creating a password and password lifecycle considerations.
- A procedure explaining common password-related processes.

Summary

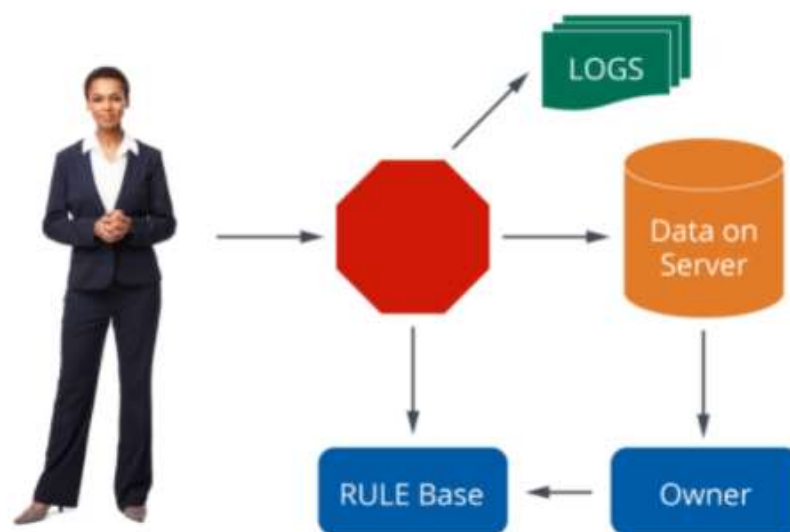
Setting the security policy is where we start to create the organizational culture of security. It's important that all parties know and understand what the organizations objectives are, what they (employees and customers) are allowed to do and required to do. This is where the policies come into play. Perhaps mandated by law or regulatory bodies, or just simply because it's what the business wants, the policy is to be followed, supported and enforced. Policy, risk assessment, and controls work together, as the risk assessment identifies the risk, the policies attempt to address the risk, the controls attempt to enforce the protection.

Module 2: Implement Access Controls (Access Control Models)

The Reference Monitor

Now we will look at the mechanism that enforces access controls between a subject and an object. This is known as the reference monitor. The reference monitor is a conceptual idea of how access controls operate. The reference monitor describes the process of access control by demonstrating the regulating of access granted to a subject through the mechanism of intercepting the access request and then granting or refusing access based on the rules mandated by the owners of the object (the asset).

In actual fact, the reference monitor does not in itself exist. It is the concept of access control that is enforced through a mechanism such as a security guard, a lock on a door; or, in a computer system, by the security kernel. In all of these cases we can see that the lock, the guard and the security kernel do not decide who should have access – instead they grant access to a person with the correct credentials, the correct key or the correct password. The security kernel enforces the decision of the data owner. The reference monitor should also have the ability to log all access requests – whether the access was granted or denied – so that the owner can review the logs later. This review serves as a part of monitoring to ensure that the access controls are set and operating correctly.



A subject wants to get access to data on a server.

The request is intercepted by the reference monitor that must determine if the access has been permitted by the owner of the asset – the data owner – it does this by checking the rules in the rule base set out by the owner

If access is permitted, then the subject gets access. The request (whether permitted or denied) is logged.

The Information Management Model (IMM)

Access to the assets of the organization – whether those assets are buildings, networks, applications, databases or personnel, should be carefully designed, implemented and maintained. The design of access controls can be facilitated through the use of an information management model (IMM). The IMM is simply a list of the three elements of access control: the subjects, the objects and the rules that govern the access a subject should have to an object.

The first step is to identify all the potential subjects that may require access. This may include employees, managers, guests, customers and auditors to name a few but it also will include processes and programs that could access the systems and other processes within the organization. Quite often the subjects will be grouped into roles of subjects that would require a similar level of access.

The next step is to identify all objects. That would include everything that could be accessed by a subject, including physical systems and technical systems. Once all objects have been identified, the third step can commence.

The third step is to determine the rules of access. That is, how will subjects be permitted to interface with objects. The rules of access are recorded and implemented onto the systems to restrict access according to the level of access required. This is often based on least privilege where an entity requesting access is only granted the minimum level of access required to do their job – and often only for the time that they require that access.

Mandatory Access Control (MAC)

An access control policy is uniformly enforced across all subjects and objects within the boundary of an information system. A subject that has been granted access to information is constrained from doing any of the following: (i) passing the information to unauthorized subjects or objects; (ii) granting its privileges to other subjects; (iii) changing one or more security attributes on subjects, objects, the information system, or system components; (iv) choosing the security attributes to be associated with newly created or modified objects; or (v) changing the rules governing access control. Organization-defined subjects may explicitly be granted organization-defined privileges (i.e., they are trusted subjects) such that they are not limited by some or all of the above constraints. [Source CNSSI 4009]

In a mandatory access control system, the user who has been granted access to a file cannot share that file with anyone else and they cannot change the security attributes of the file unless they have been specifically identified as a trusted user.

Usually, a labeling mechanism and a set of interfaces are used to determine access based on the MAC policy; for example, a user who is running a process at the Secret classification should not be allowed to read a file with a label of Top Secret. This is known as the “simple security rule,” or “no read up.” Conversely, a user who is running a process with a label of Secret should not be allowed to write to a file with a label of Confidential. This rule is called the “*-property” (pronounced “star property”) or “no write down.” The *-property is required to maintain system security in an automated environment.

A variation on this rule called the “strict *-property” requires that information can be written at, but not above, the subject’s clearance level. Multilevel security models such as the Bell-LaPadula Confidentiality and Biba Integrity models are used to formally specify this kind of MAC policy.

Non-Discretionary Access Control

According to the United States National Institute of Standards and Technology (NIST), in general, all access control policies other than DAC are grouped in the category of non-discretionary access control (NDAC). As the name implies, policies in this category have rules that are not established at the discretion of the user. Non-discretionary policies establish controls that cannot be changed by users but only through administrative action. CNSSI 4009 defines NDAC as another name for Mandatory Access Control.

Discretionary Access Control (DAC)

Discretionary Access Control (DAC) is a specific type of access control policy that is enforced over all subjects and objects in an information system. In DAC, the policy specifies that a subject that has been granted access to information can do one or more of the following:

1. pass the information to other subjects or objects;
2. grant its privileges to other subjects;
3. change security attributes on subjects, objects, information systems, or system components;
4. choose the security attributes to be associated with newly created or revised objects; and/or
5. change the rules governing access control. Mandatory access controls restrict this capability.

[Source: CNSSI 4009]

Most information systems in the world are DAC systems. In a DAC system, a user who has access to a file is usually able to share that file with, or pass that file to, someone else. This grants the user almost the same level of access as the original owner of the file. Rule-based access control systems are usually a form of DAC as per CNSSI 4009.

DAC Example

In Unix, a directory listing might yield "... rwxr-xr-x ... SSCP File 1.txt", meaning that the owner of SSCP File 1.txt may read, write, or execute it, and that other users may read or execute the file but not write it. The set of access rights in this example is {read, write, execute}, and the operating system mediates all requests to perform any of these actions. Users may change the permissions on files they own, making this a discretionary policy.

A mechanism implementing a DAC policy must be able to answer the question: "Does subject Steve have right Read for object SSCP File 1?" More practically, the same information could also be represented as an access control matrix. As shown in the table below, each row of the matrix corresponds to a subject and each column to an object. Each cell of the matrix contains a set of rights.

	SSCP FILE 1	SSCP FILE 2
Aidan	Read Write eXecute	Read eXecute
Steve	Read	Read Write

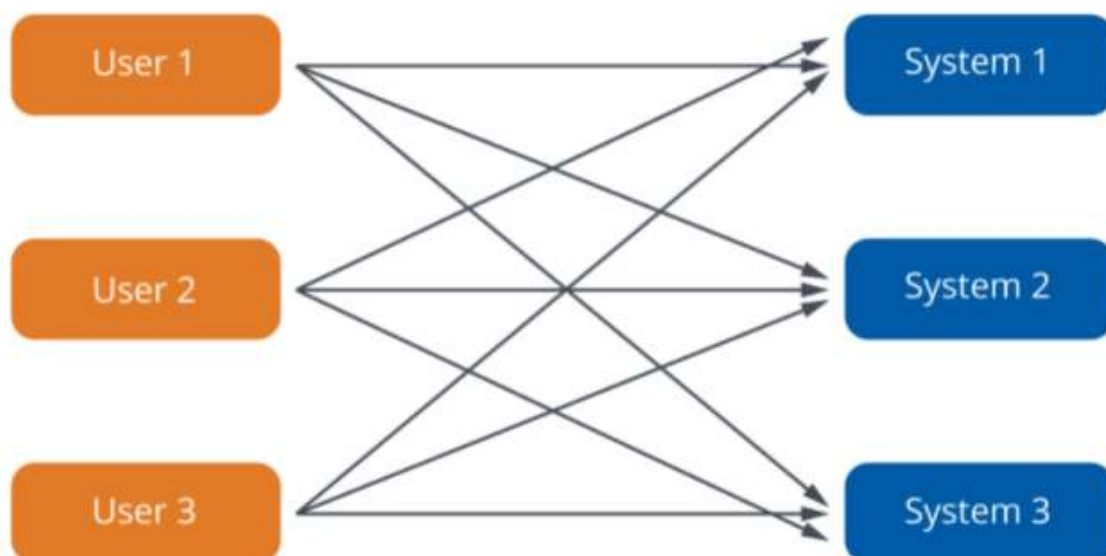
Systems typically store the information from this matrix either by columns or by rows. An implementation that stores by columns is known as an access control list (ACL). File systems in Windows and Unix typically use ACL: each file is accompanied by a list containing subjects and their rights to that file. In contrast, an implementation that stores by rows is commonly known as a capability list. It is easy in an ACL implementation to find the set of all subjects who may read a file, but it is difficult to find the set of all files that a subject may read.

The underlying philosophy in DAC is that subjects can determine who has access to their objects. In DAC, the owner of the access control object would determine the privileges (e.g. read, write, execute) of the access control subjects. The U.S. Department of Defense Standard Department of Defense Trusted Computer System Evaluation Criteria (5200.28-STD) defines Discretionary Access Control as "a means of restricting access to objects based on the identity of subjects and/or groups to which they belong. The controls are discretionary in the sense that a subject with certain access permission is capable of passing that permission (perhaps indirectly) on to any other subject (unless restrained by mandatory access control)."

This methodology relies on the discretion of the owner of the access control object to determine the access control subject's specific rights. Hence, security of the object is literally up to the discretion of the object owner. DACs are not very scalable; they rely on the decisions made by each individual access control object owner, and it can be difficult to find the source of access control issues when problems occur.

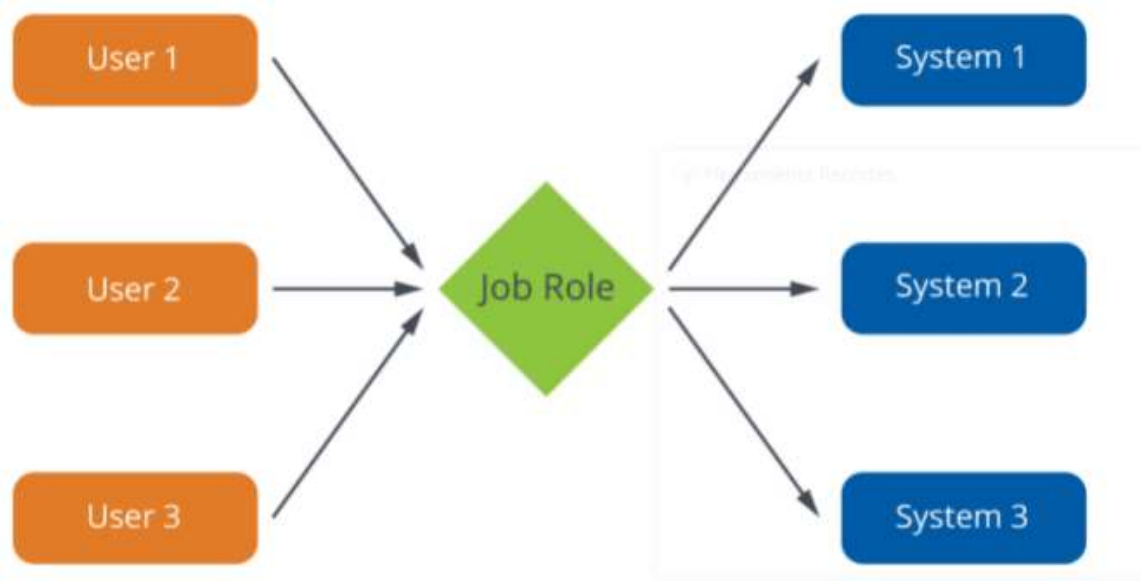
Rule-Based Access Control

Rule-based access control is based on defined rules for each subject that control what that subject can do. In a rule-based access control system each subject is granted explicit access to an object by a rule that specifies that access right. In a large organization with many users, and multiple changes in permissions, this can become an administrative nightmare as administrators need to copy or create rules for each user and maintain those rules whenever the roles and privileges of the users change. When the rules are not updated in a thorough and timely fashion, a large number of users may end up having access to systems they no longer require. In today's world of strict compliance, where access to sensitive data should only be granted on a need-to-know basis, rule-based access control can be a very difficult system to maintain.



Role-Based Access Control (RBAC)

Role-based access control (RBAC) – as the name suggests – sets up user permissions based on roles. Each role represents users with similar or identical permissions. A role is created that is assigned the access required for personnel working in that role. Then, when a user steps into that role, all the administrator has to do is enroll him or her as a member of that role. If a user leaves that role, the administrator only has to remove that one user and then all access for that user associated with that role is removed. RBAC works well in an environment with high staff turnover and multiple personnel with similar access requirements.



Role Hierarchies

Role hierarchies are a natural way of organizing roles to reflect authority, responsibility, and competency. The role in which the user is gaining membership is not mutually exclusive with another role for which the user already possesses membership. These operations and roles can be subject to organizational policies or constraints. When operations overlap, hierarchies of roles can be established. Instead of instituting costly auditing to monitor access, organizations can put constraints on access through RBAC.

RBAC works by assigning roles to access control subjects as well as labels to the access control objects that specify which roles are permitted access to the respective access control objects. Within an RBAC implementation, the ability to permit or deny the inheritance of roles within a given hierarchy is commonly available.

Constrained User Interface (CUI)

Constrained User Interface (CUI) is a methodology that restricts the user's actions to specific functions by not allowing the user to request functions that are outside of his/her respective level of privilege or role. One of the most common examples of a CUI can be found in online banking applications where the limited menus are readily apparent until after the user has properly authenticated. Once the user's identity has been established, then his/her respective role or privilege level is assigned.

Types of Restricted Interfaces

Interfaces can be restricted in a variety of ways.

- **Menu and Shells:** When menu and shell restrictions are used, the options users are given are the commands they can execute. For example, if an administrator wants users to be able to execute only one program, that program would be the only choice available on the menu. This limits the users' functionality. A shell is a type of virtual environment within a system. It is the user's interface to the operating system and works as a command interpreter. If restricted shells were used, the shell would contain only the commands the administrator wants the users to be able to execute.
- **Database views:** Database views are mechanisms used to restrict user access to data contained in databases.
- **Physically constraining a user interface:** A user interface can be physically constrained by providing only certain keys on a keypad or certain touch buttons on a screen. You see this when you get money from an ATM machine. The ATM device has an operating system (typically Windows) running underneath the ATM interface that can accept all kinds of commands and configuration changes, but it is physically constrained from being able to carry out any functions other than dispensing certain denominations of currency, such as \$10, \$20, and \$50 bills.

View-Based Access Control (VBAC)

Another type of CUI is view-based access control (VBAC); it is most commonly found in database applications to control access to specific parts of a database. The CUI in VBAC restricts or limits an access control subject's ability to view, or perhaps act on, "components" of an access control object based on the access control subject's assigned level of authority. The system dynamically creates views for each user-authorized access. Simply put, VBAC separates a given access control object into subcomponents and then permits or denies access for the access control subject to view or interact with specific subcomponents of the underlying access control object.

VBAC Examples

Here is how VBAC might work in a medical records database:

- A billing clerk (access control subject) would be able to view the procedures, supplies, and related costs in a database (access control object) to be billed to a patient, but would be restricted from seeing the result of any of the underlying tests and perhaps the doctor's notes contained within the same database (access control object).
- A nurse (access control subject) would be able to view the results of procedures and tests as well as the doctor's notes, but would be restricted from seeing the costs for the procedures and supplies.

As another example, VBAC might work in a firewall administrator's management console as follows:

- A firewall user administrator (access control subject) would be able to add new users and reset user passwords in the firewalls database (access control object), but would be restricted from seeing alerts or altering the firewall ACL rules within the same database.
- A firewall monitor (access control subject) would be able to see alerts in the firewall database (access control object), but would not be able to see or alter any information in the database relating to users or ACL rules.
- A firewall virtual private network (VPN) administrator (access control subject) would have the ability to enter VPN-related rules into the firewall database (access control object) to facilitate creating a point-to-point VPN tunnel or perhaps to permit a client-to-server VPN connection. However, the users would have to already exist in the firewall database (access control object), and the VPN administrator (access control subject) would be restricted from seeing alerts and access control rules that did not specifically relate to the VPN operations within the database.
- A firewall security officer (access control subject) would have full access to all information within the firewall database (access control object). While the view that is given to an access control subject may in fact only be a partial view of the information available from the access control object, it is important in the proper application of VBAC that the views presented to the access control subject appear normal, complete, and in context.

Content-Dependent Access Control (CDAC)

Content-dependent access control (CDAC) is used to protect databases containing sensitive information. CDAC works by permitting or denying subjects access to control objects based on the explicit content within the access control object.

For example, in a CDAC medical records database application, a healthcare worker may have been granted access to blood test records. If that record contains information about an HIV test, the healthcare worker may be denied access to the existence of the HIV test and its results. Only specific hospital staff would have the necessary CDAC access control rights to view blood test records that contain any information about HIV tests.

While high levels of privacy protection are attainable using CDAC, they come at the cost of a great deal of labor in defining the respective permissions. It should be further noted that CDAC entails high overhead in processing power as it must scan the complete record to determine whether access can be granted to a given access control subject. This scan is done by an arbiter program to determine if access will be allowed.

Temporal Access Control

Temporal, or time-based, access control is an important part of an access control implementation. Suppose Gerry is an employee of an organization and works from Monday through Friday from 8:00 AM to 5:00 PM. Gerry is given an access card that grants access to the building she works in, and an identification (ID) on the systems she logs into for work. Temporal access control would restrict Gerry's access so that her access cards and ID would not work outside of normal business hours. This means that even if an unauthorized person stole Gerry's ID or access card, that person would still be denied access outside of normal business hours. As such, temporal access control can prevent misuse of an employee's access by cleaning staff or other personnel working after hours.

Temporal role-based access control (TRBAC) effectively applies a time limitation to when a given role can be activated for a given access control subject.

- A high-level "top secret" role would be assigned to a given access control subject during the normal 8:00 a.m. to 5:00 p.m. working hours.
- A lower-level "confidential" role would be assigned to the same access control subject during nonworking hours – outside of the standard 5:00 p.m. to 8:00 a.m. time segment.

To decrease the effort associated with assigning TRBAC rules to many individual access control subjects, most implementations of TRBAC assign the time-based classification levels to the access control objects rather than to the access control subject. Hence, a given access control object would have a temporal classification level that is effective against all access control subjects.

Module Objectives

After completing this module, the participant will be able to:

1. Discuss identity management.
2. Compare identity management components.
3. Evaluate authentication methods.
4. Explain the authorization phase.
5. Discuss accounting.

Attribute-Based Access Control (ABAC)

Attribute-based access control (ABAC) goes beyond the limitations of the access control models described above. Those models used a fairly simple relationship of user to object, whereas ABAC adds attributes (descriptors) to the subjects and the objects that can enhance the granularity or precision of access controls.

For example, a user/subject may be a nurse working in a hospital cardiology department. There are many nurses in the hospital, but the access for each one is not just dependent on their job function as nurse, but also on their placement within the hospital. A nurse in one department should not be able to access medical records for patients in another department, so each nurse is assigned attributes that describe his/her role within the nursing function, and each patient record is assigned attributes according to which department they are in in the hospital. With ABAC, the attributes associated with the nurse will be compared with the attributes associated with the patient's medical record to ensure that access is only granted in accordance with laws and policy of the organization. This would ensure that only a nurse in cardiology could access the records of a patient in the cardiology department, and the nurse in cardiology would not be able to access the records of patients in other departments.

ABAC is further explained in the NIST SP800-162 at nvlpubs.nist.gov.

Key Terms

Following are some vocabulary terms that will help the security practitioner understand and apply the definitions:

- **Attributes** are characteristics of the subject, object, or environment conditions. Attributes contain information given by a name-value pair.
- A **subject** is a human user or non-person entity (NPE), such as a device, that issues access requests to perform operations on objects. Subjects are assigned one or more attributes. For the purpose of this document, assume that “subject” and “user” are synonymous.
- An **object** is a system resource for which access is managed by the ABAC system, such as devices, files, records, tables, processes, programs, networks, or domains containing or receiving information. It can be the resource or requested entity, as well as anything upon which an operation may be performed by a subject, including data, applications, services, devices, and networks.
- An **operation** is the execution of a function at the request of a subject upon an object. Operations include read, write, edit, delete, copy, execute, and modify and so forth.
- **Policy** is the representation of rules or relationships that makes it possible to determine whether a requested access should be allowed, given the values of the attributes of the subject, object, and possibly environment conditions.
- **Environment conditions** represent the operational or situational context in which access requests occur. Environment conditions are detectable environmental characteristics, which are independent of subject or object and may include the current time, day of the week, location of a user, or the current threat level.

Summary

Access controls are a critical part of the information security program. They need to be carefully designed, implemented and maintained to ensure continued protection of sensitive data and systems.

Module 3: Participate in the Identity Management Lifecycle

Module Objectives

After completing this module, the participant will be able to:

1. Discuss identity management.
2. Compare identity management components.
3. Evaluate authentication methods.
4. Explain the authorization phase.
5. Discuss accounting.

Provisioning

Provisioning is the process of creating or setting up all procedures and tools to manage the lifecycle of an identity. It includes:

- Creation of the identifier for the identity,
- Linkage to the authentication providers,
- Setting and changing attributes and privileges, and
- Decommissioning of the identity.

Proofing

Identity-proofing services, which verify people's identities before the enterprise issues them accounts and credentials, are based on "life history" or transaction information aggregated from public and proprietary data sources. These services are also used as an additional interactive user authentication method, especially for risky transactions, such as accessing sensitive confidential information or transferring funds to external accounts. Identity-proofing services are typically used when accounts are provisioned over the web or in a call center. However, they can also be used in face-to-face interactions.

Proofing includes identification and authentication.

Identification

Identification is the process of establishing a unique way to identify or distinguish one user or process from another.

FIPS 201-1 defines identification as “the process of discovering the true identity (i.e., origin, initial history) of a person or item from the entire collection of similar persons or items.”

The importance of identification is to establish accountability so that the actions of a person can be associated with the individual who committed those actions. This is important for reasons of non-repudiation and investigation.

Identification may be done in many ways, including UserIDs, Social Security numbers, account numbers, email addresses, biometrics and DNA. These are often good identifiers because they are more likely to be unique than a person's name.

A challenge faced by many organizations is to allow people to register their own accounts and set their own identities. This removes the overhead of administrators trying to manage identities on behalf of the users, but also presents the opportunity for misuse. As a result, utilities such as Completely Automated Public Turing test to tell Computers and Humans Apart (CAPTCHA) are increasingly used to try to ensure that identities are only granted to real people and not to some type of bot that is attempting to create multiple IDs on the system. The process of establishing identities on a system should be a secure process so that only legitimate users are able to obtain a UserID.

Another form of identification is using a location or device to establish an identity. This is often called node authentication. It uses a MAC (Media Access Control) address, IP (Internet Protocol) address, CPU serial number or other device authentication technique to identify the location an administrator or user is using to log in from. Many wireless devices use MAC filtering to restrict users to only being able to log in from registered wireless devices.

Authentication

Once users have stated their identity, we need to validate that they are the rightful owners of that identity. This process of verifying or proving the ID is known as authentication. There are three common methods of authentication:

- Knowledge
 - Password or paraphrases
- Ownership
 - Tokens, memory cards, smart cards
- Characteristic
 - Biometric, measurable characteristics

Single-Factor (Knowledge-Based) Authentication

Knowledge-based authentication has been in use for thousands of years. Ensuring that someone is authentic and asking them for a passphrase or secret code has been used to differentiate between authorized and unauthorized personnel. Today we use knowledge-based authentication through the use of a Personal Identification Number (PIN), password, passphrase or some other secret value that only authorized personnel should know. The problem with this type of authentication is that it is often vulnerable to shoulder-surfing or sniffing – discovery by an unauthorized person by looking over the shoulder of a user (perhaps using a camera at a bank ATM) or sniffing the communication during the login process. Since passwords and other knowledge-based systems often use the same password for a period of time (perhaps 30 days), the capture of the password would allow an attacker to log in repeatedly under the guise of the authorized user by performing a replay attack, where they replay the stolen login credentials.

Knowledge-based passwords are also subject to attacks such as brute force, dictionary and rainbow tables, which will be explained later in the course once we have examined hash values. A common problem with knowledge-based systems is a forgotten password. Within the organization a password may be reset by the helpdesk, but the challenge is always how to ensure that the passwords are only reset for the correct user and not someone else calling in pretending to be another user and having that person's password reset.

Multifactor Authentication

For many years, knowledge-based authentication in terms of passwords was the most common methodology in use in access control systems. Today, however, weaknesses in the implementation of encryption (hashing) for passwords have effectively rendered these knowledge-based methodologies obsolete.

In October 2005, the Federal Financial Institutions Examination Council provided a recommendation to U.S. banks that included, in part, a requirement to replace passwords and single-factor authentication with multifactor authentication. The recommendation clearly pointed out that passwords alone were simply no longer a secure method for authenticating users in the internet environment.

The best practice in access control is to implement at least two of the three common techniques for authentication in your access control system:

- Knowledge based
- Token based
- Characteristic based

Two-Factor vs. Three-Factor Authentication

In two-factor authentication, typically the mechanism used provides for something the user *has*, in the form of a physical token that generates a one-time password, and something the user *knows*, in the form of a PIN that is generated by the token and appended to the one-time password. This method is regarded as more secure than historical single-factor methods such as traditional passwords; however, it does little to definitively identify the user. This can be significantly improved upon by incorporating a third factor in the form of a biometric that in fact identifies the user.

An example of a three-factor authentication solution is the RSA AuthenTec Fingerprint device from Privaris. RSA AuthenTec incorporates a fingerprint reader to identify the user as well as being something the user has, and also incorporates the traditional one-time password and PIN combination found in common two-factor authentication tokens.

Dual Control

Dual control, also referred to as split knowledge, is built on the principle that no one person should have access to information that would allow the person to determine the encryption key used to encrypt protected information more quickly than a brute force attack of the entire key-space. Effectively, the determination of any part of the encryption key would require collusion between at least two different trusted individuals. Encryption – splitkeys – is just one example of dual control.

Periodic Authentication

The most common use of periodic authentication first provides for traditional challenge-response authentication requiring user interaction and then begins periodically to issue challenge-response authentication queries with the user's token to determine if the user has physically left the area where authentication had taken place.

In a simple example: CHAP (Challenge Handshake Authentication Protocol) the authentication server issues a challenge message to the peer. At random time periods the authenticator issues a new challenge and validates the response. This process provides protection against an attacker gaining control of a connected network session (a session hijack) or capturing credentials for later replay (a replay attack). Periodic authentication can also aid in reducing the risk that a user would leave a device or system unattended after gaining authenticated access and before properly logging out.

Continuous Authentication

While traditional one-time authentication, otherwise known as transactional authentication, takes place only once before granting access, continuous authentication takes place both before granting access and then continuously through the entire duration of the user's connection to maintain the granted access. This approach to authentication works on the principle that the longer a user remains connected to a system the weaker the security becomes. Using technology that examines the behavior of users, for example: how long their finger rest on keys (dwell time) or how quickly they move between keys (flight time) it becomes possible to predict whether the current user is the user who originally authenticated.

Time Outs

With time outs, if the user leaves the authenticated device unattended after a specific time period, the user is automatically logged off. The authentication process would start over, requiring user intervention to accomplish initial authentication before continuous authentication could again resume. Naturally, the shorter the timeout period, the higher the security that can be provided; however, as always, it comes at the cost of being a nuisance to the user.

Reverse Authentication

With the advent of phishing, it is no longer enough to simply authenticate the user in web-based transactions. Today, it is necessary to also authenticate the website/page to the user as part of the authentication process. Bank of America was a pioneer in reverse authentication with their roll-out of PassMark, a reverse authentication system that relies on a series of pictures that the user could identify and use to accomplish the authentication of the Bank of America website. Some had believed that the picture approach of PassMark was too simplistic and raised doubts about the technology. However, PassMark quickly grew in acceptance and was adopted by more than 50% of the online banking market.

Certificate-Based Authentication

Certificate-based authentication relies on the machine that the user authenticates from having a digital certificate installed that is used in part along with the encrypted user's password to authenticate both the user and the device he or she is using. Effectively, the use of a certificate in the authentication process provides an additional element in security by validating that the user is authorized to be authenticated from the device he or she is using because of the presence of the digital certification within the device. The certificate authority must take great care in the management of the digital certificates to ensure that the use of certificates is properly controlled and certificate renewal and revocations are accomplished in a timely and effective manner.

Authorization

The process of authorization refers to the rights, permissions and privileges granted to an authenticated user. Authorization is the last step in any identity management system: Having claimed and proved an identity access right (or permissions need to be assigned), for any given resource. Authorization can be managed through controls based on: user roles, user or resource attributes, policies etc. An Identity Access Management (IAM) policy store can be used to hold the authorization policies and comparing them to the entities access request.

Authorization is where the principles of least privilege and need-to-know apply. These principles both have a common theme, although they are slightly different. Least privilege only grants a person the minimum level of access required for them to perform their job function – perhaps read-only or guest-level access. Need-to-know is often based on classification of information that only grants access to information when required or according to the user's clearance. An example of this is to only display the last four digits of a credit card number to a person working for a merchant that accepts credit card payments. This prevents theft or misuse of the credit card by the employee.

A core element of authorization is the principle of separation of duties (also known as segregation of duties). Separation of duties is based on the security practice that no one person should control an entire high-risk transaction from start to finish. Separation of duties breaks the transaction in separate parts and requires a different person to execute each part of the transaction. For example, Bill may submit an invoice for payment, but it has to be approved by Sam prior to payment; or Bill may submit a proposal for a change to a system configuration but Sam will review and need to approve the change before it can be implemented. These steps can prevent fraud or detect an error in the process before implementation.

It could be that Sam will sometimes input an invoice for payment, but he would not be able to approve the invoices he inputs. This is mutual exclusivity: Sam can perform both operations (input and approval), but not on the same invoice.

However, if Sam and Bill work together to bypass the separation of duties they could jointly commit fraud. This is called collusion.

Another implementation of separation of duties is dual control. This would apply at a bank where there are two separate combination locks on the door of the vault. Some personnel know one of the combinations and some know the other, but no one knows both combinations. Two people have to work together to open the vault, thus the vault is under dual control.