Controlling Access to Assets

Controlling access to assets is one of the central themes of security, and you’ll find that many different security controls work together to provide access control. An asset includes information, systems, devices, facilities, and personnel.

**Information** An organization’s information includes all of its data. Data might be stored in simple fi les on servers, computers, and smaller devices. It can also be stored on huge databases within a server farm. Access controls attempt to prevent unauthorized access to the information.

**Systems** An organization’s systems include any information technology (IT) systems which provide one or more services. For example, a simple fi le server that stores user fi les is a system. Additionally, a web server working with a database server to provide an e-commerce service is a system.

**Devices** Devices include any computing system, including servers, desktop computers, portable laptop computers, tablets, smartphones, and external devices such as printers. More and more organizations have adopted bring your own device (BYOD) policies allowing employees to connect their personally owned device to an organization’s network. Although the devices are the property of their owners, organizational data stored on the devices is still an asset of the organization.

**Facilities** An organization’s facilities include any physical location that it owns or rents. This could be individual rooms, entire buildings, or entire complexes of several buildings. Physical security controls help protect facilities.

**Personnel** Personnel working for an organization are also a valuable asset to an organization. One of the primary ways to protect personnel is to ensure that adequate safety practices are in place to prevent injury or death.

**Subject** A subject is an active entity that accesses a passive object to receive information from, or data about, an object. Subjects can be users, programs, processes, computers, or anything else that can access a resource. When authorized, subjects can modify objects.

**Object** An object is a passive entity that provides information to active subjects. Some examples of objects include fi les, databases, computers, programs, processes, printers, and storage media.

**Access control includes the following overall steps:**

**1. Identify and authenticate users or other subjects attempting to access resources.**

**2. Determine whether the access is authorized.**

**Grant or restrict access based on the subject’s identity.**

**4. Monitor and record access attempts**

**The three primary control types are preventive, detective, and corrective**.

**There are also four other access control types, commonly known as deterrent, recovery, directive, and compensation access controls**.

**Recovery Access Control** A recovery control attempts l to repair or restore resources, functions, and capabilities after a security policy violation. Recovery controls are an extension of corrective controls but have more advanced or complex abilities. Examples of recovery access controls include backups and restores, fault-tolerant drive systems, system imaging, server clustering, antivirus software, and database or virtual machine shadowing.

**Directive Access Contro**l A directive control attempts to direct, confine, or control the actions of subjects to force or encourage compliance with security policies. Examples of directive access controls include security policy requirements or criteria, posted notifications, escape route exit signs, monitoring, supervision, and procedures.

**Compensation Access Control** A compensation control provides an alternative when it isn’t possible to use a primary control, or when necessary to increase the effectiveness of a primary control. As an example, a security policy might dictate the use of smartcards by all employees but it takes a long time for new employees to get a smartcard. The organization could issue hardware tokens to employees as a compensating control. These tokens provide stronger authentication than just a username and password.

Access controls are also categorized by how they are implemented. Controls can be implemented administratively, logically/technically, or physically.

**Administrative Access Controls** Administrative access controls are the policies and procedures defined by an organization’s security policy and other regulations or requirements. **They are sometimes referred to as management controls.** These controls focus on personnel and business practices. Examples of administrative access controls include policies, procedures, hiring practices, background checks, classifying and labeling data, security awareness and training efforts, reports and reviews, personnel controls, and testing.

**Logical/Technical Controls** Logical access controls (also known as technical access controls ) are the hardware or software mechanisms used to manage access and to provide protection for resources and systems. As the name implies, they use technology. Examples of logical or technical access controls include authentication methods (such as passwords, smartcards, and biometrics), encryption, constrained interfaces, access control lists, protocols, firewalls, routers, intrusion detection systems, and clipping levels.

**Physical Controls** Physical access controls are items you can physically touch. They include physical mechanisms deployed to prevent, monitor, or detect direct contact with systems or areas within a facility. Examples of physical access controls include guards, fences, motion detectors, locked doors, sealed windows, lights, cable protection, laptop locks, badges, swipe cards, guard dogs, video cameras, mantraps, and alarms.

**Authentication Factors**

The three basic methods of authentication are also known as types or factors. They are as follows:

**Type 1** A Type 1 authentication factor is something you know. Examples include a password, personal identification number (PIN), or passphrase.

**Type 2** A Type 2 authentication factor is something you have. Physical devices that a user possesses can help them provide authentication. Examples include a smartcard, hardware token, smartcard, memory card , or USB drive.

**Type 3** A Type 3 authentication factor is something you are or something you do. It is a physical characteristic of a person identified with different types of biometrics. Examples in the something-you-are category include fingerprints, voice prints, retina patterns, iris patterns, face shapes, palm topology, and hand geometry. Examples in the something-you-do category include signature and keystroke dynamics, also known as behavioral biometrics.

These types are progressively stronger when implemented correctly**, with Type 1 being the weakest and Type 3 being the strongest. In other words, passwords (Type 1) are the weakest, and a fingerprint (Type 3) is stronger than a password. However, attackers can still bypass some Type 3 authentication** factors. For example, an attacker may be able to create a duplicate fingerprint on a gummi bear candy and fool a fingerprint reader.

Passwords are rarely stored in plain text. Instead, a system will create a hash of a password using a hashing algorithm such as Password-Based Key Derivation Function 2 (PBKDF2). The hash is a number and the algorithm will always create the same number if the password is the same. When a user enters the password for authentication, the system hashes the password and compares it to the stored password’s hash. If they are the same, the system authenticates the user.

**Creating Strong Passwords**

**Maximum Age** This setting requires users to change their password periodically, such as **every 45 days.**

**Password Complexity** The complexity of a password refers to how many character types it includes. An eight-character password using uppercase characters, lowercase characters. symbols, and numbers is much stronger than an eight-character password using only numbers.

**Password Length** The length is the number of characters in the password. Shorter passwords are easier to crack. As an example, password crackers can discover a complex five-character password in less than a second but it takes thousands of years to crack a complex 12-character password. Many organizations require privileged account passwords to be at least 15 characters long. This specifically overcomes a weakness in how passwords are stored in some Windows systems

**Password History** Many users get into the habit of rotating between two passwords. A password history remembers a certain number of previous passwords and prevents users from reusing a password in the history. This is often combined with a minimum password age setting, preventing users from changing a password repeatedly until they can set the password back to the original one. Minimum password age is often set to one day.

It is difficult to crack a passphrase using a brute-force tool, and it encourages the use of a lengthy string with

numerous characters but it is still easy to remember.

**Cognitive Passwords**

Another password mechanism is the cognitive password . A cognitive password is series of questions about facts or predefined responses that only the subject should know. Authentication systems often collect the answers to these questions during the initial registration of the account, but they can be collected or modified later. As an example, the subject might be asked three to five questions such as these when creating an account:

■ What is your birth date?

■ What is your mother’s maiden name

**Smartcards and Tokens**

Smartcards and hardware tokens are both examples of a Type 2, or something you have, factor of authentication. They are rarely used by themselves but are commonly combined with another factor of authentication, providing multifactor authentication.

**Smartcards**

A smartcard is a credit card–sized ID or badge and has an integrated circuit chip embedded in it. Smartcards contain information about the authorized user that is used for identification and/or authentication purposes. Most current smartcards include a microprocessor and one or more certificates. The certificates are used for asymmetric cryptography such as encrypting data or digitally signing email. Smartcards are tamper

resistant and provide users with an easy way to carry and use complex encryption keys. Users insert the card into a smartcard reader when authenticating. It’s common to require users to also enter a PIN or password as a second factor of authentication with the smartcard.

**Note that smartcards can provide both identification and authentication. However, because users can share or swap smartcards, they aren’t effective identification methods by themselves. Most implementations require users to use another authentication factor such as a PIN, or with a username and password**

Personnel within the US government use either Common Access Cards (CACs) or Personal Identity Verification (PIV) cards. CACs and PIV cards are smartcards that include pictures and other identifying information about the owner. Users wear them as a badge while walking around and insert them into card readers at their computer when logging on.

**Tokens**

A token, or hardware *token* , is a password-generating device that users can carry with them. A common token used today includes a display that shows a six- to eight-digit number. An authentication server stores the details of the token, so at any moment, the server knows what number is displayed on the user’s token. Tokens are typically combined with another authentication mechanism. For example, users might enter a username and password (in the something-you-know factor of authentication) and then enter the number displayed in the token (in the something-you-have factor of authentication). This provides multifactor authentication.

Hardware tokens use dynamic one-time passwords, making them more secure than static passwords. The two types of tokens are *synchronous dynamic password tokens* and *asynchronous dynamic password tokens* .

**Synchronous Dynamic Password Tokens** Hardware tokens that create *synchronous dynamic passwords* are time-based and synchronized with an authentication server. They generate a new password periodically, such as every 60 seconds. This does require the token and the server to have accurate time. A common way this is used is by requiring the user to enter a username, static password, and the dynamic one-time password into a web page.

**Asynchronous Dynamic Password Tokens** An asynchronous dynamic password does not use a clock. Instead, the hardware token generates passwords based on an algorithm and an incrementing counter. When using an incrementing counter, it creates a dynamic one-time password that stays the same until used for authentication. Some tokens create a one-time password when the user enters a PIN provided by the authentication server into the token. For example, a user would first submit a username and password to a web page. After validating the user’s credentials, the authentication system uses the token’s identifier and

incrementing counter to create a challenge number and sends it back to the user. The challenge number changes each time a user authenticates, so it is often called a nonce (short for “number used once”). The challenge number will only produce the correct one-time password on the device belonging to that user. The user enters the challenge number into the token and the token creates a password. The user then enters the password into the website to complete the authentication process. Hardware tokens provide strong authentication, but they do have failings. If the battery dies or the device breaks, the user won’t be able to gain access.

One-time passwords are dynamic passwords that change every time they are used. They can be effective for security purposes, but most people find it difficult to remember passwords that change so frequently. One-time password generators are token devices that create passwords, making one-time passwords reasonable to deploy. With token-device based authentication systems, an environment can benefit from the strength of one-time passwords without relying on users to be able to memorize complex passwords.

**Biometrics**

Another common authentication and identification technique is the use of biometrics. Biometric factors fall into the Type 3, something-you-are, authentication category. Biometric characteristics are often defined as either physiological or behavioral. Physiological biometric methods include fingerprints, face scans, retina scans, iris scans, palm scans (also known as palm topography or palm geography), hand geometry, and voice patterns. Behavioral biometric methods include signature dynamics and keystroke patterns (keystroke dynamics). These are sometimes referred to as something-you-do authentication.

**Keystroke Patterns** Keystroke patterns (also known as keystroke dynamics) measure how a subject uses a keyboard by analyzing flight time and dwell time. Flight time is how long it takes between key presses, and dwell time is how long a key is pressed.

**Type 1 Error** A Type 1 error occurs when a valid subject is not authenticated. This is also known as a false negative authentication. For example, if Dawn uses her fingerprint to authenticate herself but the system incorrectly rejects her, it is a false negative. The ratio of Type 1 errors to valid authentications is known as the false rejection rate (FRR).

**Type 2** Error A Type 2 error occurs when an invalid subject is authenticated. This is also known as a false positive authentication. For example, if hacker Joe doesn’t have an account but he uses his fingerprint to authenticate and the system recognizes him, it is a false positive. The ratio of Type 2 errors to valid authentications is called the false acceptance rate (FAR).

**Most biometric devices have a sensitivity adjustment. When a biometric device is too sensitive, Type 1 errors (false negatives) are more common. When a biometric device is not sensitive enough, Type 2 errors (false positives) are more common.**

**You can compare the overall quality of biometric devices with the crossover error rate (CER), also known as the equal error rate (ERR). the FRR and FAR percentages when a device is set to different sensitivity levels. The point where the FRR and FAR percentages are equal is the CER, and the CER is used as a standard assessment value to compare the accuracy of different biometric devices. Devices with lower CERs are more accurate than devices with higher CERs.**

**For a biometric device to work as an identification or authentication mechanism, a process called enrollment (t or registration) must take place. During enrollment, a subject’s biometric factor is sampled and stored in the device’s database. This stored sample of a biometric factor is the reference profile (also known as a reference template**)

**Multifactor Authentication**

**Device Authentication**

Organizations typically use third party tools, such as the Secure Auth Identity Provider (IdP), for device authentication.

Implementing Identity Management

Identity management techniques generally fall into one of two categories: centralized and decentralized/distributed.

■ **Centralized access control** implies that all authorization verification is performed by a single entity within a system.

■ **Decentralized access control** (also known as distributed access control) implies that various entities located throughout a system perform authorization verification.

**Single Sign-On**

Single sign-on (SSO) is a centralized access control technique that allows a subject to be authenticated only once on a system and to access multiple resources without authenticating again. For example, users can authenticate once on a network and then access resources throughout the network without being prompted to authenticate again.

**LDAP and Centralized Access Control**

Within a single organization, a centralized access control system is often used. For example, a directory service is a centralized database that includes information about subjects and objects. Many directory services are based on the Lightweight Directory Access Protocol (LDAP). For example, the Microsoft Active Directory Domain Services is LDAP based.

**LDAP and PKIs**

A Public Key Infrastructure (PKI) uses LDAP when integrating digital certificates into transmissions.

PKI is a group of technologies used to manage digital certificates during the certificate life cycle. There are many times when clients need to query a certificate authority (CA) for information on a certificate and LDAP is one of the protocols used. LDAP and centralized access control systems can be used to support single sign-on capabilities.

A federation can be composed of multiple unrelated networks within a single university campus, multiple college and university campuses, multiple organizations sharing resources, or any other group that can agree on a common federated identity management system. Members of the federation match user identities within an organization to federated identities.

**Federated identity systems often use the Security Assertion Markup Language (SAML) and/or the Service Provisioning Markup Language (SPML) to meet this need. As background, here’s a short description of some markup languages.**

**Hypertext Markup Language (HTML) is commonly used to display static web pages. HTML was derived from the Standard Generalized Markup Language (SGML)**

**Extensible Markup Language Extensible Markup Language (XML) goes beyond describing how to display the data by actually describing the data. XML can include tags to describe data as anything desired**

**Databases from multiple vendors can import and export data to and from an XML format, making XML a common language used to exchange information**

**Security Assertion Markup Language** *Security Assertion Markup Language (SAML)* is an XML-based language that is **commonly used to exchange authentication and authorization (AA) information between federated organizations. It is often used to provide SSO capabilities for browser access.**

**Service Provisioning Markup Language Service Provisioning Markup Language (SPML) is a newer framework based on XML but specifically designed for exchanging user information for federated identity single sign-on purposes. It is based on the Directory Service Markup Language (DSML), which can display LDAP-based directory service information in an XML format.**

**Extensible Access Control Markup Language Extensible Access Control Markup Language (XACML) is used to define access control policies within an XML format, and it commonly implements role-based access controls.**

**SAML is a popular SSO language on the Internet. XACML has become popular with software defined networking applications.**

Two newer examples of SSO used on the Internet are OAuth (implying open authentication) and OpenID. OAuth is an open standard designed to work with HTTP and it allows users to log on with one account. For example, users can log onto their Google account and use the same account to access Facebook and Twitter pages.

**RADIUS**

*Remote Authentication Dial-in User Service* (RADIUS) centralizes authentication for remote connections. It is typically used when an organization has more than one network access server (or remote access server). A user can connect to any network access server, which then passes on the user’s credentials to the RADIUS server to verify authentication and authorization and to track accounting. In this context, the network access server is the RADIUS client and a RADIUS server acts as an authentication server. The RADIUS server also provides AAA services for multiple remote access servers. Many Internet service providers (ISPs) use RADIUS for authentication. Users can access the ISP from anywhere and the ISP server then forwards the user’s connection request to the RADIUS server. Organizations can also use RADIUS, and organizations can implement it with callback security for an extra layer of protection. **It can use either TCP or UDP**

**TACACS+**

Terminal Access Controller Access-Control System (TACACS) was introduced as an alternative to RADIUS. Cisco later introduced extended TACACS (XTACACS) as a proprietary protocol. However, TACACS and XTACACS are not commonly used today. TACACS Plus (TACACS+) was later created as an open publicly documented protocol, and it is the most commonly used of the three.

TACACS+ provides several improvements over the earlier versions and over RADIUS. It separates authentication, authorization, and accounting into separate processes, which can be hosted on three separate servers if desired. The other versions combine two or three of these processes. Additionally, TACACS+ encrypts all of the authentication information, not just the password as RADIUS does. **TACACS and XTACACS used UDP port 49, while TACACS+ uses Transmission Control Protocol (TCP) port 49, providing a higher level of reliability for the packet transmissions.**

**Diameter**

Building on the success of RADIUS and TACACS+, an enhanced version of RADIUS named Diameter was developed. It supports a wide range of protocols, including traditional IP, Mobile IP, and Voice over IP (VoIP). Because it supports extra commands, it is becoming popular in situations where roaming support is desirable, such as with wireless devices and smart phones. While Diameter is an upgrade to RADIUS, it is not backward compatible to RADIUS.

**Diameter uses TCP port 3868 or Stream Control Transmission Protocol (SCTP) port 3868, providing better reliability than UDP used by RADIUS. It also supports Internet Protocol Security (IPsec) and Transport Layer Security (TLS) for encryption**

**Kerbers uses UDP port 88.**