Understanding and selecting authentication methods

www.techrepublic.com/article/understanding-and-selecting-authentication-methods/

Computer/network security hinges on two very simple goals:

1. Keeping unauthorized persons from gaining access to resources
2. Ensuring that authorized persons *can* access the resources they need

There are a number of components involved in accomplishing these objectives. One way is to assign access permissions to resources that specify which users can or cannot access those resources and under what circumstances. (For example, you may want a specific user or group of users to have access when logged on from a computer that is physically on-site but not from a remote dial-up connection.)

Access permissions, however, work only if you are able to verify the identity of the user who is attempting to access the resources. That's where authentication comes in. In this Daily Drill Down, we will look at the role played by authentication in a network security plan, popular types of authentication, how authentication works, and the most commonly used authentication methods and protocols.

Authentication and security
Authentication is an absolutely essential element of a typical security model. It is the process of confirming the identification of a user (or in some cases, a machine) that is trying to log on or access resources. There are a number of different authentication mechanisms, but all serve this same purpose.

Authentication vs. authorization
It is easy to confuse authentication with another element of the security plan: authorization. While authentication verifies the user's identity, authorization verifies that the user in question has the correct permissions and rights to access the requested resource. As you can see, the two work together. Authentication occurs first, then authorization.

For example, when a user who belongs to a Windows domain logs onto the network, his or her identity is verified via one of several authentication types. Then the user is issued an access token, which contains information about the security groups to which the user belongs. When the user tries to access a network resource (open a file, print to a printer, etc.), the access control list (ACL) associated with that resource is checked against the access token. If the ACL shows that members of the Managers group have permission to access the resource, and the user's access token shows that he or she is a member of the Managers group, that user will be granted access (unless the user's account, or a group to which the user belongs, has been explicitly *denied* access to the resource).

Another example of authorization is the Dialed Number Identification Service (DNIS), which authorizes a dial-in connection based on the number called.

Logon authentication
Most network operating systems require that a user be authenticated in order to log onto the network. This can be done by entering a password, inserting a smart card and entering the associated PIN, providing a fingerprint, voice pattern sample, or retinal scan, or using some other means to prove to the system that you are who you claim to be.

Network access authentication
Network access authentication verifies the user's identity to each network service that the user attempts to access. It differs in that this authentication process is, in most cases, transparent to the user once he or she has logged on.

Otherwise, the user would have to reenter the password or provide other credentials every time he or she wanted to access another network service or resource.

IPSec authentication
IP Security (IPSec) provides a means for users to encrypt and/or sign messages that are sent across the network to guarantee confidentiality, integrity, and authenticity. IPSec transmissions can use a variety of authentication methods, including the Kerberos protocol, public key certificates issued by a trusted certificate authority (CA), or a simple pre-shared secret key (a string of characters known to both the sender and the recipient).

An important consideration is that both the sending and receiving computers must be configured to use a common authentication method or they will not be able to engage in secured communications.

IPSec configuration
If IPSec policies have been configured to require that communications be secured, the sending and receiving computers will not be able to communicate at all if they do not support a common authentication method.

Remote authentication
There are a number of authentication methods that can be used to confirm the identity of users who connect to the network via a remote connection such as dial-up or VPN. These include:

- The Password Authentication Protocol (PAP)
- The Shiva PAP (SPAP)
- Challenge Handshake Authentication Protocol (CHAP)
- Microsoft CHAP (MS-CHAP)
- The Extensible Authentication Protocol (EAP)

Remote users can be authenticated via a Remote Authentication Dial-In User Service (RADIUS) or the Internet Authentication Service (IAS). Each of these will be discussed in more detail in the section titled Authentication Methods and Protocols.

It is especially important that remote users be properly authenticated, as they generally pose a greater security risk than on-site users.

Single Sign-On (SSO)
Single Sign-On (SSO) is a feature that allows a user to use one password (or smart card) to authenticate to multiple servers on a network without reentering credentials. This is an obvious convenience for users, who don't have to remember multiple passwords or keep going through the authentication process over and over to access different resources.

There are a number of SSO products on the market that allow for single sign-on in a mixed (hybrid) environment that incorporates, for example, Microsoft Windows servers, Novell NetWare, and UNIX.

Details on SSO
For a more detailed discussion of SSO, see *Single Sign-On Solutions in a Mixed Computing Environment* .

Authentication types
There are several physical means by which you can provide your authentication credentials to the system. The most common—but not the most secure—is password authentication. Today's competitive business environment

demands options that offer more protection when network resources include highly sensitive data. Smart cards and biometric authentication types provide this extra protection.

Password authentication
Most of us are familiar with password authentication. To log onto a computer or network, you enter a user account name and the password assigned to that account. This password is checked against a database that contains all authorized users and their passwords. In a Windows 2000 network, for example, this information is contained in Active Directory.

To preserve the security of the network, passwords must be “strong,” that is, they should contain a combination of alpha and numeric characters and symbols, they should not be words that are found in a dictionary, and they should be relatively long (eight characters or more). In short, they should not be easily guessed.

Password authentication is vulnerable to a password “cracker” who uses a brute force attack (trying every possible combination until hitting upon the right one) or who uses a protocol “sniffer” to capture packets if passwords are not encrypted when they are sent over the network.

Smart card authentication
Smart cards are credit card-sized devices that hold a small computer chip, which is used to store public and private keys and other personal information used to identify a person and authenticate him or her to the system. Logging onto the network with a smart card requires that you physically insert the card into (or slide it through) a reader and then enter a Personal Identification Number (PIN) in much the same way that you use an ATM card to access an automatic teller machine.

Smart cards use cryptography-based authentication and provide stronger security than a password because in order to gain access, the user must be in physical possession of the card *and* must know the PIN.

For more detailed information about how smart cards work, see my TechProGuild Daily Drill Down “Enhancing security with the use of smart cards.”

Biometric authentication
An even more secure type of authentication than smart cards, biometric authentication involves the use of biological statistics that show that the probability of two people having identical biological characteristics such as fingerprints is infinitesimally small; thus, these biological traits can be used to positively identify a person.

In addition to fingerprints, voice, retinal, and iris patterns are virtually unique to each individual and can be used for authentication purposes. This method of proving one’s identity is very difficult to falsify, although it requires expensive equipment to input the fingerprint, voice sample, or eye scan. Another advantage over smart cards is that the user does not have to remember to carry a device; his or her biological credentials are never left at home.

Biometrics
For more information about biometrics, see this article at Network Computing.

How does authentication work?
In theory, authentication is relatively simple: A user provides some sort of credentials—a password, smart card, fingerprint, digital certificate—which identifies that user as the person who is authorized to access the system. There are, however, a multiplicity of methods and protocols that can be used to accomplish this. Regardless of the method, the basic authentication process remains the same.

The authentication process
In most instances, a user must have a valid user account configured by the network administrator that specifies the

user’s permissions and rights. User credentials must be associated with this account—a password is assigned, a smart card certificate is issued, or a biometric scan is entered into the database against which future readings will be compared.

When the user wants to log on, he or she provides the credentials and the system checks the database for the original entry and makes the comparison. If the credentials provided by the user match those in the database, access is granted.

Advantages of multilayered authentication
In a high-security environment, multilayered authentication adds extra protection. In other words, you can require that the user provide more than one type of credential, such as both a fingerprint and a logon password. This further decreases the chances of an unauthorized person circumventing the security system.

Authentication methods and protocols
There are a large number of authentication methods and protocols that can be used, depending on the application and security requirements. In the following sections, we will discuss:

- Kerberos
- SSL
- Microsoft NTLM
- PAP and SPAP
- CHAP and MS-CHAP
- EAP
- RADIUS
- Certificate services

These are by no means the only authentication methods in existence, but they are some of the most common.

Kerberos
Kerberos was developed at MIT to provide secure authentication for UNIX networks. It has become an Internet standard and is supported by Microsoft’s latest network operating system, Windows 2000. Kerberos uses temporary certificates called tickets, which contain the credentials that identify the user to the servers on the network. In the current version of Kerberos, v5, the data contained in the tickets is encrypted, including the user’s password.

A Key Distribution Center (KDC) is a service that runs on a network server, which issues a ticket called a Ticket Granting Ticket (TGT) to the clients that authenticates to the Ticket Granting Service (TGS). The client uses this TGT to access the TGS (which can run on the same computer as the KDC). The TGS issues a service or session ticket, which is used to access a network service or resource.

The name
Kerberos derives its name from the three-headed dog of Greek mythology (spelled *Cerberus* in Latin) that guarded the gates to Hades. Kerberos likewise stands guard over the network to ensure that only those who are authorized can enter.

Secure Sockets Layer (SSL)
The SSL protocol is another Internet standard, often used to provide secure access to Web sites, using a combination of public key technology and secret key technology. Secret key encryption (also called symmetric

encryption) is faster, but asymmetric public key encryption provides for better authentication, so SSL is designed to benefit from the advantages of both. It is supported by Microsoft, Netscape, and other major browsers, and by most Web server software, such as IIS and Apache.

SSL operates at the application layer of the DoD networking model. This means applications must be written to use it, unlike other security protocols (such as IPSec) that operate at lower layers. The Transport Layer Security (TLS) Internet standard is based on SSL.

SSL authentication is based on digital certificates that allow Web servers and clients to verify each other's identities before they establish a connection. (This is called mutual authentication.) Thus, two types of certificates are used: client certificates and server certificates.

SSL overview
An excellent overview of how SSL works, *Introduction to SSL,* can be found at Netscape.

Microsoft NTLM (NT LAN Manager)
NTLM authentication is used by Windows NT servers to authenticate clients to an NT domain. Windows 2000 uses Kerberos authentication by default but retains support for NTLM for authentication of pre-Windows 2000 Microsoft servers and clients on the network. UNIX machines connecting to Microsoft networks via an SMB client also use NTLM to authenticate.

Native mode
If you convert your Windows 2000 domain's status to native mode, NTLM support will be disabled.

NTLM uses a method called challenge/response, using the credentials that were provided when the user logged on each time that user tries to access a resource. This means the user's credentials do not get transferred across the network when resources are accessed, which increases security. The client and server must reside in the same domain or there must be a trust relationship established between their domains in order for authentication to succeed.

PAP
PAP is used for authenticating a user over a remote access control. An important characteristic of PAP is that it sends user passwords across the network to the authenticating server in plain text. This poses a significant security risk, as an unauthorized user could capture the data packets using a protocol analyzer (sniffer) and obtain the password.

The advantage of PAP is that it is compatible with many server types running different operating systems. PAP should be used only when necessary for compatibility purposes.

SPAP
SPAP is an improvement over PAP in terms of the security level, as it uses an encryption method (used by Shiva remote access servers, thus the name).

The client sends the user name along with the encrypted password, and the remote server decrypts the password. If the username and password match the information in the server's database, the remote server sends an Acknowledgment (ACK) message and allows the connection. If not, a Negative Acknowledgment (NAK) is sent, and the connection is refused.

CHAP and MS-CHAP
CHAP is another authentication protocol used for remote access security. It is an Internet standard that uses MD5, a

one-way encryption method, which performs a hash operation on the password and transmits the hash result—instead of the password itself—over the network.

This has obvious security advantages over PAP/SPAP, as the password does not go across the network and cannot be captured.

CHAP specs
The specifications for CHAP are discussed in RFC 1994.

The hash algorithm ensures that the operation cannot be reverse engineered to obtain the original password from the hash results. CHAP is, however, vulnerable to remote server impersonation.

MS-CHAP is Microsoft's version of CHAP. MS-CHAPv2 uses two-way authentication so that the identity of the server, as well as the client, is verified. This protects against server impersonation. MS-CHAP also increases security by using separate cryptographic keys for transmitted and received data.

EAP
EAP is a means of authenticating a Point-to-Point Protocol (PPP) connection that allows the communicating computers to negotiate a specific authentication scheme (called an EAP type).

A key characteristic of EAP is its extensibility, indicated by its name. Plug-in modules can be added at both client and server sides to support new EAP types.

EAP can be used with TLS (called EAP-TLS) to provide mutual authentication via the exchange of user and machine certificates.

RFC
EAP-TLS is defined in RFC 2716.

EAP can also be used with RADIUS (see below).

RADIUS
RADIUS is often used by Internet service providers (ISPs) to authenticate and authorize dial-up or VPN users. The standards for RADIUS are defined in RFCs 2138 and 2139. A RADIUS server receives user credentials and connection information from dial-up clients and authenticates them to the network.

RADIUS can also perform accounting services, and EAP messages can be passed to a RADIUS server for authentication. EAP only needs to be installed on the RADIUS server; it's not required on the client machine.

Windows 2000 Server includes a RADIUS server service called Internet Authentication Services (IAS), which implements the RADIUS standards and allows the use of PAP, CHAP, or MS-CHAP, as well as EAP.

Certificate services
Digital certificates consist of data that is used for authentication and securing of communications, especially on unsecured networks (for example, the Internet). Certificates associate a public key to a user or other entity (a computer or service) that has the corresponding private key.

Certificates are issued by certification authorities (CAs), which are trusted entities that "vouch for" the identity of the user or computer. The CA digitally signs the certificates it issues, using its private key. The certificates are only valid for a specified time period; when a certificate expires, a new one must be issued. The issuing authority can also revoke certificates.

Certificate services are part of a network's Public Key Infrastructure (PKI). Standards for the most commonly used certificates are based on the X.509 specifications.

Information on certificate services
Windows 2000 includes support for certificate services. For more information, see this page on Microsoft's support site.

Conclusion
Authentication is a vital part of a network's security scheme, as it is the mechanism for ensuring that the identity of a user, computer, or service is valid. There are a number of ways that authentication can be accomplished, depending on network operating system and connection type. In this Daily Drill Down, I have provided an overview of some of the most common authentication methods, under what circumstances each is used, and how they work.

Full Bio

Debra Littlejohn Shinder, MCSE, MVP is a technology consultant, trainer, and writer who has authored a number of books on computer operating systems, networking, and security. Deb is a tech editor, developmental editor, and contributor to over 20 additional books on subjects such as the Windows 2000 and Windows 2003 MCSE exams, CompTIA Security+ exam, and TruSecure's ICSA certification.