Xray ou les faiblesses de la sécurité en pratique (LM & NTLM) et ses remèdes (NTLMv2, SUS)

Laurent.Klinq@epfl.ch, EPFL-STI

Dans la jungle informatique, il est nécessaire de remettre à jour ses connaissances, en particulier dans le domaine délicat de la sécurité.

Un utilisateur sous observation

Historique

À l'époque où l'informatique consistait encore à explorer l'usage de ces étranges lucarnes, un constructeur décida de mettre en place un système de réseau adapté à la communauté des usagers, Lan Manager 2.1 (LM).

Ce gestionnaire de réseaux naît en juin 1987 pour des clients limités (à l'époque) pour DOS, Windows 3.x et OS/2.

Son successeur NTLM, comme son nom l'indique, fut son incarnation pour NT.

L'intérêt pour ce protocole n'est pas purement historique, car dans un environnement Active Directory, il peut être utilisé pour identifier un usager.

Un usager en pratique

À partir de Windows NT, l'identité de l'usager est réalisée avec *Graphical Identification and Authentification* (GINA):

- l'usager désire s'identifier, il tape le *Security Attention Sequence* (SAS) = Ctrl + Alt + Delete;
- le SAS démarre un mode protégé, et toutes les autres applications de l'usager sont arrêtées, ceci évite toute tentative de capture des éléments de sécurité;
- il entre son identifiant et son mot de passe;
- celui-ci est transmis au *Local Autority Server* (LSA) qui authentifie l'usager et retourne une session sécurisée;
- la session sécurisée démarre le système Win32 qui démarre une session graphique ou permet d'accéder aux ressources (partage de fichier, impression).

Ce processus ne semble pas contenir de faille.

Le vers est dans le fruit, car NTLM peut être utilisé pour identifier l'accès à une ressource. Par défaut, Active Directory utilise Kerberos comme source d'authentification primaire, mais si celle-ci n'est pas disponible, il utilise NTLM comme source d'identification secondaire.

LM (n')est (plus) un protocole sûr

Pour comprendre la faiblesse de NTLM, il est nécessaire de comprendre son parent direct LM (LAN Manager).

Lan Manager utilise une clé de hachage, c'est-à-dire qu'il transforme un mot de passe de taille variable dans un code de taille fixe en appliquant une fonction mathématique. La faiblesse n'est pas issue de cette technique, mais dans sa manière d'être implémentée.

En pratique, le mot de passe contient jusqu'à 14 caractères au maximum. Il suit les étapes suivantes:

- ajout de 0 pour atteindre une taille de 14 caractères ou octets;
- convertir en MAJUSCULE;
- diviser la chaîne de caractère en deux (2 x 7 octets);
- une clé Data Encryption Standard (DES) 56 bits (7 x 8 bits) est construite à partir de chacune des deux moitiés (2 x 7 octets);
- le résultat est la concaténation des deux clés DES en une clé de hachage (16 octets).

La principale faiblesse est issue de la division du mot de passe en deux parties au lieu d'utiliser un cryptage DES 112 bits (14 x 8 bits). En plus, l'algorithme DES 56 bits est en passe d'être mis au rebut par l'organisme américain de normalisation NIST en faveur du triple DES: ***http://csrc.nist.gov/Federal-register/July26-2004-FR-DES-Notice.pdf***

NTLMv2 utilise un chiffrement de 128 bits, c'est le protocole que je suggère de garder en complément de Kerberos.

Windows Active Directory, une plateforme sûre !

Échaudé par l'apparition d'outil permettant de trouver dans un délai raisonnable un mot de passe LM, Microsoft a décidé d'utiliser une autre technologie pour Active Directory avec Windows 2000, XP et 2003, Kerberos.

Kerberos

Issu de la mythologie (c'est Cerbère, le chien aux trois têtes qui garde la porte d'Hadès, le gardien des Enfers), Kerberos a été développé au MIT: ***http://web.mit.edu/kerberos/www/***.

Il est considéré comme sûr, car les clés sont uniques avec une durée de validité limitant le risque d'une attaque par la force (générer toutes les clés possibles).

Le problème potentiel ne vient pas de là, mais de la compatibilité ascendante avec les anciens produits. Pour satisfaire des usagers qui ne désirent pas évoluer, la compatibilité avec des versions antérieures est le cauchemar de l'informaticien.

Pour Windows, ce syndrome est encore plus répandu, car le nombre d'usagers est particulièrement important. De ce fait, l'utilisation de LM ou NTLM est autorisée par défaut pour un domaine Active Directory, entraînant un trou de sécurité issu de la faiblesse du cryptage de Lan Manager (LM).

Xray pour Lan Manager

Des développements récents réalisés par un chercheur de l'école, Pierre Oechslin, du laboratoire IC-LASEC ont démontré la vulnérabilité de ces protocoles: ***http://lasecwww.epfl.ch/~oechslin/publications/sstic04.pdf***. Avec les outils issus directement de cette recherche, on peut trouver très rapidement un mot de passe LM si on possède la chaîne de hachage Lan Manager:

Mot de passe	Temps [s] {Pentium 4 2.4 GHz}
unmotdepasse	1.05
PlusDur123	3.44
PLUSDUR123	3.44
plusdur123	3.45
administrateur	3.47
-------45a67	80.86

Contrairement à une idée répandue, l'utilisation d'une mixité majuscule - minuscule ne modifie pas la durée de la recherche (cela est logique, car LM convertit en majuscule les caractères). Les outils utilisent la propriété qu'une chaîne de hachage peut être comparée avec tous les mots de passe d'une machine. Ainsi, une fois le mot de passe LM identifié, il est facile avec la puissance des machines actuelles de trouver la bonne combinaison majuscule-minuscule d'un mot de passe alphanumérique.

Le dernier résultat est peut-être le plus intéressant, en effet la première partie du code de hachage (7 caractères) n'a pas pu être décodée, en raison de caractères exotiques en son sein. Par contre, les caractères 8 à 12 ont pu être décodés, car présents dans la 2e partie de la chaîne de hachage.

Sécuriser le domaine Active Directory de la Faculté STI

Après la prise de conscience de l'apparition d'outils utilisant ces derniers développements, il reste à sécuriser le domaine Active Directory STI en plusieurs étapes:

1. sécuriser le domaine
2. éviter de conserver des chaînes de hachage Lan Manager
3. changer le mot de passe de tous les usagers
4. maintenir sa machine dans un état sanitaire correct
5. éduquer les usagers.

Les premières étapes ont été réalisées le 6 août 2004; dans le détail:

1. sécuriser le domaine

Pour éviter les problèmes potentiels de sécurité évoqués dans cet article, il faut bannir l'identification LM ou NTLM, cette opération est la plus simple à réaliser: simplement, implémentez dans une GPO la restriction d'utilisation à NTLMv2 qui peut être considérée comme sûre.

sti-nolmhash

Computer Configuration (Enabled)

Windows Settings

Security Settings

Account Policies/Password Policy

Network Access

Policy	Setting
Network access: Do not allow anonymous enumeration of SAM accounts and share	Enabled

Network Security

Policy	Setting
Network security: Do not store LAN Manager hash value on next password change	Enabled
Network security: LAN Manager authentication leve	Send NTLMv2 response only\refuse LM

Les valeurs possibles pour le niveau d'authentification sont:

* Niveau 0 *Envoyer une réponse LM et une réponse NTLM; ne jamais utiliser la sécurité de session NTLMv2*
* Niveau 1 Utiliser la sécurité de session NTLMv2 si elle est négociée
* Niveau 2 Envoyer l'authentification NTLM uniquement
* Niveau 3 Envoyer l'authentification NTLMv2 uniquement
* **Niveau 4 DC refuse l'authentification LM**
* **Niveau 5 DC refuse l'authentification LM et NTLM (accepte uniquement NTLMv2)**

Le niveau 0 défini par défaut pour un domaine Active Directory n'est vraiment pas adapté. Les valeurs adéquates sont les niveaux 4 ou 5.

On peut également profiter de cette modification pour éviter d'autoriser à des usagers non référencés de voir les ressources disponibles. Cette GPO supprime la conservation des chaînes de hachage sur des serveurs Windows 2003 ou des clients Windows XP.

Comme l'usage de Lan Manager est très répandu, en particulier par son utilisation dans SMB, il est nécessaire d'observer les conséquences d'une telle action sur les différents clients d'un domaine Active Directory

Pour les clients Windows 2000

Le passage à un niveau de sécurité plus élevé se fait pratiquement sans douleur. Il faut être attentif au fait que des problèmes de connexion peuvent survenir (dénis de

connexion) si la chaîne de hachage LM est encore présente dans les contrôleurs de domaine.

En effet, si la connexion d'une session se fait toujours avec Kerberos (s'il est disponible), cela n'est pas le cas avec une connexion utilisant RPC (Remote Procedure Call).

Les connexions RPC comme l'utilisation de Robocopy ou le montage d'un point de partage réseau à travers un tunnel VPN peuvent envoyer des requêtes LM.

Le problème provient du fait que le protocole NTLMv2 est uniquement permis. Il refuse donc cette demande de connexion LM ou NTLM.

La solution consiste à supprimer la chaîne de hachage LM du domaine. Ceci est obtenu par le changement du mot de passe de l'usager.

Pour les clients NT4 et antérieurs

Il est nécessaire d'activer le protocole NTLMv2, pour cela je vous renvoie aux articles de la base de connaissances qui expliquent les opérations à réaliser. Un article s'adresse aux clients suivants:

- Microsoft Windows NT 4
- Microsoft Windows 98 Seconde Édition
- Microsoft Windows 98
- Microsoft Windows 95

Procédure pour activer l'authentification NTLM 2 sous Windows 95/98/2000 et NT: ***http://support.microsoft.com/default.aspx?scid=kb;fr;239869.***

Pour Windows NT4

Une description plus détaillée existe: installer l'extension du client Active Directory: ***http://support.microsoft.com/default.aspx?scid=kb;fr;288358.***

Pour Windows 95 ou 98

Le client est disponible sur le CD-ROM Windows 2000 Server. Si vous possédez un client encore plus vieux, Windows 3.11 par exemple, la solution consiste à mettre à disposition depuis l'ordinateur concerné les données souhaitées, par exemple les mesures pour un poste d'instrumentation. Je vous mets en garde contre la faiblesse de la sécurité des mots de passe de Lan Manager.

Pour les utilisateurs de Macintosh

Si vous accédez à un serveur PC avec le protocole AFP dans ce domaine, il est nécessaire d'installer le logiciel UAM *(User Identification Module)* pour continuer d'utiliser celui-ci.

- UAM for Mac OS 8.5-9.2: ***http://download.microsoft.com/download/win2000srv/Install/1/MacOS/EN-US/MSUAM_for_Classic.hqx***
- UAM for OS X from 10.1: ***http://download.microsoft.com/download/win2000srv/Install/1/MacOS/EN-US/MSUAM_for_X.hqx.***

Attention: un bug dans Stuffit 8.0! Il est impératif de ne pas utiliser Stuffit 8.0, car il corrompt les installeurs. Il faut donc le mettre à jour pour la version courante (8.0.2), merci à Dragan Damjanovic d'avoir découvert ce problème.

Il est maintenant obligatoire d'utiliser le protocole AFP pour accéder à un partage de fichier Windows (le protocole SMB intégré dans les MacOS X est proscrit, car il transmet les mots de passe en clair sur le réseau).

Pour les usagers de Samba:

Si vous utilisez un serveur Samba qui se base sur le protocole SMB avec LM, il n'est plus possible de vous identifier en utilisant le domaine Active Directory STI. Il est impératif de mettre à jour les serveurs Samba en version 3.0 qui supportent l'identification Kerberos: ***http://www.samba.org/***.

2. éviter de conserver des chaînes de hachage Lan Manager

Cette étape est essentielle, il est inutile de supprimer une source d'attaque si on conserve localement les informations néfastes. Pour des plates-formes récentes (Windows XP et 2003), une GPO peut facilement réaliser cette opération. Pour des systèmes plus anciens, comme Windows 2000, il est nécessaire de modifier la base de registre de chaque machine, en particulier sur tous les contrôleurs de domaine, pour éviter de conserver ces chaînes localement. Elle est décrite dans la base de connaissances sous l'article: ***http://support.microsoft.com/default.aspx?scid=kb;en-us;299656.***

- lancer l'éditeur de registre (**démarrer->exécuter ; Regedt32.exe**)
- sélectionner la clé de registre suivante: **HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Lsa**
- dans le menu **Edit->Add Key, NoLMHash, Enter**
- quitter l'éditeur de registre
- redémarrer l'ordinateur
- changer les mots de passe locaux (ou ceux du domaine dans le cas de contrôleurs).

Il est indispensable de suivre cette procédure pas par pas.

3. changer le mot de passe de tous les usagers

Default Domain Policy

Computer Configuration (Enabled)

Windows Settings

Security Settings

Account Policies/Password Policy

Policy	Setting
Enforce password history	10 passwords remembered
Maximum password age	999 days
Minimum password age	1 days
Minimum password length	9 characters
Password must meet complexity requirements	Enabled
Store passwords using reversible encryption	Disabled

Peut-être l'étape nécessitant le plus d'entregent, il est toujours douloureux de modifier ses habitudes, en particulier pour un objet (qui devrait rester) personnel comme un mot de passe. Cette mesure peut sembler difficile, mais c'est la seule qui élimine les chaînes de hachage des contrôleurs de domaine (si l'étape 2 est réalisée). En contrepoint de cette mesure, il est préférable d'augmenter la complexité des mots

de passe. Elle est augmentée de manière globale pour tout le domaine AD STI (voir tableau de la GPO ci-dessus).

Cette nouvelle règle de sécurité n'autorise que des mots de passe de 9 caractères au minimum avec la complexité suivante:

- ne pas être le même que le mot de passe précédent.
- ne pas contenir une partie de l'identifiant.
- contenir au moins un caractère de trois des quatre catégories suivantes:
  - a..z
  - A..Z
  - 0..9
  - autres caractères

Il est recommandé d'inclure au moins un des caractères décrits dans le tableau suivant avec la combinaison de touches: touche ALT enfoncée + touches chiffres du clavier numérique déporté.

1 = ☺	19 = ‼	132 = ä	166 = ª	184 = ╕	202 = ╩	220 = ▄	238 = ∈
2 = ☻	20 = ¶	134 = å	167 = º	185 = ╣	203 = ╦	221 = ▌	239 = ∩
3 = ♥	21 = §	135 = ç	168 = ¿	186 = ║	204 = ╠	222 = ▐	240 = ≡
4 = ♦	22 = ▬	142 = Ä	169 = ⌐	187 = ╗	205 = ═	223 = ▀	241 = ±
5 = ♣	23 = ↨	143 = Å	170 = ¬	188 = ╝	206 = ╬	224 = α	242 = ≥
6 = ♠	24 = ↑	144 = É	171 = ½	189 = ╜	207 = ╧	225 = ß	243 = ≤
7 = •	25 = ↓	145 = æ	172 = ¼	190 = ╛	208 = ╨	226 = Γ	244 = ⌠
8 = ◘	26 = →	146 = Æ	173 = ¡	191 = ┐	209 = ╤	227 = π	245 = ⌡
9 = ○	27 = ←	148 = ö	174 = «	192 = └	210 = ╥	228 = Σ	246 = ÷
10 = ◙	28 = ∟	153 = Ö	175 = »	193 = ┴	211 = ╙	229 = σ	247 = ≈
11 = ♂	29 = ↔	154 = Ü	176 = ░	194 = ┬	212 = ╘	230 = µ	248 = °
12 = ♀	30 = ▲	155 = ¢	177 = ▒	195 = ├	213 = ╒	231 = τ	249 = •
13 = ♪	31 = ▼	156 = £	178 = ▓	196 = ─	214 = ╓	232 = Φ	250 = ·
14 = ♫	32 = S	157 = ¥	179 = │	197 = ┼	215 = ╫	233 = Θ	251 = √
15 = ☼	127 = ⌂	158 = ₧	180 = ┤	198 = ╞	216 = ╪	234 = Ω	252 = ⁿ
16 = ►	128 = Ç	159 = ƒ	181 = ╡	199 = ╟	217 = ┘	235 = δ	253 = ²
17 = ◄	129 = ü	164 = ñ	182 = ╢	200 = ╚	218 = ┌	236 = ∞	254 = ■
18 = ↕	130 = é	165 = Ñ	183 = ╖	201 = ╔	219 = █	237 = φ	255 = ʙ

ou des caractères Unicode suivants (le 0 est nécessaire):

0127 = ?	0162 = ¢	0170 = ª	0181 = µ	0188 = ¼	0198 = Æ	0220 = Ü	0231 = ç
0131 = ƒ	0163 = £	0171 = «	0182 = ¶	0189 = ½	0199 = Ç	0223 = ß	0233 = é
0135 = ‡	0164 = ¤	0172 = ¬	0183 = ·	0191 = ¿	0201 = É	0228 = ä	0241 = ñ
0149 = •	0165 = ¥	0176 = °	0186 = º	0196 = Ä	0209 = Ñ	0229 = å	0246 = ö
0160 = ʙ	0166 = ¦	0177 = ±	0187 = »	0197 = Å	0214 = Ö	0230 = æ	0247 = ÷
0161 = ¡	0167 = §	0178 = ²					

Pour éviter toutes mésaventures, il est préférable de tester ces caractères spéciaux dans un traitement de texte avant de les employer comme mot de passe.

Ces caractères ne sont pas présents dans les tables de hachage précalculées ou dans les outils disponibles. Ainsi, leur utilisation augmente la durée du calcul pour casser le code. En conjonction avec les autres mesures (uniquement NTLMv2 et pas de chaîne de hachage LM), la sécurité est raisonnablement établie.

Remarque: Si votre mot de passe dépasse 14 caractères, il n'est par définition, pas conservé sous la forme d'une chaîne de hachage Lan Manager. Ainsi dans ce cas, il n'est pas nécessaire de le changer.

4. Maintenir sa machine dans un état sanitaire correct

La tendance hygiéniste de la fin du 19e ou du début du 20e dans le monde occidental peut être appliquée dans le domaine informatique. La multiplication des trous de sécurité, en particulier issue de l'intégration du butineur Internet (IE) dans le noyau du système (peut-être la plus mauvaise idée de la décennie chez Microsoft), entraîne une profusion de mises à jour. Seule une méthode automatique d'application des rustines (ou patches) permet d'assurer un état sanitaire correct.

Software Update Service

L'outil décrit dans mon article du FI9/2003: **Vers, virus et autres calamités**, ***http://dit.epfl.ch/publications-spip/article.php3?id_article=239*** permet de réaliser sans frais de licence cette opération. Le principal reproche qu'on peut faire à Software Update Service (SUS) est son opacité de fonctionnement et l'incapacité de vérifier sur le serveur son action sur les clients. Heureusement, dans la communauté des développeurs, Stanley Appel a réalisé une application qui répond à ce problème et l'a rendue disponible avec une licence GPL: ***http://susreport.perot.nl***. Cet outil semble parfaitement convenir avec un problème mineur, le tri des ordinateurs: SUS fonctionne de manière similaire à Windows Update, par l'utilisation d'un serveur Web. SUSreports utilise l'historique du serveur Web, il ne possède que les noms DNS statiques des ordinateurs qui ne correspondent pas forcément à la réalité d'Active Directory.

Mon apprentie, Aline Genoud, a réalisé comme travail pratique de fin d'apprentissage une modification de ce

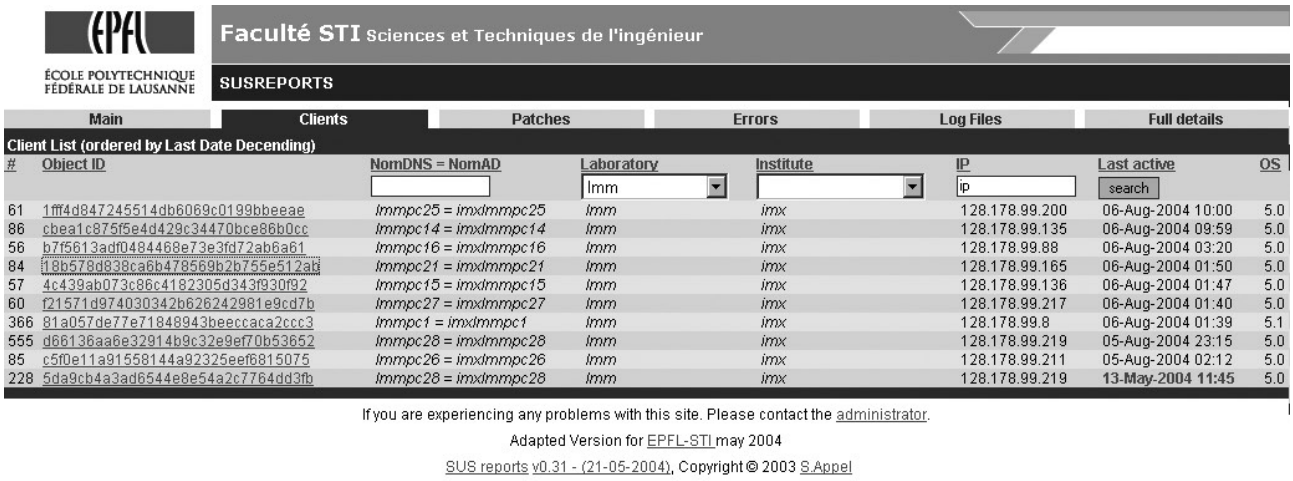
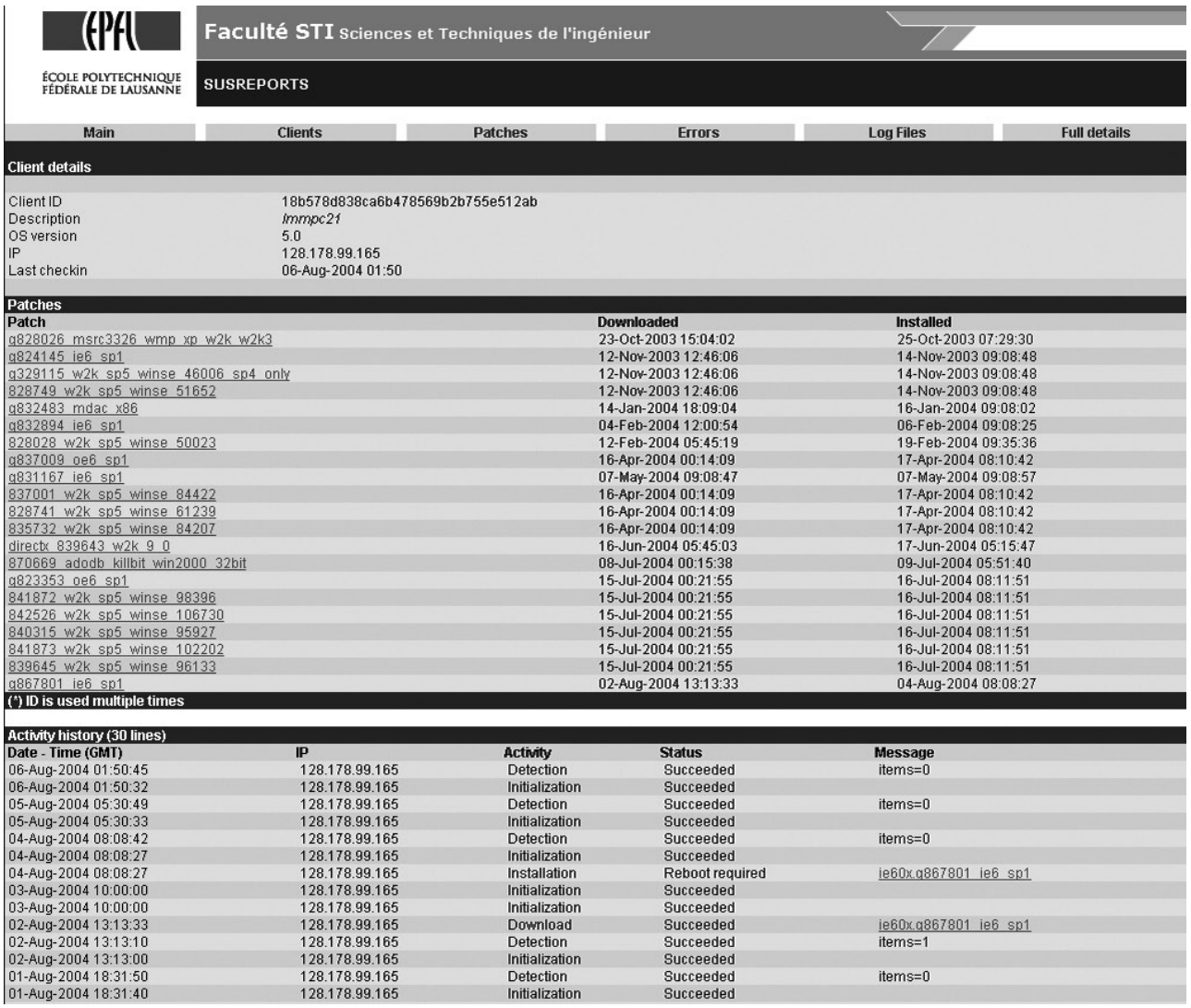


fig. 1 – SusReport pour un laboratoire



ÉCOLE POLYTECHNIQUE FÉDÉRALE DE LAUSANNE

Faculté STI Sciences et Techniques de l'ingénieur

SUSREPORTS

Main | Clients | Patches | Errors | Log Files | Full details

Client details

Client ID	18b578d838ca6b478569b2b755e512ab
Description	*lmmpc21*
OS version	5.0
IP	128.178.99.165
Last checkin	06-Aug-2004 01:50

Patches

Patch	Downloaded	Installed
q828026_msrc3326_wmp_xp_w2k_w2k3	23-Oct-2003 15:04:02	25-Oct-2003 07:29:30
q824145_ie6_sp1	12-Nov-2003 12:46:06	14-Nov-2003 09:08:48
q329115_w2k_sp5_winse_46006_sp4_only	12-Nov-2003 12:46:06	14-Nov-2003 09:08:48
828749_w2k_sp5_winse_51652	12-Nov-2003 12:46:06	14-Nov-2003 09:08:48
q832483_mdac_x86	14-Jan-2004 18:09:04	16-Jan-2004 09:08:02
q832894_ie6_sp1	04-Feb-2004 12:00:54	06-Feb-2004 09:08:25
828028_w2k_sp5_winse_50023	12-Feb-2004 05:45:19	19-Feb-2004 09:35:36
q837009_oe6_sp1	16-Apr-2004 00:14:09	17-Apr-2004 08:10:42
q831167_ie6_sp1	07-May-2004 09:08:47	07-May-2004 09:08:57
837001_w2k_sp5_winse_84422	16-Apr-2004 00:14:09	17-Apr-2004 08:10:42
828741_w2k_sp5_winse_61239	16-Apr-2004 00:14:09	17-Apr-2004 08:10:42
835732_w2k_sp5_winse_84207	16-Apr-2004 00:14:09	17-Apr-2004 08:10:42
directx_839643_w2k_9_0	16-Jun-2004 05:45:03	17-Jun-2004 05:15:47
870669_adodb_killbit_win2000_32bit	08-Jul-2004 00:15:38	09-Jul-2004 05:51:40
q823353_oe6_sp1	15-Jul-2004 00:21:55	16-Jul-2004 08:11:51
841872_w2k_sp5_winse_98396	15-Jul-2004 00:21:55	16-Jul-2004 08:11:51
842526_w2k_sp5_winse_106730	15-Jul-2004 00:21:55	16-Jul-2004 08:11:51
840315_w2k_sp5_winse_95927	15-Jul-2004 00:21:55	16-Jul-2004 08:11:51
841873_w2k_sp5_winse_102202	15-Jul-2004 00:21:55	16-Jul-2004 08:11:51
839645_w2k_sp5_winse_96133	15-Jul-2004 00:21:55	16-Jul-2004 08:11:51
q867801_ie6_sp1	02-Aug-2004 13:13:33	04-Aug-2004 08:08:27

(*) ID is used multiple times

Activity history (30 lines)

Date - Time (GMT)	IP	Activity	Status	Message
06-Aug-2004 01:50:45	128.178.99.165	Detection	Succeeded	items=0
06-Aug-2004 01:50:32	128.178.99.165	Initialization	Succeeded	
05-Aug-2004 05:30:49	128.178.99.165	Detection	Succeeded	items=0
05-Aug-2004 05:30:33	128.178.99.165	Initialization	Succeeded	
04-Aug-2004 08:08:42	128.178.99.165	Detection	Succeeded	items=0
04-Aug-2004 08:08:27	128.178.99.165	Initialization	Succeeded	
04-Aug-2004 08:08:27	128.178.99.165	Installation	Reboot required	ie60x:q867801_ie6_sp1
03-Aug-2004 10:00:00	128.178.99.165	Initialization	Succeeded	
03-Aug-2004 10:00:00	128.178.99.165	Initialization	Succeeded	
02-Aug-2004 13:13:33	128.178.99.165	Download	Succeeded	ie60x:q867801_ie6_sp1
02-Aug-2004 13:13:10	128.178.99.165	Detection	Succeeded	items=1
02-Aug-2004 13:13:00	128.178.99.165	Initialization	Succeeded	
01-Aug-2004 18:31:50	128.178.99.165	Detection	Succeeded	items=0
01-Aug-2004 18:31:40	128.178.99.165	Initialization	Succeeded	

fig. 2 – Historique des mises à jour d'un ordinateur

programme pour intégrer les informations issues d'Active Directory (fig. 1).

Ainsi, il est possible d'isoler les clients issus d'un laboratoire ou d'un institut, et de vérifier les modifications appliquées à un ordinateur spécifique (fig. 2).

Les administrateurs seraient tentés d'attendre le successeur de SUS, Windows Update, mais la dernière date annoncée aux personnes qui désirèrent tester ce nouvel outil est mi-2005. On peut donc continuer à utiliser SUS et son corollaire SUSreports.

Pour l'utilisation d'un antivirus mis à jour automatiquement, voir l'article de Christian Raemy du FI6/2003: **VirusScan 7.0 se dope à l'ePO - Legalize It !**, ***http://dit.epfl.ch/publications-spip/article.php3?id_article=112***, est également une bonne mesure de prophylaxie

5. éduquer les usagers

Comme école, notre credo est l'enseignement. Il est difficile à faire admettre, que contrairement à la tendance actuelle de n'avoir qu'un seul mot de passe valable pour toutes nos activités, il est largement plus sûr de posséder un mot de passe par type d'accès. Ainsi, un trou de sécurité n'affecte qu'un service. Je sais que cette règle semble rétrograde, en particulier avec la mise en œuvre de technologie comme Passport chez Microsoft ou KeyChain chez Apple, mais elle reste une garantie contre l'usurpation d'identité.

Une mesure éducative beaucoup plus simple est de demander à un usager de ne jamais communiquer un mot de passe à une autre personne, même à un administrateur système. Si le mot de passe est communiqué, de le changer après sa communication.

On pourrait également imaginer que la curiosité n'est pas toujours bien placée, en particulier quand on reçoit un courriel. Que faire d'un message dont le contenu est un fichier Zip avec un mot de passe sous la forme d'une image (un peu complexe comme méthode de transfert ?). Il faut évidemment le mettre à la poubelle !

En conclusion, la lutte entre l'épée et le bouclier n'est pas près de s'arrêter. La vigilance permet d'éviter le plus possible de se retrouver avec des problèmes de sécurité. ■