Global Information Assurance Certification Paper

Access Management and Authentication
The need to know

Vilma Palmer
August 27, 2002
Version 1.4

INTRODUCTION

The need to share information resources in the Network environment has created a major need for authentication, and access management. It has also become a major concern with e-commerce and the Internet. Protecting the security of any computer and network requires different measures, including controlling access, managing user accounts, virus protection, firewalls and encryption. All of these processes are used to protect the integrity, confidentiality and availability of network systems and it's data. The first steps in this process would be Access Management and Authentication. This paper is to explain access management and authentication; it will prove that together they are essential in protecting a network. Access management allows a system administrator to manage user access to certain systems and it also helps to ensure security. There are several ways to control access. This paper will focus on access control list (ACL), firewalls technologies and IP addressing. Implementation of these technologies will help to control system access. Authentication is define as the process of proving someone is who he/she claims to be. Authentication can be accomplished through many different methods. This paper focuses on the three most commonly used methods:
Password - "something you know,"
Token/smart cards - "something you have,"
Biometrics - "something you are"
It will give an overview of Kerberos Network Protocol and how it works; and it also explains how it is implemented in Windows 2000. Finally, this paper will show that there is no one solution for network security rather a combination of two or more techniques are needed. It will also make its readers aware of some of the things to consider when choosing or deciding on the right authentication methods.

AUTHORIZATION/ACCESS MANAGEMENT

Authorization is the process of determining whether an identity is permitted to perform certain action, such as accessing a resource. Access management and authentication are so closely related; it is difficult to discuss one and not the other. Authentication determines "who" the valid user is while authorization or access control determines "what" resources can be access and how it is accessed. Access management protects against unauthorized access to system resources, including computer applications, networks and data files.

Access Control
Access control list (ACL)

Access control list is one of the most common implementation of access management. The user is checked against a list of users and /or groups, then service is granted or denied based on whether or not there is a match. ACL is a table that tells a computer operating system what access rights each user has to a particular system object, such as a file directory or individual file. In Windows 2000, the access control list is a list of entries that grant or deny specific access rights to individuals or groups. Windows 2000 allows system administrators to grant access rights to a user or group, rights that govern who can access a specific object, a group of properties or an individual property of an object. When a process tries to access a secure object, the system checks the access control entries in the object's access control list to determine whether to grant access. If the object does not have an access control list, the system grants full access to everyone. If the objects access control list has no entries; the system denies all attempts to access the object. The system examines each access control entry item in sequence until it finds one or more that allows all the requested access rights, or until any of the requested access rights are denied. To read more on Access Control List see the following URL:
http://msdn.microsoft.com/library/default.asp?url=/library/en-us/cpref/html/frlrfSystemMessagingAccessControlListClassTopic.asp

The ACL infrastructure of Microsoft Windows functions to balance the resource access and system security needs of an organization. Access control lists are very important to system administrators who need to secure a network resource, however, this could become a problem for large organizations. Let us consider an organization's whole security infrastructure, its application, its hardware and its physical security mechanisms; they generally rely on different access control mechanism. As the organization grows, the type and number of network connections will also increase. The organizations will then need to address the issue of integrating multiple access control mechanism.

Firewalls

Firewalls protect organizations on the Internet by providing secure access. Firewalls help to ensure that valid users can access the network resources they need. The three main firewall technologies are:

- Packet Filter

  Packet filtering systems selectively route packets between trusted and untrusted networks. They allow or deny packets depending on a site's security policy. They are application independent and examine each packet at the network layer, allowing them to deliver high performance and scalability as long as the Access Control List (ACL) remains small.

As ACL grows in complexity and length, packet filter functionality degrades. Packet filters are the least secure types of firewall.

- Proxy

  Proxy firewall functions at the application layer. They take request for Internet service and forward them to the actual services. A proxy provides replacement connection and acts as a gateway, they are sometimes known as application level gateways. Instead of talking to each other directly, each system talks to a proxy. Proxies handle all the communication between users and Internet services behind the scenes. Your internal network never directly connects to the Internet. The proxy is then acting as the central control point for the organization's access management [2].

- Stateful Inspection

  With stateful inspection, the firewall maintains a table of active Transmission Control Protocol (TCP) sessions and User Datagram Protocol (UDP) pseudo-sessions. Stateful inspection firewalls determine whether a packet can get through the firewall based on the source and destination IP address, port number and current TCP sequence number. Only those that satisfy a define security policy are allowed entry. Sessions that do not match any policy are denied access. With stateful inspection, the packet is intercepted at the network layer [10].

IP Addressing

Each Transmission Control Protocol/Internet Protocol (TCP/IP) host is identified by a logical IP address. This address is unique for each host that communicates by using TCP/IP. Each 32-bit address identifies a location of a host system on the network in the same way that a street address identifies a house on a city street. The host ID, also known as the host address, identifies a TCP/IP node (a workstation, server, router, or other TCP/IP device) within each network. IP addresses must be assigned to each device on the network. If a computer has multiple network adapters installed, each adapter needs its own IP address. IP addresses are defined into five different classes Class A, B, C, D and E. Class A, B, and C addresses are used for assignment to TCP/IP nodes. It's the value of the first number of the IP address that determines the class to which a given IP address belongs. Class D address is used for multi-cast application and Class E is designed for future use. IP addresses are used to deliver packets of data across a network and have what is termed end-to-end significance. This means that the source and destination IP address remains constant as the packet travels a network. Each time a packet travels through a router, the router checks its routing table to see if it has a match for the network number of the destination IP address. If it does, the packet is forwarded to the next hop router for the

destination network in question. If a match is not found then the packet is either forwarded to the router defined as the default gateway or the packet may be dropped [3]. IP addressing based access management tracks the activities of machine rather than people.

Any type of access control mechanism that is implemented on a network will only be as effective as its implementation and maintenance. The challenge here will not be to set up barriers to access; it is to facilitate access in a responsible manner, and recognizing the needs of all parties involved in the access arrangement.

AUTHENTICATION

The first step in providing security is determining who is trying to access the system. Authentication is the process of proving someone is who he/she claims to be and it is one of the most important components of a security infrastructure. Identification, authentication and authorization are collectively referred to as access control. They answer four very important questions:

1. Who are you?
2. Do you belong here?
3. What rights do you have?
4. How do I know you are who you say you are?

Authentication can function at all levels of a security infrastructure but most people are familiar with authentication to a Network Operating System (NOS), such as a Windows NT domain. Users are required to authenticate to almost everything, including a firewall, to gain access to the internet, mail server to check e-mail, intranet web server to gain access to corporate information, the database to access customer data, and many other applications that enabled day-to-day activities. A user name does not need to correspond to the usual name of individuals in the physical world and a user may have rights to use more than one name. This can be viewed as an assumption in the cross-organizational environment. An organization will need to consider the cost associated with unauthorized access and also corporate liability when deciding on what method of authentication to use. They will need to keep in mind that if a computer is connected to the Internet an attacker can use it as a jumping-off point for an attack, an organization could be judged guilty of not controlling its systems. Passwords are the traditional and still the most commonly used method of authentication [2]. However, there are several types of authentication methods in use, such as token or smart card and biometrics. Access management is not independent of the authentication process; they both work together in proving a secure network.

Authentication Methods
Password (something you know)

User ID's and passwords are the primary means for accessing systems. One of the biggest problems, we all may agree, is that there are too many; however, they serve an important purpose. User ID's tell the system "who we are," known as identification. Passwords are used by systems to make us "prove it," known as authentication. The Federal Information Processing Standards Publications (FIPS PUBS 112) explain a password as a sequence of characters that can be used for several authentication purposes. It can be used to authenticate the identity of a system user and, to grant or deny access to private or shared data. FIPS PUBS specifies basic security criteria for two different uses of passwords in an automated data processing system, (1) personal identity authentication and (2) data access authorization. A password used for personal identity authentication is called a personal password; a password used for authorizing access is called an access password. A personal password should not also be used as an access password. It's the organization's security officer, through policies who will specify the criteria of a password. The generation process by which a password is obtained should have a large set of acceptable passwords in order to prevent an unauthorized person from determining a valid password. The length of a password is also important in helping to prevent an intruder from exhausting all possibility of guessing a password. With the number of password cracking tools that are freely available on the web today, it's important to choose a combination of alpha and numeric characters for passwords. It's good to also use what is called the "keyword reminder technique" when choosing a password. An example of this would be " I take 2 sugar with my coffee," pick the first letter of each word, which would then be "it2swmc." In order to have a secure password, it should be changed on a periodic basis and be changed whenever "compromised" is confirmed or suspected. Password storage in the authentication system should be done in a manner that will minimize disclosure or unauthorized replacement. In most systems the password file is protected by a file access mechanism which checks a protection bit in a file access table. Some systems separate the passwords file from the authorized user file and also encrypt the password [7].

The site http*://www.itl.nist.gov/fipspubs/fip112.htm* provides important information on the usage of password. Passwords are vulnerable to brute force attacks, dictionary attacks, theft, and forgetfulness. If a password is sent in plain text to the authenticating server, any network sniffers can figure it out. One can agree that the biggest security problem with a password is its user. In order for a password to be a successful authentication method, the users need to select a strong password. Users should use a combination of upper and lower case letters plus a number or a special character. Users should try not to use dictionary words, proper names or any information about themselves that can be easily guessed, for example phone numbers, birth dates or children's name. If users are educated about the usage of password, chances are they will follow

security guidelines more carefully. Passwords as an authentication method would best serve non-critical systems. Organizations where data is not of a critical nature, for example a University or even a Library system could implement strong password mechanism as a solution.

Token/Smart Cards (something you have)

The most common type of "something you have" scheme is the authentication token. Tokens can be in the form of a password-generated device that a user carries, called hardware token, or in the form of verification code, called software token. The hardware token is a credit card-size device with a computer chip and a display screen that shows a string of numbers, which changes every minute. When a user enters their username followed by the numbers shown on the card, the host system knows what the numbers are suppose to be at that particular time because the two devices are synchronized. If the number matches, the user is allowed access to the appropriate systems or network. Software tokens are also called a digital certificate and works similar to the hardware token, except it uses a password along with an encoded digital certificate. Digital certificate contains personal information on a user, which is linked to an information network that has the organization's computerized certificates. The software token can be stored on a floppy disk, hard drive or smart cards. With token-based authentication, it is assumed that the user with the token is the one the token was originally assigned to. Token-based systems should incorporate a strong means of authenticating the user to the token device [9].

One advantage of authentication tokens is, if a hacker/unauthorized person sees the password generated by the token while a legitimate user is logging on, the unauthorized person will not be able to use the password to hack into the system. This is because the one-time generated password only works for a brief, specified period of time; it is immediately replaced by another password known only to the security server and hardware token. Two disadvantages are that the system assumes that the user with the hardware device is legitimate; and if the two devices (hardware tokens and host system) are out of sync, the user is denied access until an administrator resets it; this is a problem if an administrator is not available.

SecurID, developed by Security Dynamics and purchased by RSA (Rivest, Shamir and Adleman), has become the de facto standard for token authentication. RSA SecurID uses a two - factor authentication solution, meaning users will need to identify themselves with two unique factors (something they know and something they have) before they are granted system access. Many applications are configured to support SecurID as a means of authentication. RSA SecurID Software Token is also available for Windows PC or laptop workstations, for secure access to network and valuable resources. The software security token resides on a user's computer hard drive [6].

With the growing security concerns that are facing organizations today, a smart card solution would offer stronger authentication to e-business and remote access than that of password and user name. Password and user name can be easily cracked.

Biometrics (something you are eg. finger prints)

Biometrics is automated methods of identifying a person or verifying the identity of a person based on a physiological or behavioral characteristic. Physiological characteristic includes; hand or finger images, facial characteristics and iris recognition, where as behavioral characteristics deals with traits that are learned or acquired. Biometric requires comparing a registered or enrolled biometrics sample against a newly captured sample. Biometrics-based authentication applications include workstation and network access, single sign-on, application logon, data protection, remote access and Web security. Biometrics as authentication is considered to be a stronger method of authentication as opposed to passwords and tokens because it cannot be forgotten, lost or stolen. Finger prints as a type of biometrics authentication; is based on the patterns of friction edges on an individual's fingertip, which are unique to that individual; it's also unique for each finger of a person including identical twins. Iris recognition or retina scan, uses the iris of the eye which is the colored area surrounding the pupil [7]. With biometrics a user simply touch a device with a finger or glance at a camera for authentication. Hand and fingerprints are the most common method of Biometrics authentication. The Biometrics Consortium web site (http://www.biometrics.org) is an excellent location for information on biometrics. It gives information on Common Biometrics Exchange File (CBEFF); this is the set of data elements necessary to support biometrics technologies in a common way independently of the application and the domain of use (eg. mobile devices). CBEFF facilitates biometrics data enter-change between different system components or between systems; it promotes inter-operability of biometrics-based application programs and provides compatibility for technology improvement [8]. Biometrics has been around for many years, but the technology to make it accurate or economically feasible did not exist. Now it seems an ideal solution to many authentication problems. Biometrics devices can be integrated with Windows NT or Windows 2000 and even provides support for the Unix/Linux platform. Biometrics-based authentication can be used by itself or it can be integrated with other technologies such as smart card, encryption keys and digital cameras. Many companies are now developing biometrics authentication systems; BioID is one such company (http://www.bioid.com). They develop systems that can be easily integrated into existing network applications.

Although biometrics offers a better security solution than other authentication methods, it does have some limitations. For example, if a user has a bandage on the finger used for authentication or if the device fails, some other backup

method of authentication should be in place. As with any method or technology, a combination of measures will offer a better security. In the Health Care environment, (eg. hospitals) finger prints as authentication solution may not be the ideal choice, because of the frequent use of gloves. In that type of organization iris recognition or retina scanning would be a better choice. Biometrics authentication could be argued as expensive, but it seems to be the ideal choice for authentication because of its uniqueness. Biometrics technologies is widely used by the US government (fingerprints) and is expected to be incorporated in solutions for Homeland Security including applications for improving airport security, strengthening of our national borders, in travel documents, visas and in preventing ID theft.

KERBEROS: The network Authentication Protocol

Kerberos is a network authentication protocol. It was created by MIT (Massachusetts Institute of Technology) to provide strong authentication for client/server application by using secret-key cryptography. Hackers use different tools to sniff passwords off the network, which makes sending unencrypted passwords over the network extremely vulnerable. Kerberos was created as a solution to this network security problem. The protocol uses strong cryptography so that a client can prove its identity to a server across an insecure network connection. Kerberos is actually used when a user attempts to use a network service. Kerberos is a Digital Encryption Standard (DES) with a key distribution system. The Key Distributed Center (KDC) is a trusted intermediary between each participating entity on the network; the KDC shares a separate secret master key for each. When an entity wants to communicate in a trusted manner with another entity over the network, the KDC issues a “ticket” which becomes the basis for establishing a trust between the two entities.

How Kerberos works

There are five main steps that are performed when Kerberos is used.

1. Clients connect to the KDC and send a ticket granting ticket request (TGT) (This is what a client uses to request a ticket from the ticket granting server)
2. When the client request a TGT, the KDC sends back an encrypted TGT.
3. The client then decides what resources they need access to, then a ticket request and the TGT are sent to the tickets granting server.
4. The ticket granting server replies by sending an encrypted ticket for that resource requested.
5. The client then sends the ticket the ticket5 and an authenticator to the server the client wants to access and if everything is verified, access is granted [1].

Kerberos make an assumption that the user password choice is good and that the machine is secure. This is important because when Kerberos issues a ticket, the ticket shows that the bearer knows something only its intended user would know, for example, a password. Kerberos can be used to provide single sign on capabilities, where the authenticated ticket can be used to sign on to multiple devices.

Microsoft Windows 2000 implements Kerberos v5 with extensions for public key authentication. The Kerberos Key Distribution Center (KDC) is integrated with other Windows 2000 security services running on the domain controller and uses the domain's Active Directory as its security account database. Microsoft describes Kerberos protocol as more flexible, efficient and secure than NT LAN Manager (NTLM), which was the default for network authentication in the Windows NT 4.0 operating system. With NTLM authentication, an application sever must connect to a domain controller in order to authenticate each client. Kerberos authentication provides faster connection because it does not need to go to a domain controller; it can authenticate by examining credentials presented by the client. Mirosoft implementation of the Kerberos protocol is based on standard-track specifications recommended to the Internet Engineering Task Force (IETF). As a result, the implementation of the protocol in Windows 2000 lays a foundation for interoperability with other networks where Kerberos v5 is used for authentication [4].

CONCLUSION

In today's global enterprise both organizations and users need to be protected or at least feel protected when they conduct business on any network. A combination of access management and strong authentication can offer some comfort and security. Understanding the functions of both access management and authentication, why they are necessary and how they function will help to manage rights and permission on network and local resource more effectively. When a user travels, or accesses a resource over a network they want to have an authentication system that is portable, secure and convenient. Authentication and access management system need to be able to allow access to all systems, a range of systems, or a limited set of hosts. There is no one solution that can solve security issues today, a two-factor authentication concept should be considered, for example smart cards along with biometrics. As information technology grows and e-commerce becomes a popular way of business, organization will have to focus more on security. Authentication and access management can be considered as essential for information security. Choosing the right combination will be a challenge. Whether an organization chooses IP addressing or Proxies as a method of access managing, they will need to combine it with a strong authentication method. Passwords can be used as an authentication method, but keep in mind it depends a lot on its user. Password authentication could be done on non-critical systems. Token/Smart Cards and

Biometrics are considered to be a more secure method of authentication, however, they too have limitation. Smart card can get lost and, it can also get out of sync with the server. Smart cards can also be stolen and if it falls in the hands of the wrong person can be used to access critical information. Biometrics on the other hand can be very expensive and can still incur false negative (denying access to an authorized user) and false positive (providing access to an unauthorized user). This too would depend on the type of biometrics authentication method chosen, fingerprints, shape of user's face, pattern of their eye's iris, signature or sound of their voice, etc. Finger print, iris recognition or retina scanning seems to be the best choice, because of its uniqueness. On the issue of cost one has to consider the facts that many users work from home and travels. Also, with the growing use of wireless Internet services and modems a user can work from virtually anywhere. Making the decision to purchase biometrics devices for all users could prove to be very costly. You would have to consider more than just the workstation in their offices. Organizations would need to consider laptops with built-in biometrics device; at least for their traveling employees who need to access the network when they are out of town. Deploying Kerberos as a means of authentication can be useful, but keep in mind it has to be combined with a strong password.

Organizations are facing some difficult security questions; how do they welcome customers with open arms while simultaneously protecting core information assets? How do they open mission-critical systems to employees and partners while monitoring and guarding against internal threats? Access management and the right authentication method is the first step in addressing these questions.

REFERENCES

1. SANS Institute. Encryption and Exploits, Kerberos.
   SANS, Security Essential. 2001 Online Class. Day 4 page 1.31-32 (Aug. 2000)

2. Andress,Mandy. Surviving Security How to Integrate People, Process and Technology. Indianapolis, Indiana: Sams Publishing 2001, Chapter 5 and 7 (August 2002)

3. Lewis, Chris, IP 101: All About IP Addresses.
   URL: http://www.networkcomputing.com/netdesign/ip101.html (14 Sept. 2002)

4. Microsoft Tech Net. Windows 2000 Kerberos Authentication, White Paper
   URL:
   http://www.microsoft.com/technet/treeview/default.asp?url=/TechNet/prodtechnol/windows2000serv/deploy/kerberos.asp (17 Sept. 2002)

5. National Institute of Standard and Technology. Information Technology Laboratory Password Usage FIPS PUB 112, May 30,1985
   URL: http://www.itl.nist.gov/fipspubs/fip112.htm (19 Aug 2002)

6. RSA Security. RSA SecurID, Authenticators.
   URL: http://www.rsasecurity.com/products/securID/datasheets/SID_DS_0702.pdf (17 Aug 2002)

7. Fernando L.Podio & Jeffrey S. Dunn. Biometrics Resource Center, "Biometrics Authentication Technology: From the movies to your desktop"
   URL: http://www.itl.nist.gov/div895/biometrics/Biometricsfromthemovies.pdf (29 Aug. 2002)

8. Biometrics Consortium. Common Biometric Exchange File Format. 3 Jan. 2001
   URL: http://www.itl.nist.gov/div895/isis/bc/cbeff/ (18 Sept. 2002)

9. Baker, D. B., Cooper, N., Culp, K. S., et. al The 2000 Guide to Health Data Security. 1999 New York, New York: Faulkner & Gray Inc. Chapter 4, pages 46 – 47 (19 Aug. 2002)

10. NetScreen. White paper on Stateful-Inspection Firewalls.
URL: http://www.netscreen.com/products/firewall_wpaper.html (20 Sept. 2002)