Sécuriser Vista

Laboratoire de transmission de données

Professeur : LITZISTORF Gérald
Etudiant : PEREZ Thomas
Travail de diplôme
Année 2005-2006

Sections de la présentation

- ✓ Définitions
- ✓ Initialisation
- ✓ Windows Services Hardening
- ✓ User Account Control
- ✓ Mandatory Integrity Control
- ✓ BitLocker Drive Encryption
- ✓ Firewall
- ✓ Conclusion

Définitions

- Défense en profondeur
  - Sécurité accrue
  - Plusieurs couches de sécurité
- Moindre privilège
  - Uniquement les privilèges nécessaires
  - Limite les dommages
- But : réduction de la surface d’attaque

Initialisation

(1 semaine d'étude)

Smss : *Session Manager Subsystem*

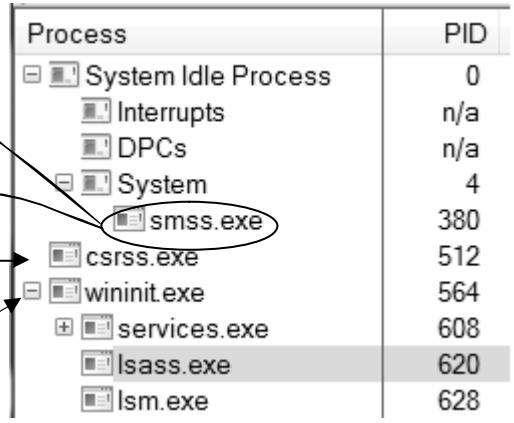
- 1er processus utilisateur
- Gestionnaire de sessions

Mode *Kernel*

Mode *User*

Gestion interface graphique

Lance *services.exe lsass.exe* et *lsm.exe*



- Création des sessions utilisateur

Session 0

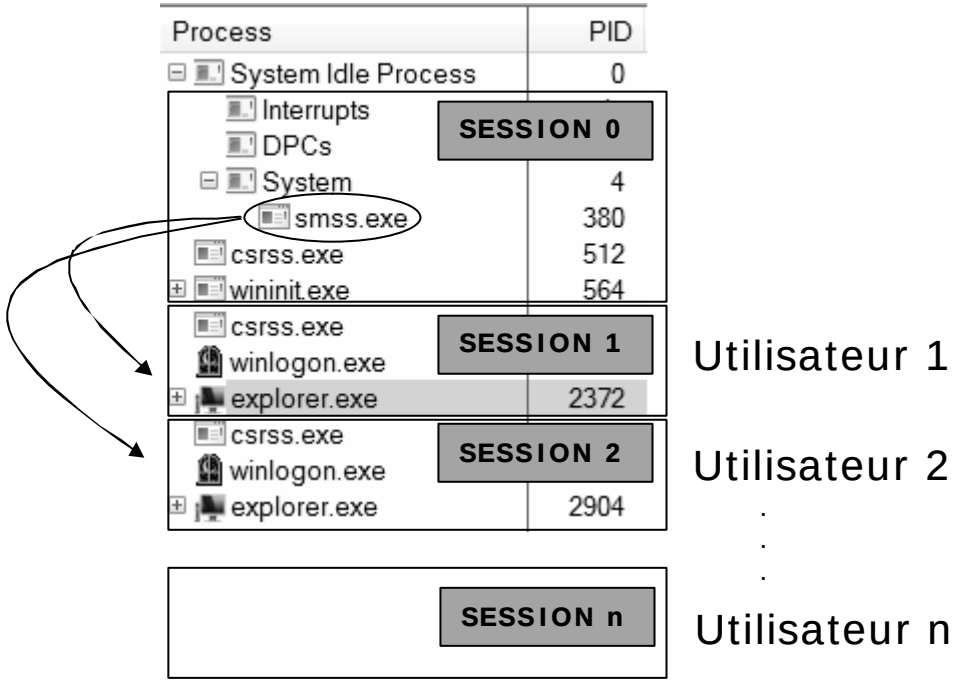
- Isoler les services
- Session non interactive

winlogon

- Authentification
- Attribution les jetons

explorer

- Bureau interactif
- Lancement processus



Windows Services Hardening

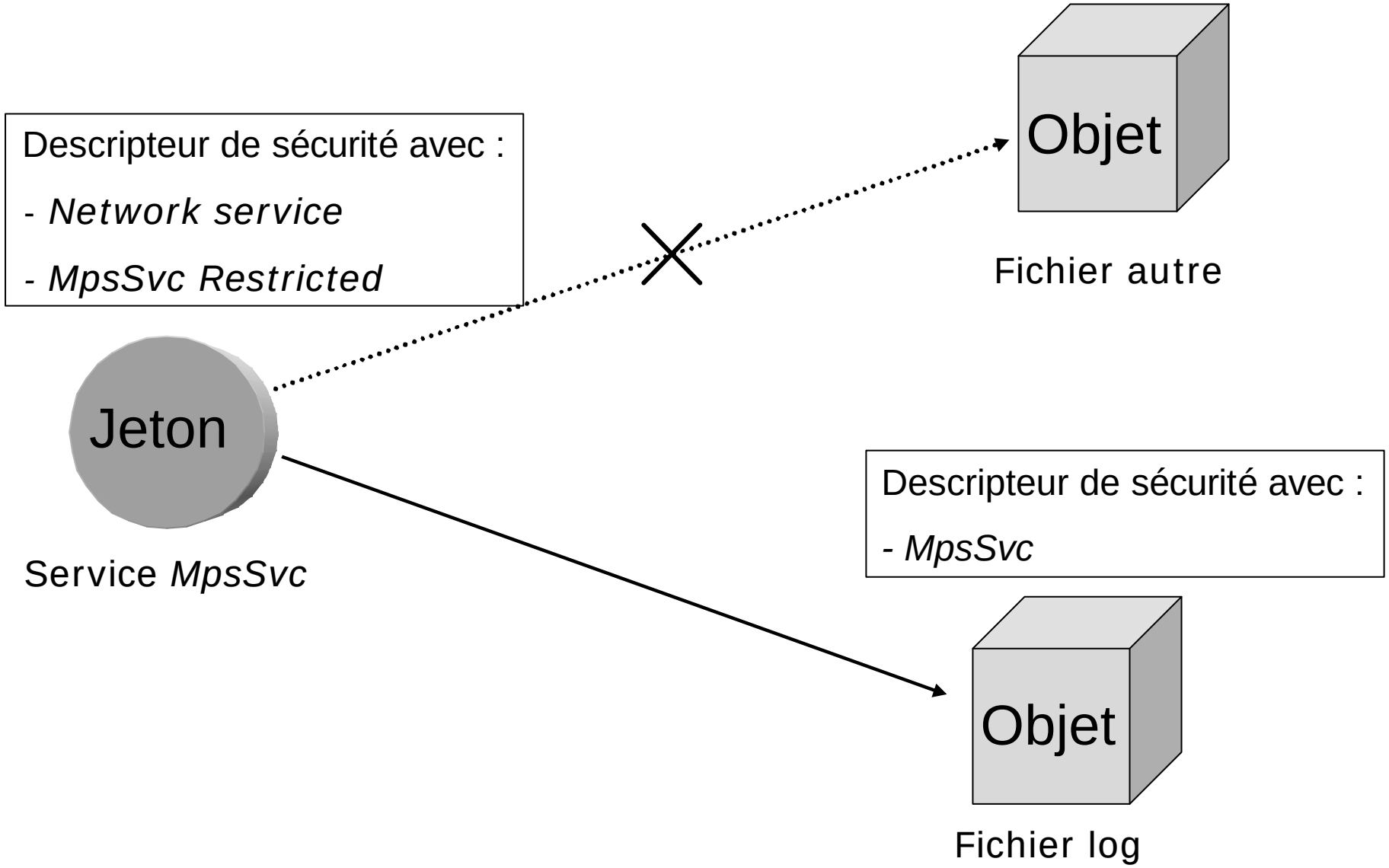
(2 semaines d'étude)

- Les services, une cible parfaite
  - Exécution sur un grand nombre de machines
  - Exécution sur une longue période
  - Accès au réseau
  - Plus de droits que l'utilisateur

- But
  - Limiter les dégâts

- Mise en oeuvre
  - Déplacer les services
  - Supprimer les privilèges inutiles
  - Isolation des services (Authentification)

- Authentification des services



Audit des services

- Par défaut : 63 services lancés au démarrage

LocalSystem	*LocalService*	*NetworkService*
44	10	9

- 23 seulement utilisent un compte restreint

Compte	Groupe	Nbr services
LocalService	*LocalServiceNoNetwork*	3
LocalService	*LocalServiceRestricted*	0
LocalService	*LocalServiceNetworkRestricted*	5
NetworkService	*NetworkServiceRestricted*	0
NetworkService	*NetworkServiceNetworkRestricted*	1
LocalSystem	*LocalSystemNetworkRestricted*	14

- Supprimer les services inutiles ou/et sensible (accès réseau)
- Méthodologie : étude + test
- Résultat 46 services désactivés

User Account Control

(3 semaines d'étude)

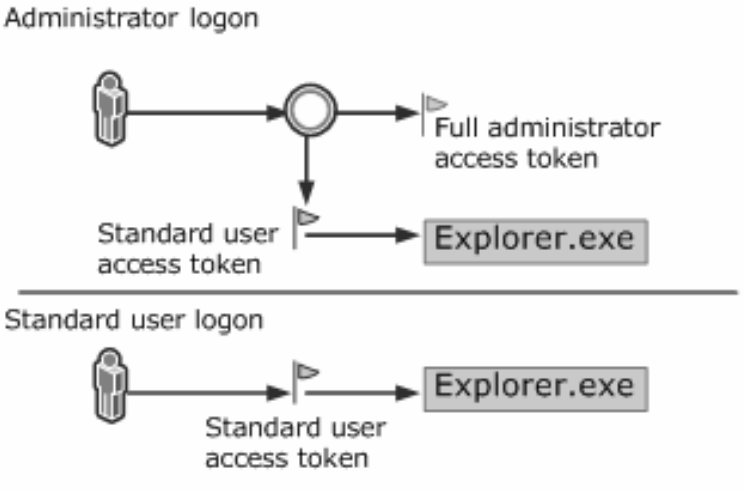
- Mise en œuvre par le service *AIS (Application Information Service)*

- Désignations :

  - Utilisateur à moindre privilège *LUA* (Least-privileged User Account)
  - Administrateur protégé *PA* (Protected Administrator)

utilisateur *LUA* => **1 jeton restreint**

administrateur *PA* => **1 jeton restreint** + **1 jeton complet**



Descriptions

- Principe de moindre privilèges

  - Diminution :
    Des privilèges nécessaires pour effectuer une tâche courante
    Des privilèges d'un administrateur

- Elévation de privilèges
  - Interface utilisateur sécurisée

- Marquage des applications
  
  - Le bouclier informe que l'application nécessite des privilèges.

- Virtualisation
  - Compatibilité des applications

- Paramétrable
  - Politiques de sécurité

Fonctionnement

- Elévation de privilèges :

  But => Obtenir le jeton complet

- Utilisateur *LUA* => demande de mot de passe
- Administrateur *PA* => consentement

  Configurable via `secpol.msc - Local Policies - Security Options`

  consentement : protège => *over the shoulder*, *keylogger*

  mot de passe : protège => accès physique

- *Secure Desktop* : protection interface utilisateur d'élévation, processus système uniquement, contre *spoofing*

Fonctionnement

- Marquage des applications :

  - Utilisation d'un manifeste
    - 3 niveaux d'exécution : ***asInvoker,***
      requireAdministrator,
      highestAvailable

```
<security>
        <requestedPrivileges>
            <requestedExecutionLevel
                level="asInvoker"
                uiAccess="false"
            />
        </requestedPrivileges>
    </security>
```

  - Compatibilité : méthodes heuristiques de détection

  - Attaque : modifier le manifeste => ***Unmarked***

DEMO

Fonctionnement

- Virtualisation :

  - Assure la compatibilité des applications

  - Possibilité d'écrire et de modifier des éléments dans des zones protégées

  - C:\Users\<user name>\AppData\Local\VirtualStore\Program Files\test\config.ini

  - Nombreuses failles

  - Futur => *Code Integrity*

Mandatory Integrity Control

(2 semaines d'étude)

- No write-up

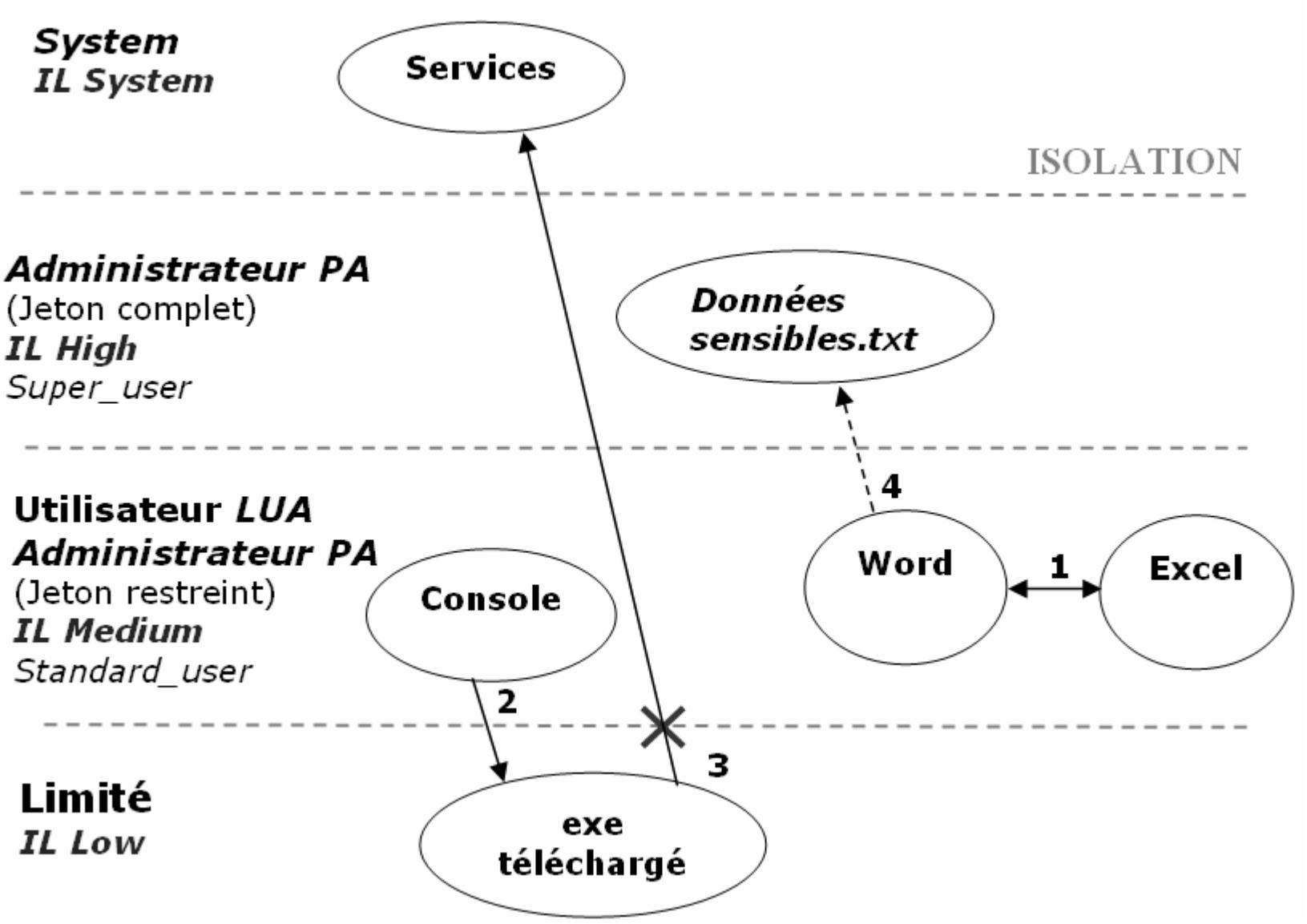
- Contrôle d'accès (renforce *DACL*)

- Session 0 => isolation entre les sessions
- *MIC* => isolation à l'intérieur de la session

- Principe => ajout d'un niveau d'intégrité au jeton

- Outil *chml* modifie niveau intégrité

Fonctionnement



DEMO

BitLocker Drive Encryption

(1 semaines d'étude)

- Attaques
  - Vol, Perte
  - Mode déconnecté

- Confidentialité
  - Chiffrement de la partition Windows

- Dispositifs matériels
  - *Trusted Module Plateform*
  - Clé *USB*

- But
  - Attaque coûteuse

Spécificités

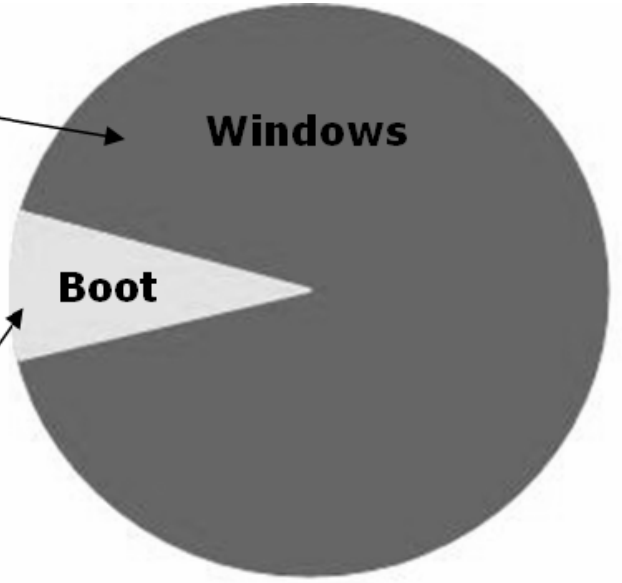
- *TPM* version 1.2
- *BIOS* compatible *Trusted Computing Group (TCG)*
- 2 partitions : la première de 1,5 GB et la seconde de taille suffisante pour installer *Vista*.
- La partition active formatée *NTFS*
- Une édition *Entreprise* ou *Ultimate* de Vista installée sur la partition active

La partition *Windows* **chiffrée** contient :

- Le système d'exploitation
- Le fichier de pagination
- Les fichiers temporaires
- Les données
- Le fichier d'hibernation

La partition de *boot* **non chiffrée** contient :

- *Master Boot Record*
- *Winload*
- Utilitaires de *boot*



Les Clés

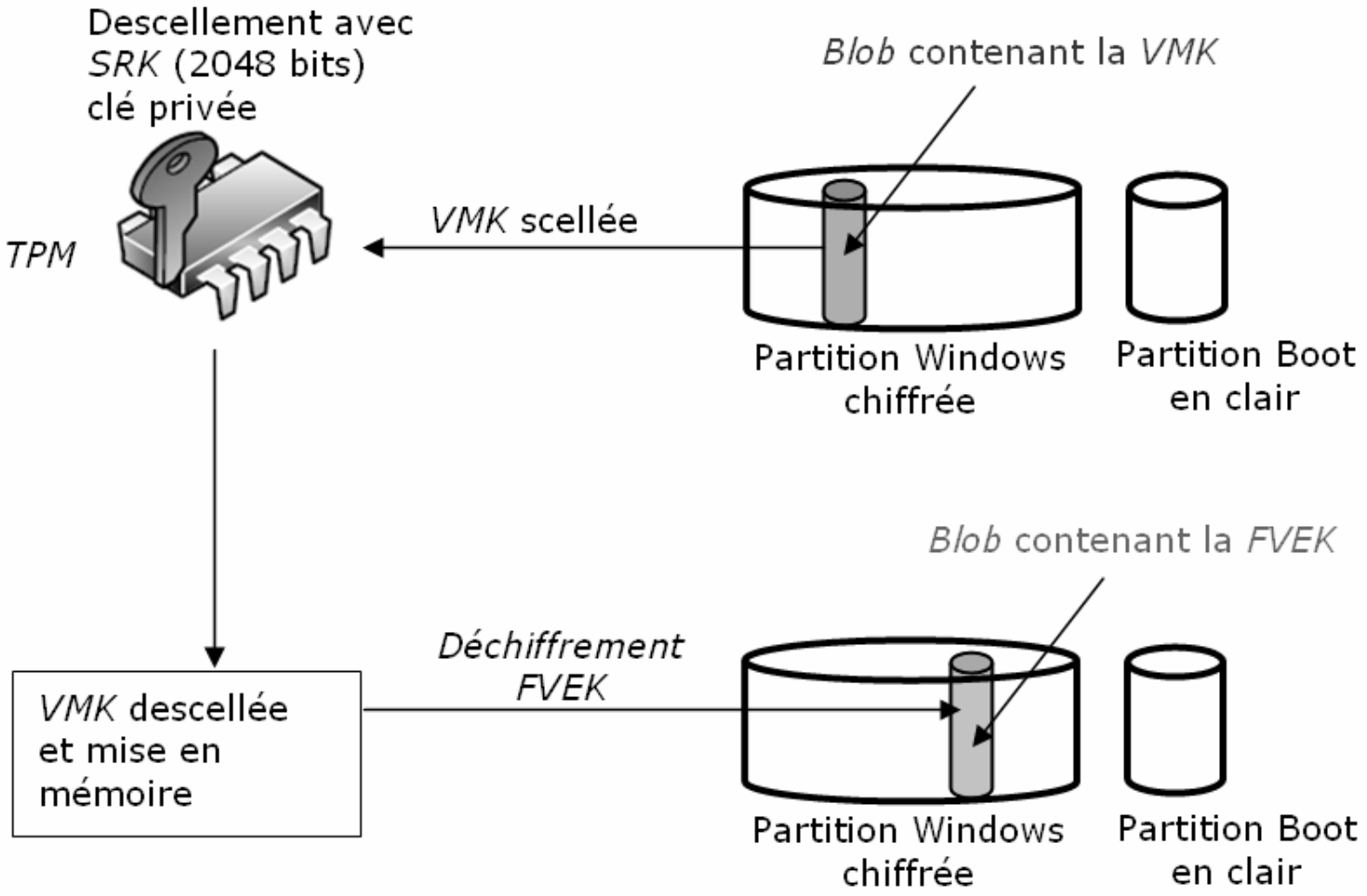
- *Volume Master Key (VMK)*
  - Protège (*FVEK*) chiffrement AES 256 bits
  - Activation de *BDE*
  - Symétrique 256 bits
  - Remplacement ou modification impossible
  - Protégée par RSA 2048 (*SRK*) ou AES 256 (*USB*)

- *Full Volume Encryption Key (FVEK)*
  - Protège les données, AES 128 bits + *elephant*
  - Activation de *BDE*
  - Symétrique 128,256,512 bits
  - Ne chiffre pas les *blobs*

- Mot de passe de récupération (option)
  - 128 bits
  - formaté : 111111–222222–333333–444444–55555–66666–77777-888888
  - avec salage 128 bits = clé *AES* 256 bits
  - protège *VMK*

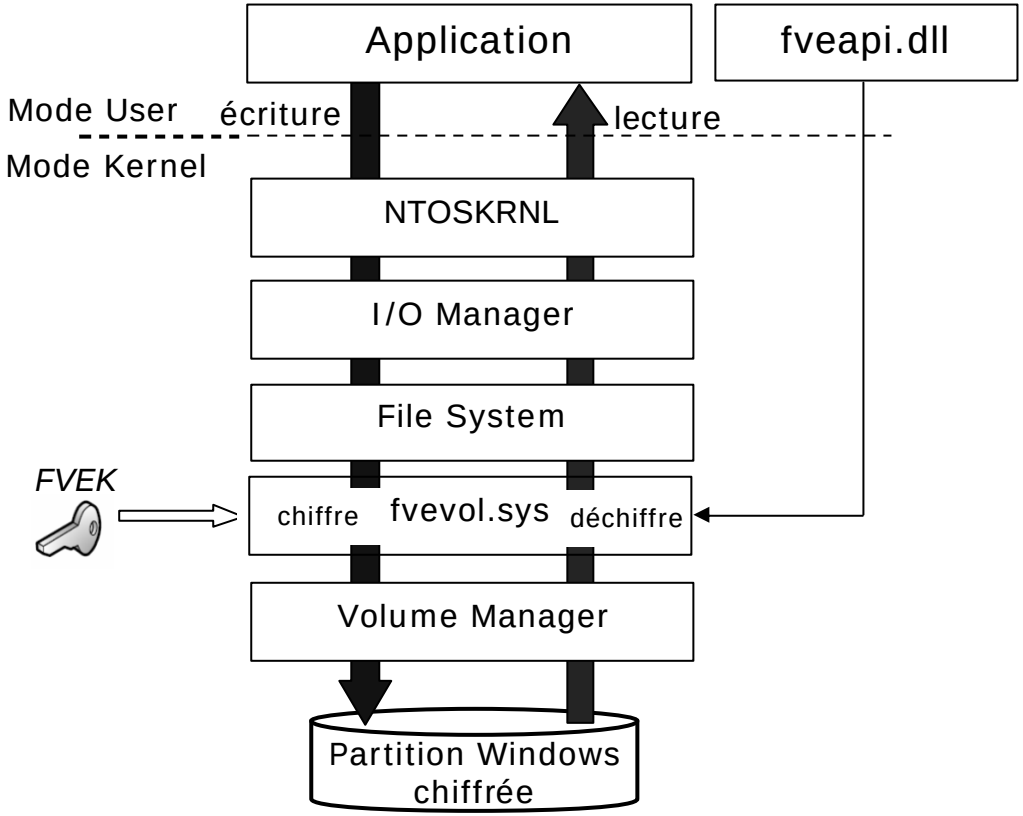
  VMK, FVEK et mot de passe de récupération stockés dans des *blobs* sur la partition chiffrée

Descellement



Chiffrement/Déchiffrement

- Procédé temps réel, transparent
- Utilisation d'un *driver* filtre
- Dialogue avec le mode *User* via *API*



Attaques

- *TPM* seul
  - *Warm Ghosting*
  - *Cold Ghosting*
  - *PCI BUS exploit (PC Card – DMA)*

  Contre-attaque => *BitLocker* avec *USB* ou *PIN*

- *TPM + PIN*
  - *Brute Force* => utiliser un code *PIN* + long (*policy*)
  - Analyse des touches => utiliser touches numériques

- *TPM* + clé *USB*
  - Attaques mode *online* pré-vol
  - *RootKits* => Configuration sécurisée du poste

  BDE ne protège PAS une machine *online* !

- Administration
  - Vol du mot de passe de récupération
  - Vol clé *USB*

Firewall

(2 semaines d'étude)

- *Windows Services Hardening*
- Contrôle des applications
- Augmentation de la granularité
- Connexions sortantes paramétrables
- IPV6
- Profile => environnement de connexion

Profils

- But
  - Mobilité
  - Configuration prédéfinie du firewall

- *Network Location Awareness (NLA)*
  - Network Service
  - Connectivité, Connexion, Profils

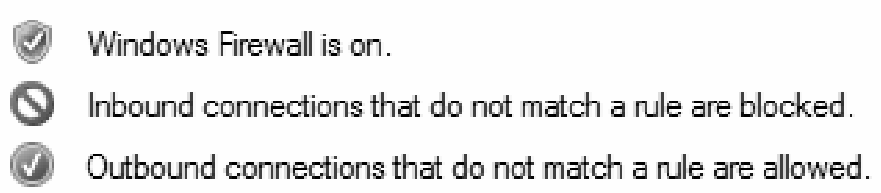
- 3 profils :
  - *Domain* : si DC présent
  - *Public* : utilisateur LUA
  - *Private* : Administrateur PA

Network Connection Details:

Property	Value
Connection-specific DN...	tdeig
IPv4 IP Address	10.1.3.6
IPv4 Subnet Mask	255.255.0.0
IPv4 Default Gateway	10.1.0.1
IPv4 DHCP Server	10.1.1.10
IPv4 DNS Server	10.1.1.10

Configuration

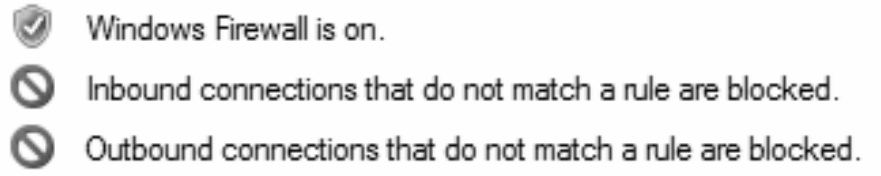
- Par défaut :



Connexions entrantes => *White List*

Connexions sortantes => *Black List*

- Configuration restrictive :



- Outil *netshell*

```
Netsh advfirewall firewall>add rule name=”navigation
web” protocol=TCP dir=out program=”program
files\Internet Eplorer\iexplore.exe” action=allow
profile=public interfacetype=lan localip=10.1.2.90
remoteport=80,143
```

Sécurité

- Intrusions (*nmap*)
  - Bonne isolation
- Contrôle des applications (*LeakTest*)
  - Aucun contrôle d'intégrité
  - Aucun contrôle des sources
- Services *DNS* (*LeakTest*)
  - Aucun contrôle des Modules chargés
- Conclusion
  - Bonne sécurité flux entrant
  - Mauvaise sécurité flux sortant => indispensable ?

DEMO

Conclusion

- Augmentation des sécurités (*UAC,MIC,CI,WSH,Bitlocker,firewall*)
- Toujours trop de services par défaut
- Mauvaise information
- Moins sécurisé que XP ?

MERCI DE VOTRE ATTENTION

Place aux questions !