13.5.2 Authentication Facts

To access resources on a network, a user must prove who he is and that he has permissions to access the resources. This process consists of the following phases:

- *Identification* is the initial process of confirming the identity of a user requesting credentials. It occurs when a user types in a user ID to log on.
    - *Identity proofing* occurs during the identification phase as users prove their identity. If a user has previously been identified but cannot provide their assigned authentication credentials (such as a lost password), then identity proofing is called on again.
- *Authentication* is the verification of the issued identification credentials.
    - Usually the second step in the identification process, authentication establishes the user's identity.

Authentication Methods

The following table lists the ways a user can prove their identity to an authentication server.

Type	Description
Type 1: Something You Know	*Something you know* authentication requires users to provide a password or some other data that they know. This is the weakest type of authentication. The most common types of this authentication include the following: - Passwords, codes, or IDs - PINs - Passphrases (long sentence-length passwords) - *Cognitive* information, often in the form of security questions such as: - Your mother's maiden name - The model or color of your first car - The city where you were born - Composition passwords, which are created by the system and are usually two or more unrelated words divided by symbols on the keyboard Usernames are not a form of Type 1 authentication. Usernames are often easy to discover or guess. Only the passwords and other information associated with the username can be used to validate identity.
Type 2: Something You Have	*Something you have* (also called *token-based*) authentication is based on something users have in their possession. This type of authentication includes the following: - *Swipe cards* (similar to credit cards) with authentication information stored on a magnetic strip - *Photo IDs*, which are very useful when combined with other forms of authentication, but when used alone, can pose a security risk because they: - Are easily forged - Require personnel for verification - Cannot be verified against a system - *Smart cards* containing a memory chip with encrypted authentication information. Smart cards: - Can require contact (such as swiping) or can be contactless. - Contain microprocessor chips with the ability to add, delete, and manipulate their data. - Can store digital signatures, cryptography keys, and identification codes. - Use a private key for authentication to log a user into a network. The private key is also used to digitally sign messages. - Are sometimes based on challenge-response. A user is given a code (the challenge) that is entered into the smart card. The smart card then displays a new code (the response) that the user can present to log in. Types of token-based authentication include the following: - A *static* password that is saved on the token device. Swiping the token supplies the password for authentication. - A *synchronous dynamic* password that generates new passwords at specific intervals on the hardware token. Users must read the generated password and enter it along with a PIN to gain access. - An *asynchronous dynamic* password that generates new passwords based on an event, such as pressing a key. - A *challenge-response* password that generates a random challenge string. The challenge text is entered into the token along with a PIN. The token then uses both to generate a response used for authentication.
Type 3: Something You Are	*Something you are* authentication uses a *biometric system*. A biometric system attempts to identify a person based on *metrics*, or a mathematical representation of the subject's biological attributes. This is the most expensive and least accepted authentication method, but it is generally considered the most secure form of authentication. There are many attributes that can be used for biometric systems:

	▪ Fingerprints (end point and bifurcation pattern) ▪ Hand topology (side view) or geometry (top down view) ▪ Palm scans (pattern, including fingerprints) ▪ Retina scans (blood vein pattern) ▪ Iris scans (color) ▪ Facial scans (pattern) ▪ Heartbeat scans ▪ Voice recognition ▪ Handwriting dynamics ▪ Keyboard or keystroke dynamics (behavioral biometric systems) ▪ Dwell time (key press time) ▪ Flight time (how fingers move from key to key) Biometric systems include multiple scans of the biological attribute. Scans are then translated into a numeric constellation map of critical points. This mathematical representation is bound to a digital certificate that links to the subject's user account in the user database. Most biometric systems require you to implement a PKI system.
Type 4: Somewhere You Are	*Somewhere you are* takes into account where you are accessing the information from. Examples include: ▪ IP address ▪ Coordinates ▪ Address
Type 5: Something You Do	*Something you do* takes into account the unique way you do something, such as: ▪ Signing your name ▪ Writing a specific word or phrase ▪ Writing numbers

Authentication Terms

All authentication attempts should be logged with success or error messages. When you measure the effectiveness of authentication solutions, you need to be aware of the following key terms:

Measure	Description
False Negative	A *false negative* (or Type I error) occurs when a person who should be allowed access is denied access. The false rejection rate (FRR) is a measure of the probability that a false negative will occur.
False Positive	A *false positive* (or Type II error) occurs when a person who should be denied access is allowed access. The false acceptance rate (FAR) is a measure of the probability that a false positive will occur. False positives are more serious than false negatives and represent a security breach.
Crossover Error Rate	The *crossover error rate*, also called the *equal error rate*, is the point where the number of false positives matches the number of false negatives in a biometric system. It is best to select the system with the lowest crossover error rate within your budget.
Processing Rate	The *processing rate*, or system throughput, identifies the number of subjects or authentication attempts that can be validated. An acceptable rate is ten subjects per minute or above.

Authentication Method Combinations

To increase security, you can use a combination of authentication methods as described in the following table.

Authentication Method	Description	Example
One-Factor	Uses credentials of only one type, but may require multiple methods within the same type.	To log in, you provide a username and a password (the username is not used for authentication, so the only credential supplied for authentication is the password). To log in, you provide a username, PIN, and a passphrase (all credentials are of the same type).
Two-Factor Three-Factor Multi-Factor	Requires two or more different authentication types.	To enter a secured building, you must insert your key card (Type 2) and undergo a retina scan (Type 3).

Strong	Requires two or more methods, but they can be of the same type.	To log on to an online banking system, you enter your username and password, and then you must answer a personal question (such as your birthplace or mother's maiden name).
Mutual	Requires that both parties authenticate with each other before beginning communications.	To log in, your computer sends its digital certificate to prove its identity to a network server. The server then proves its identity to your computer. Only then will they exchange messages.

Single Sign-on

Enterprise environments frequently implement a type of single sign-on (SSO) authentication. SSO is a distributed access method that allows a subject to log in (sign on) once to a network and access all authorized resources on the network. The SSO system authenticates the subject against a master system and automatically logs the subject on to all of the servers the subject is authorized to access. Once authenticated, the subject can request access to additional resources without additional login credentials or passwords. SSO systems are commonly used in directory systems and some types of scripted access.

Using SSO offers the following advantages:

- It is a more efficient logon process because users only needs to type their user ID and password once.
- The user can create stronger passwords because there are fewer to remember.
- The need for multiple passwords and change synchronization is avoided.
- Users gain access to all authorized resources with a single instance of authentication through a single set of user credentials.
- Inactivity timeout and attempt thresholds are applied closer to the user point of entry.
- SSO has the ability to add and delete accounts across the entire network from a centralized database and one user interface, improving the process of disabling all network and computer accounts for terminated users.

However, SSO also has the following disadvantages:

- If a user's ID and password are compromised in the system, an intruder can access all of the resources authorized for the user.
- The system security policy must be followed to ensure that access is granted and/or limited to appropriate users.
- Implementation with microcomputer systems is difficult and can prevent full implementation.
- Ticket schemes do not scale very well.
- SSO presents a single point of failure.

Common Authentication Services

There are many authentication services, but three are the most common common:

Type	Description
Kerberos	*Kerberos* is a free protocol that provides strong authentication for client/server applications using a secret-key cryptography so the client can prove its identity even across an unsecure network connection. Kerberos is also available in many commercial products.
IEEE 802.1X	*IEEE 802.1X* is a port-based authentication service where: ▪ The client, called *supplicant*, initiates the authentication. ▪ A network device, called *authenticator*, negotiates the authentication. ▪ An authentication server, called *host*, is accessed after the supplicant is authenticated.
Captive Portal	A *captive portal* is a web page that pops up when you access a public Wi-Fi. This portal usually summarizes terms disclosing types of activities the Wi-Fi provider is not liable for during public access.