The following questions have been submitted by INTERNET2 ([www.internet2.edu](http://www.internet2.edu)) after collection and collation from their member universities.

This document is meant to act as a collection point for the data used in discussion and response to Internet2.

The intended outcome is to address questions about how Internet2’s “InCommon” identity framework can leverage Active Directory to offer SILVER LEVEL security…

<https://spaces.internet2.edu/display/InCAssurance/AD+Silver+Cookbook>

While many of these questions deal with Windows SERVER and CLIENT equipment, the Internet2 community tends to have \*some\* leeway in suggesting SERVER VERSIONS, but does not have any leverage at dictating the CLIENT VERSION. In general, Internet2 recommends a \*minimum\* Windows Server version of “2008”. For clients that are older (say, Win XP), it is requested that Microsoft provide details about security options relative to the version of the software being used. If tighter security option are possible (but may not be the DEFAULT setting), it should be indicated that more secure options are available – and could possibly be enforced by Group Policies.

JOHN KRIENKE PROVIDED THIS COMMENTARY: (ANN WEST was also added to threads)

Currently, Microsoft Active Directory Domain Services has issues with compliance with our US Government-approved Identity Assurance Profiles and can not be used as an authentication methodology in a federated context with Federal Agencies without developing alternative means for our specification. Most research universities will be looking to adopt Profiles over the next couple years as the federal agencies that issue grants begin to require identity assurance via the Federal ICAM program.

Diving several layers down, the key issue is that NTLMv1 has replay, eavesdropper, and protected channel vulnerabilities as defined by NIST. Use of NTLMv1 thus invalidates the assurance associated with a given digital identity (user account), unless alternatives means to mitigate these vulnerabilities is employed.

We have a group developing the alternative means and recommended practices for campuses wishing to use AD-DS, but we need an AD-DS expert to help with our analysis and have a set of questions:

<https://spaces.internet2.edu/display/InCAssurance/Questions+for+Microsoft>.

Question posed…

*In what scenario(s) is NTLM \*VERSION #1\* still used?*

*Is this a holdover from XP?*

*If this is a legacy XP (or before) issue, are there blockers from insisting on using NTLMv2 (or Kerberos)?*

REFERENCED WESBITE:

**Background**

On October 6, 2011, Steven VanRoekel, the Federal Chief Information Officer, issued a memorandum (<http://www.howto.gov/sites/default/files/omb-req-externally-issued-cred_0.pdf>), specifying a timetable for federal agencies to begin leveraging externally-issued credentials.  The Federal Identity, Credential, and Access Management Subcommittee (FICAM - <http://www.idmanagement.gov/pages.cfm/page/ICAM>) is named as responsible for certifying the entities that may issue such credentials.

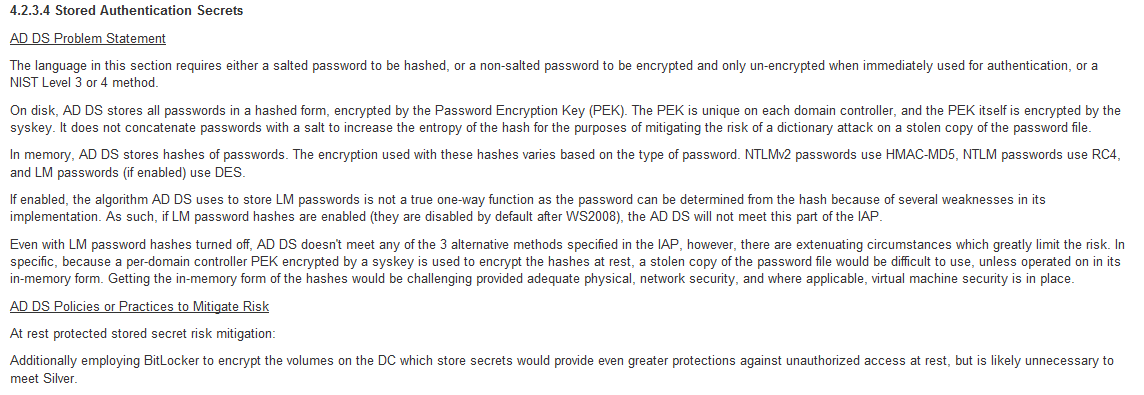
InCommon (<http://www.incommon.org>) is a Trust Framework Provider, certified by FICAM under the Trust Frame Provider Adoption Process (TFPAP - <http://www.idmanagement.gov/documents/FICAM_TFS_TFPAP_v1.1.0.pdf>) at assurance levels 1 (InCommon Bronze) and 2 (InCommon Silver). As a certified trust framework provider, InCommon is authorized to certify campuses to issue identity assertions over the Internet to government agency service providers at assurance levels 1 and 2. The documents governing InCommon's trust framework are available at <http://www.incommon.org/assurance/components.html>; of particular relevance here is "Identity Assurance Profiles - Bronze and Silver" (IAP - <http://www.incommon.org/docs/assurance/IAP.pdf>).

The InCommon Assurance Program is currently sponsoring a group of university representatives who are exploring means that can be used to certify for InCommon Silver when password credentials used for Silver-level authentication are stored in an Active Directory instance.  "IAP Requirements and Gaps for Active Directory Domain Services" (<https://spaces.internet2.edu/x/BA8wAg>) is a brief summary of that work.

Finally, universities are "BYOD" environments. While standards for end-user devices are often established, typically little enforcement is exercised over the types and configuration of devices that may be used to access services.  It is important that services be capable of protecting themselves from non-compliant end-user behavior.

**Questions**

1. Protected Channels - IAP 4.2.3.6.1b - Gaps (Addresses channels used between DC’s, as well as DC’s AD storage of passwords on disk and in memory.)
   1. RC4 HMAC encryption is not NIST or FIPS approved, and we would like to determine if it's comparable to those methodologies that are.  Can you help with this? (See <http://www.incommon.org/assurance/alternativemeans.html> for the criteria we will consider.) RC4 HMAC is not considered a suitable encryption method moving forward, and its use within future deliverables is not practical. Per Microsoft Crypto Standard Procedures, stream ciphers such as RC4 HMAC should be replaced with block ciphers such as AES with a minimum key length of 128 bits. UPDATE: after discussing with the AD-Assurance Team from Internet2, the issue arises from the method used by AD to store user credentials. Some clients may be locked at a given version – say Windows CE or XP embedded running in a client’s monitoring device or medical equipment (as an example). Internet2 is seeking SILVER level service, which entails NIST approved algorithms for encryption. NIST Pub 800-118 “Guide to Enterprise Password Management” defers to FIPS-approved algorithms. FIPS 140-2 has an appendix: “Annex A: Approved Security Functions for FIPS 140-2, Security Requirements for Cryptographic Modules”. The specific question around “sChannel” support is noted as FIPS-approved per TechNet FIPS documentation at <http://technet.microsoft.com/en-us/library/cc750357.aspx>.



* 1. Currently, it is not very practical to crack RC4 HMAC, even though it has long-known vulnerabilities.  If that were to change (e.g., a simple crack program posted on the Internet), does Microsoft have a response procedure for such compromises? How will this procedure protect Microsoft's customers that may be operating at LoA-2 via an alternate means exception? Microsoft operates a vulnerability reporting mechanism via the Microsoft Security Response Center ([MSRC](http://www.microsoft.com/security/msrc/)). This website documents the methodology of reporting, tracking and responding to any such vulnerability.
  2. What encryption algorithms does Windows Secure Channel use? Based upon the user’s settings, the ALG\_ID can be assigned to include settings such as 3DES, two-key 3DES @ 112bits, AES, AES @ 128bits, AES @ 192bits, AES @ 256bits, mutually-agreed algorithm via Diffie-Hellman, etc. More details on algorithm choices @ <http://msdn.microsoft.com/en-us/library/windows/desktop/aa375549(v=vs.85).aspx>. Note that of these, only AES is considered strong and is approved. Also, if your definition of “encryption” for this question extends to asymmetric encryption/key exchange, SChannel also supports RSA, DH and ECDH. All of these are SDL-approved.
  3. What's the impact of turning on the FIPS setting on all Domain Clients? What's the impact on Domain Controllers? As with any cryptographic session, establishing a FIPS-secured communication session is a mathematically-intense operation. Given the nature of algorithms choices, and various key lengths, the exact impact of any given encryption selection is dependent upon the client hardware and the server hardware, plus the overall load applied to the server. While it is not feasible to outline all of the permutations of varied client hardware and server hardware, the FIPS settings and config data can be referenced at: <http://support.microsoft.com/kb/811833>. Also refer to the THREATS AND COUNTERMEASURES GUIDE @ <http://www.microsoft.com/en-us/download/confirmation.aspx?id=26137>

1. What should one do to enable distinguishing between NTLM v1 and v2 in the logs? We would like to downgrade a user's assurance level if they access a service that employs NTLM v1.
   1. In the SECURITY LOG, you have to inspect the Detailed Authentication Information section:

**Log Name: Security**

**Source: Microsoft-Windows-Security-Auditing**

**Event ID: 4624**

**Task Category: Logon**

**Level: Information**

**Keywords: Audit Success**

**Description:**

**An account was successfully logged on.**

**Account Name: user**

**Account Domain: contoso**

**Detailed Authentication Information:**

**Logon Process: NtLmSsp**

**Authentication Package: NTLM**

**Transited Services: -**

**Package Name (NTLM only): NTLM V1**

1. When BitLocker full disk encryption is used are disk sectors decrypted only as they are read? What is the recommended/supported BitLocker configuration for use with AD-DS? Reference for BL and AD: <http://technet.microsoft.com/en-us/library/cc766015(v=ws.10).aspx>

UPDATE: the BitLocker question arise from a recommendation (albeit, misguided) from NIST that it would add tighter security around the storage of credentials on a domain controller. The desired outcome would be to strengthen the security of AD credential storage on disk and in memory. This could be reflected by the NTLM version in use – seeking to implement an approved algorithm such as AES-128, etc.

1. Does Syskey use NIST/FIPS Approved Algorithms for encryption? The algorithm used within SysKey is not published. SysKey does provide levels of relative security, with a system-generated password used and stored on a startup key.
2. Are AD-DS password credentials stored by other Microsoft identity management components, such as ADFS?  If so, what are those components? UPDATE: since the goal is to provide a single sign-on ecosystem, if a user authenticates with their single username/password credentials (the same creds that could be used to login to a secure government R&D server, for example) – how can we account for any storage of those credentials within our systems? As an example – if you use something like IMAP to connect to an Exchange Online service, you would likely use NTLMv1 authentication, which does not meet NIST standards.
3. Does Microsoft have a strategy for supporting compliance with the Federal Identity, Credential, and Access Management (FICAM) requirements at LoA-2, perhaps through Microsoft's partnership with the Kantara Initiative? If so, what is the time frame? ***NO UPDATE AVAILABLE AT THIS TIME.***
4. Does Microsoft have a strategy for AD integration of non-Windows and old-Windows client platforms that will use NIST/FIPS approved algorithms for transport of passwords over a network? If so, what is the time frame? Making sure that I am understanding the intent … the goal would be to maintain AD as an IdP for clients that transmit password encrypted using NIST algorithms? ***THIS TOPIC IS UNDER INVESTIGATION.*** (*If the understanding is incorrect, please advise.*)
5. Is it possible to configure AD so that the NetUserChangePassword and NetUserSetInfo protocols require NIST approved algorithms for encrypting the session over which the password data is passed? ***THIS TOPIC IS UNDER INVESTIGATION***.
6. Please review "[IAP Requirements and Gaps for Active Directory Domain Services](https://spaces.internet2.edu/display/InCAssurance/IAP+Requirements+and+Gaps+for+Active+Directory+Domain+Services+%28AD-DS%29)" to verify the information it contains. [Content from this link pasted below.] Storage security of credentials in the SAM can be augmented using SysKey. Please advise if this is a suitable method, given that cracking the SAM requires some elevated privileged access to the system already.

IAP REQUIREMENTS AND GAPS FOR ACTIVE DIRECTORY DOMAIN SERVICES

# [https://spaces.internet2.edu/download/attachments/25865531/InCAssurance?version=2&modificationDate=1330008038664](https://spaces.internet2.edu/display/InCAssurance)[IAP Requirements and Gaps for Active Directory Domain Services (AD-DS)](https://spaces.internet2.edu/display/InCAssurance/IAP+Requirements+and+Gaps+for+Active+Directory+Domain+Services+%28AD-DS%29)

* Added by [Eric Goodman](https://spaces.internet2.edu/display/~eric.goodman-ucop.edu@ucop.edu), last edited by [BRIAN ARKILLS](https://spaces.internet2.edu/display/~barkills@washington.edu) on Apr 26, 2013  ([view change](https://spaces.internet2.edu/pages/diffpages.action?pageId=36704004&originalId=38667152))

**Comment:**



|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **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. Bitlocker2 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 SSL5, or Kerberos6 does not transmit cleartext passwords. | 2. LDAP without SSL5 transmits plaintext passwords.  Enforcing LDAP signing4 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 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 passwords are sent between services for verification purposes. | 2. Verification using NTLMv2, Kerberos6, or LDAP with SSL5 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. | 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 applications3. Enforcing LDAP signing4 prevents unsigned LDAP connections by using SSL. As mentioned above, this may cause compatibility issues depending on the environment. |  |  |
|  | 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. | 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 perserving 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 authentication by recording and replaying a previous 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 signing4 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. | **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/SSL5 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). | LM - Vulnerable to eavesdropping\*  NTLMv1 - Vulnerable to eavesdropping\*  NTLMv2 - Resists eavesdropping (strength of encryption)7  LDAP - Vulnerable to eavesdropping if LDAP signing4 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](http://www.incommon.org/docs/assurance/IAAF.pdf):

* **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](http://technet.microsoft.com/en-us/library/cc749438(WS.10).aspx) and [Understanding Active Directory Domain Services (AD DS) Functional Levels](http://technet.microsoft.com/en-us/library/understanding-active-directory-functional-levels(v=ws.10).aspx) explain that in Windows Server 2008 and later, Kerberos uses AES (an Approved Algorithm) for encryption.  [How Replication Works](http://technet.microsoft.com/en-us/library/cc736978(v=ws.10).aspx) explains that RPC is used for replication over IP and that Kerberos is used for encryption.

2[BitLocker Drive Encryption Overview](http://technet.microsoft.com/en-us/library/cc732774.aspx) and [BitLocker Drive Encryption Technical Overview](http://technet.microsoft.com/en-us/library/cc732774(v=WS.10).aspx) 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](http://support.microsoft.com/kb/935834) and [LDAP Signing](http://technet.microsoft.com/en-us/library/dd941832(v=ws.10).aspx)

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](http://msdn.microsoft.com/en-us/library/windows/desktop/ff468651(v=vs.85).aspx) (applies to Windows 2008 as well), [Restrict the Use of Certain Cryptographic Algorithms and Protocols in Schannel.dll](http://support.microsoft.com/kb/245030) (very old reference but I read claims that the information is still relevant), and [IIS Crypto](https://www.nartac.com/Products/IISCrypto/) (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](http://blogs.msdn.com/b/openspecification/archive/2011/05/31/windows-configurations-for-kerberos-supported-encryption-type.aspx), [Changes in Kerberos Authentication](http://technet.microsoft.com/en-us/library/dd560670(v=ws.10).aspx), and [Hunting down DES in order to securely deploy Kerberos](http://blogs.technet.com/b/askds/archive/2010/10/19/hunting-down-des-in-order-to-securely-deploy-kerberos.aspx).

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.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>