Global Information Assurance Certification Paper

Mike Murphy
May 01, 2001
GCNT Practical Version 2.1

Authentication in Windows NT and Windows 2000

After the fantastic growth and development of the Internet, and the subsequent growth of support industries and technologies over the last two years, there are still a few simple concepts that drive consumer demand for network services:

- Enough bandwidth (speed/capacity when you need it)
- Killer applications (automate, automate, automate)
- Interoperability (disparate technologies that can work together)
- Availability (it is there when you want it; the world never sleeps)
- Simplicity (ease of use and implementation)
- Security (the Internet and Intranets can be very dangerous places)

The first five are pretty much the same driving factors that were around in the very beginning. The last one, security, has grown exponentially in importance. Companies are not only concerned about the integrity of a network of hosts and the possible loss of valuable data, time, and materials, but also that the mere impression of poor security can cause a company to lose much more. Lost potential revenue through the loss of current customers and the failure to attract high caliber employees are the potential result of a damaged reputation and loss of consumer trust. The issues now are not only privacy and the integrity of huge amounts of money and commodities, but also non-repudiation, which is when it can be proven that someone sent and/or received something.

Clearly a simple password scheme is no longer enough. Over time, new methodologies and technologies have emerged to meet the growing demand for stronger, yet scalable security products. Currently, one of the fastest growing segments of security is that of authentication products.

"Authentication is the verification of the identity of a party who generated some data, and of the integrity of the data" (Neuman). In other words, how can the other party be sure someone is who they say they are? If a user is an imposter and it is not discovered and the request is not denied, then the user could be granted access and privileges, which he normally would not have. In addition, authentication does not stop with successfully logging onto a server or workstation. There are more places where authentication can and does take place in a networked environment. Client or object credentials may be passed on to other applications like a web server, a running service, or another computer entirely. The process of passing-on authenticated credentials is

essential for secure networked computing in Windows, or any other operating system for that matter.

With networked computing being the major design strength and selling point for today's operating systems and with the worldwide use of Windows operating systems of all types, the ability to have secure and configurable authentication methods is essential for computing in today's and tomorrow's technological environment.

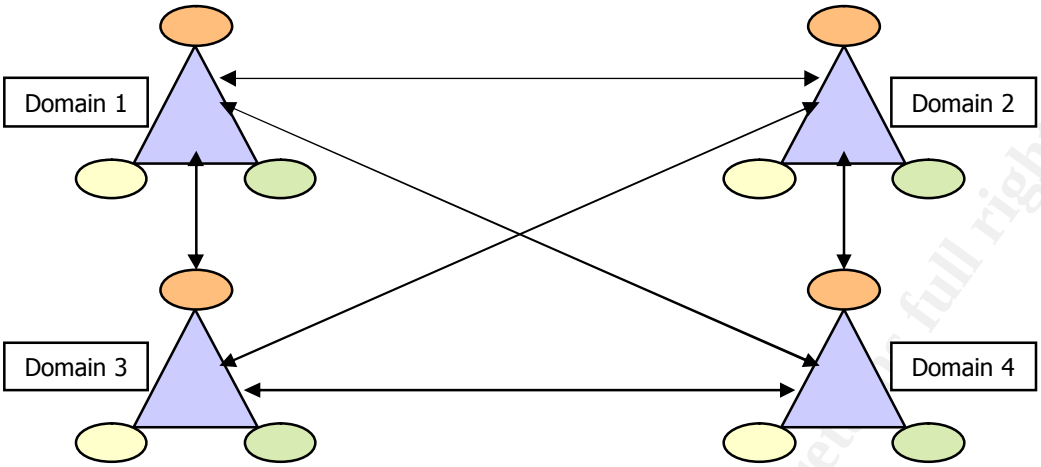
Windows 2000 has incorporated multiple authentication methodologies into its security structure. NT also has had some authentication concepts since its inception and has had some added during its lifespan. We will look closer at each platform in order to better understand their limitations and advantages.

Authentication in NT

In general, NT boxes by default can talk to each other very casually, as in a workgroup or be added to a structured domain. When logging onto a host with a local account, the domain, if configured, is not a factor. The profile assigned will be designed for use at the local level for that particular machine. Rights and privileges are not automatically portable to other computers or network devices; they only affect the computer currently logged onto. When logging onto a host with a domain account, everything changes. The profile assigned is maintained on the Primary Domain Controller or PDC (Taylor). This profile can be quite different than the local account as it is designed to be portable. The same profile is given no matter which NT box you log onto on the network. The advantages of a domain account, however, can be very handy as they often include access—often no login required—to other network components such as printers, file servers and the like. Because a consistent domain database with high availability is crucial to the process of authentication in a domain, it is important to look at the roles played by Windows NT Servers and how they keep the domain database consistent (Taylor).

The concept of trust between domains themselves in NT is explicit. You must configure explicit relationships with each and every domain you wish to trust and vice versa. Without the proper configuration, extending privileges outside your domain is not possible. So we have local - to domain - to inter-domain levels of trust that needs configuration if desired.

The diagram below illustrates Domain Trust - NT style.



The next two paragraphs speak to NT concepts related to authentication, I have included them for completeness of the overall picture.

The assigning of a profile, default permissions, and other rights on NT is accomplished through the User Manager application in the Administrative tools section of the Start Menu. This application is present on both workstations and servers. If users have a local account, the administrator of this particular machine would set the profile for the users and would likely deny access to change anything in the User Manager for obvious reasons. For domain accounts, the profiles are set and stored on the PDC and sent down to the workstation during the login process. Once a user is authenticated, he will get the profile that authorizes certain functionalities.

NT does provide for auditing users. Directories and files can have specific auditing options turned on. If you look at a new installation of NT, you will see that auditing is not automatic out of the box; configuration is required. NT by default is pretty much wide open security-wise. Many settings must take place before some reasonable level of security is attained, based on the purpose of the platform. Once auditing is properly configured, if someone without the proper privileges tries to access a directory or file, it will be reported in the Security Event Log. Also, if an application does not have the proper rights to logon to a service or access a file, it can also be logged as a security event. If authentication fails at some point, the Security Event Log should capture it for subsequent analysis and investigation. It will describe the details of the failure, such as, "invalid Key", "unknown user" and much more, allowing for further investigation.

NT uses a process known as Windows NT LAN Manager, or NTLM, authentication. This is also known as the NT challenge/response mechanism (MSDN Online). This process is, in part, a carry over from the early days when the Microsoft LAN Manager, or LM, product was used for network communications. As you might expect from an aging technology, it is no longer adequately secure and thus no longer used as a whole; however, there are parts that continue to linger in today's Windows products. As we look closer, its limitations will become apparent.

The NTLM Authentication Process

The authors of MSDN Online Library give a description of how a non-interactive over a network session proceeds--

1. The client sends the user name to the server (in plaintext).
2. The server generates a 16 byte random number, called a challenge or nonce, and sends it to the client.
3. The client encrypts this challenge with the hash of the user's password and returns the result to the server. This is called the response.
4. The server sends the following three items to the domain controller: the user name, the challenge sent to the client, and the response received from the client.
5. The domain controller uses the user name to retrieve the hash of the user's password from the Security Account Manager database. It uses this password hash to encrypt the challenge.
6. The domain controller compares the encrypted challenge it computed (in step 6) to the response computed by the client (in step 4). If they are identical, authentication is successful.

A closer look at LM and NTLMv1

Two hashes, the NT and LM hashes, of the user's password are stored in the Security Account Manager, or SAM, database. Both are used in parallel during the authentication of Windows NT clients. Because of this, a server's challenge is encrypted twice and both responses are returned to the server. Dual authentication is used to provide compatibility with Windows 95/98, which by design can only use the LM hash. This authentication method is generally weak in that attackers can deduce the NT and LM password hashes. If hackers can sniff the challenge/response authentication session and can catch the authentication packets, they can crack the NT and LM hashes with an easily obtainable program such as L0ftCrack.

The LM Password Hash Used in NTLMv1

There are inherent weaknesses in the LM hashing process. Jason Fossen, a security specialist, describes some of the important shortcomings as follows:

- Passwords longer than 14 characters are no stronger than 14-character passwords because they are truncated.
- Case-sensitivity is lost because the password is converted to uppercase, which reduces the "keyspace" which needs to be searched to break the encryption because there are fewer possible characters.
- The 14-byte password is broken into two 7-byte strings. These strings are used to separately encrypt the big string, which reduces the effective length of the encryption key from 14 to 7 bytes which is a reduction in encryption strength by orders of magnitude.
- If a password is seven characters or less, it will be instantly apparent because the second DES key will be all null characters or blanks. This will greatly reduce the effort required to crack the padded password segment.
- No "salt" or random bytes are added to the hashing process; therefore, two identical passwords will have identical LanManager hashes. This allows an attacker to use a pre-computed dictionary of LanManager hashes to quickly search for matches.
- When used during NTLMv1 challenge/response authentication, the 16-byte LanManager hash is padded with five bytes of "0" (zero) characters to produce the 21-byte session key. This is cut into three 7-byte pieces that are each used as DES Block Mode keys to encrypt the challenge. The three encrypted challenges are concatenated and returned to the Domain Controller as the client's response. It is a simple problem to "reverse out" the original LM hash given the server's challenge and the client's response.

The NT Password Hash Used in NTLMv1

As a comparison to the LM hash, the NT hash has fewer weaknesses and some improvements were made. Paraphrased below are Fossen's descriptions of some of the characteristics of the NT hash:

- The NT hash is produced by truncating or padding the password to 14 characters.
- This string is converted to Unicode, which preserves the case of the letters.
- This 14-byte string is hashed with the MD4 algorithm to produce a 16-byte output. This output is the NT hash of the password. The NT hash is

many times stronger than the LM because the full password length is used and case-sensitivity is retained.
- No "salt" is added to the NT hash; therefore, two identical passwords will yield identical hashes. Hence, pre-computed dictionaries of hashes can be used to quickly crack the encryption.
- Because both the NT and LM hashes are used in parallel during authentication, the strength of the NT hash is no longer relevant. For NTLMv1 challenge/response authentication, the NT hash is padded with 0's to create the 21-byte session key used to DES-encrypt the challenge the same way the LM hash is used. It is also easy to compute the NT hash from the server's challenge and the client's response.

As can be seen by the above lists, the NTLMv1 process was limited in effectiveness. Beginning with Service Pack 4, version 2 of the NT LanManager authentication scheme became available. It was an improvement over v1. NTLMv2 also uses a challenge/response method of confirming the user's password.

NTLMv2 improvements/characteristics

Jason Fossen then looked at the important changes and improvements in NTLMv2 as compared to NTLMv1:

- The LM hash of the user's password plays no role whatsoever.
- A "salt" is input by the client to prevent chosen plain text attacks. This prevents the use of pre-computed databases of hashes/keys to speed the cracking. The client's response is different with each session even if the user's password stays the same.
- Use of the HMAC-MD5 algorithm for the 128-bit password hashes was added.
- Timestamp utilized to verify that response is timely. Using a time value helps defend against attacks that use the lack of a timer to "replay" the captured packets at a later time for various purposes.
- Replay attacks are also infeasible because a server's challenge is different each time.
- Mutual authentication—client to server and server to client—based on client challenge to the server is now available.
- The most efficient cracking method is a dictionary/brute force search of all possible passwords. Hence, NTLMv2 is just as strong, or only as strong, as the password itself.
- Man-in-the-middle, or MITM, attacks are infeasible because of mutual authentication. The MITM attacks allow someone in-between two sides to effectively assume the role of one of the legitimate sides of the communication.

- Downgrade attacks can be made infeasible by registry values that will require NTLMv2 from either the server or client's side.
- L0phtCrack 2.52 cannot extract password hashes from NTLMv2 authentication sessions, nor is any future version expected to be able to do so with any useful efficiency.
- NTLMv2 is also used to negotiate the exchange of a key for the sake of integrity checking and encrypting other data. The client generates a 128-bit pseudo-random RC4 key, also called the "session key." The session key is re-keyed every 8192 bytes of data encrypted with the RC4 key and is not based on the user's password.

Obviously, then, the introduction of NTLMv2 was a vast improvement over SP3 and earlier implementations.

The relationship of the Domain structure to authentication

In "How Authentication Works," Paul Taylor describes the roles of domain structures in relation to authentication as follows**:**

> A Windows NT Server can be configured to assume one of three roles in a Windows NT domain:
> - PDC
> - BDC
> - Member server
>
> Only the PDC and the BDC hold copies of the domain database that is known as the Security Account Manager (SAM**).** A member server provides such resources to the domain as file and print services and such application services as SQL or Exchange. A member server, however, plays no part in domain authentication and does not hold a copy of the domain database**.**

It is apparent there needs to be some assurance of synchronization of the SAM database in a Domain structure. This is accomplished with the Netlogon system service, which runs on each domain controller. It is responsible for ensuring that each copy of the SAM is up-to-date (Taylor).

For portability of credentials, NT authentication uses Security Access Tokens, or SAT. The SAT is constructed from the user's rights and group memberships as defined in the SAM. NT uses this SAT to access objects on behalf of the user, which is known as impersonation. For example, when a user starts a Word or Excel session, a SAT is attached to it, giving it the proper access and rights for that user (Taylor).

Pass-through Authentication

In order to move to other hosts or services on other domains, the SAT is again utilized to "pass-through" a user's credentials to the destination object. After the user has been authenticated in the new domain, the SAT is returned to the users workstation in the originating domain and the login is completed to the new domain (Taylor). This is also possible through the action of "trust" between domains. How domains react and interact with each other in a multiple domain environment is configurable. If the user tries to go to another domain that does not have a trust relationship with the user's domain, the SAT will not be accepted and the logon or access will be denied. When trusts have been configured between domains, users can logon and use any network resource, regardless of whether the resource's account is in the domain they are logging on from.

NT Summary

We have looked at the primary ingredients in the implementation of authentication in NT. The Domain concept and the Logon process itself, using SAM and NetLogon as well as the LanManager and NT hashing characteristics and their inherent weaknesses. There are other ways to defeat or circumvent different phases of the NT authentication scheme. For example, lets say that an account has been disabled or deleted from a domain. To circumvent the fact that the domain authorizes access to the workstation, the user can physically disconnect the workstation from the LAN and then, because the last 10 logons are cached locally, log onto the workstation (Fossen). This process changes the authentication method. Social engineering is not accounted for because all that is needed is the correct login and password the login will succeed. Furthermore, without the proper patching and current service packs, some of the above and many, many more attacks are possible. However, even with patching and upgrades, there is no provision for more advanced technology to be integrated into the security subsystems. Improving NT authentication and security in general would not only take major code changes, but a re-design of the framework of how to address not only current, but also future security considerations. This brings us to Windows 2000. Next we will look at how Microsoft has addressed the security shortcomings of NT and implemented its vision of authentication in its latest major operating system.

Authentication in Windows 2000

We must begin the discussion of authentication in Windows 2000 with a look at the new components introduced, and how they work together to achieve a higher level of security as required by today's e-commerce business model.

The implementation of secure channel security protocols, or SSL 3.0/TLS, supports strong client authentication by mapping user credentials in the form of public-key certificates to existing Windows NT accounts. Common administration tools are used to manage account information and access control, whether using shared secret authentication or public-key security.

In a Windows 2000 magazine article, R. Franklin Smith describes another new feature:

> In addition to passwords, Windows 2000 supports the use of smart cards for interactive logon. Smart cards support cryptography and secure storage for private keys and certificates, enabling strong authentication from the desktop to the domain.

In this case then, smart cards add hardware to the process. This gives the user an easy way to carry and present powerful credentials in a secure way. It can be combined with remembered information to present something the user knows, such as a password or login ID, and something he has, such as a smart card with a certificate or a private key.

Active Directory

"AD is Win2K's flagship component" (Smith).

The Active Directory, or AD, has an essential relationship with the OS.
The list below shows the importance this relationship has to our subject of authentication (Secure Networking).

- AD stores the account and policy information for the operating system.
- AD relies on the OS to control access to its objects.
- AD enforces permissions to objects within the AD.
- AD trusts information stored in itself.
- AD authenticates access to itself.

Another big change from NT Domains is the scalability of Active Directory. NT Domains could handle 20,000 users. An AD domain can handle over a million objects and does not use a PDC and NT did for management (Smith).

AD also supports "Transitive Trust." For example, if domain A trusts domain B and domain B trusts domain C, then domain A trusts domain C (Taylor). Authentication is based on credentials stored in the AD. In this way user credentials can be passed through to other domains. PKI-based authentication is accomplished by mapping elements of a certificate to the proper AD user object. This works together with the transitive trust structure to provide flexibility + security.

The Active Directory provides significant improvement over NT's registry-based implementation in the areas of performance and scalability, and offers a feature-rich administrative environment.

SSPI (Security Support Provider Interface)

SSPI has been around since NT 4.0. Its role in Windows 2000, however, is much more integral and essential to the security infrastructure. The SSPI provides authentication services through an API—application programming-- interface. Client/server applications need to authenticate the client to the server and sometimes the server to the client. This way, SSPI allows applications to be written without having to know the details of network security protocols (Smith). It also provides an interface to multiple authentication protocols for an application; therefore, application code for each protocol is not needed. Using SSPI shared-secret or public-key, authentication protocols can be used (Smith).

Crypto API – PKI support

Although available since NT 4.0, the CryptoAPI is as fundamental a component of the Win2K security architecture as AD is. The CryptoAPI allows application developers to use cryptography, encryption, and PKI in their applications written for Windows. CryptoAPI provides a standard interface between applications and Cryptographic Service Providers, or CSPs. The CSPs in turn, provide services like hashing, key generation, digital signatures, encryption and certificate service (Smith). CryptoAPI also uses the industry standards X.509v3 and PKCS (Smith). This is helpful for PKI since it allows for managing and publishing of certificates and revocation lists. So by design, as encryption or certification changes, developers will not need to redesign applications (Smith). This concept allows for use of Smart Cards, Biometrics, and other technologies available now and in the future.

Kerberos Authentication Protocol

Kerberos addresses problems that have plagued NTLM in particular. Windows 2000 will still support NTLM for backward compatibility with NT. Kerberos v5 is the default authentication protocol for Win2K. J. Kohl of Digital Equipment Corporation and C. Neuman of ISI describe Kerberos v5 in RFC1510, the Kerberos authentication service. Like many others features incorporated into Windows 2000, it is an industry standard.

RFC1510 describes the authentication process:

A Client sends a request to the authentication server (AS) requesting "credentials" for a given server. The AS responds with these credentials, encrypted in the client's key.

The credentials consist of
1) A "ticket" for the server
2) A temporary encryption key (often called a "session key").

The client transmits the ticket (which contains the client's identity and a copy of the session key, all encrypted in the server's key) to the server. The session key (now shared by the client and server) is used to authenticate the client, and may optionally be used to authenticate the server. It may also be used to encrypt further communication between the two parties or to exchange a separate sub-session key to be used to encrypt further communication.

Kerberos provides a "trusted third party" model for authentication (Kohl). It was developed to fill the need for authentication across open networks. Under other conditions, packets can be sniffed and otherwise subverted. Kerberos uses encryption and shared secret keys to thwart session and packet hijacking. This model assumes that the host addresses may be spoofed, hosts may not be physically secured and that packets can be hijacked, inserted, tampered with etc.

Kerberos was also designed to operate across boundaries (Kohl), thus making it perfectly suited for the Active Directory concept in Windows 2000. It can utilize "inter-realm" (Kohl) or inter-domain keys of trust. Thus enabling pass-through authentication that can travel with the user or object.

Kerberos does not solve all authentication attacks, however. It does not address password guessing; so poorly constructed passwords will allow brute force dictionary attacks. This could compromise messages encrypted with a user's password. It does not stop Denial of Service. An application can be stopped from participating in the proper steps of authentication at certain points. Secret keys must stay secret; if they are stolen, then the attacker can masquerade as the rightful owner of the credentials. Host clocks must be synchronized to a certain degree; otherwise, replay attacks and other timing disruptions can occur.

According to the online How it works article, Windows 2000 Kerberos Authentication, some of the positive characteristics of Kerberos are--

- Kerberos authentication allows a client to obtain credentials for a specific server once and then reuse them during the logon session, rather than the server contacting a domain controller to authenticate each client; connections therefore can be faster.

- Kerberos allows clients to verify the identity of the server, as well as allowing servers to verify the identity of clients.

- Kerberos utilizes the concept of Transitive Trust. Kerberos trusts are two-way and transitive (meaning if domain A trusts B, and B trusts C, then A trusts C as well). Even better, these trust relationships within a Windows 2000 Active Directory forest are implicit. There is no need for an administrator to create trusts, as they already exist by default.

Kerberos authentication offers some very real benefits. They make a network administrator's job easier while improving the security of network communications. Another important reason for the switch to Kerberos is interoperability with other network operating systems. Kerberos v5 is used for authentication by UNIX servers, and adopting a standard authentication protocol makes it easier for Windows-based networks to interoperate with other networks.

Kerberos Mechanisms – a closer look

An important service within Kerberos v5 is the Key Distribution Center, or KDC. The KDC runs on each domain controller as part of Active Directory. Remember that the AD stores all client passwords and other account information.

The Key Distribution Center (KDC) is a service that runs on a trusted server. The KDC actually runs two services:

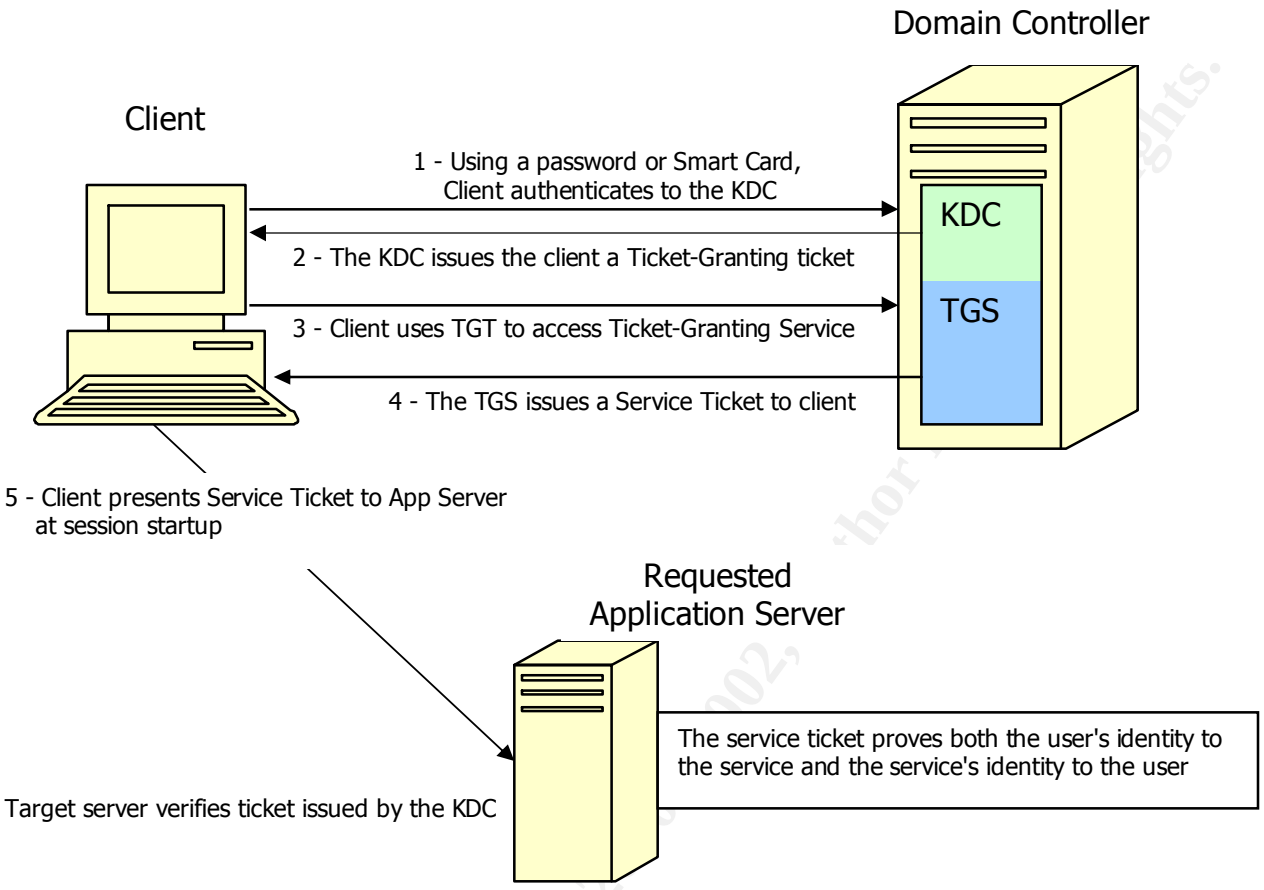
- The Authentication Service (AS)
- The Ticket Granting Service (TGS)

The KDC holds a database in which the cryptographic keys associated with each security principal or object, such as users and computers, are stored (Neuman).

Kerberos is designed around the concept of "realms." Realms are a division of the network representing an organization that runs a Kerberos server. In Windows 2000, a domain is the equivalent of a Kerberos realm (Kohl).

A client, which can be a host or an application on a host, that wishes to access a resource on a server must first be configured to interoperate with Kerberos services. This is also known as being "kerberized" (Neuman). Once configured, the client negotiates a trusted session for the duration of the network connection. To do this, it must "apply" to the KDC for credentials that can be presented to the server to be accessed.

The diagram below outlines the authentication process:



Kerberos authentication is based on the use of tickets to prove the identity of a Kerberos client. A ticket carries information that helps authenticate the bearer. It contains information such as a ticket number, a random number, realm info and other encrypted data (Kohl). Along with the ticket comes an Authenticator.

RFC1510 describes the use of Authenticators:

> An authenticator is a record sent with a ticket to a server to
> Certify the client's knowledge of the encryption key in the ticket,
> To help the server detect replays, and to help choose a "true session
> Key" to use with the particular session. The encoding is encrypted
> In the ticket's session key shared by the client and the server

The Authenticator information, which is packed with credential information fields similar to a ticket, also includes time information and a checksum, and it is encrypted with the session key of the accompanying ticket. This combination of

Ticket, Authenticator, and a fresh time interval prove the validity of the credentials.

Using this trusted third party model, the KDC allows for better efficiency in that if the client wants to access a server, the server does not have to go through the time-consuming process of contacting a domain controller and verifying the client's credentials. Session tickets can be reused, so that the client doesn't have to return to the KDC each time it wants to access the same server during the logon session (Schinder). Only tickets and encryption keys, together called credentials, are cached for a limited period. Users can obtain tickets and encryption keys using these time-sensitive credentials without re-entry of their password. The ticket-granting ticket, or TGT, has a relatively short life of approximately eight hours (Neuman). The decrypted response and the ticket and session key are then saved and the user's password is forgotten. Subsequently, when the user wishes to prove its identity to a new host or service, a new ticket is requested from the KDC on the Domain controller using the ticket granting service (Neuman). Finally, "when a user logs off, all session tickets are destroyed. Additionally, the administrator can set an expiration period for the session tickets" (Windows 2000 online).

To summarize this section, a Kerberos client is any entity that requests a service ticket for a Kerberos service, such as the server service on a Windows 2000 machine where resources are stored that the client wants to access. Below are two kinds of tickets issued:

- Ticket Granting Ticket - this ticket is granted by the KDC to allow the client to communicate with the KDC. When the client logs onto the network, the client's credentials are verified with a domain controller, and the KDC issues this TGT.

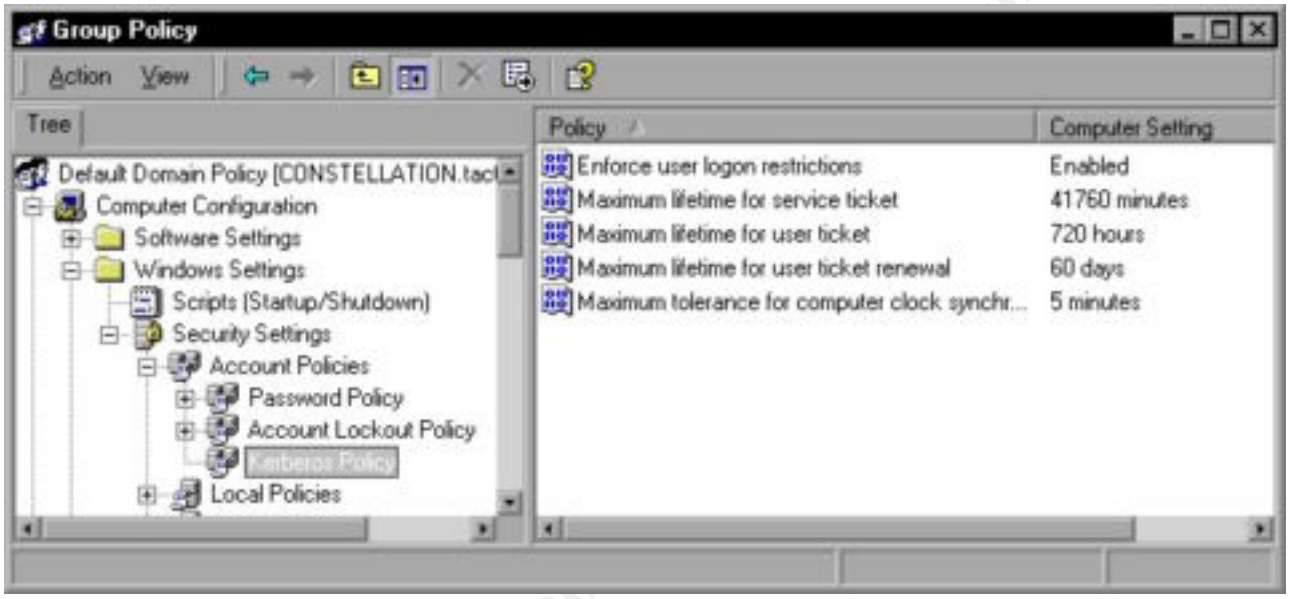
- Session Ticket - this ticket is granted by the Ticket Granting Service component of the KDC to allow clients to access specific servers on which resources are located.

Tickets are accompanied by an authenticator, which includes a time interval, encrypted data and time intervals which, all together prove the identity of the client to the requested resource and the identity of the resource to the client.

Kerberos Policies

With Kerberos, the security administrator can set policies to control how tickets are handled. For example, the expiration times for KDC issued tickets may be a valuable parameter to adjust in high security environments.

Kerberos policies are set, as are most types of policies in Windows 2000, by using Windows 2000 Group Policy. The Kerberos policy settings are under Computer > Configuration > Windows Settings > Security Settings > Account Policies > Kerberos Policy. Below is a screen shot originally created by Debra Schinder:



Certificate Services

> Certificate Services support the use of certificates in PKI. Certificate Services is more powerful and better integrated into the rest of the OS than its predecessor in NT, Certificate Server. The Microsoft Management Console (MMC) snap-ins provides GUI tools for both the client side and the server side. Certificate Services uses the AD to store and publish certificates to achieve enterprise wide functionality although it can maintain its own standalone data store. Using the AD, you can easily map certificates to users and control for whom, by whom, and for what purposes Certificate Services issues certificates. Certificate Services also supports multilevel hierarchies. (Smith)

Certificate Services were introduced in NT. They were commonly used to add PKI authentication to IIS. Windows 2000 uses Certificates as an integral part of its authentication structure. Now, a user from the outside of a domain can use a certificate from a trusted third party that is on the list of trusted certificate entities in the Active Directory to gain access and rights on the domain. The certificate can also be mapped to specific directories so that file access and rights given are specific to a particular individual. This process is described in the Windows 2000 Server Documentation, Mapping Certificates to User Accounts.

This concept allows for improved flexibility and efficiency of access while maintaining granularity of security.

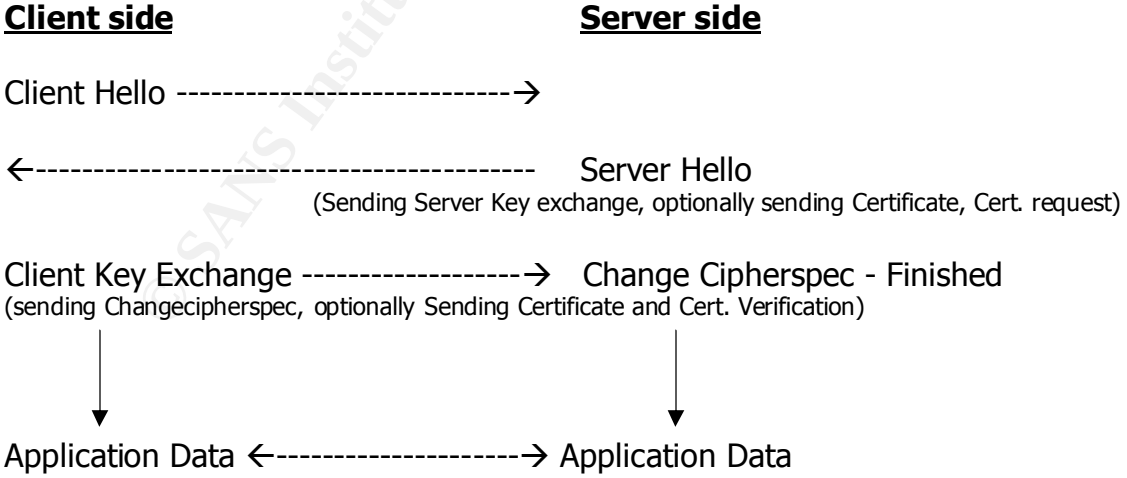
Client Authentication with SSL 3.0/TLS 1.0

According to Microsoft experts in the white paper "Secure Networking using Windows 2000 Distributed Security Services,"

> Secure Socket Layer and Transport Layer Security are public-key-based security protocols. These security protocols are used by Internet browsers and servers for mutual authentication, message integrity, and confidentiality. Authentication of the Internet server is performed by the client's browser when the server's certificate is presented as part of the SSL/TLS secure channel establishment. The client program accepts the server's certificate by verifying the cryptographic signatures on the certificate, and any intermediate CA certificates, to one of several known or configured root CAs.

Client authentication is also supported by SSL 3.0 and TLS. Client authentication using public-key certificates is completed as part of the secure channel session establishment. SSL 3.0 was developed into SSL 3.1 and essentially re-titled as TLS 1.0. Transport Layer Security, or TLS, was described in RFC2246 by Dierks and Allen of Certicom in January of 1999.

The illustration below shows the SSL 3.0 handshake messages between the client and server for secure connection establishment:



According to RFC2246, "The change cipher spec protocol exists to signal transitions in ciphering strategies." This is a way to implement synchronization

for the cipher as "the change cipher spec message is sent by both the client and server to notify the receiving party that subsequent records will be protected under the newly negotiated CipherSpec and keys." (Allen)

Later, more strength was added to the TLS specification. RFC2712 describes the addition of new cipher suites to the TLS protocol, specifically to support the Kerberos authentication protocol. The previously assigned 40-bit cipher suites were insecure and inadequate for today and their use now is highly discouraged (Hur).

Authentication of the client by the server is the same process as server authentication. In the Windows 2000 security architecture, access control is defined by the group memberships and privileges in the security access token, or SAT.

Mapping certificates to resources determines what authorization the client has to access resources on the server system. Support for client authentication by the Microsoft Internet Information Server is available by managing an authorization database to map user certificate information to existing Windows 2000 accounts (Windows 2000 Server Documentation, Mapping). The authorization database can be as simple or complicated as needed to meet the application requirements. The mapping can be performed using a search of the certificate subject name in the Windows directory or by searching for directory properties that identify the client certificate.

What this shows is that support for client authentication via public-key certificates is integrated into the Windows 2000 security architecture. No separate database is required to define the access rights associated with public-key certificates. The access control information is maintained by the group membership stored in the Windows directory. Common Windows Directory Service administration tools are used for granting access rights by adding Windows users to groups.

NT vs. Windows 2000 – Authentication comparisons

Now that the major components of authentication schemes in the two operating systems have been presented, we will look at the advantages and disadvantages of each to get a better idea of where authentication has been and where it is going on the Windows platform. We will also touch on some of the other security enhancements of Windows 2000.

Certificate Services

Certificate Server – NT

Certificate Server in NT provided the basic functionality of a CA, which requests issues, publishes, and manages certificates. Certificate Server offered Authenticode authentication and Secure MIME, or S/MIME, integration for Exchange Server, but it was geared mostly for public-key-based client authentication to Internet Information Server, or IIS. Administrators had to manually edit text files to control Certificate Server's configuration. Certificate Server lacked management features important to enterprise usage of PKI, such as tools to customize certificate types and policy settings and support for two-level CA hierarchies only. This is inadequate for large-scale PKI deployment.

Certificate Services – Win2K

Certificate Services is more powerful and better integrated into the rest of the OS. The Microsoft Management Console, or MMC, snap-ins provides GUI tools for both the client side and the server side. Certificate Services uses Active Directory, or AD, to store and publish certificates. Using AD, you can easily map certificates to users and control for whom, by whom, and for what purposes certificates are issued. Certificate Services now supports multilevel hierarchies. Microsoft added the Certificate Services certificate management functions to the CryptoAPI and moved the default certificate data store to the AD. Because Certificate Services accesses its certificate store through the CryptoAPI, Certificate Services can publish certificates in other third-party directories.

There is more flexibility, granularity, control and power for enterprise computing in the Win2K implementation.

The Authentication protocols

LM, NTLMv1 and 2 – NT

Using the legacy LanManager protocol is the anchor around the neck of NTLM. LM was inherently weak. It takes a 14-byte password and breaks it into two 7-byte sections making it easier to crack. If the password is less than 7 characters, then the second section would be known to be zeros. There are other flaws as well. Both an NT and LM hash was made. The NT hash is stronger than the LM hash, but still does not use a "salt" of random numbers. Without a "salt," you can compare hashes. Even though the password is not known, two hashes of the two identical passwords will be exactly the same. This allows for brute force dictionary attacks. Since both an LM and NT hash is used, the NT hash becomes almost irrelevant since the LM hash is weaker. NTLMv1 also makes it easy to

sniff the challenge/response session off the wire. Once the passwords are captured, they are easy to crack (Fossen).

NTLMv2 made some significant improvements. A "salt" was added, a new 128-bit hash algorithm, the LM hash was made irrelevant, the challenge/response session cannot be sniffed by L0ftcrack, therefore, passwords are not obtainable to crack. The passwords are as strong as they were created, whereas in NTLMv1, passwords longer than 14 characters were not stronger than a 14-character password since the length was truncated past 14 characters. NTLMv2 did not truncate longer passwords. NTLMv2 also added a timestamp to show if responses were timely.

Kerberos – Win2K

Kerberos is more secure than NTLM and addresses problems that have plagued NTLM in particular. Kerberos authentication allows a client to obtain credentials for a specific server once and then reuse them during the logon session. It allows clients to verify the identity of the server, as well as allowing servers to verify the identity of clients. It utilizes the concept of Transitive Trust. There is no need for an administrator to create trusts, as they already exist by default. Kerberos uses a Key Distribution Center, or KDC, to issue credentials and tickets to allow users to access required objects. The KDC acts as a trusted third party. Policies for Kerberos can be setup in the Windows 2000 Group Policy application. Here you can apply a great deal of flexibility and granularity to the security policy.

Although NTLMv2 was significantly better than NTLMv1, the flexibility, granularity and overall security of Kerberos is a vast improvement. Via group policy GUI, it allows for better administration and interoperability as well as moving from straight hashes and replicated user profiles between PDCs and BDCs to using trusted third party authentication with the KDC, transitive trust, use of certificates and integration with the Active Directory, which is the cornerstone of Windows 2000.

Kerberos is more efficient. With Kerberos authentication, the server does not need to go to a domain controller. It can authenticate the client by examining credentials presented by the client. Clients can obtain credentials for a particular server once and reuse them throughout a network logon session. (Schinder)

Kerberos can mutually authenticate. NTLM allows servers to verify the identities of their clients; however, "it does not allow clients to verify a server's identity, or one server to verify the identity of another" (Windows 2000 Kerberos). The Kerberos protocol makes no assumption that one side is genuine, so "parties at

both ends of a network connection can know that the party on the other end is who it claims to be" (Windows 2000 Kerberos).

Kerberos can delegate authentication. Windows services impersonate clients when accessing resources on their behalf. "Both NTLM and Kerberos provide the information that a service needs to impersonate its client locally" (Windows 2000 Kerberos). Some distributed applications, however, require client impersonation when connecting to services on other computers. "The Kerberos protocol has a proxy mechanism that allows a service to impersonate its client when connecting to other services. No equivalent is available with NTLM" (Windows 2000 Kerberos).

Kerberos can simplify trust management. One of the benefits of the Kerberos protocol is that trust between the security authorities for Windows 2000 domains is, by default, two-way and transitive. Networks with multiple domains require complex, explicit, point-to-point trust relationships in NT. In Windows 2000, many domains can be organized in a tree of transitive, mutual trust. "Credentials issued by the security authority for any domain are accepted everywhere in the tree. If the network includes more than one tree, credentials issued by a domain in any tree are accepted throughout the forest" (Windows 2000 Kerberos).

Microsoft's implementation of the Kerberos protocol is based on standards-track specifications recommended to the Internet Engineering Task Force, or IETF. As a result, the implementation of the protocol in Windows 2000 allows for interoperability with other networks where Kerberos v5 authentication is used. For example, Unix can use Kerberos v5.

SSPI and CryptoAPI – an evolution

Although available in NT, it is worthwhile to note that both of these concepts are much more fully developed and essential to the security infrastructure in Windows 2000, which is for the better.

The CryptoAPI acts as a platform for applications to interact with lower security layer services. This allows for Biometrics and Smart Cards today, and possible future technologies. Another big advance in Crypto API is ability to incorporate Public Key Infrastructure, or PKI, into various aspects of Win2K computing. PKI is strong and can be used for digital signatures, encryption of data, authentication and non-repudiation through the use of Public/Private keys. Windows 2000 uses APIs to make it easier for developers as opposed to using proprietary applications or protocols.

R. Franklin Smith summarizes:

> The SSPI separates applications from the details of lower security protocols. Developers do not need to write the application-level code needed to support multiple authentication protocols. SSPI gives them that interface. It also supports authentication based on shared-secret or public-key protocols.

Therefore, we can say that these two areas have improved as well.

Active Directory – The driving force

The concept of Active Directory is one of the cornerstones of Windows 2000. As such it plays a big role in the implementation of authentication in Windows 2000. There is really nothing to compare it to in NT as it uses domains as well. The AD is the engine that makes all the enterprise concepts work together. As for authentication, among other capabilities, the AD

- Stores the account and policy information for the operating system.
- Enforces permissions to objects within the AD.
- Trusts information stored in itself.
- Authenticates access to itself.

The concepts of transitive trust, sites, the AD domain replacing WINS and NetBios with dynamic DNS, and other new functionalities all contribute to overall security and thus affect the implementation of authentication within Windows 2000.

Administration and configuration

One of the problems with NT was the limitations found in configuration management because the GUI or application to do so was limited or non-existent. This resulted in directly editing the registry—always a danger—or writing many scripts. With Windows 2000, there have been advances in this area as well. Group Policy for example, has replaced the User Manager in NT in the Administrative tool application. Here you can set user and group policy and configure Kerberos among others. Group Policy is contained in the Administrative Tool. This tool is a big improvement because it contains many sub categories of tools available to Windows 2000 administrators.

There is more granularity and functionality in almost all administrative tools. There are Security Policy templates and a Security Configuration editor. Not only permissions and rights, but also auditing and other security options for high and low security workstations can be set here. Windows 2000 has made a major

effort to add templates and wizards, as well as integrating tools instead of adding on a package that is not really part of the whole system.

Using NT and Windows 2000 in a mixed environment should not be a major problem. Windows 2000 has planned for interoperability with NT. This includes authentication and domain structure. Make no mistake: Windows 2000 is better by itself. It can run in a different mode when the domain has both NT and Win2K boxes. You cannot fully take advantage of some of Windows 2000's features and power until you run it homogeneously.

And the Winner is . . .

To put it simply, Windows 2000 has left NT behind when it comes to the packaging of security concepts into the OS. Of course wouldn't the industry be very disappointed if it didn't? A major step forward is something we have all been waiting for. If the installation and configuration of Windows 2000 Workstations and Servers prove to be manageable in practice, then we will have made quite a leap forward in Windows enterprise computing.

References and Sources

Works Cited

Allen, Christopher and Tim Dierks. "The TLS Protocol Version 1.0." RFC2246. The Internet Society. 1999. http://www.faqs.org/rfcs/rfc2246.html

Fossen, Jason. "Securing NT." Online GIAC course, SANS 2001.

Hur, Matthew and Ari Medvinsky. "Addition of Kerberos CipherSuites to TL." RFC2712. The Internet Society. 1999. http://www.faqs.org/rfcs/rfc2712.html

Neuman, B. Clifford and Ts'o, Theodore, Kerberos: An Authentication Service for Computer Networks, USC/ISI Technical Report number ISI/RS-94-399. http://www.isi.edu/gost/publications/kerberos-neuman-tso.html

Kohl, John and B. Clifford Neuman. "Kerberos Authentication Service (V5)." RFC1510. 1993. http://www.faqs.org/rfcs/rfc1510.html

MSDN Online Library, Microsoft NTLM. http://msdn.microsoft.com/library/psdk/secpack/ntlmssp_0k19.htm

Schinder, Debra Littlejohn. "Guarding the Gates – Understanding Kerberos in Windows 2000." Microsoft Technet 2000.

"Secure Networking Using Windows 2000 Distributed Security Services." Microsoft Technet. http://www.microsoft.com/WINDOWS2000/library/howitworks/security/distsecservices.asp

Smith, R. Franklin. "Windows 2000 Security Gains." Windows 2000 Magazine. Microsoft Technet, March 2000. http://www.win2000mag.com/Articles/Index.cfm?ArticleID=7434

Taylor, Paul. "How Authentication Works." Miller Freeman, 1999. http://ntsystems.com/db_area/archive/1999/9906/306fe3.shtml

"Windows 2000 Kerberos Authentication." Windows 2000 Web Site, 1999. http://www.microsoft.com/TechNet/win2000/win2ksrv/technote/kerberos.asp

Windows 2000 Online Library, How it Works, Default page – Microsoft. http://www.microsoft.com/windows2000/library/howitworks/default.asp

Windows 2000 Server Documentation, Kerberos v5 Authentication – Microsoft. http://www.windows.com/windows2000/en/server/help/sag_SEconceptsUnAuthKerb.htm

Windows 2000 Server Documentation, Mapping Certificates to User Accounts – Microsoft. http://www.microsoft.com/windows2000/en/server/help/sag_cs_certmapaccounts.htm

Sources for Further Study

Kerberos: The Network Authentication Protocol – MIT Web site http://web.mit.edu/kerberos/www/

"Step-by-Step guide to Kerberos 5 Interoperability." Microsoft Windows 2000 Web Site, December 2000. http://www.microsoft.com/WINDOWS2000/library/planning/security/kerbsteps.asp

"Step-by-Step guide to using the Security Configuration Tool." Microsoft Technet, 2000. http://www.microsoft.com/TechNet/win2000/seconfig.asp

"Windows 2000 Certificate Services." Microsoft Technet. March 2000. http://www.microsoft.com/TechNet/win2000/2000cert.asp