msDS-SupportedEncryptionTypes – Episode 1 - Computer accounts

Introduction

In order to be concise with this article, I need to assume that the reader is familiar with Kerberos and Active Directory.

If not, then I can quickly think of two scenarios:

1) Your favorite search engine (Bing, in my case) took you here as a misunderstanding.
2) You came because you stumbled upon the name "msDS-SupportedEncryptionTypes" somewhere and you really, really want to understand what it is related to, even if you need to learn about Kerberos and Active Directory as a pre-requisite.

Let's assume (for the sake of the posting) that the option you fall into is #2 and that you are eager to know where to find the documents that are applicable to this article.

Here are the links:

Encryption and Checksum Specifications for Kerberos 5: http://www.ietf.org/rfc/rfc3961.txt
The Kerberos Network Authentication Service (V5): http://www.ietf.org/rfc/rfc4120.txt

[MS-ADA2]: Active Directory Schema Attributes M: http://msdn.microsoft.com/en-us/library/cc220154.aspx
[MS-ADA3]: Active Directory Schema Attributes N-Z: http://msdn.microsoft.com/en-us/library/cc220699.aspx
[MS-ADTS]: Active Directory Technical Specification: http://msdn.microsoft.com/en-us/library/cc223122.aspx
[MS-KILE]: Kerberos Protocol Extensions: http://msdn.microsoft.com/en-us/library/cc233855.aspx

ADS_USER_FLAG_ENUM Enumeration: http://msdn.microsoft.com/en-us/library/aa772300(VS.85).aspx

Also, please note the attachment to this blog (msDS-SupportedEncryptionTypes-Network_Captures.zip) contains Wireshark tcpdump (.pcap) captures for Windows clients (Windows 2000 through Windows 7 joining a Windows 2008 R2 domain.

Juicy information

In order for the KDC to be able to generate tickets that the target server can read, there has to be some mean of communicating what type of encryptions the involved actors can understand.

For quite a while, that was not an issue because the older versions of Windows that had Kerberos5 implementations (Windows 2000 all flavors, Windows XP and Windows 2003 all flavors) only supported DES (RFC3961) and RC4 (RFC4757) as the methods of encryption.

However, Windows Vista, Windows Server 2008, Windows 7 and Windows Server 2008 R2 incorporated the newer and more secure algorithm AES (RFC3962) (128 AND 256). With this new addition, and with so many machines running previous versions of Windows, it was imperative to have a way to inform which algorithms each particular account could handle and to make sure that when newer algorithms should become available they would not necessarily represent many changes.

msDS-SupportedEncryptionTypes came up as the solution. This AD attribute (defined in MS-ADA2, section 2.324) is present in the Computer, User and Trust objects for Schema version 44 (Windows 2008) and later. Its sole purpose is to hold the values of the encryption types that the account owner supports.

Well, I guess that you could have deducted that from the name of the attribute so; I better go a little deeper.

Its size is 4 bytes, its type is Unsigned Integer, and its format is a Bit Mask. The values that it can accept are defined in the following table (and originally in MS-KILE section 2.2.5 Supported Encryption Types Bit Flags):

0	1	2	3	4	5	6	7	8	9	10	1	2	3	4	5	6	7	8	9	20	1	2	3	4	5	6	7	8	9	30	1
0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	E	D	C	B	A

Where the bits are defined as:

[MS-KILE] 2.2.5 Supported Encryption Types Bit Flags	[MS-ADTS] 7.1.6.7.3 msDs-supportedEncryptionTypes
A (DES-CBC-CRC)	CRC (KERB_ENCTYPE_DES_CBC_CRC, 0x00000001)
B (DES-CBC-MD5)	MD5 (KERB_ENCTYPE_DES_CBC_MD5, 0x00000002)
C (RC4-HMAC)	RC4 (KERB_ENCTYPE_RC4_HMAC_MD5, 0x00000004)
D (AES128-CTS-HMAC-SHA1-96)	A128 (KERB_ENCTYPE_AES128_CTS_HMAC_SHA1_96, 0x00000008)
E (AES256-CTS-HMAC-SHA1-96)	A256 (KERB_ENCTYPE_AES256_CTS_HMAC_SHA1_96,

[MS-KILE] 2.2.5 Supported Encryption Types Bit Flags	[MS-ADTS] 7.1.6.7.3 msDs-supportedEncryptionTypes
	0x00000010)

Table 1: Supported Encryption Types

This is an example of how it looks like in AD (formatted per RFC2989):

CN=server2008,CN=Computers,DC=testdomain,DC=com

…

msDS-SupportedEncryptionTypes: 0x1F = (DES_CBC_CRC | DES_CBC_MD5 | RC4_HMAC_MD5 | AES128_CTS_HMAC_SHA1_96 | AES256_CTS_HMAC_SHA1_96);

This attribute is present on a computer object if and only if the client system (or an administrator) creates and sets it to a particular value. This is typically done by a Windows client (Windows Vista or newer) via an LDAP Modify Request during the first reboot after successfully joining the domain (see Windows7_RebootAfterJoin.cap, Frames 194 & 198, from this blog attachment).

Legacy Windows clients (Windows 2000 through Windows 2003 R2) never set the msDS-SupportedEncryptionTypes attribute.

msDS-SupportedEncryptionTypes common attribute values

0x1F = (DES_CBC_CRC | DES_CBC_MD5 | RC4_HMAC_MD5 | AES128_CTS_HMAC_SHA1_96 | AES256_CTS_HMAC_SHA1_96);

0x1C = (RC4_HMAC_MD5 | AES128_CTS_HMAC_SHA1_96 | AES256_CTS_HMAC_SHA1_96);

The following table lists the value of msDS-SupportedEncryptionTypes, as set (or not set) by various Windows clients, in response to the presence or absence of ADS_UF_USE_DES_KEY_ONLY (0x200000, 2097152d) in the userAccountControl attribute of the computer account:

Windows Client	userAccountControl	
	ADS_UF_USE_DES_KEY_ONLY = 0	ADS_UF_USE_DES_KEY_ONLY = 1
Windows 2000 (SP4)	never set by the client	never set by the client
Windows XP (SP3)	never set by the client	never set by the client
Windows 2003 (SP2)	never set by the client	never set by the client
Windows 2003 R2	never set by the client	never set by the client
Windows Vista (SP2)	0x1F (set by the client)	not set by the client
Windows 2008 (SP2)	0x1F (set by the client)	not set by the client
Windows 2008 R2	0x1C (set by the client)	0x1C (set by the client)
Windows 7	0x1C (set by the client)	0x1C (set by the client)

Table 2: userAccountControl versus ADS_USE_DES_KEY_ONLY

The following table lists the Etypes offered by Windows clients for a Kerberos AS Request (krbtgt/domain). The numeric values indicate the order in which the types are presented in the request. See *_RebootAfterJoin.cap files in the blog attachment.

AS Request: krbtgt/domain.name: Etype	2000 (SP4)	XP (SP3)	2003 (SP2)	2003 (R2)	Vista (SP2)	2008 (SP2)	2008 (R2)	Win 7
aes256-cts-hmac-sha1-96 (18) [1]					1	1	1	1
aes128-cts-hmac-sha1-96 (17) [1]					2	2	2	2
rc4-hmac (23) [1]	1	1	1	1	3	3	3	3
rc4 hmac old (0xff7b) [2]	2	2	2	2				
old rc4 md4 (-128) 2	3	3	3	3				
des-cbc-md5 (3) [1]	4	4	4	4	4	4	4	6
des-cbc-crc (1) [1]	5	5	5	5	5	5	5	
rc4-hmac-exp (24) [1]	6	6	6	6	6	6	6	4
rc4 hmac old exp (0xff79) [2]	7	7	7	7	7	7	7	5

Table 3: Windows Client Offered Encryption Types

[1] Defined in RFC 3961 Encryption and Checksum Specifications for Kerberos 5 : 8. Assigned Numbers

[2] Defined in the Windows Driver Kit (WDK) 7600.16385.0: inc\api\ntsecapi.h

[3] `#define KERB_ETYPE_RC4_HMAC_OLD -133 // FFFFFF7B`

[4] `#define KERB_ETYPE_RC4_HMAC_OLD_EXP -135`

When the KDC checks the msDS-SupportedEncryptionTypes attribute to decide what encryption algorithm to use in order to encrypt the ticket, it could find basically two scenarios:

1) msDS-SupportedEncryptionTypes is populated
2) msDS-SupportedEncryptionTypes is empty (does not exist)

If the attribute is populated, then the deal is done, since the KDC can determine the best common algorithm to encrypt the ticket with the value present.

However, if the attribute is empty, then the KDC will have to work harder, and check another attribute - userAccountControl. This attribute is defined in [MS-ADA3] section 2.341 Attribute userAccountControl and described in MS-ADTS section 2.2.15 userAccountControl Bits. This attribute is a 4 byte Bit Mask that defines many aspects of the account - but the only one the KDC is interested in is the DK (ADS_UF_USE_DES_KEY_ONLY) bit.

ADS_UF_USE_DES_KEY_ONLY is essentially for MIT Kerberos-based client and host systems. Generally, a new user account is pre-created for the system in question. The following white paper discusses this in depth, with respect to Windows 2000 (please note that ADS_UF_USE_DES_KEY_ONLY was first defined in Windows 2003):

Step-by-Step Guide to Kerberos 5 (krb5 1.0) Interoperability: http://technet.microsoft.com/en-us/library/bb742433.aspx

More information is available in the following white papers:

Windows 2000 Kerberos Interoperability: http://technet.microsoft.com/en-us/library/bb742432.aspx

Windows 2000 Kerberos Authentication: http://technet.microsoft.com/en-us/windowsserver/2000/bb742431.aspx

The userAccountControl ADS_UF_USE_DES_KEY_ONLY bit defines what legacy encryption method will be used:

3) If the bit is set, then only DES will be used (if the only offered Etypes are recognizable as DES: des-cbc-md5 (3) and des-cbc-crc (1), for example).
4) If the bit is NOT set, then DES and RC4 may be used.

If ADS_UF_USE_DES_KEY_ONLY is set on a (Windows) computer account, Windows 2003 and newer Domain Controllers will fail Kerberos AS and TGS Requests for the krbtgt/domain.name with KDC_ERR_ETYPE_NOSUPP, since Windows clients offer non-DES encryption types (see Table 3: Windows Client Offered Encryption Types).

However, this does not break Windows client system functionality, as necessary operations will fall back to NTLM authentication. Needless to say, it is not recommended to set the userAccountControl ADS_UF_USE_DES_KEY_ONLY bit on a Windows-based computer account.

Conclusion

Windows 2008, Vista, Windows 7 and Windows 2008 R2 have expanded the options available when securing resources and communications on the network.

Having the msDS-SupportedEncryptionTypes attribute is a good starting point to further incorporating newer and more secure encryption algorithms in the future.