Kerberos Enhancements

2 out of 3 rated this helpful - Rate this topic

Updated: February 20, 2009

Overview

Microsoft's implementation of the Kerberos authentication protocol in Windows Vista and Windows Server 2008 includes the following features:

- AES support
- Improved security for Kerberos Key Distribution Centers (KDCs) located on branch office domain controllers

AES

This Windows Vista and Windows Server 2008 security enhancement enables the use of AES 128 and AES 256 encryption with the Kerberos authentication protocol. This enhancement includes the following changes from Windows XP:

- **AES support for the base Kerberos authentication protocol**. The base Kerberos protocol in Windows Vista supports AES for encryption of ticket-granting tickets (TGTs), service tickets, and session keys.
- **AES support for the Generic Security Service (GSS)-Kerberos mechanism**. In addition to enabling AES for the base protocol, GSS messages (which conduct client/server communications in Windows Vista) are protected with AES.

Requirements

All Kerberos authentication requests involve three different parties: the client requesting a connection, the server that will provide the requested data, and the Kerberos KDC that provides the keys that are used to protect the various messages.

This discussion focuses on how AES can be used to protect these Kerberos authentication protocol messages and data structures that are exchanged among the three parties. Typically, when the parties are operating systems running Windows Vista or Windows Server 2008, the exchange will use AES. However, if one of the parties is an operating system running Windows 2000 Professional, Windows 2000 Server, Windows XP, or Windows Server 2003, the exchange will not use AES. The specific exchanges are:

- **TGT.** The TGT is created by the KDC and sent to the client if authentication to the KDC succeeds.
- **Service ticket.** A service ticket is the data created by the KDC, which is provided to the client and then sent by the client to the server to establish authentication of the client.
- **AS-REQ/REP.** The authentication service request/response (AS-REQ/REP) exchange is the Kerberos TGT request and reply messages sent to the KDC from the client. If the exchange is successful, the client is provided with a TGT.
- **TGS-REQ/REP.** The ticket-granting service request/response (TGS-REQ/REP) exchange is the Kerberos service ticket request and reply messages that are sent to the KDC from the client when it is instructed to obtain a service ticket for a server.
- **GSS.** The Generic Security Service application programming interface (GSS-API) and the Generic Security Service Negotiate Support Provider (GSS-SPNEGO) mechanisms negotiate a secure context for sending and receiving messages between the client and server by using key material derived from the previous ticket exchanges.

The following table shows whether AES is used in each exchange for different combinations of Windows operating systems.

Usage of AES with different Windows operating systems

Client	Server	KDC	Ticket/Message encryption
Operating systems earlier than Windows Vista	Operating systems earlier than Windows Server 2008	Windows Server 2008	TGT might be encrypted with AES based on policy
Operating systems earlier than Windows Vista	Windows Server 2008	Windows Server 2008	Service ticket encrypted with AES
Windows Vista	Windows Server 2008	Windows Server 2008	All tickets and GSS encrypted with AES
Windows Vista	Windows Server 2008	Operating systems earlier than Windows Server 2008	GSS encrypted with AES
Windows Vista	Operating systems earlier than Windows Server 2008	Windows Server 2008	AS-REQ/REP and TGS-REQ/REP encrypted with AES
Operating systems earlier than Windows Vista	Windows Server 2008	Operating systems earlier than Windows Server 2008	No AES
Windows Vista	Operating systems earlier than Windows	Operating systems earlier than Windows	No AES

	Server 2008	Server 2008	
Operating systems earlier than Windows Vista	Operating systems earlier than Windows Server 2008	Operating systems earlier than Windows Server 2008	No AES

There are three factors that contribute to the difference in logon times between Windows Server 2003 and Windows Server 2008:

- Windows Server 2008 now uses AES 256 encryption for Kerberos where possible. Therefore, it generates an additional AES 256 hash.
- Windows Server 2008 can use AES 128 encryption for Kerberos. Therefore, it generates an additional AES 128 hash.
- Windows Server 2008 now uses Password-Based Key Derivation Function (PBKDF2) to protect cached logon information.

These changes account for the differences in logon times, and they are by design. The following table lists the multiplier that you can use to estimate the time that is required to authenticate an interactive or network logon using the new encryption algorithms compared to Windows Server 2003 using NTLM.

Protocol	Multiplier compared to Windows Server 2003 logon using NTLM
AES 128	2
AES 256 (Default for noncached logons)	4
PBKDF2 (Default for cached logons)	5

The more secure algorithms proportionally increase the time that is required to authenticate an interactive or network logon. The time that is required to run logon scripts or load user profiles or the user desktop is not affected. Typically, individual users will not notice the additional authentication time. The difference is observable when benchmarking tools are used to compare interactive and network logon throughput between Windows Server 2008 domain controllers and Windows Server 2003 domain controllers

Read-only domain controller and Kerberos authentication

Windows Vista includes new Kerberos authentication protocol features to further protect a Windows Server 2008 domain controller that is physically located in a branch office. With the read-only domain controller (RODC), the KDC issues TGTs to branch users only and forwards other requests to the hub domain controller.

In the Windows implementation, the keys used to create TGTs are derived from the password of the **krbtgt** account. This account and its password are typically replicated to every domain controller in the domain. In the branch office scenario, the risk of theft or unauthorized access to the local domain controller—and therefore the security of the **krbtgt** account—is typically greater. To mitigate this risk, the RODC has a unique **krbtgt** account that does not have all of the capabilities of a standard **krbtgt** account on a standard domain controller. If the RODC is compromised, the scope of the breach in regards to the **krbtgt** account information is limited to that RODC, not the other KDCs.