IAP Requirements and Gaps for Active Directory Domain Services (AD-DS)

IAP v1.2 Section	Requirements (paraphrased)	AD-DS Baseline Controls	Baseline Gaps	AM Proposal	Remaining Gaps
4.2.3.4 - Stored Authentication Secrets (S)	Do not store passwords as plaintext. Limit access to admins and apps that require access.	Passwords are stored in the ntds.dit file. They are not stored as plaintext. The operating system normally prevents access to the file.	No gaps.		
	Protect stored passwords with one of the following alternatives: 1. Concatenate a variable salt to the password and hash with an ***Approved Algorithm***.	1. The "NT hash" is an unsalted MD4 hash. The "LM hash" isn't a cryptographic hash.	1. MD4 is not an ***Approved Algorithm*** and a variable salt is not employed.		
	2. Encrypt the password with an ***Approved Algorithm*** and decrypt only when immediately needed for authentication.	2. Encrypts the "NT hash" with DES and the users RID, then encrypts again with RC4 and the PEK. The "LM hash" is the output from encrypting a constant with the password and DES.	2. DES and RC4 are not ***Approved Algorithms***. Full-disk encryption (FDE) solutions (hardware or software) that utilize ***Approved Algorithms*** and only decrypt passwords when immediately needed (i.e. decrypt disk sectors as needed to support read operations while keeping the data on disk encrypted) provide a compensating control. Bitlocker[2] is an example FDE solution that ships with Windows 2008 and newer.		
	3. Any method allowed for NIST 800-63 Level 3 or 4.				
4.2.3.5 - Basic Protection of Authentication Secrets (B)	1. Do not store passwords as plaintext. Limit access to admins and apps that require access.	1. Passwords are stored in the ntds.dit file. They are not stored as plaintext. The operating system normally prevents access to the file.	1. No gaps		
	2. Do not transmit plaintext passwords over the network	2. Authentication using LM, NTLMv1, NTLMv2, LDAP over SSL[5], or Kerberos[6] does not transmit cleartext passwords.	2. LDAP without SSL[5] transmits plaintext passwords. Enforcing LDAP signing[4] prevents LDAP connections without SSL, but this may cause compatibility issues with some clients (e.g. Mac and Linux clients using Samba).		
4.2.3.6 - Strong Protection of Authentication Secrets (S)	1a. Any credential store with passwords used by the IdP or verifier is subject to 4.2.3.4 and 4.2.8.	1a. See the relevant sections in this table.	1a. See the relevant sections in this table.		
	1b. Use ***Protected Channels*** when IdP passwords are sent from one credential store to another.	1b. AD-DS uses RPC and Kerberos when synchronizing between domain controllers. For Windows Server 2008 and later, AES is used for Kerberos encryption if properly configured.[1] Alternatively, an appropriately configured mechanism such as IKE/IPSEC may be used to create the Protected Channel. This requirement also applies to provisioning of passwords into or out of AD-DS.	1b. Gaps? There may be implementation specific issues based on local technology choices for password provisioning. These issues are not specific to AD-DS.		
	2. Use ***Protected Channels*** when IdP passwords are sent between services for verification purposes.	2. Verification using NTLMv2, Kerberos[6], or LDAP with SSL[5] uses a protected channel between services. Use of LM and NTLMv1 protocols for verification is precluded by subjects holding a Silver IAQ due to the definition of a protected channel. Use of LDAP without SSL is also precluded for the same reason.			
	3. Have policies and procedures to minimize the risk of transient password exposure to non-IdP apps.	3. AD-DS is considered part of the IdMS when included in an assurance assessment, Since AD-DS can act as a verifier for non-IdP applications that exist outside of IdMS, the organization as IdPO must have policy in place to enforce the IAP requirements for any application that password transits through between subject and AD-DS.	2. Use of LM and NTLMv1 protocols may be prevented by disabling the protocols centrally at the AD-DS. Disabling these protocols may cause compatibility issues with older applications[3]. Enforcing LDAP signing[4] prevents unsigned LDAP connections by using SSL. As mentioned above, this may cause compatibility issues depending on the environment. 3. A general principle of following the password and applying risk management at any point where the protected channel between the subject and the verifier is compromised should be applied. Common examples that require additional attention are non-privacy preserving authentication interfaces, externally hosted applications and applications that require proprietary authentication API's. Involving Information Security, Audit and Procurement staff would be recommended.		
4.2.5.1 - Resist Replay Attack (B, S)	Ensure it's impractical to achieve IdP authentication by recording and replaying a previous IdP authentication message.	Windows maintains a cache of used authenticators to allow it to recognize a replay of a specific authentication event.	LM - Does not resist replay attacks* NTLMv1 - Does not resist replay attacks* NTLMv2 - Resists replay attacks7 LDAP - Does not resist replay attacks if LDAP signing[4] is not enforced Kerberos - Resists replay attacks7 * Not allowed per AD Silver Cookbook	Require LDAP signing OR Enable LDAP signing and monitor & mitigate non-LDAP signed use by those with an assurance level.	

4.2.5.2 - Resist Eavesdropper Attack (B, S)	Ensure it's impractical to learn the password or otherwise obtain information that would allow impersonation of a subject by network eavesdropping during an IdP authentication event.	**LM, NTLMv1, NTLMv2 and Kerberos** all provide some level of security based on their native encryption. Strength of encryption determines how well the protocol resists eavesdropping. **LDAP** Fails to resist eavesdropping if using Simple Binds without TLS/SSL. Simple Binds with TLS/SSL[5] or signing should resist eavesdropping. Binds using SASL (and not TLS/SSL) will use the native encryption of the underlying SASL mechanism (LM, NTLM, etc), so may or may not effectively resist eavesdropping.	LM - Vulnerable to eavesdropping* NTLMv1 - Vulnerable to eavesdropping* NTLMv2 - Resists eavesdropping (strength of encryption)7 LDAP - Vulnerable to eavesdropping if LDAP signing[4] is not enforced Kerberos - Resists eavesdropping7 * Not allowed per AD Silver Cookbook	1. Use protected channel (e.g., VPN)	
4.2.8.2.1 - Network Security (S)	***Protected Channels*** should be used for communication between IdMS systems.	For native IdMS components (AD Domain Controllers), replication is described above in 4.2.3.6, 1b. Not clear that other IdMS are relevant, in that they will not be native AD components. * * Assumes that AD-LDS replication is the same as AD-DS replication.	As 4.2.3.6., 1b.		

Definitions from the Identity Assurance Assessment Framework:

- ***Approved Algorithm*** - Any implementation of an algorithm or technique specified in a FIPS standard or NIST recommendation, or any algorithm or technique that conforms to an alternative means identitified by InCommon as approved for specified IAPs.
- ***Protected Channel*** - A Protected Channel uses cryptographic methods that implement an Approved Algorithm to provide integrity and confidentiality protection, resistance to replay and man-in-the-middle attacks, and mtual authentication.
- ***IdP Operator (IdPO)*** - The legal entity that signs contracts, is a registered participant in InCommon, and is responsible for the overall processes supporting the IdP.
- ***Identity Management System (IdMS)*** - A set of functions to supports enterprise Identity and access management and typically includes a database of subject information, electronic identifiers, credentials linked to the identifiers, and verification functions. See the IAAF for a complete description of the IdMS.

Footnotes:

[1]Kerberos Enhancements and Understanding Active Directory Domain Services (AD DS) Functional Levels explain that in Windows Server 2008 and later, Kerberos uses AES (an Approved Algorithm) for encryption. How Replication Works explains that RPC is used for replication over IP and that Kerberos is used for encryption.

[2]BitLocker Drive Encryption Overview and BitLocker Drive Encryption Technical Overview explain that AES (an Approved Algorithm) is used for encryption of the drive and that sectors are only decrypted as they are read.

[3] Detailed discussions of the issues and mitigations of LM and NTLMv1 technologies/protocols can be found in the AD Silver Cookbook. Please refer to the AD Silver Cookbook for further explanation.

[4]How to enable LDAP signing in Windows Server 2008 and LDAP Signing

[5] LDAP simple binds depend on SSL/TLS for a protected channel. Windows supports many SSL/TLS cipher suites as provided in schannel.dll. Only some of the cipher suites rely only on ***Approved Algorithms***. It's possible to disable weak cipher suites via registry settings or through 3rd-party tools. See Schannel Cipher Suites in Windows Vista (applies to Windows 2008 as well), Restrict the Use of Certain Cryptographic Algorithms and Protocols in Schannel.dll (very old reference but I read claims that the information is still relevant), and IIS Crypto (free 3rd-part tool, no endorsement implied).

[6] Windows Server 2008 R2 supports five "encryption types". The two strongest (AES256-CTS-HMAC-SHA1-96 and AES128-CTS-HMAC-SHA1-96) rely on ***Approved Algorithms***. The two weakest encryption types (DES_CBC_CRC and DES-CBC-MD5) do not rely on ***Approved Algorithms*** and are disabled by default. RC4-HMAC is also supported and is generally categorized as strong, but it doesn't use only ***Approved Algorithms***. This might be a place for an alternative means argument. See Windows Configurations for Kerberos Supported Encryption Type, Changes in Kerberos Authentication, and Hunting down DES in order to securely deploy Kerberos.

7

For the purposes of analyzing replay and eavesdropper attacks, we decided that a vulnerability to a combination of multiple attack styles {eavesdropper (passive), replay, man-in-the-middle} did not constitute an IAP gap of the individual section. However, for both Kerberos and NTLMv2 there are known vulnerabilities that include replay which can be leveraged to establish a session to a network resource. There are mitigations involving good security practice for these combination attacks, with the most relevant to the IAP revolving around security practices involving the domain controllers and domain admins. Practitioners should review the following material to make sure they are familiar with these combination attacks and have taken reasonable steps to mitigate:

Pass the hash:

http://www.sans.org/reading_room/whitepapers/testing/crack-pass-hash_33219

Turning off NTLMv2:

http://technet.microsoft.com/en-us/library/dd560653(v=ws.10).aspx

Kerberos "pass the ticket" attack:

http://csis.bits-pilani.ac.in/faculty/sundarb/courses/old/spr06/netsec/evals/project/projrefs/kerb/AIWSC03_kerberos_replay_attacks.pdf

http://www.blackhat.com/presentations/bh-europe-09/Bouillon/BlackHat-Europe-09-Bouillon-Taming-the-Beast-Kerberous-whitepaper.pdf

NTLMv2 (and NTLMv1) not-truly random challenge + replay + "pass the hash" relay:

http://media.blackhat.com/bh-us-10/presentations/Ochoa_Azubel/BlackHat-USA-2010-Ochoa-Azubel-NTLM-Weak-Nonce-slides.pdf

http://www.hexale.org/advisories/OCHOA-2010-0209.txt

http://blogs.technet.com/b/srd/archive/2009/04/14/ntlm-credential-reflection-updates-for-http-clients.aspx?Redirected=true

http://www.h-online.com/security/news/item/Authentication-under-Windows-A-smouldering-security-problem-1059422.html

http://www.tarasco.org/security/smbrelay/index.html

Pass the hash:http://www.sans.org/reading_room/whitepapers/testing/crack-pass-hash_33219
Turning off NTLMv2:http://technet.microsoft.com/en-us/library/dd560653(v=ws.10).aspx
Kerberos "pass the ticket" attack:http://csis.bits-pilani.ac.in/faculty/sundarb/courses/old/spr06/netsec/evals/project/projrefs/kerb/AIWSC03_kerberos_replay_attacks.pdfhttp://www.blackhat.com/presentations/bh-europe-09/Bouillon/BlackHat-Europe-09-Bouillon-Taming-the-Beast-Kerberous-whitepaper.pdf
NTLMv2 (and NTLMv1) not-truly random challenge + replay + "pass the hash" relay:http://media.blackhat.com/bh-us-10/presentations/Ochoa_Azubel/BlackHat-USA-2010-Ochoa-Azubel-NTLM-Weak-Nonce-slides.pdfhttp://www.hexale.org/advisories/OCHOA-2010-0209.txthttp://blogs.technet.com/b/srd/archive/2009/04/14/ntlm-credential-reflection-updates-for-http-clients.aspx?Redirected=truehttp://www.h-online.com/security/news/item/Authentication-under-Windows-A-smouldering-security-problem-1059422.htmlhttp://www.tarasco.org/security/smbrelay/index.html