Sécurité :

Mots de passe windows

(Attack/defense)

Abd Amesrouy
{Epitech.}
4ème année

21 Janvier 2002

Table des matières

Introduction

Cette présentation va aborder six points :

- Les différents algorithmes de chiffrement
- La localisation des empreintes
- Les méthodes de crackage
- Les logiciels de crackage
- La protection des mots de passe
- Le durcissement des mots de passe

Pour chaque point les spécificités Unix et Windows NT seront soulignées

Chapitre 1

Les différents algorithmes de chiffrement

L'algorithme utilisé dépend fortement du contexte :
- Unix
- Windows NT
- Réseau

1.1 Stockage d'un mot de passe

- Le mot de passe n'existe qu'en version chiffrée

1.2 Chiffrement d'un mot de passe

- L'algorithme utilisé doit être non inversible.
- Le mot de passe sert de clé
- Une graine (ou piment) sert de diversifiant

1.3 Vérification d'un mot de passe

- La comparaison s'effectue toujours sur le mot de passe chiffré.

1.4 Les différents algorithmes de chiffrement sous Windows NT

- LanMan :

  - Le mot de passe est mis en majuscule et divisé en deux parties de 7 caractères Chaque moitié sert à chiffrer en DES la chaîne "zéro" :
  - Attaques limitées à des mots de 7 caractères
  - Aucune graine n'est utilisée pour empêcher les attaques par dictionnaires pré-calculés
- NTLM :
  - Le MD4 du mot de passe en Unicode
  - Aucune graine n'est utilisée pour empêcher les attaques par dictionnaires pré-calculés

1.5 Les différents algorithmes de chiffrement sur le Réseau (1/2)

L'algorithme utilisé dépend fortement du protocole applicatif utilisé mais aussi de son niveau

- En clair : telnet, ftp, r* commandes, pop, http, etc.
- Challenge / réponse : principe
  - A la connexion d'un client, le serveur envoie une chaîne nommée challenge.
  - Le client calcule la réponse à partir du challenge, du mot de passe, d'autres données éventuellement et d'une fonction donnée.
  - Le client renvoie la réponse au serveur qui a effectué le même calcul de son côté.
  - L'accès est autorisé si les deux réponses sont identiques.

1.6 Les différents algorithmes de chiffrement sur le Réseau (2/2)

- Challenge / réponse :
  - apop (rfc1939) : la réponse est le md5 de la concaténation du challenge et du mot de passe.
  - HTTP Digest (rfc2617) : la réponse est le md5 de la concaténation de plusieurs chaînes
  - SMB :
    - chaque tiers du mot de passe chiffré sert de clé au chiffrement du challenge en DES.
    - Suivant les versions du client et du serveur, ce sont les empreintes LanMan et/ou NTLM qui sont utilisées.

- NTLMv2 utilise HMAC-MD5 (rfc2104).
  - Particularité : quand la longueur de la clé est supèrieure à 64 bits, les autres bits sont jetés alors que le RFC implique le calcul du md5 de la clé.

Chapitre 2

La localisation des empreintes

Une empreinte est le résultat du hachage d'un mot de passe par un algorithme non réversible. Cette opération permet d'enregistrer dans le système une "image" du mot de passe et empêche quiconque d'accéder au mot de passe en clair. La localisation des empreintes dépend fortement du contexte :

- Unix
- Windows NT
- Applications

2.1 La localisation des empreintes sous Windows NT

Avertissement :

- De nombreux clients sauvegardent les mots de passe des utilisateurs de façon réversible et accessible à tous dans la base de registre ou dans des fichiers utilisateurs.
- Les problèmes engendrés par ces mots de passe dépassent l'objet de cette présentation.
- SAM :
  - `$windir$\system32\config\sam`
  - `$windir$\repair\sam`
  - Disquette de réparation
- Contenu de la SAM :
  - Chaque moitié de chaque empreinte est obscurci par du chiffrement DES
    - Cela permet que deux utilisateurs ayant le même mot de passe n'aient pas la même entrée dans la SAM.
  - La première moitié est chiffrée avec le RID de l'utilisateur.

    - Le RID est composé des 32 bits de poids faible du SID.
  - La seconde moitié est chiffrée avec une valeur calculée à partir du RID de l'utilisateur.
  - voir "Offline NT Password & Registry Editor" ¡ http ://home.eunet.no/ pnordahl/ntpasswd/¿
- frontpage : attention aux fichiers *.pwd

2.2 La localisation des empreintes applicatives

- apache : les fichiers .htpasswd contiennent des mots de passe DES / MD5 / SHA ou en clair
- apop : les fichiers /.apop/secret contiennent des mots de passe en clair
- wwwboard, discus board, etc. : les fichiers suivants contiennent des mots de passe DES
  - admin.txt
  - passwd.txt
  - users.txt

Chapitre 3

Les méthodes de crackage

- Par ingéniérie sociale
- Par dictionnaires
- Par force brute

3.1 Ingéniérie sociale

- login
- nom et prénom de l'utilisateur
- nom de films preferes, phrases utilisees, nom des membre de sa famille..

3.2 Dictionnaires

- Types de dictionnaires :
  - Mots courants de la langue natale de l'utilisateur
  - Prénoms et noms de même origine que l'utilisateur
  - Noms de personnages et d'acteurs
  - Vocabulaires propres à des livres, films, séries, jeux...
- ftp ://sable.ox.ac.uk/pub/wordlists/

3.3 Dictionnaires : transformations

- Types de transformations :
  - Zéro, une, toutes les lettres en majuscule
  - mot renversé, dupliqué
  - suffixer et/ou préfixer un chiffre et/ou un caractère de ponctuation
  - substitution de lettres par des chiffres

3.4 Dictionnaires : pré-calculés

- Chaque mot d'un dictionnaire est chiffré et sauvegardé dans une base de données :
  - nécessite une phase de préparation longue
  - utilisation de mémoire de masse importante
  - phase de crackage très rapide puisque limité à des recherches dans une base
- Seule une image du mot de passe chiffré est sauvegardé dans la base :
  - économie d'utilisation de mémoire de masse
  - phase de crackage moins rapide puisque nécessite des chiffrements

3.5 Force brute

- toutes les combinaisons possibles d'un ensemble de caractères
- "force brute intelligente" :
  - Génération de statistiques sur l'ensemble des mots de passe déjà crackés
  - Utilisation de ces statistiques pour ordonner la génération de mots de passe

Chapitre 4

Les logiciels de crackage

- Crack
- John the Ripper
- L0phtCrack
- Password Appraiser
- c2myazz
- Autres...

4.1 Crack

- Crack 5.0a du 21/12/1996 - Open Source
- Auteur : Alec Muffett
- HomePage : http ://www.users.dircon.co.uk/ crypto/
- Seul le chiffrement DES est supporté en standard
- Peut utiliser la fonction crypt du système pour supporter d'autres algorithmes

4.2 John the Ripper

- John the Ripper v1.6 du 03/12/1998 - Open Source
- Auteur : Solar Designer
- HomePage : http ://www.openwall.com/john/
- Supporte les chiffrements DES , BSDI DES , MD5 , Blowfish et LanMan et les processeurs x86 , sparc , alpha , ppc , pa-risc et mips 32 et 64 bits
- Fournit des fonctions avancées de génération de mots de passe à partir de règles de transformations, de statistiques ou de programmation.
- Possède les implémentations DES et MD5 les plus rapides

4.3 L0phtCrack

- L0phtCrack 2.52 for Win95/NT du 13/01/1999 - ShareWare
- Auteurs : L0pht (Mudge et d'autres)
- HomePage : http ://www.l0pht.com/l0phtcrack/
- Supporte les chiffrements LanMan et NTLM avec et sans challenge / réponse
- Fournit un sniffer permettant de récupérer des empreintes sur le réseau
- Permet de récupérer la SAM par SMB
- Possède l'implémentation LanMan la plus rapide

4.4 Password Appraiser

- Password Appraiser 3.20 for Microsoft Windows NT Systems (1998) - Commercial version de démonstration disponible
- Editeur : Quakenbush Consulting, Inc.
- HomePage : www.quakenbush.com
- Ne supporte que le chiffrement LanMan
- Fonctionnement par dictionnaire pré-calculé
- La version commerciale fourni un dictionnaire pré-calculé sur CDROM
- Attention : les empreintes peuvent être envoyées au site web pour interrogation de la base centrale.

4.5 c2myazz

- c2myazz pour MSDOS du 11/04/97 - Open Source
- Auteur : inconnu
- HomePage : aucune
- Ne supporte que les mots de passe en clair lors de connexions à des partages SMB
- Fonctionnement par attaque active :
  - Ecoute le réseau,
  - Attend qu'un client envoie à un serveur la liste des dialectes qu'il connait,
  - Demande au client d'envoyer son mot de passe en clair en répondant plus rapidement que le serveur.

4.6 Autres logiciels de crackage

Liste non exhaustive :

- DES : de très nombreux...
- Windows NT : principalement sous Unix à utiliser avec pwdump
  - NTCrack
  - lc15 (L0phtCrack v1.5)
- cisco (mode 7) : ciscocrack , cisco_decrypt7
- bases LDAP : utiliser une fonction sha1 standard
- Basic HTTP : echo 'ZHVjYW1wOlBldGl0Q3VyaWV1eDstKQ==' — mimencode -u
- et tant d'autres...
- fichiers *.pwl de windows 3.x à windows 95 : Pwlcrack et beaucoup d'autres...
- mots de passe POP / IMAP
  - fichier preferences.js de Navigator
  - clés de registre de MSIE

Chapitre 5

La protection des mots de passe

- La protection des mots de passe peut être réalisée à plusieurs niveaux :
  - dans le système
  - sur le réseau
  - au niveau applicatif

5.1 La protection des mots de passe Windows NT

- syskey
  - Chiffrement du contenu de la SAM en DES
  - Le mot de passe est :
    - soit sauvegardé sur une disquette
    - soit sauvegardé dans la partition système
    - soit demandé lors du démarrage du système
  - Toujours accessible "en clair" pour tout utilisateur avec les droits de débogage : pwdump2 DLL Injection sur le processus lsass.exe
  - Défaut d'implémentation (trouvé mi décembre 99 par bindview.com) :
    - Le même flux RC4 chiffre les empreintes LanMan et NTLM d'un utilisateur La clé est basée sur le numéro de l'utilisateur (RID)
    - Attaque possible en calculant les empreintes LanMan et NTLM de chaque mot de passe candidat.

5.2 La protection des mots de passe sur le réseau : pourquoi ?

- linsniff666.c : début des connexions ftp, telnet, pop2, pop3, imap2, login.
- readsmb2.c / l0phtcrack 2.x : challenge et réponse smb.
- dsniff ¡ http ://naughty.monkey.org/ dugsong/dsniff/¿ par Dug Song ¡ mailto :dugsong@monkey.org¿ : les mots de passe en clair (ou obscurcis) dans 28 protocoles :
- FTP, Telnet, HTTP, POP, poppass, NNTP, IMAP, SNMP, LDAP, Rlogin, RIP, OSPF,
- NFS, YP, SOCKS, X11, CVS, IRC, AIM, ICQ, Napster, PostgreSQL, Meeting Maker,
- Citrix ICA, Symantec pcAnywhere, NAI Sniffer, Microsoft SMB, Oracle SQL*Net.

5.3 La protection des mots de passe sur le réseau : SMB

- SMB :
  - Sur chaque client : Interdire l'envoi du mot de passe en clair sur le réseau
    - Win95 & Win98 :
    - `[HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\VxD\VNETSUP]`
    - "EnablePlainTextPassword"=dword :00000000
    - Windows NT (par défaut depuis NT4-SP3) :
    - `[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Rdr\Parameters]`
    - "EnablePlainTextPassword"=dword :00000000
    - Windows 2000 (par défaut) :
    - `[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\LanmanWorkStation\Pa`
    - "EnablePlainTextPassword"=dword :00000000
  - Sur chaque serveur : Limiter le chiffrement à NTLM (NTLMv2 à partir du SP4 de NT4) voir "How to Disable LM Authentication on Windows NT" ¡ http ://support.microsoft.com/support/kb/articles/q147/7/06.asp¿

5.4 La protection des mots de passe sur le réseau : extensions MicroSoft

- challenge / réponse NTLM :
  - Microsoft a porté son système de challenge / réponse NTLM dans plusieurs protocoles ouverts : HTTP, IMAP, LDAP, NNTP et POP3
  - Avantages :
    - Le mot de passe n'est plus envoyé en clair
  - Inconvénients :
    - Dans une implémentation modifiée d'un client : la connaissance de l'empreinte du mot de passe suffit à s'authentifier.
    - Il s'agit d'extensions non documentées implémentées seulement dans
      - les serveurs IIS et Exchange
      - les clients Internet Explorer et Outlook.
  - Internet Explorer refuse d'utiliser NTLM dans HTTP au travers d'un relai
  - fetchmail permet d'utiliser l'authentification NTLM dans IMAP.

Chapitre 6

Le durcissement des mots de passe

- Permet de n'accepter un nouveau mot de passe seulement après s'être assuré qu'il suit un certain nombre de règles.
- Le durcissement des mots de passe est toujours lié au système

6.1 Pourquoi durcir les mots de passe ?

- Constitution des mots de passe crackés
- 2215 (100.00 %) Mots de passe crackés
-
- 1015 (45.82 %) Un mot en minuscules
- 441 (19.91 %) Un mot en minuscules suivi du chiffre '1'
- 209 (9.44 %) Un mot en minuscules suivi d'un chiffre autre que '1'
- 2 (0.09 %) Un mot en minuscules suivi d'une majuscule
- 40 (1.81 %) Un mot en minuscules suivi d'un autre caractère
-
- 38 (1.72 %) Le chiffre '1' suivi d'un mot en minuscules
- 12 (0.54 %) Un chiffre autre que '1' suivi d'un mot en minuscules
- 7 (0.32 %) Un autre caractère suivi d'un mot en minuscules
-
- 191 (8.62 %) Plusieurs chiffres suivis d'un mot en minuscules
- 5 (0.23 %) Un mot en minuscules suivis de plusieurs chiffres
- 12 (0.54 %) minuscule(s) chiffre(s) minuscule(s)
- 2 (0.09 %) chiffre(s) minuscule(s) chiffre(s)
- 57 (2.57 %) nombre
- 9 (0.41 %) minuscules et chiffres

–
– 88 (3.97 %) Une majuscule suivi de minuscule(s)
– 22 (0.99 %) Une majuscule suivi de minuscule(s) et du chiffre '1'
– 11 (0.50 %) Une majuscule suivi de minuscule(s) et d'un chiffre autre que '1'
– 1 (0.05 %) Une majuscule suivi de minuscule(s) et de chiffres
– 1 (0.05 %) Une majuscule suivi de minuscule(s) et d'une majuscule
– 8 (0.36 %) Une majuscule suivi de minuscule(s) et d'un autre caractère
–
– 24 (1.08 %) Un mot en majuscules
– 1 (0.05 %) Un mot en majuscules suivi du chiffre '1'
– 2 (0.09 %) Un mot en majuscules suivi d'un autre chiffre
– 1 (0.05 %) Un mot en majuscules suivi de plusieurs chiffres
– 0 (0.00 %) Un mot en majuscules suivi d'un autre caractère
– 1 (0.05 %) Une suite de majuscule(s) et de minuscule(s)
– 0 (0.00 %) Une suite de majuscule(s) et de chiffre(s)
– 1 (0.05 %) Une suite de majuscule(s), de minuscule(s) et de chiffre(s)
–
– 14 (0.63 %) Toute autre combinaison de caractères
– Longueur des mots de passe crackés
– 0 0.32
– 1 0.09
– 2 0.81
– 3 4.56
– 4 7.04
– 5 10.47
– 6 34.22
– 7 19.68
– 8 22.89
– 16.6 % des mots de passes crackés sont directement déductibles du login
– 29,2 % avec les informations associées à l'utilisateur
– Les temps de crackage de plus en plus courts :
  – DES (206182 c/s) :
    – chiffrement DES de 7 caractères en minuscules : 11 heures
    – chiffrement DES de 7 caractères alphanumériques : 4,5 jours
    – chiffrement DES de 8 caractères en minuscules : 12,2 jours
    – chiffrement DES de 8 caractères alphanumériques : 5,3 mois
  – LANMAN (1883174 c/s) :
    – chiffrement LANMAN de 7 caractères alphabétiques : 1 heure 15
    – chiffrement LANMAN de 7 caractères alphanumériques : 12 heures
    – chiffrement LANMAN de 7 caractères (69 caractères) : 1,5 mois

- DES avec une machine "EFF" (4,5E9 c/s) :
  - chiffrement DES de 8 caractères (95 caractères) : 17,5 jours...
    - Le nombre de tests possibles pour les autres chiffrements sont :
- BSDI DES : 7169 c/s
- FreeBSD MD5 : 1180 c/s
- OpenBSD Blowfish : 84.4 c/s
  - Les mots de passe choisis par les utilisateurs non avertis sont trop simples
  - Pour accéder à un système il suffit d'un seul mot de passe

6.2 Le durcissement des mots de passe sous Windows NT

- passfilt.dll
  - Fourni avec les Services Packs de Windows NT depuis NT4 SP2 Attention : installation manuelle par changement d'une clé de registre
  - Trop basique et non configurable :
    - Au moins 6 caractères
    - 2 caractères parmi les majuscules, les chiffres et les signes de ponctuation. Par exemple, Bonjour1 est accepté!!!
  - Il est conseillé d'utiliser une implémentation d'un fournisseur tiers.

6.3 Quelques règles de constitution d'un mot de passe

- Il doit contenir 6 à 7 caractères au moins.
- Il doit utiliser :
  - des caractères de contrôle,
  - et/ou de ponctuation,
  - et/ou des chiffres
  - et/ou des lettres majuscules et minuscules.
- Il ne doit pas faire référence à une information :
  - générale ou personnelle.
  - liée à l'installation du système, à l'entreprise ou à l'organisation.
- Ne doit pas être un simple mot référencé dans un dictionnaire (français, anglais ou autre)
- Ne doit pas être un des exemples donnés dans le cours
- Méthodes simples pour obtenir de bons mots de passe faciles à retenir :

  - combiner deux mots existants en introduisant des chiffres et/ou des caractères de ponctuation,
  - utiliser des mots écrits en phonétique, et de préféférence d'une autre langue.
  - utiliser les premières lettres de vers, phrases, expressions, adresses, etc.
- Exemples de bons mots de passe :
  - Beau !C', Atout ;Kc, C2much+, Love4evEr, 10Cquer, 13abilE, 47AdlDL, HqcUafulv.
- Exemples de mauvais mots de passe
  - racine, rootroot, toor, super, tOtO, vax, foobar, CB3506, 8786VL92, charlotte, azerty, Paris, 28Jul92, 24/04/89, 12345678.