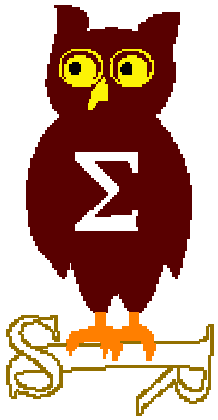
EdelWeb

OSSIR
Groupe Sécurité Windows

Réunion du 11 juin 2001
Le chiffrement de fichiers sous Windows 2000



Ordre du jour

- Windows 2000 : EFS (EdelWeb)
- Présentation du produit SafeGuard Easy (Utimaco)
  - Rodolphe LEFEBVRE
  - Belkacem OULD LAZAZI
- Présentation du produit CryptoGram Folder (CryptoGram)
  - Pierre LAMAGNERE
- Revue des dernières vulnérabilités de Windows 2000 (EdelWeb)

EFS : Sommaire

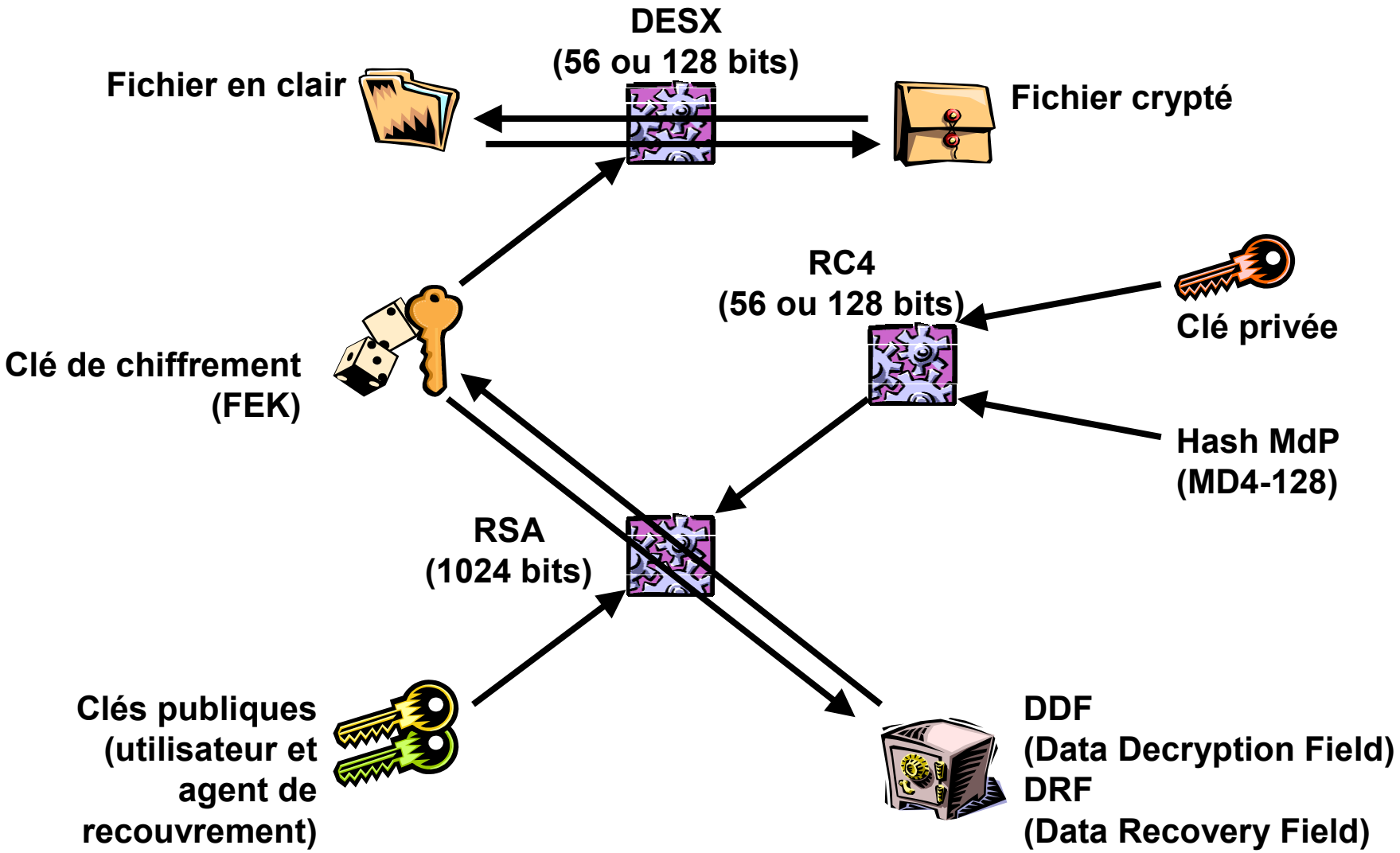
1. Introduction
2. Mécanismes
3. Algorithmes
4. Gestion des clés
5. Recouvrement
6. Outils complémentaires
7. Possibilités et limites
8. Remarques

1. Introduction

- **Les inconvénients de NTFS**
  - L'accès physique au disque dur outrepasse les permissions
    - Accès non autorisé par disquette de boot
    - Vol de portable
  - Les fichiers temporaires permettent de récupérer de l'information
  - Les solutions de cryptage manuelles ne sont pas efficaces
    - Lourdes à utiliser
    - Mot de passe choisi par l'utilisateur faible
    - Pas d'agent de récupération
- **La solution EFS**
  - Sur couche transparente de NTFS (pilote EFS.SYS)
  - Cryptage par fichier ou par répertoire
  - Clé aléatoire, différente pour chaque fichier
  - Présence d'un agent de récupération

EFS
2. Mécanismes

EdelWeb



3. Algorithmes

- DESX
  - 3 clés : k1 (64 bits), k2 (64 bits), DES (56 bits)
  - Blocs de 64 bits
  - Sortie = k2 XOR (DES(k1 XOR Entrée))
  - Robustesse : 2^120 / nombre de « plaintexts » connus
  - http://www.rsasecurity.com/rsalabs/faq/3-2-7.html
  - http://crypto.radiusnet.net/archive/DESX/desx.algorithm.description
- Windows XP utilise 3DES

EFS

4. Gestion des clés

- Clé publique
  - \Documents & Settings\<UID>\Application Data\Microsoft\SystemCertificates\My\Certificates\<nom de fichier>
  - <nom de fichier> = empreinte 128 bits du certificat
- Clé privée
  - \Documents & Settings\<UID>\Application Data\Microsoft\Protect\<SID>\<nom de fichier>
  - <nom de fichier> = empreinte 128 bits du certificat
  - Chiffrée avec l'empreinte MD4 du mot de passe utilisateur
  - Algorithme de chiffrement : RC4-56 ou RC4-128
  - L'accès à la clé privée nécessite le SID et le mot de passe
    - Lié à un compte utilisateur donné (compte local <> compte réseau)
    - La LSA gère les changements de mot de passe mais pas les changements de SID
- La paire de clés utilisateur fait partie de son profil errant
  - Si l'utilisateur n'a pas de profil errant, une clé différente est générée sur chaque station (!)

EFS

5. Recouvrement

EdelWeb

- Un (ou plusieurs) agents de recouvrement doivent être définis dans la stratégie de sécurité
  - Dans le cas contraire, EFS est inutilisable
  - Par défaut l'administrateur local est agent de recouvrement *(En fait il s'agit du premier administrateur à se logguer)*
  - Pour réinitialiser la stratégie de recouvrement locale (Q257705) `regsvr32 [-u] sclgntfy.dll`
    - Les DRF sont mis à jour lorsque les utilisateurs ouvrent les fichiers
- Recommandations
  - Supprimer les clés privées des agents de recouvrement
    - Utiliser le snap-in « certificats » pour la MMC
    - Exporter la clé privée sur un support amovible, et la protéger par un mot de passe
  - Pour le recouvrement, transférer le fichier vers la station de recouvrement au lieu de transférer la clé sur la station utilisateur
  - Ne pas déployer EFS sans une bonne stratégie de recouvrement et une PKI opérationnelle (Q273856 – utiliser une PKI externe avec EFS)

EFS
6. Outils complémentaires

- **Snap-in « Certificats » pour la MMC**
- **EFSINFO (Resource Kit) (Q243026)**

```
C:\>EFSINFO /U /R /C test.txt
   Test.txt: Encrypted
   Users who can decrypt:
   WIN2K\administrateur (CN=Administrateur)
   Certificate thumbprint: 783A 816D 918B B130 4A46 F4C7 2CA3 C6D3 3668 9FAD
   Recovery Agents:
   Unknown (CN=Agent de recouvrement secondaire)
   Certificate thumbprint: ED21 9FED 3F75 380B E838 F38E 3571 D8A1 3E75 B1AB
   Unknown (CN=Agent de recouvrement principal)
   Certificate thumbprint: 122D 577A 45CF 132F F9CA 5C96 5783 A756 ACA7 A9F5
```

- **EFSDUMP (Winternals)**

```
C:\>EFSDUMP test.txt
test.txt :
DDF Entry:
    WIN2K\administrateur:
        CN=Administrateur
DRF Entries:
    Unknown user:
        CN=Agent de recouvrement secondaire
    Unknown user:
        CN=Agent de recouvrement principal
```

EFS

7. Possibilités & Limites (1/2)

EdelWeb

- **Mise en oeuvre**
  - Ne peuvent être chiffrés :
    - Les fichiers « système » (sinon le système ne boote pas)
      Si AUTOEXEC.BAT est chiffré, aucun utilisateur ne peut se logguer (Q269397)
    - Les fichiers compressés
  - Les fichiers chiffrés peuvent être archivés chiffrés
  - Le chiffrement modifie la date du fichier
  - Recommandation : chiffrer les répertoires temporaires
- **Accès aux fichiers chiffrés**
  - Système mono-utilisateur
    - Évolution multi-utilisateurs prévue pour Windows XP
  - Les fichiers peuvent être chiffrés sur un partage réseau NTFS
    - Mais ils circulent en clair sur le réseau : utiliser IPSec (➔ Windows XP)
    - La fenêtre de l'utilisateur se fige si il tente d'accéder à des fichiers chiffrés par d'autres (Q255554)

EFS

7. Possibilités & Limites (2/2)

- **Gestion des clés**
  - Le changement du mot de passe et suppression d'un utilisateur sont gérés (coopération entre LSA et MSCryptoProvider)
  - Par contre rien n'est prévu si l'utilisateur change de SID (changement de domaine, nouveau compte, etc.)
  - Le compte local et le compte réseau n'ont pas le même SID (cas des portables)
- **Vulnérabilités**
  - Une attaque sur le mot de passe utilisateur reste possible
  - Dans le cas d'un chiffrement fichier par fichier, un fichier EFS0.TMP est créé puis effacé dans la racine du disque (Q288183)
  - Le chiffrement ne remplace pas les droits : il ne protège pas contre la suppression, le déplacement, le renommage
  - Il n'est pas possible de restreindre l'accès utilisateur aux fonctions de chiffrement
  - En cas de mise en veille prolongée, les clés sont paginées sur le disque
  - Les fichiers synchronisés offline ne sont pas chiffrés (➔ Windows XP)

EFS

8. Remarques

EdelWeb

- L'API WinEFS est incomplète
- Le SP2 met à niveau le chiffrement vers 128 bits de manière irréversible
- Il est possible de mettre SYSKEY au niveau 2 ou 3 pour éviter la compromission de la clé privée par la compromission du compte administrateur local (Q143475)

EFS : Conclusion

- **Bilan**
  - **Portables : EFS réduit les risques mais ne les annule pas contre un attaquant déterminé**
    - **Supprimer les clés de recouvrement du poste local**
    - **Vider le cache de connexions**
    - **Attention aux fichiers de mise en veille prolongée**
  - **Postes de travail et serveurs : contraignant à mettre en œuvre comparativement à la sécurité apportée - sauf cas particuliers (ex. disques durs extractibles)**
  - **Le mot de passe utilisateur reste le point faible**
  - **Une bonne gestion des clés est indispensable (PKI)**
- **Pointeurs intéressants**
  - **MSKB : mots clés w2000efs, edrp**
  - **Fichier d'aide livré avec « Windows 2000 Server Resource Kit »**
  - **http://www.microsoft.com/TechNet/security/analefs.asp**
  - **http://www.microsoft.com/technet/security/efs.asp**
- ***Merci à Cyril VOISIN de Microsoft France***

EdelWeb

Revue des dernières vulnérabilités de Windows 2000

Nicolas RUFF

nicolas.ruff@edelweb.fr

Avis de sécurité Microsoft

- Depuis le 02/04/2001 :
  - MS01-021 : Déni de service sur ISA Server
  - MS01-022 : WebDAV exécute les scripts dans le contexte de l'utilisateur
  - MS01-023 : Exploit SYSTEM distant sur IIS 5 par IPP
  - MS01-024 : Fuite mémoire exploitable à distance sur contrôleurs de domaine Windows 2000
  - MS01-025 : « Buffer Overflow » avec Index Server 2.0 (contexte SYSTEM)
  - MS01-026 : Exécution de commandes dans le contexte IUSR_XXX par double décodage des requêtes dans le répertoire « scripts »
  - MS01-027 : Vulnérabilité sur la validation des certificats par IE
  - MS01-028 : Les documents RTF permettent l'exécution de macros dans Word sans confirmation
  - MS01-029 : « Buffer Overflow » dans Media Player 6.4 et 7
  - MS01-030 : Exécution de scripts sans confirmation dans l'interface de consultation Web d'Exchange 2000
  - MS01-031 : Exploit SYSTEM local par le service Telnet (nom de canal prédictible)

Autres avis de sécurité

- Obtention de privilèges SYSTEM par les registres de déboguage (DR0-DR7) – *Georgi Guninski*
- Le patch MS01-020 (vulnérabilité EML) introduit une nouvelle vulnérabilité : le nom d'un fichier téléchargé peut être masqué ou modifié à l'affichage – *Kriptopolis*
- Déni de service sur IIS si le compte IUSR_XXX suit la stratégie de verrouillage de compte
- Outlook et Outlook Express ne supportent pas les « subjects » de plus de 256 caractères

- « Securing Windows 2000 - Step by Step » disponible chez SANS

Mises à jour

EdelWeb

- **Pseudo-SP pour IIS 5 : Q293826**
  - Corrige toutes les vulnérabilités jusqu'à MS01-026
- **Sortie du SP2**
  - Corrige environ 700 bogues
  - « High-Encryption Pack » intégré de manière irréversible
    - La mise à jour du magasin protégé doit être effectuée manuellement comme décrit dans MS00-032
  - Impact non négligeable sur des machines de production
    - Incompatibilités avec ISA Server, BlackIce, Norton Antivirus, Easy CD Creator, …
    - Nombreuses évolutions fonctionnelles
  - Fait disparaître tous les hotfixes pré-SP3 de la registry

Questions / réponses