HERVÉ SCHAUER CONSULTANTS
Cabinet de Consultants en Sécurité Informatique depuis 1989
Spécialisé sur Unix, Windows, TCP/IP et Internet

SSTIC 2007 – Rump Session

Jeudi 31 mai 2007

RainbowTables et caractères accentués sous Windows

Guillaume Lehembre
<Guillaume.Lehembre@hsc.fr>

Introduction

- RainbowTables = Tables pré-calculées
  - Contient une combinaison d'empreintes (*hashes*) et de mots de passe
  - Amélioration compromis temps-mémoire (*Time Memory TradeOff*) inventé par Martin Hellman – Philippe Oechslin (LASEC/EPFL)
- RainbowCrack = Implémentation des RainbowTables
  - Supporte les empreintes Windows (LM & NTLM), MD2, MD4, MD5, SHA1, MySQL (v3.23, SHA1), RIPEMD160, Cisco PIX, Oracle (graîne), MsCash (graîne), etc.
- Empreintes LM stockées par défaut sur tous les Windows
  - Suppression de l'enregistrement des empreintes LM possible pour tous les OS supérieurs à Windows 2000 SP2
    - Attention aux « effets de bord » avec les anciens systèmes/applicatifs
  - Windows NT supporte le NTLM depuis le SP3
  - Plus de stockage des empreintes LM dans Vista (enfin)

Table de correspondance

- Les tables LM disponibles publiquement sont basées sur les caractères anglo-saxons
  - ↳ Pas de support des caractères accentués
- Création de la table de correspondance :
  - Génération des empreintes de tous les caractères accentués sur des OS français et anglais (= création d'un jeu de test complet)
  - Création d'une table RainbowTables d'un caractère avec un espace de caractères (*charset*) complet
  - Cassage des empreintes et découverte du/des codes hexadécimaux des caractères trouvés par RainbowCrack
  - Création d'une table de correspondance permettant de connaître les permutations possibles pour un caractère découvert par RainbowCrack (ex : caractère découvert E → combinaisons possibles : è, È, ê, Ê, ë, Ë)
  - ↳ Pourrait être généralisé en utilisant les fonctions utilisées par Windows

Table de correspondance


```
            - CAIN & ABEL (LM) -
            - ENG -        - FR -     - Rcrack -
à [0xE0] -> A [0x41] -> À [0xC0] -> A [0x41] & · [0xB7]
À [0xC0] -> A [0x41] -> À [0xC0] -> A [0x41] & · [0xB7]
â [0xE2] -> A [0x41] -> Â [0xC2] -> A [0x41] & ¶ [0xB6]
Â [0xC2] -> A [0x41] -> Â [0xC2] -> A [0x41] & ¶ [0xB6]

ç [0xE7] -> Ç [0xC7] -> Ç [0xC7] -> [0x80]
Ç [0xC7] -> Ç [0xC7] -> Ç [0xC7] -> [0x80]

é [0xE9] -> É [0xC9] -> É [0xC9] -> [0x90]
É [0xC9] -> É [0xC9] -> É [0xC9] -> [0x90]
è [0xE8] -> E [0x45] -> È [0xC8] -> E [0x45] & Ô [0xD4]
È [0xC8] -> E [0x45] -> È [0xC8] -> E [0x45] & Ô [0xD4]
ê [0xEA] -> E [0x45] -> Ê [0xCA] -> E [0x45] & Ò [0xD2]
Ê [0xCA] -> E [0x45] -> Ê [0xCA] -> E [0x45] & Ò [0xD2]
ë [0xEB] -> E [0x45] -> Ë [0xCB] -> E [0x45] & Ó [0xD3]
Ë [0xCB] -> E [0x45] -> Ë [0xCB] -> E [0x45] & Ó [0xD3]

ï [0xEF] -> I [0x49] -> Ï [0xCF] -> I [0x49] & Ø [0xD8]
Ï [0xCF] -> I [0x49] -> Ï [0xCF] -> I [0x49] & Ø [0xD8]
î [0xEE] -> I [0x49] -> î [0xEE] -> I [0x49] & × [0xD7]
Î [0xCE] -> I [0x49] -> î [0xEE] -> I [0x49] & × [0xD7]

ô [0xF4] -> O [0x4F] -> Ô [0xD4] -> 0 [0x4F] & â [0xE2]
Ô [0xD4] -> O [0x4F] -> Ô [0xD4] -> 0 [0x4F] & â [0xE2]

ù [0xF9] -> U [0x55] -> Ù [0xD9] -> U [0x55] & ë [0xEB]
Ù [0xD9] -> U [0x55] -> Ù [0xD9] -> U [0x55] & ë [0xEB]
ü [0xFC] -> Ü [0xDC] -> Ü [0xDC] -> [0x9A]
Ü [0xDC] -> Ü [0xDC] -> Ü [0xDC] -> [0x9A]
û [0xFB] -> U [0x55] -> Û [0xDB] -> U [0x55] & ê [0xEA]
Û [0xDB] -> U [0x55] -> Û [0xDB] -> U [0x55] & ê [0xEA]
```

Création des tables

- 13 caractères à mettre dans le *charset* pour supporter les accents français (0x80, 0x90, 0x9A, 0xB6, 0xB7, 0xD2, 0xD3, 0xD4, 0xD7, 0xD8, 0xE2, 0xEA, 0xEB)
- Création de tables avec support des accents :
  - Complexité équivalente aux tables alpha-numeric-symbol32-space
    - 64 tables de 1Go non compressées
    - ~ 9,6 jours de calcul par table, ~ 10 mois de calcul global avec un Core 2 Duo 6400 (Bi-CPU @2.4 Ghz 4Mo cache) avec un rtgen sur chaque CPU
    - Incluant 20 caractères spéciaux (dont l'espace)

```
alpha-numeric-symbol20-accents=
[ABCDEFGHIJKLMNOPQRSTUVWXYZ0123456789,;:!*$?./%&-_@+"'#| [0x80 ... 0xEB]]
```

- Patch + Brève disponible sur le site www.hsc.fr au courant de la semaine prochaine :-)

Exemple

```
testlm:1003:62C6E157263286A35F46BF0576E9C247:37AD8F77155D61A0226575546E0C2041:::

[...]

plaintext of 5f46bf0576e9c247 is C COUL$
plaintext of 62c6e157263286a3 is L@SST1C
statistics
------------------------------------------------------
plaintext found:           2 of 2 (100.00%)
total disk access time:    38.65 s
total cryptanalysis time:  269.26 s
total real/user/system time: 308.67/294.81/1.59 s
total chain walk step:     357837069
total false alarm:         2304
total chain walk step due to false alarm: 11816692

result
------------------------------------------------------
testlm          L@SsT1CcéCôùL$  hex:4c4053735431436 3e943f4f94c24
```

[0x90]

- Note : La casse du mot de passe est obtenue en testant les permutations possibles pour chaque caractère vis à vis de l'empreinte NTLM.

Recommandations

- Utiliser uniquement le stockage des empreintes dans le format NTLM :
  - Au delà de 9 caractères avec un *charset* conséquent, les Rainbowtables deviennent trop longues à calculer
  - Supprimer les empreintes LM :
    - Empêcher le stockage des empreintes LM (Win 2000 SP2 et supérieurs)
      - http://support.microsoft.com/kb/299656/
    - Désactiver l'authentification LM
      - http://support.microsoft.com/kb/147706/
    - Supprimer les empreintes LM existantes – ThrashLM
      - http://www.toolcrypt.org/index.html?thrashlm
- Aucune empreinte LM n'est stockée si :
  - le mot de passe fait plus de 14 caractères;
  - le mot de passe contient certains caractères non présents dans les « pages de code » (*codepage*) originales (0x8X → 0x9X dont €) !

Références & Remerciements

- « *Making a Faster Cryptanatycal Time-Memory Trade-Off* » – Philippe Oechslin – CRYPTO 2003
  - http://lasecwww.epfl.ch/~oechslin/publications/crypto03.pdf
- « Les compromis temps-mémoire et leur utilisation pour casser les mots de passe Windows » – Philippe Oechslin – SSTIC04
  - http://lasecwww.epfl.ch/~oechslin/publications/sstic04.pdf
- RainbowCrack - Zhu Shuanglei
  - http://www.antsight.com/zsl/rainbowcrack/
- RainbowTables en téléchargement libre
  - http://www.freerainbowtables.com/

- Remerciements : Nicolas Collignon & l'équipe HSC & Aurélien Bordes