Understanding Authentication

Authentication proves that a user or system is actually who they say they are. This is one of the most critical parts of a security system. It's part of a process that is also referred to as *Identification and Authentication* (*I&A*). The identification process starts when a user ID or logon name is typed into a sign-on screen. Authentication is accomplished by challenging the claim about who is accessing the resource. Without authentication, anybody can claim to be anybody.

Authentication systems or methods are based on one or more of these three factors:

- Something you know, such as a password or PIN
- Something you have, such as a smart card or an identification device
- Something physically unique to you, such as your fingerprints or retinal pattern

Systems authenticate each other using similar methods. Frequently, systems pass private information between each other to establish identity. Once authentication has occurred, the two systems can communicate in the manner specified in the design.

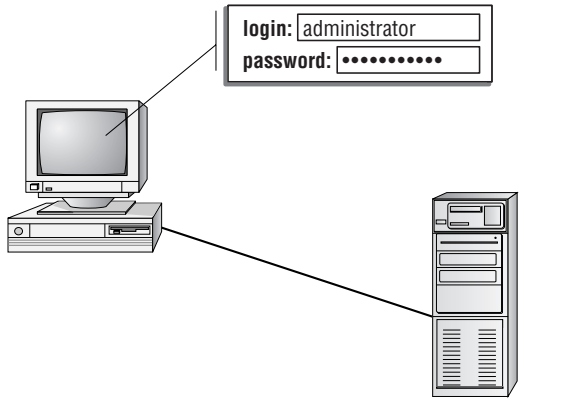
Several common methods are used for authentication. Each has advantages and disadvantages that must be considered when you're evaluating authentication schemes or methods.

Username/Password

A username and password are unique identifiers for a logon process. When users sit down in front of a computer system, the first thing a security system requires is that they establish who they are. Identification is typically confirmed through a logon process. Most operating systems use a user ID and password to accomplish this. These values can be sent across the connection as plain text or can be encrypted.

The logon process identifies to the operating system, and possibly the network, that you are who you say you are. Figure 1.3 illustrates this logon and password process. Notice that the operating system compares this information to the stored information from the security processor and either accepts or denies the logon attempt. The operating system may establish privileges or permissions based on stored data about that particular ID.

FIGURE 1.3 A logon process occurring on a workstation



Password Authentication Protocol (PAP)

Password Authentication Protocol (PAP) offers no true security, but it's one of the simplest forms of authentication. The username and password values are both sent to the server as clear text and checked for a match. If they match, the user is granted access; if they don't match, the user is denied access. In most modern implementations, PAP is shunned in favor of other, more secure, authentication methods.

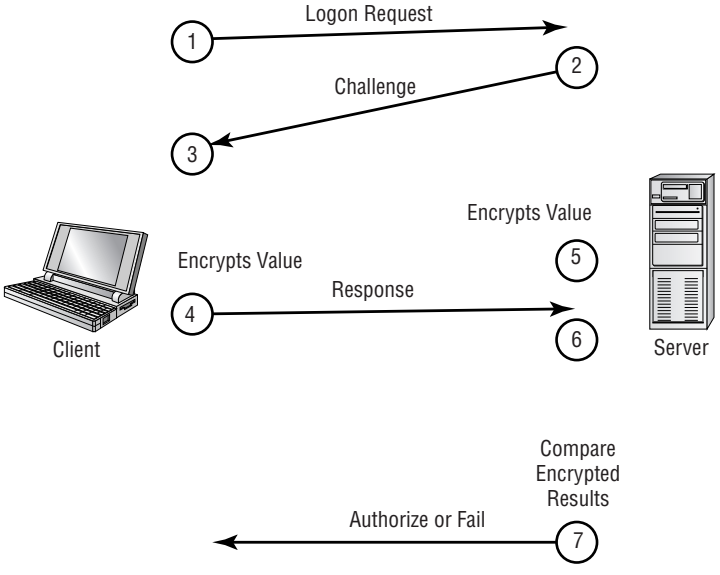
Challenge Handshake Authentication Protocol (CHAP)

Challenge Handshake Authentication Protocol (CHAP) challenges a system to verify identity. CHAP doesn't use a user ID/password mechanism. Instead, the initiator sends a logon request from the client to the server. The server sends a challenge back to the client. The challenge is encrypted and then sent back to the server. The server compares the value from the client and, if the information matches, grants authorization. If the response fails, the session fails, and the request phase starts over. Figure 1.4 illustrates the CHAP procedure. This handshake method involves a number of steps and is usually automatic between systems.

Certificates

Certificates are another common form of authentication. A server or *certificate authority (CA)* can issue a certificate that will be accepted by the challenging system. Certificates can be either physical access devices, such as smart cards, or electronic certificates that are used as part of the logon process. A *Certificate Practice Statement (CPS)* outlines the rules used for issuing and managing certificates. A *Certificate Revocation List (CRL)* lists the revocations that must be addressed (often due to expiration) in order to stay current.

FIGURE 1.4 CHAP authentication



This chapter provides only an overview of certificates. Certificates, along with Public-Key Infrastructure (PKI) and related topics, are discussed in detail in Chapters 7, "Cryptography Basics and Methods," and Chapter 8, "Cryptography Standards."

A simple way to think of certificates is like hall passes at school. Figure 1.5 illustrates a certificate being handed from the server to the client once authentication has been established. If you have a hall pass, you can wander the halls of your school. If your pass is invalid, the hallway monitor can send you to the principal's office. Similarly, if you have a certificate, then you can prove to the system that you are who you say you are and are authenticated to work with the resources.

Security Tokens

Security tokens are similar to certificates. They contain the rights and access privileges of the token bearer as part of the token. Think of a token as a small piece of data that holds a sliver of information about the user.

Many operating systems generate a token that is applied to every action taken on the computer system. If your token doesn't grant you access to certain information, then either that information won't be displayed or your access will be denied. The authentication system creates a token every time a user connects or a session begins. At the completion of a session, the token is destroyed. Figure 1.6 shows the security token process.

Kerberos

Kerberos is an authentication protocol named after the mythical three-headed dog that stood at the gates of Hades. Originally designed by MIT, Kerberos is becoming very popular as an authentication method. It allows for a single sign-on to a distributed network.

FIGURE 1.5 A certificate being issued once identification has been verified

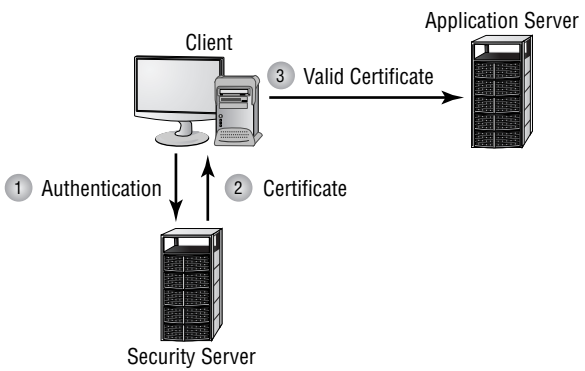
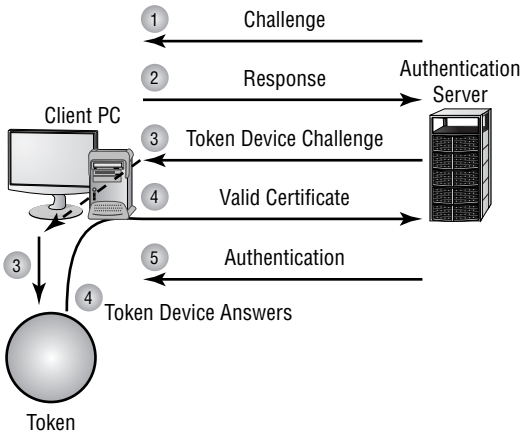


FIGURE 1.6 Security token authentication



Kerberos authentication uses a *Key Distribution Center* (*KDC*) to orchestrate the process. The KDC authenticates the *principle* (which can be a user, a program, or a system) and provides it with a ticket. Once this ticket is issued, it can be used to authenticate against other principles. This occurs automatically when a request or service is performed by another principle.

This chapter provides an overview. Key management is covered in more detail in Chapter 8.

Kerberos is quickly becoming a common standard in network environments. Its only significant weakness is that the KDC can be a single point of failure. If the KDC goes down, the authentication process will stop. Figure 1.7 shows the Kerberos authentication process and the ticket being presented to systems that are authorized by the KDC.

Multi-Factor Authentication

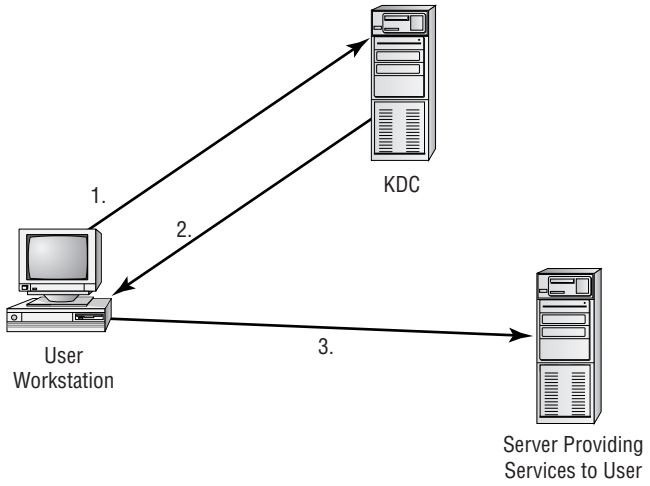
When two or more access methods are included as part of the authentication process, you're implementing a *multi-factor* system. A system that uses smart cards and passwords is referred to as a *two-factor authentication* system. Two-factor authentication is shown in Figure 1.8. This example requires both a smart card and a logon password process.

Smart Cards

A *smart card* is a type of badge or card that gives you access to resources including buildings, parking lots, and computers. It contains information about your identity and access privileges. Each area or computer has a card scanner or a reader in which you insert your card.

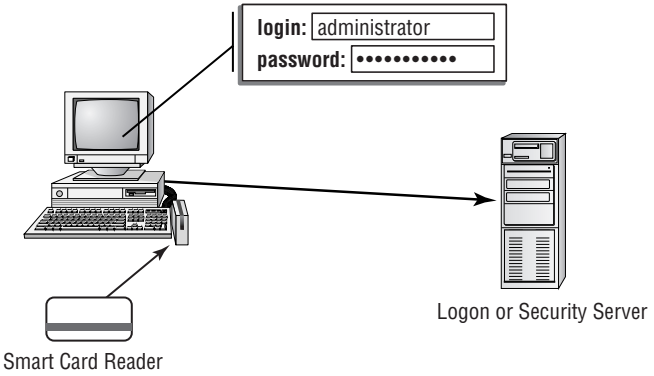
Figure 1.9 depicts a user inserting a smart card into a reader to verify identity. The reader is connected to the workstation and validates against the security system. This increases the security of the authentication process because you must be in physical possession of the smart card to use the resources. Of course, if the card is lost or stolen, the person who finds the card can access the resources allowed by the smart card.

FIGURE 1.7 Kerberos authentication process



1. User requests access to service running on a different server.
2. KDC authenticates user and sends a ticket to be used between the user and the service on the server.
3. User's workstation sends a ticket to the service.

FIGURE 1.8 Two-factor authentication



Both factors must be valid:
•User ID and Password
•Smart Card

Biometrics

Biometric devices use physical characteristics to identify the user. Such devices are becoming more common in the business environment. Biometric systems include hand scanners, retinal scanners, and soon, possibly, DNA scanners. In order to gain access to resources, you must pass a physical screening process. In the case of a hand scanner, this may include fingerprints, scars, and markings on your hand. Retinal scanners compare your eye's retinal pattern to a stored retinal pattern to verify your identity. DNA scanners will examine a unique portion of your DNA structure in order to verify that you are who you say you are.

Authentication Issues to Consider

You can set up many different parameters and standards to force the people in your organization to conform. In establishing these parameters, it's important that you consider the capabilities of the people who will be working with these policies. If you're working in an environment where people aren't computer savvy, you may spend a lot of time helping them remember and recover passwords. Many organizations have had to re-evaluate their security guidelines after they've already gone to great time and expense to implement high-security systems.

Setting authentication security, especially in supporting users, can become a high-maintenance activity for network administrators. On one hand, you want people to be able to authenticate themselves easily; on the other hand, you want to establish security that protects your company's resources.

Be wary of popular names or current trends that make certain passwords predictable. For example, during the first release of *Star Wars*, two of the most popular passwords used on college campuses were C3PO and R2D2. This created a security problem for campus computer centers.

FIGURE 1.9 The smart card authentication process