Global Information Assurance Certification Paper

Kerberos – Windows 2000 Authentication
MWC MBUS 543 / GIAC Windows Security
Practical Option 1 – Windows 2000 Security
Robert C. Ashworth (ashwort002)

Background

The original "Kerberos" was the mythical ferocious 3-headed dog that guarded the entrance to Hades (gates of the Underworld) from anyone who was not authorized entry (except for Heracles (Hercules) who on at least one occasion found a "vulnerability" and gained entrance), all according to Greek Mythology.

The authentication protocol of the same name was created at Massachusetts Institute of Technology by the Project Athena" engineers. It was aptly labeled after the mythical ferocious beast to signify the protection of server files through proper authentication, and the three heads represented by the three sub-protocols explained herein. Network authentication is simply a method to verify that the person or process requesting access to a system, service, or network is actually who they have indicated they are. Authorization is the process of ensuring that the authenticated user or process has pre-determined permission to access the file or service (object) that he, she, or it is attempting to access. Kerberos was developed to provide a very secure, interactive, real-time service to provide such user authentication and to pass (not provide) object access authorization. It is a much more definitive method of ensuring confidentiality than trusting the network access policy rules are abided by in individual users. More specifically, the Kerberos protocol was created to provide a high degree of assurance for secure transactions between the authenticated and authorized user and the object that the user requires without interception, masquerading, or other compromise that might mitigate the confidentiality or integrity of the transaction. This results in valid protection from not only the outside attacker, but the insider as well. The first publicly available version of the protocol was version 4. The Windows 2000 implementation of Kerberos is the most recent available, version 5, became available to with updated features to counteract Denial of Service and buffer overrun vulnerabilities that were reported through the public availability and thus testing-under-fire within the industry and educational circles. Version 5 was formally released by the Internet Engineering Task Force in Request-for-Comment 1510[14] in September 1993.

Kerberos Components – The "Key" Pieces

The Kerberos Key Distribution Center is the core of Kerberos. It is implemented as a network service standardized in the Internet Engineering Task Force (IETF) Request For Comments 1510[14] and is made up of the Authentication Service and the Ticket-Granting Service, and contains the "Active Directory" account database and primary Key Database. Every Domain Controller has a Kerberos Key Distribution Center. This Center acts on behalf of (issues tickets for) its domain, only. However, can also act in coordination with other remote domains to permit its clients access to the Center's resources. It may also control slave Key servers to lighten its load. It receives authentication requests from the clients and validates their identities through the Authentication Service, and grants tickets from the Ticket-Granting Service. In support of these services, the sub-protocols that act within the Kerberos service are the Authentication Server Exchange, the Ticket-Granting Service Exchange, and the Client/Server Authentication Exchange. The Key Database can include replicas or slave servers to assist in the administration of the Kerberos domain.

Ticket information in detail can be located in the IETF Request for Comments 1510. For further elucidation of the Kerberos protocol, the ticket contents require some summarization. All but the first three fields in a ticket are not encrypted. These unencrypted "header" fields allow the cache to be managed by the host, as the clients do need to understand some things about each ticket for cache management. The dissected fields of a Kerberos ticket are as follows[9]:

- Tkt-vno: (plaintext) is the ticket format (Kerberos) version number.
- Realm: (plaintext) is the name of the domain that granted the ticket to the client.
- Sname: (plaintext) is the server's name.
- Flags: (ciphertext) provides ticket options
  - Forwardable – Notifies ticket-granting service it is free to issue new Ticket-Granting Ticket.
  - Forwarded – Indicates Ticket-Granting Ticket has been forwarded or a ticket was issued from a forwarded Ticket-Granting Ticket.
  - Proxiable – Notifies the ticket-granting service that it can issue tickets with a different network address than that in the Ticket-Granting Ticket.
  - Proxy – Identifies that the address in the ticket is different from that in the Ticket-Granting Ticket.
  - Renewable – Used to ensure periodic update to long-lived tickets.

    - Initial – Identifies this ticket as a Ticket-Granting Ticket.
    - Invalid – Ticket is not valid, requiring server rejection.
- Key: (ciphertext) Session key.
- Crealm: (ciphertext) Domain name
- Cname: (ciphertext) Client's name
- Transited: (ciphertext) List of Kerberos domains that were involved in the ticket's client-authentication.
- Authtime: (ciphertext) Timestamp for the client's Ticket-Granting Ticket's authentication.
- Starttime: (ciphertext) Valid ticket start time.
- Endtime: (ciphertext) Ticket's expiration timestamp.
- Renew-till: (ciphertext) Maximum endtime for a ticket with a "Renewable" Flag set.
- Caddr: (ciphertext) Addresses that can use the ticket. If not set, then the ticket can be used from any address.
- Authorization-data: (ciphertext) Client rights or privilege attributes.

There are various utilities that are defined in Request For Comments 1510 for interoperable use in all Kerberos implementations. However, Microsoft has added two more utilities that are added to the originals in the Windows 2000 implementation. The pertinent utilities are summarized below.[8][10]

- The Kadmin utility is used by Kerberos for the update of account entries in the Key Database. It ensures that mirrored slave servers to the KDC are updated with ticket information. This utility is not in the Kerberos standard.

- The Kprop utility is used to update the replica Key databases with the primary at the Key Distribution Center. This utility is not in the Kerberos standard.

- The Kinit utility is used to log into Kerberos within the domain. Upon successful authentication, the Ticket-Granting Ticket is granted. This can be an automatically instigated utility within the user logon script, allowing transparent and automatic authentication within the domain.

- Ktpass is the utility allowing Kerberos administrators to set the password, maps accounts and sets up the account on the host.

- Kpasswd is the utility allowing Kerberos users to change passwords. This utility is not in the Kerberos standard.

- The Ksetup utility allows the System Administrator to configure Kerberos domains, the Key Distribution Center, and the "Kpasswd" servers.

- The Klist is the utility that is used to display the granted keys from the credential cache.

- Kdestroy is the utility that allows the user to irrevocably delete the credential cache upon termination of need for it. This utility is useful to preclude the cache from being reused by an unauthorized user. This may be an automatically called utility when invoking the logout script for transparent and automatic security initiation. (After using Kdestroy, executing Klist can verify that the destruction of the keys in the cache is complete.)

How Kerberos Works

Kerberos is a "trusted third party authentication system" which allows clients and servers to authenticate and communicate securely via their mutual trust in the authentication service provided by the Kerberos protocol over an essentially untrusted network. It uses an exchange (handshake) process and subsequent validation of symmetric encryption keys and, once validated, searches through the authenticated user profile to know what systems the user may access. Thereby, when a user requests access to an object, the Kerberos service process can not only validate the user but also can pass information of granted access to an object. If the access-control mechanism's review of the user's profile is supported by the object's controller's access control list and comparison indicates that the user is authorized then access that object is granted. The user must use a strong password for authentication. Authentication to the domain does not imply authorization to access any particular file or service; that part of the protocol encompasses the authorization-passing phase of the overall process through coordination with other native or third-party (as dictated by the domain security policy) authorization mechanisms.

All implementations of Kerberos support Digital Encryption System (DES) with Cipher Block Chaining (CBC) and RSA Message Digest - 5 (MD5) or the simple Cyclic Redundancy Check – 32 mechanism. This researcher has seen the Triple-DES implemented which increases security at the cost of overhead processing cycles (ultimately, speed). The unavailability of MD4 Kerberos

option in Windows 2000 implementation is understandable as MD5 is well-known as a more secure hash algorithm of the same result length (128-bit).

There are three important services, or sub-protocols, in the Kerberos authentication and authorization process included in the Kerberos protocol, the Authentication Server Exchange, the Ticket Granting Service Exchange, and the Client/Server Authentication Exchange (the three heads of the mythical Kerberos guard-dog)[4]. The authentication process is valid for a client and a server (or for two servers). The main Kerberos coordination center is the Key Distribution Center service, which has the database of user keys for client or server validation and is composed of the Authentication Service and the Ticket-Granting Service. The general process of how a client (or server) is authenticated is graphically summarized in Figure 1 and described in more lucid detail, using input from many of the listed references, below the figure.

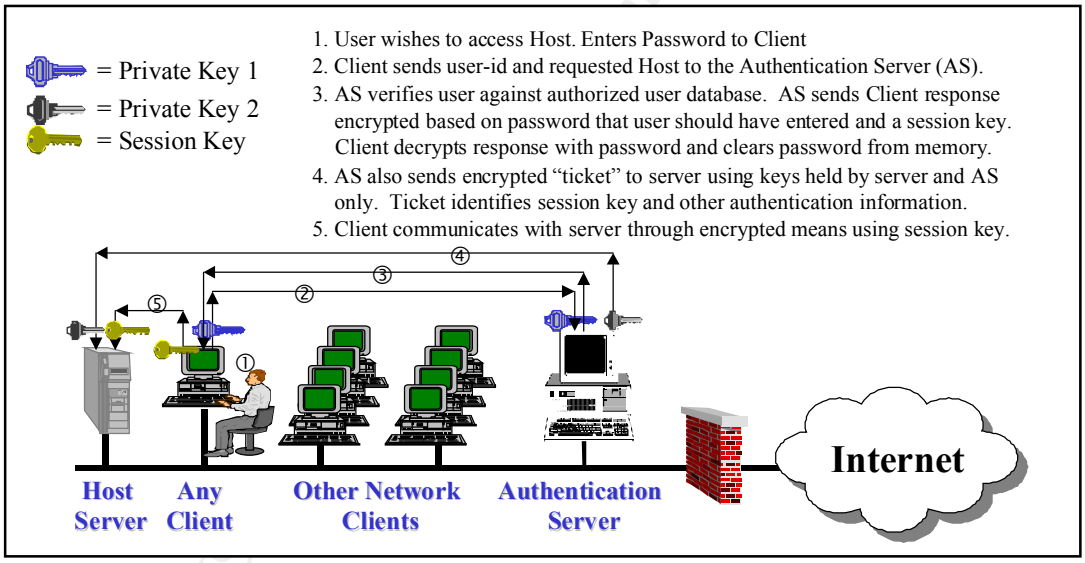

Figure 1

a) The process begins when the user logs on by entering their UserID and password, as in any other interactive logon process. Native logon processes may be used.
b) The Kerberos client software initiates the first part of the handshake by encrypting this information with a pre-determined user key and other network authentication configuration information, and sends the result, the "Kerberos Authentication Server Request", to the Kerberos Authentication Service.

c) This Authentication Server Request identifies the client to the Key Distribution Center, which in turn searches and retrieves the user's long-term key from the user's record in the database. The message is evaluated for authenticity by looking up the client information in the Key Distribution Center database, and decrypting and validating the time stamp. The user is then verified by the Key Distribution Center by comparing the hashes of the password as sent and a hash of the retrieved password. The user's password (MD5) hash, stored in the Active Directory so that the process doesn't need to be repeated at any time during the logon session, and the hash is then used as an initial encryption key between the Key Distribution Center and the client.
d) If the client input appears genuine, then the Authentication Server replies to the client and includes a "ticket" in an encapsulated encrypted transmission. It sends a "Ticket-Granting Ticket" (kind-of a Ticket-to-Get-Tickets), valid for the local domain, that only the Ticket Granting System can decrypt. This main use of this initial ticket is to access the Ticket Granting Service that checks requests against, and holds, the profile or access control list to authorize user access to servers or files. The policy default "time-to-live" for the Ticket-Granting Ticket is 10 hours, and may be renewed during the user's session. In addition, it also sends another key, known as the "session key", encrypted with the user's password hash for further communication with the Key Distribution center, and used to maintain the authentication during the online session.
e) Using the Ticket-Granting Ticket, the client requests access to whatever server they need access to for a file (object) by submitting the request with the Ticket-Granting Ticket to the Ticket Granting System. Once the destination authenticates this request, and ensures authorization, it creates a ticket and session key (service ticket) for the client and requested server for their communication. The client can the use this "service ticket" to authenticate to the requested server.
f) The server will decrypt the information sent to it by the Ticket-Granting System about the authentication of the user using its pre-established symmetric key with the Key Distribution Center. The service ticket then provides the server information to authenticate the user.
g) Without the ability to view the contents, the client still uses the server portion of the server ticket to authenticate to the server. Upon mutual authentication, the server returns a time stamp encrypted

using the service ticket as the session key. Non-repudiation is verified if the client can then decrypt the time stamp correctly.

h) The client will use the session key to request access to the server. The request includes an Authenticator encrypted using the session key, which the server can decrypt with its copy of the session key, obtained from the Ticket-Granting System. In return, the server authenticates to the client for full non-repudiation. Upon mutual authentication, the application service session begins, and data can be encrypted between server and client using the session key.

Windows 2000 Implementation

Users must have a Windows 2000 user account in the Active Directory for successful log on to the domain in the Windows 2000 security environment. In Windows 2000, the domain may implement Windows NT LAN Manager (NTLM) version 2 as the authentication method for domain environments that include other operating systems. This would allow clients to log into services with local credentials. This is not the most secure (preferred) method. If Kerberos is available as the domain authentication process, then it is the method that must be used by all.

Kerberos version 5 comes bundled with Windows 2000 as an integral part of the Active Directory implementations. To deliver the security that Kerberos provides during network implementation requires rigorous understanding of not only the basics of how Kerberos works, but the technical details of its structure within Windows 2000[20]. Although there was a Kerberos Version 4 implementation for NT, the version 5 Windows 2000 implementation is not compatible with version 4, however, it is compliant with Internet Task Force Request for Comments 1964 and 1510 (Reference 14). Systems Administrators should also install "kerbtray" from the *Windows 2000 Server Resource Kit* utility to indicate what Kerberos tickets a Windows 2000 client has. The Kerbtray icon is displayed in the system tray on the lower right of the Windows Desktop computer screen. Its options include listing and purging tickets. The first ticket in the list is the Ticket-Granting Ticket, and the session tickets immediately follow the Ticket-Granting Ticket. "NetDom" is the other Kerberos administration utility. Also available from the *Windows 2000 Server Resource Kit*, it provides a method of determining the available domain servers and trusts[5].

The Windows 2000 implementation Kerberos provides a unique added feature to standard Kerberos version 5 through the allowance of public key

certificates rather than limiting implementation to the standard use of shared synchronous keys. This implementation is ideal for DoD and other security features of adding a token to the authentication process in the form of state-of-the-art smart-cards[9], as well as for "IPSec" implementation[12]. As a side note, Windows 2000 services provide their own security initiatives when accessing resources for themselves[9].

Within the Windows 2000 domain, Kerberos policy is implemented by System Administrators' feature configuration of the Key Distribution Center. Policy data is stored in Active Directory under the domain security policy attributes. Policies can be viewed or modified by starting the Microsoft Management Console and access the "Default Domain Policy", then, follow the path: "Computer Settings", "Windows Settings", "Security Settings", "Account Policies", and "Kerberos Policy." The names of the five policies summarize their purposes. The following are these policies that may be set, and their defaults[4]:

- Enforce User Logon Restrictions: This policy option allows the KDC to review user permissions to ensure the user is valid, and to verify requisite permissions upon client request to access a particular computer. Activation of this policy provides strong security, but operationally adds delay to the access process. Its default setting is "enabled".

- Maximum Lifetime That a User Ticket Can Be Renewed: This policy allows the setting of a ticket maximum life-span, with a default of 7 days.

- Maximum Service Ticket Lifetime: Allows setting the life of a session ticket. Such settings are a minimum of 10 minutes and less than the setting in the previous policy (above). The default for this policy is set for 10 hours.

- Maximum Tolerance for Synchronization of Computer Clocks: Provides a tolerance level in minutes between the Key Distribution Center clock and that of the Kerberos client to protect against "replay attacks" (an attacker re-sending the same packet that was sniffed from the network again any number of times). If the difference between the clocks exceeds the setting of this policy, then the client is not permitted the requested tickets. The default for this policy is 5 minutes.

- Maximum User Ticket Lifetime: This policy sets the maximum life span for the Ticket-Granting Tickets issued. The default for this policy is 10 hours.

Advantages of Windows 2000 Kerberos Implementation

Beginning in Windows NT Service Pack 4, the LMCompatabilityLevel registry key was added for enhancement of security authentication using NT LAN Manager. This key can be set to only permitting version 2, which limits backward computability with authentication. However, as noted herein, the Kerberos implementation in Windows 2000 also is not backward-compatible with version 4 in order to preclude the vulnerabilities to that version.

Windows NT and 9x provide an authentication method known as "Challenge-Response". It has been available in previous versions of Windows through a few authentication implementations that are still available. The Challenge-Response authentication methodology has been used in the earlier versions of Windows remote access primarily through use of the "Challenge-Handshake Authentication Protocol" (CHAP) as described in IETF Requests for comments numbers 1994 and 2433, the latter being Microsoft's own modified release. In this methodology, the client requests access to a principal (server) for an object or service. The server (authenticator) checks on the user's profile and does not trust, yet. It sends the requesting client an arbitrary string of characters (challenge). Depending on the configuration, the client uses the password and the arbitrary string, or just the string, and hashes this. It then sends the hashed result to the server. The server pulls the password (if it is using this as part of the message content) and combines the arbitrary string and hashes the combination. If the server's hash matches what the client sent, then the user's password is relatively securely validated and the client is authenticated. Authentication is one-way but this process can be performed in the other direction for mutual authentication.[12] Windows 2000 has this capability, and uses the Message Digest 5 hash algorithm. This is a relatively secure method, particularly when embedding the password which does not traverse over the untrusted network. However, although part of the CHAP protocol is the understanding that the session can be hijacked, for a time, because periodically, the server re-authenticates the client. Additionally, a problem with CHAP is that the authentication profile database is maintained by the server, unencrypted. Therefore, if the authenticating server's access security features are compromised, for example by an insider, then the result is a compromised database.

Besides remote access methods, local authentication has also been available using this methodology, originally through LAN Manager Challenge and Response Protocol. This effort, originally an IBM and Microsoft joint endeavor, is based on normal ASCII characters in upper case. Lower case letters are automatically converted to upper case. It was available to Windows 95 and 98 clients to authenticate to LAN Manager (early 1990's NT precursor) servers. The client is provided the 16-byte with a 16-byte LAN Manager One-way function password that upon performing a one-way hash by the client produces a 24-bit hash which is sent back to the server for comparison and client authentication[12]. However, passwords using this methodology were found to be crack-able.

The LAN Manager Challenge and Response Protocol was found not to be very robust, and thus led to NT LAN Manager (NTLM) when Windows NT materialized. This provided a more robust encryption and hashing scheme. However, for backward compatibility while the robust NTLM hashes were the predominant part of the transmissions, the LAN Manager Challenge and Response hashes were also sent so that Windows 95 and 98 workstations could be brought into the mix. This meant that once again, the passwords were crack-able, the same way as before through the LAN Manager hashes[12].

Then, upon release of NT Service Pack 4, NTLM version 2 was released, which was an even more robust challenge and response mechanism (with large 128-bit keys). This implementation must be configured both at the server and at the clients prior to its being available for negotiation between the two. Because the Windows 95, 98, and native NT clients can't use Kerberos, this becomes the authentication mechanism of choice for domains with these workstations. However, as noted above, each client and server must be appropriately configured to use and accept NTLM version 2. The new Active Directory client scheduled for release with NT Service Pack 7 will enable the use of NTLM version 2 authentication for clients, even for Windows 95, and 98 via the "Lightweight Directory Access Protocol (LDAP) version 3 which is available to Windows 2000 computers now[12].

Windows 2000 has the capability to use various services for managing user authentication, including Remote Authentication dial-in User Service (RADIUS), NT LAN Manager, LAN Manager, and Secure Sockets Layer/Transport Security Layer.

The default and primary authentication method for Windows 2000 is, of course, Kerberos version 5[12]. However, NT LAN Manager is the primary

authentication protocol that comes with combination Windows NT and Windows 2000 work group environments. Windows 2000 comes with implemented security support provider dynamic link library files for Kerberos, and also for NT LAN Manager[9]. NT LAN Manager It is available for use when there is a network domain of NT and Windows 2000 servers. However, when the domain is Windows 2000, then Kerberos is the default authentication service[20].

In contrast, default authentication methods are defined in Windows 2000 Security[12] for Windows operating systems in the following table, note that even in a fully Windows 2000 domain, there is the possibility of requiring "NT LAN Manager".

Client	***Server***	***Default Method***
Win 2000	Win 2000	Kerberos (NTLM as backup)
Win 2000	Win NT	NTLM
Win NT	Win NT	NTLM (or NTLM v2)
Win NT	Win 2000	NTLM (or NTLM v2)
Win 95/98/Me	Win NT	LAN Manager
Win 95/98/Me	Win 2000	LAN Manager

Similar to Challenge-Response, there are third-party token-based one-time password generators that are synchronized with the authentication server. The passwords, seemingly random characters, but totally in synch with the server, change once each minute for each user! This allows the user the one-minute timeframe to log on using that password. This method ensures that an attacker who sniffs the password from the untrusted network cannot use the password to gain access at a future date. Implementations for the user's token are seldom on the personal computer itself, to ensure that theft of the computer does not compromise the organizational network. Instead, they have Palmpilot implementations but primarily use small tokens that the user maintains on a chain or in their wallet. A primary vendor example of this method is "SecureID". Problems with this method begin with the understanding many users will forget to bring or will lose the token upon occasion; these issues and that battery loss at crucial periods (e.g., when the report is due) can result in denial of service. Finally, the authentication server and the token must maintain perfect synchronization, clock differences over time reduce the window of opportunity to log on as the server's acceptable password for the one-minute period varies more and more from that displayed for the one-minute by the token.

The Massachusetts Institute of Technology did develop an early version of Kerberos for the Windows environment ("Kerberos for Windows") that is

available for download at http://web.mit.edu/network/kerberos-form.html, including the installer, binaries and the source code. Kerberos 4 and 5 are available for to run on Intel platforms with the Windows NT operating system, as well as Windows 95 and 98. Although this is an authentication and authorization option, there are various other competing technologies for Windows operating systems that predate Windows 2000. It should be noted that Kerberos version 4 implementation available to Windows NT is not compatible with the Windows 2000 implementation because of version 4 vulnerabilities.

The Kerberos protocol has been tested for over a decade, and provides a more flexible and secure authentication solution than the Challenge and Response and other less robust methodologies that are available in older Windows operating systems. The benefits of this new authentication mechanism to Microsoft operating systems were primarily obtained from the Windows 2000 Authentication white paper[9], the Windows 2000 Interoperability white paper[10], and Windows 2000 Security[12] and are provided below.

- Network security is improved. Committed Kerberos implementation in the distributed network environment provides more robust identity verification than previous methods, such as Challenge/Response.

- Network performance and scalability is improved because the domain controllers are not responsible for the authentication and authorization overhead. The alleviation of the bottlenecks that were present in NT allows the support of more users and higher-bandwidth services processes due to speedier throughput.

- Under NTLM, the server authenticates a client by contacting the domain controller. Under Kerberos authentication mechanism, such authentication occurred between the client and the Key Management Center, and the session key for the server is all that the server or the client require for verification of the identity of the user by the server. Once the ticket to the server has been obtained, they maintain their electronic ticket stub throughout the logon session, allowing them to re-access the same server by providing the session ticket.

- The two-way transitive trust relationship is simplified and maintained within the Kerberos protocol. Full non-repudiation (mutual authentication) is obtained as the clients and the servers validate

each other during the initial handshake of the communication session. Under NTLM this was not the case, and while the servers validated the clients, the clients were not able to verify the identity of the servers.

- The Kerberos implementation ensures that the ticket cache resides in protected volatile memory, and is never paged to disk.

- Authentication can cross Windows 2000 domains by sharing an inter-domain key, through registration of each with the Key Distribution Center Ticket-Granting Service of the other.

- Certain Internet services, many of which are available in Windows environments, can act as proxy, in service to the client and as the client, then pass the information to the client. Both Kerberos and NTLM can act as a client locally. However, the Kerberos protocol alone has the feature to act as the client when connecting to other services.

- Kerberos provides centralized trust management hierarchy for the network, instead of dealing with numerous trust relationships.

- Kerberos roots are with portable Unix-based operating systems. Kerberos version 5 is fully compatible with other Kerberos version 5 authentication implementations, thereby providing enhanced interoperability within the context of the Internet Engineering Task Force Request for Comments number 1510 [14]. However, Windows 2000 encryption choices that permit compatibility with standard Kerberos are limited to two[8]. Regardless, implementation is very possible through Kerberos version 5 between servers and clients in a domain that are non-Windows and Windows, as long as Kerberos version 5 standard is available to them all.

Security Issues with Windows 2000 Kerberos

Technology that is not perfectly protected (and besides turning a machine off, even is standalone mode, cannot be guaranteed) is vulnerable, even if the risk is remote. However, just as Heracles found a vulnerability in the original legendary Kerberos, the technology of the same name can also be thwarted by varying known means, depending of the configuration and implementation, and of course, there is the potential of unknown vulnerabilities, as well. Authentication that is intended to truly protect the

organization's assets from unauthorized accesses must be relatively strong to ensure that it does more than keep accidental or rudimentary unauthorized access attempts at bay. It must be strong such that it is extremely difficult for even the most clever of hackers from circumventing the safeguards. The system employed must be carefully engineered and well tested to mitigate the number and impacts from potential vulnerabilities to the process. It should be noted that in the IETF Request for Comments 1510[14] that environmental assumptions were provided in the beginning of the document that stressed that such issues as Denial of Service and Password Guessing are not solved with Kerberos. It also relies on the "Principals" (servers) to keep their own private keys secure.

- Strong passwords are a necessity because an attacker who intercepts the encrypted transmission of the password may use a dictionary attack method to gain credential information from the victim user for eventual use in masquerading [18][19].

- To support applications that cannot use the Kerberos security features, there is an account option "Do not require Kerberos".

- CERT Coordination Center Advisory CA-2000-11 identifies a Denial of Service vulnerability with Kerberos version 5 with the features for backward-compatibility to version 4. However, in that the Widows 2000 implementation is not backward compatible, this vulnerability has been resolved.

- An early security issue existed regarding the inability of Kerberos packets to be secured in transit by IPSec due to the design of the packets. This issue has been resolved in the available Windows 2000 Service Pack (SP-1) in combination with a registry modification to provide IPSec protection to Kerberos traffic on domain controllers.

- IIS is fully integrated with the Kerberos v5 authentication protocol implemented in Microsoft Windows 2000, allowing the system to pass authentication credentials among connected computers running Windows.

- Workstations running Windows 95 or Windows 98 do not have the advanced security features required to be included in the secure authentication within a Windows 2000 domain[11].

- The Key Distribution Center does not support post-dated tickets[8].

- All accounts that are upgraded in a new domain require a password change before standard non-Windows Kerberos clients can use them.

Conclusion

This paper has brought together the best available references to provide a concise description of the Kerberos authentication protocol and to further describe its implementation in Windows 2000. It explains that Kerberos provides an outstanding and time-tested methodology for authentication and authorization. The overhead that it creates through its long series of coordination messages to obtain tickets, whether the initial Ticket-Granting Ticket or session tickets, are justified by both the overhead that is alleviated from the primary domain servers and the security that is provided to the domain. Its process is based on solid foundations, and Kerberos version 5 implementation 1.2 and above have eliminated dangerous known vulnerabilities to the security of the authentication. The inherent value-added to the security it provides to the domain will be in the interoperability of this authentication scheme with Unix-based add-on compatible Kerberos implementations. The research for this paper was certainly an education for me.

References

(1) Anonymous. "Q102716 – User Authentication with Windows NT." 25 October 2000,
URL: support.microsoft.com/support/kb/articles/Q102/7/16.asp, 2001

(2) Anonymous. "Q147706 – How to Disable LM Authentication on Windows NT." 1 March 2001, URL:
support.microsoft.com/support/kb/articles/Q147/7/06.asp, 2001

(3) Anonymous, "Q217098 – Basic Overview of Kerberos User Authentication Protocol in Windows", 29 December 1999, URL:
support.microsoft.com/support/kb/articles/Q127/0/98.asp, 2001

(4) Anonymous, "Q231849 – Description of Kerberos Policies in Windows 2000", URL: support.microsoft.com/support/kb/articles/Q231/8/49.asp, 2001

(5) Anonymous, "Q232179 - Kerberos Administration in Windows", URL: support.microsoft.com/support/kb/articles/Q231/1/79.asp, 2001

(6) Anonymous. "Q239869 – How to Enable NTLM Authentication for Windows 95/98/2000 and NT." 1 March 2001, URL: support.microsoft.com/support/kb/articles/Q239/8/69.asp, 2001

(7) Anonymous. "Q254728 – IPSec Does Not Secure Kerberos Traffic Between Domain Controllers". 15 November 2000, URL: support.microsoft.com/support/kb/articles/Q254/47/28.asp, 2001

(8) Anonymous, "Step-by-Step Guide to Kerberos 5 (krb5 1.0) Interoperability", 10 January 2000, URL: www.microsoft.com/Windows2000/library/planning/security/kerbsteps.asp

(9) Anonymous, "Windows 2000 Kerberos Authentication", 9 July 1999, URL: www.microsoft.com/Windows2000/library/howitworks/security/kerberos.asp

(10) Anonymous, "Windows 2000 Kerberos Interoperability", 11 November 1999, URL: www.microsoft.com/Windows2000/library/howitworks/security/kerbinit.asp

(11) Anonymous, "Windows 2000 Security Technical Overview", 30 August 2000, URL: www.microsoft.com/technet/win2000/win2ksrv/sectech.asp

(12) Bragg, R., Windows 2000 Security, New Riders Publishing, Indianapolis, IN 46290. (2001)

(13) Brezak, J., "Interoperability with Microsoft Windows 2000 Active Directory and Kerberos Services", February 2000, URL: msdn.microsoft.com/library/techart/kerberossamp.htm

(14) Kohl, J. and Neuman, C., "RFC 1510, The Kerberos Network Authentication Service (V5)." September 1993, URL: http://www.ietf.org/rfc/rfc1510.txt.

(15) Malmgren R ., "NT Security - Frequently Asked Questions version 0.41", http://www.it.kth.se/~rom/ntsec.html, (1997)

(16) Neuman, C., "Kerberos: The Network Authentication Protocol", 9 December 2000, URL: http://web.mit.edu/kerberos/www/#what_is

(17) Neuman, C., "Kerberos 5 Release 1.2", 28 February 2001, URL: http://web.mit.edu/kerberos/www/krb5-1.2/index.html

(18) Neuman, C. and Ts'o, T., Kerberos: An Authentication Service for Computer Networks, IEEE Communications, 32(9):33-38. September 1994. URL: http://www.isi.edu/gost/publications/kerberos-neuman-tso.html

(19) Tung, B. "The Moron's Guide to Kerberos, Version 1.2.2", 19 December 1996. URL: http://www.isi.edu/gost/brian/security/kerberos.html#whatis

(20) Walla, M., "Kerberos Explained", 22 June 2000, URL: www.microsoft.com/technet/win2000/kerberos.asp (2000)