Objet :	**Authentifications sous Windows**	Date : Version :	**19/06/2010** **1.0**

Présentation des mécanismes d'authentification de Windows de NT4 à Windows 2008 R2 en passant par Windows Seven.

I Définition :

Parmi toutes les définitions, voici celle qui semble le mieux correspondre à ce qui s'applique à une « authentification Windows ».
*Petite remarque : on ne parlera ici que de l'authentification Windows basée sur le couple login + password, autrement dit l'identifiant +mot de passe. Ce couple d'authentification fait partie de la catégorie des authentification de type **« ce que je sais »**, à la différence des authentifications de type **« ce que je possède »** comme les cartes magnétiques, ou encore les authentifications **« ce que je suis »** comme la biométrie.*

L'authentification est le mécanisme qui permet à un élément X de se faire identifier de manière sûre par un élément Y. L'authentification permet à l'élément Y de vérifier que l'élément X satisfait aux exigences d'identification minimales requises par Y .

Par exemple : X peut être un utilisateur (un compte utilisateur), un ordinateur, un périphérique, un logiciel qui a besoin d'accéder à une ressource (une donnée, un service d'application, un fichier, une application, un réseau,…) : l'accès à cette ressource par Y (un serveur, un routeur, une application, …) à la condition première que X se soit authentifié auprès de Y de manière formelle (et à la condition seconde que X ait les autorisations pour accèder à la ressource…).

L'authentification mutuelle est donc le mécanisme qui consiste à ce que le demandeur (ci dessus appelé X) s'authentifie auprès du possesseur de l'information (ci-dessous appelé Y), mais aussi que ce même demandeur authentifie de manière formelle le possesseur de l'information.

Tout ceci pour dire que l'objectif est de permettre de protéger des données, des informations, des services et d'en restreindre leur accès aux seuls utilisateurs (ou comptes) autorisés, donc dûment authentifiés.
C'est ce fonctionnement qu'on retrouve lorsqu'il s'agit d'accéder à sa boite mail, à un fichier, d'obtenir un accès réseau.

II Le problème.

Le souci principal qu'on rencontre avec l'authentification basée sur le couple identifiant + mot de passe, c'est que l'information qui permet d'être authentifiée peut facilement s'évader, être connue de tierce personne, partagée volontairement ou non, usurpée,…
Autre souci : comme cette forme d'authentification est la plus simple, parfois aussi la plus « cheap », c'est donc la plus répandue : ce qui en fait une bonne raison pour vouloir la rendre efficace et la plus sûre possible.
Les risques concernant ce type d'authentification est que celle-ci soit dérobée, mais surtout « dupliquée » à l'insu du propriétaire avec la conséquence de voir les ressources normalement protégées, devenir accessible à un publique plus large que prévu.

Les premiers vecteurs qui ont contribué à rendre les authentifications fragiles est le réseau par lequel circule l'identifiant+ mot de passe, et également le stockage qui contient les identifiants+ mot de passe.
Si ces deux éléments (réseau ou stockage) laissent les authentifications lisibles, en clair : cela facilite grandement l'interception de l'identifiant, ou l'obtention des bases d'identifiants.
Côté réseau : l'authentification FTP laisse circuler login et mot de passe en clait, idem pour le protocole Telnet, l'authentification dite « de base » sur un serveur http, l'authentification POP3 pour l'accès à sa boite aux lettre personnelle,…
Côté stockage : une base de type SQL qui contient dans sa tables les identifiants en clair pour l'accès à une application, un fichier texte d'installation,…

III Les solutions

Passer par le chiffrement des données qui vont être transportées sur le réseau ou lorsqu'elles seront stockées.
C'est globalement ce qui est pratiqué dans les environnements Wndows lorsqu'un utilisateur s'authentifie sur un serveur. L'utilisateur saisi son login et son mot de passe sur un poste informatique, ces informations sont transmises de manières chiffrées à un serveur qui vérifie dans sa base d'identifiant (elle aussi chiffrée) que l'authentification est valide.
Mais alors si c'est le cas : pourquoi ce document ?
Parce que les protocoles utilisés pour chiffrer le mot de passe sur le réseau, (voire pour stocker les mots de passe) ne se valent pas tous, ne sont pas tous aussi sécurisés les uns que les autres et que pour renforcer l'authentification sous Windows, de nombreuses implémentations de l'authentification ont été proposées dans les environnements Windows.

L'authentification sur une base locale ou sur un Active Directory

Sur un poste de travail unique (un Windows XP personnel par exemple), il existe une base de compte utilisateur locale (base SAM pour Security Account Manager) qui est stockée dans le registre de l'ordinateur. Lorsque vous démarrez votre session Windows, le compte utilisateur est authentifié (avec ou sans mot de passe) auprès de la base SAM locale avant de vous donner le droit d'ouvrir la session.
Sur un réseau local constitué de quelques postes Windows et d'un serveur Windows : lorsque les utilisateurs se connectent au serveur (pour imprimer, accès aux fichier,…), le serveur demande l'authentification du poste client avant d'autoriser l'accès à la ressource (fichier, imprimante,….). Le serveur s'appuie également sur sa base SAM locale. Chaque poste, chaque serveur de ce type de réseau restreint possède sa propre base de comptes utilisateurs sans lien avec les autres bases de comptes.
Ce principe existe depuis que Windows 3.1 existe… Plus proprement depuis l'apparition de Windows 95 ou Windows NT 3.51.

Sur un réseau plus étendu, les postes de travail font partie d'un domaine Windows : dans ce domaine sont centralisés les comptes utilisateurs+ mot de passe sur une base de données (Active Directory) gérée par au moins serveur qui a cette fonction principale d'authentifier les utilisateurs avant qu'il ne tente d'accèder à une ressource du domaine ou pour ouvrir une session Windows sur leur poste informatique. C'est l'authentification sur un Active Directory (disponible depuis Windows 2000 à 2008 R2)

IV Les types d'authentification

Ces protocoles ne se chargent que de vérifier l'identité de l'utilisateur ou du couple identifiant/mot de passe, ils ne se chargent de vérifier ou de donner un accès aux ressources.

1 - LanMan

Ce premier type est utilisé pour le stockage des mots de passe, afin de mieux saisir l'intérêt des protocoles qui suivent.
Le Hash LanMan est le format dans lequel est stocké le mot de passe sous Windows (jusque Windows Millénium côté client et Windows 2000 côté serveur) lorsque celui fait moins de 15 caractères. Lorsqu'il est trop long, le mot de passe est décomposé en 2 parties de 7 caractères qui sont chacun codés avec DES.
Ce stockage présente de nombreuses faiblesses : DES déjà à éviter, le fait que le Hash LanMan n'est pas une implémentation parfaitement « Sens Unique » , c'est dire que le mot de passe peut être retrouvé à partir du hash, stockage des données en ASCII = réduction du nombre de possibilités, conversion des mots de passe en majuscules = réduction du nombre de possibilités … Bref : un ordinateur de bureau ne demande que quelques minutes pour trouver le mot de passe à partir d'un hash.
Ce type de stockage étant considéré comme très très bas, le protocole NTLM v1 a remplacé progressivement le hash LM.

2 - NTLM v1

A la base, le premier protocole d'authentification est NTLM pour NT Lan Manager (ou plus détaillé New Technology Lan Manager) v1 introduit avec Windows NT3.5.
L'authentification repose sur un mécanisme de « challenge/response » ou « simulation/réponse » qui permet à l'utilisateur de s'authentifier auprès d'un serveur sans avoir à lui communiquer son mot de passe en clair.
Cela se fait en 3 échanges :
1 – le client envoie au serveur une liste de caractéristiques supportées par le client (force de cryptage, type de client, version ntlm, version d'OS,…), ainsi que le nom de l'utilisateur associé.
2 – le serveur précise dans la liste précédente, quelles fonctionnalités sont acceptées par ce dernier pour l'échange ainsi qu'une clé chiffrée sur 16 bits par le serveur (le challenge)
3 – le client répond en fournissant une ou plusieurs réponses au challenge. Cette réponse sera constituée du résultat de l'expression de la clé envoyée par le serveur associée au mot de passe de l'utilisateur soumis par le client, le message de retour intègre aussi le nom de l'utilisateur et le contexte pour lequel l'authentification est demandée.
Ensuite, le serveur n'aura qu'à vérifier que la « réponse » au challenge fourni le même résultat que pour le compte+mot de passe en possession par le serveur : si la comparaison est OK, l'authentification est réussie.

Les différences avec LM ? Le stockage du mot de passe utilise Unicode, et introduit le chiffrement avec RC4 : ce qui rend un tout petit peu plus sécurité l'échange ou le stockage des mots de passe… mais très peu.

Tous les détails : http://davenport.sourceforge.net/ntlm.html

3 - NTLM v2

Arrivé pour véritablement compenser les lacunes des prédécesseurs, NTLM v2 apporte les modifications suivantes :

- le hash NT est peut être contenir jusque 256 caractères (bien que les interfaces graphiques de gestion de mots de passe ne dépassent pas 127 caractères),
- le challenge/response ait appel à des chaines de 16 et 8 octets.
- Signature des chaines de réponses,
- Utilisation du MD5 pour la création de Hash….

Notons que l'authentification NTLM ne traverse pas les proxies, et circule « mal » sur de grand réseaux comme internet.

4 - Kerberos

Kerberos est un protocole d'authentification réseau unifiée largement répandu et disponible pour des environnements hétérogènes. L'authentification entre un client et un serveur nécessite que ces derniers fassent confiance à un tiers de confiance.
Kerberos assure confidentialité, intégrité des données et non répudiation.

La version courante de Kerberos est la version 5, décrite dans la RFC 1510. Nous nous limitons ici à son implémentation sous Active Directory de Microsoft (à partir de Windows 2000). En effet, Kerberos sous Windows n'est disponible que dans un domaine Active Directory, sans quoi NTLM v1 ou v2 seront utilisés (enfin presque parce qu'un client Windows peut se voir implémenter un client GINA qui ouvre alors l'authentification Windows sur n'importe quel autre protocole…).

Le principe simplifié de Kerberos est basé sur :

- un client
- un serveur (ou une ressource)
- un serveur de clé (Key Distribution Center, KDC est en charge de la distribution des clés entre le client et la ressource, il fournit le secret partagé entre le client et le serveur, et seulement connu par eux)
- des tickets de service (aussi appelés Ticket de Session hors monde Microsoft).
- des tickets utilisateurs (aussi appelés Ticket d'octroi de Tickets ou TGT, hors monde Microsoft).
- Un service d'octroi de Tickets (le TGS)

(Ticket Granding Service, TGS délivre le ticket de session, celui qui pour une courte durée permettra au client de se présenter auprès du serveur pour demander l'accès à une ressource.)
que si un client X souhaite se connecter à une ressource Y, il doit obtenir un Ticket d'authentification auprès d'un serveur de clés/tickets qui possède une durée de vie limitée (quelques heures). C'est ce ticket que le client X devra présenter au serveur Y pour que le serveur Y authentifie le client X.
Dans cette situation, le serveur Y ne connaît pas le mot de passe du client X, le serveur Y authentifie le client X et vice-versa, de plus la gestion des clés est centralisée .
Un serveur KDC est présent sur chaque controleur de domaine (sous forme de service), tous les KDC utilisent le même compte utilisateur du domaine krbtgt (ce compte est désactivé et doit le rester)

Negiocate SSP : mécanisme présent à partir de Windows XP et Windows 2003 qui permet à une application de demander une authentification sur SSP (Security Provider), et SSP se charge de gérer l'authentification par NTLM, par Kerberos, etc… en lieu et place des applications.

6 - Les versions de Windows, les protocoles supportés.

	Windows XP	Windows Vista	Windows 7	Windows 2000	Windows 2003	Windows 2008
Stockage LanMan	A	A	S	A	A	S
NT LM v1	A	A		A	A	
NT LM v2	A	A	A	A	A	A
Kerberos	A	A	A	A	A	A

A pour Activé par Défaut,
S pour Supporté, donc Activable si nécessaire.
N pour Non Supporté.

Interdire LM, NTLMv1, NTLMv2 sur les clients, sur les serveurs.

http://www.windowsitpro.com/article/protocols/inside-sp4-ntlmv2-security-enhancements.aspx

http://technet.microsoft.com/fr-fr/magazine/2006.08.securitywatch%28en-us%29.aspx

Pour interdire LM, le moyen le plus immédiat est d'employer un mot de passe supérieur à 15 caractères (au delà de ce que supporte le protocole LM), ainsi le mot de passe sera au moins stocké en NTLMv1 mais les authentifications avec les postes antérieurs à Windows Millénium seront HS.