BitLocker™ : mise en œuvre des spécifications du TCG au sein de Windows

Bernard Ourghanlian,
Directeur Technique et Sécurité
Microsoft France

Avertissement

Les informations données dans cette présentation se fondent sur une version préliminaire de Windows Vista (beta 2) ; celles-ci peuvent être soumises à changement et ce, jusqu'à la mise à disposition du logiciel dans sa version finale

Sommaire

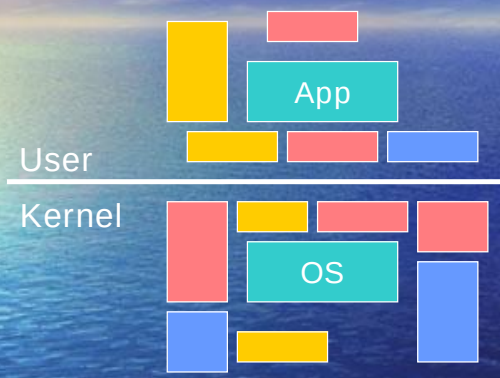
- Introduction : un peu d'histoire
- BitLocker™
  - Pourquoi BitLocker™ ?
  - Aperçu de *BitLocker™ Drive Encryption* (BDE)
  - Pré-requis de BitLocker™ et déploiement
  - Administration de BitLocker™ et récupération
  - Comment fonctionne BitLocker™ ?
- Quelques perspectives en guise de conclusion


Introduction : un peu
d’histoire

Petit rappel…

- En juin 2002, Microsoft annonçait les premiers éléments du projet « Palladium »
- En janvier 2003 Microsoft annonçait sa volonté de changer le nom de « Palladium »
  - « Palladium » s'appelle maintenant *Next-Generation Secure Computing Base* (NGSCB)
- BitLocker™ est la première mise en œuvre de cette génération de technologies qui vise à ancrer la confiance du logiciel dans le hardware

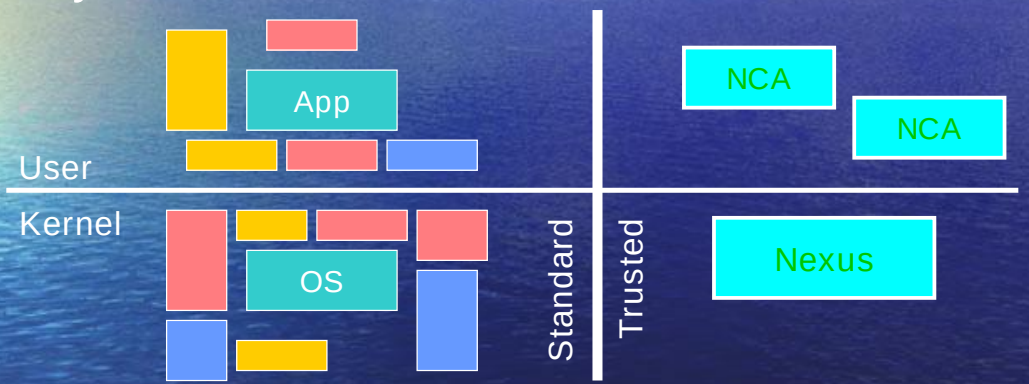
NGSCB « vu d'avion » : la conception originelle (1/3)



- Comment préserver la flexibilité et l'extensibilité qui ont tant contribué à la richesse de l'écosystème du PC, tout en fournissant à l'utilisateur final un environnement sûr ?
- En particulier, comment peut-on garder quoi que ce soit de secret, quand des composants du noyau enfichables contrôlent la machine ?

NGSCB « vu d'avion » : la conception originelle (2/3)

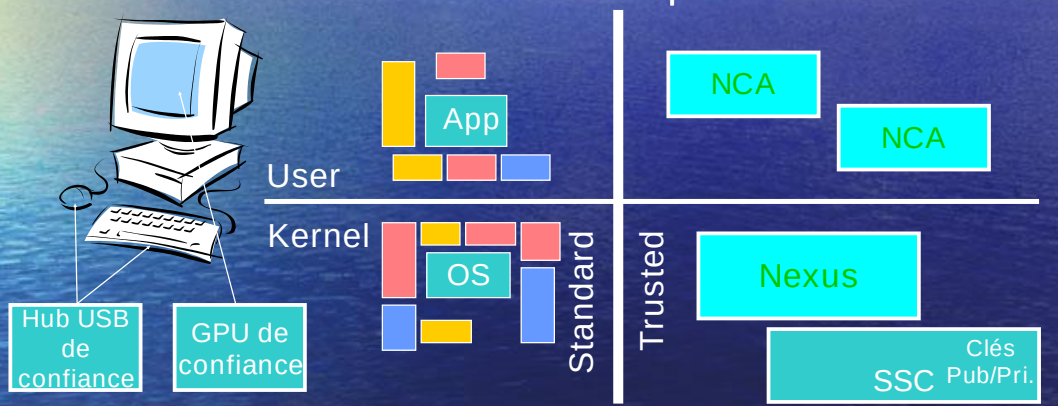
- La solution : subdiviser l'environnement d'exécution en ajoutant un nouveau mode au CPU



- Le CPU est soit en mode « standard » soit en mode « trusted »
- Les pages de la mémoire physique peuvent être marquées comme « trusted ». Les pages dites « trusted » ne peuvent être accédées que lorsque le CPU est en mode « trusted »

NGSCB « vu d'avion » : la conception originelle(3/3)

- Les agents ont aussi besoin de laisser l'utilisateur entrer des secrets et d'afficher des secrets pour l'utilisateur



- Les entrées sont sécurisées par un « hub » USB de confiance pour le clavier et la souris qui permet de transporter une conversation sécurisée avec le *nexus*
- Les sorties sont sécurisées par un GPU de confiance qui transporte une conversation chiffrée avec le *nexus*
- Ceci permet une sécurité de bout en bout

Le problème fondamental avec cette conception originelle

- Pour pouvoir exploiter pleinement NGSCB, il faut utiliser les API correspondante afin de pouvoir écrire des NCA
- Ceci nécessite, dans la pratique, de réécrire la majorité des logiciels
- Une telle approche n'était guère réaliste…

Nous avons donc revu nos plans
et avons donc changé de fond en comble
l'architecture (et le calendrier) de NGSCB


Pourquoi BitLocker™ ?

Pourquoi BitLocker™ ?

Une multinationale qui désire garder l'anonymat perd en moyenne un portable par jour dans les taxis, rien que dans la ville de New York....

"An estimated 11,300 laptop computers, 31,400 handheld computers and 200,000 mobile telephones were left in taxis around the world during the last six months ... Passengers had lost three times more handheld computers in the second half of 2004 than in 2001"

CNN, 24 janvier 2005

"Dutch public prosecutor ... was condemned yesterday for putting his old PC out with the trash. It contained sensitive information about criminal investigations in Amsterdam, and also his email address, credit card number, social security number and personal tax files."

The Register, 8 octobre 2004

La situation actuelle

- Aujourd'hui, il existe, de manière très largement diffusée, des programmes de récupération de mots de passe qui permettent des attaques contournant les mécanismes de sécurisation des données de Windows XP
- Les attaques en mode déconnecté exposent les clés utilisées par le système, ce qui permet la compromission des données sécurisées
- Il y a des centaines de milliers de PC portables perdus ou volés chaque année


Aperçu de Bitlocker™

Description de *Bitlocker™ Drive Encryption*

« *BitLocker™ Drive Encryption* vous fournit une meilleure protection de vos systèmes Windows Vista, même quand ces systèmes sont dans des mains non autorisées ou exécutent un système d'exploitation différent.

BDE atteint ce résultat en interdisant à un voleur qui démarre un autre système d'exploitation ou utilise un outil de hacking spécifique de casser les protections du système et des fichiers ou même de visualiser les fichiers constitutifs du système lui-même »

Conception de la solution Bitlocker™

Besoin d'une solution qui

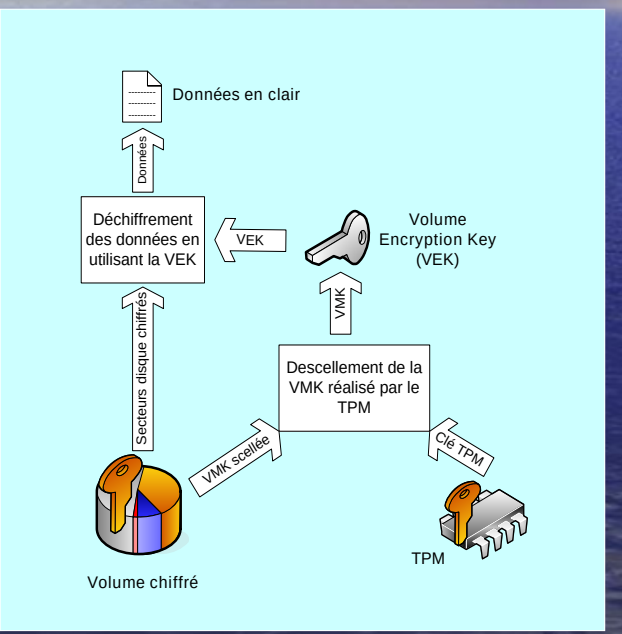
- Se trouve en dessous de Windows
- A des clés disponibles au démarrage
  - Impossibilité de demander à l'utilisateur de se connecter pour fonctionner
- Sécurise les données système
- Sécurise les données utilisateur
- Sécurise la base de registre
- Fonctionne de manière transparente avec la plateforme (intégrité du code)
- Sécurise les secrets « racine »
- Protège contre les attaques en mode déconnecté
- Soit très facile à utiliser

Solution

- Chiffrer (presque) le disque entier
- Protéger la clé de chiffrement en la « scellant » au moyen d'un *Trusted Platform Module* (TPM) au bénéfice unique d'un *loader* autorisé
  - Plus d'autres options (voir plus loin)
- Seuls les *loaders* autorisés peuvent récupérer la clé de chiffrement du volume
- Les *loaders* autorisés pourront amorcer correctement le système d'exploitation

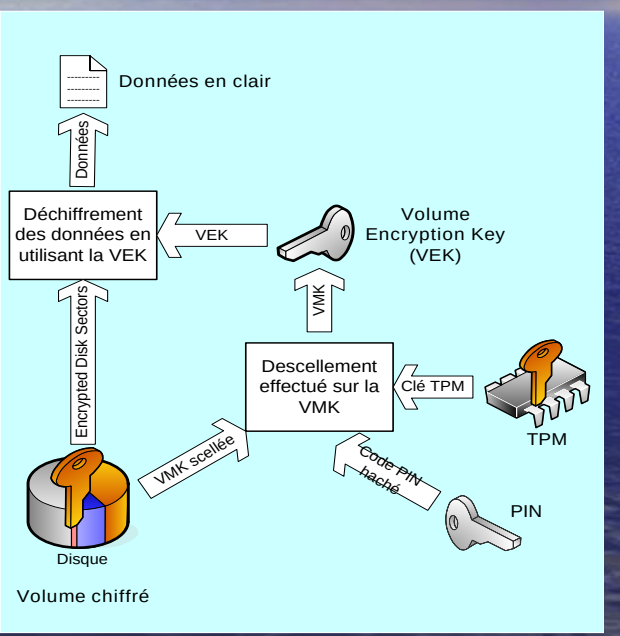
Scénario TPM seul

- Valide de manière transparente les premiers composants d'amorçage
- Le cas le plus facile à utiliser
- Protège contre des attaques uniquement logicielles
- Vulnérable à certaines attaques hardware



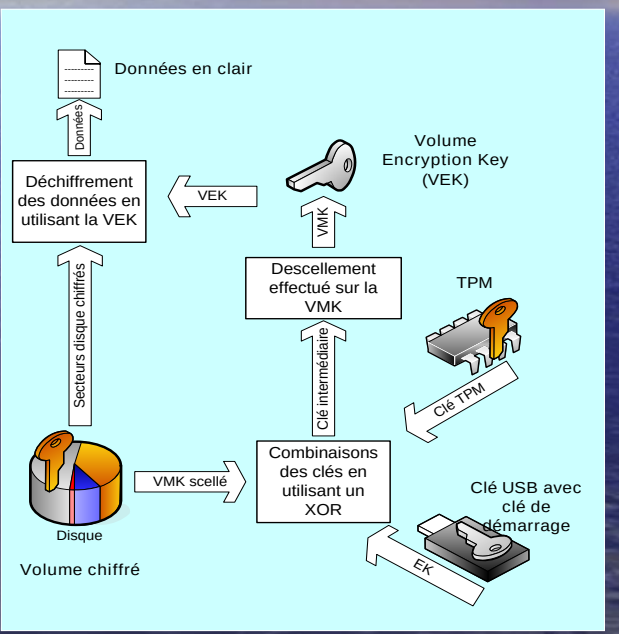
2 facteurs : scénario TPM + PIN

- On doit entrer un code PIN de 4 à 20 digits lors du démarrage du système
- Valide le code PIN et les composants initiaux de l'amorçage
- Protège contre des attaques uniquement logicielles et contre de nombreuses attaques matérielles
- Vulnérable aux attaques contre le TPM



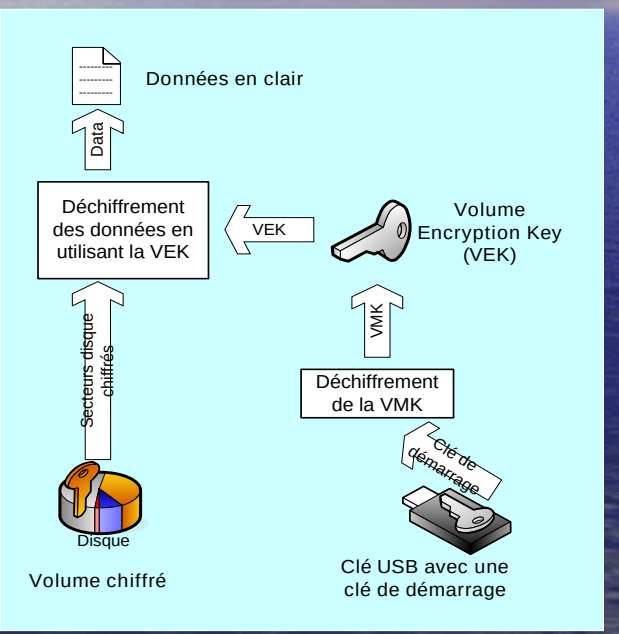
2 facteurs : scénario TPM + Clé de démarrage

- Recherche d'une clé USB avec une clé de démarrage
- Valide la clé sauvegardée et les composants initiaux de l'amorçage
- Protège contre de nombreuses attaques matérielles
- Protège contre les attaques du TPM



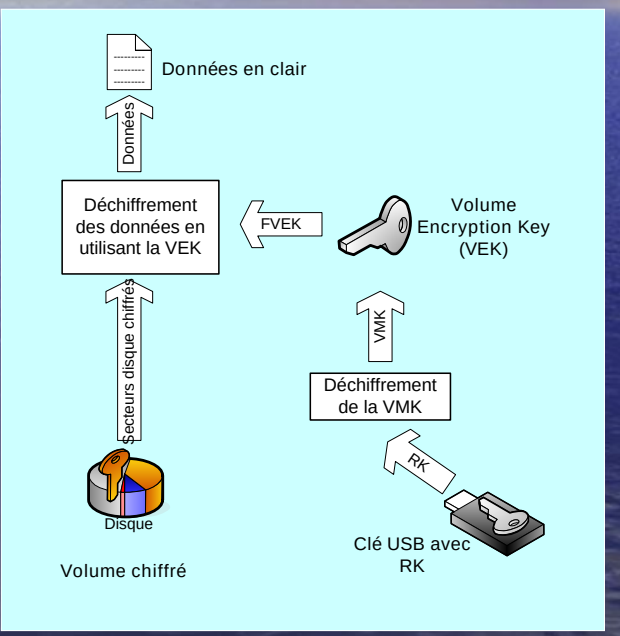
1 facteur : scénario avec une clé de démarrage

- Recherche d'une clé USB avec une clé de démarrage
- Valide la clé sauvegardée
- Vulnérable à la perte de la clé ou aux attaques pré-OS



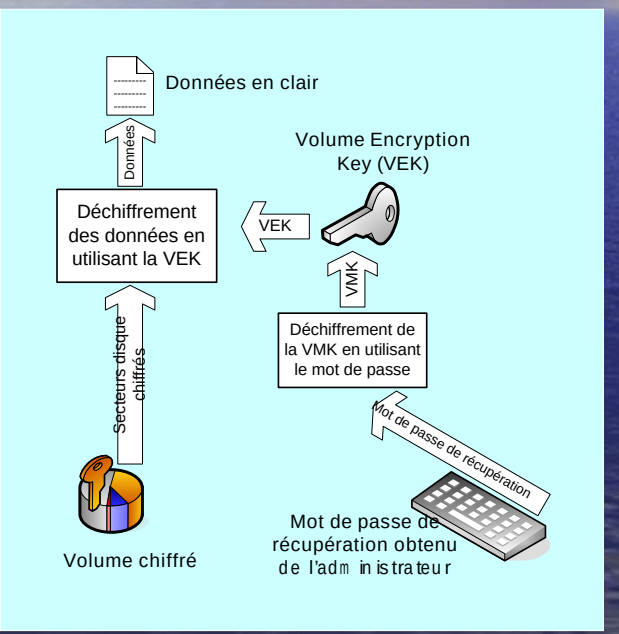
Scénario de récupération de clé

- Recherche d'une clé USB avec une clé de démarrage
- Valide la clé sauvegardée
- Déverrouille le volume pour permettre le déchiffrement



Scénario de récupération de mot de passe

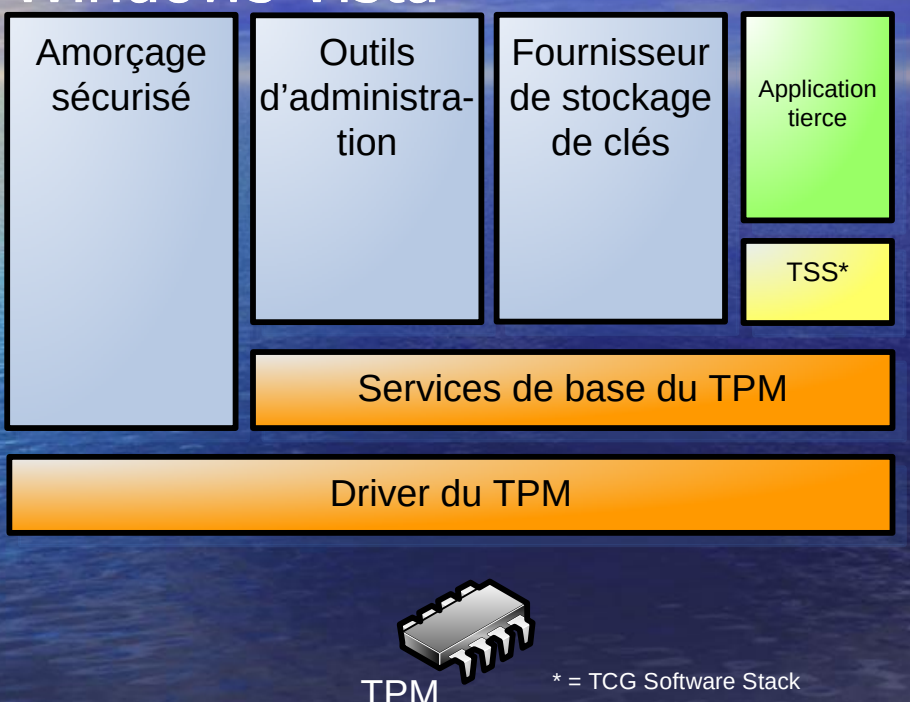
- Demande à l'utilisateur d'entrer un mot de passe de récupération
- Valide le mot de passe
- Déverouille le volume pour permettre le déchiffrement



Aperçu des fonctionnalités de Bitlocker™

- *BitLocker Drive Encryption* (BDE)
  - Permet d'éviter le contournement du processus d'amorçage de Windows
- *TPM Base Services* (TBS)
  - Accès par Windows et des logiciels tiers au TPM
- Authentification à plusieurs facteurs préalablement à l'amorçage du système d'exploitation
  - Clé USB, BIOS, identité logicielle garantie par le TPM
- Re-déploiement
  - Outil réservé aux administrateurs pour accélérer le re-déploiement des PC de manière sécurisée
- Un seul driver Microsoft pour le TPM
  - Amélioration de la stabilité et de la sécurité
- Scénarios
  - Perte ou vol d'un portable
  - Serveur en agence

L'architecture (simplifiée) du TPM de Windows Vista



Qu'est-ce qu'un *Trusted Platform Module* (TPM)?

Un module sur la carte mère ressemblant fonctionnellement à une carte à puce qui :

- Protège les secrets
- Effectue des opérations de chiffrement
  - RSA, SHA-1, génération de nombre aléatoire
- Peut créer, stocker et gérer des clés
  - Fournit une *Endorsement Key* (EK) unique
  - Fournit une *Storage Root Key* (SRK) unique
- Effectue des opération de signature numérique
- Détient les « mesures » (*hashes*) de la plateforme
- Enracine la chaîne de confiance pour les clés et les lettres de créance
- Se protège contre les attaques

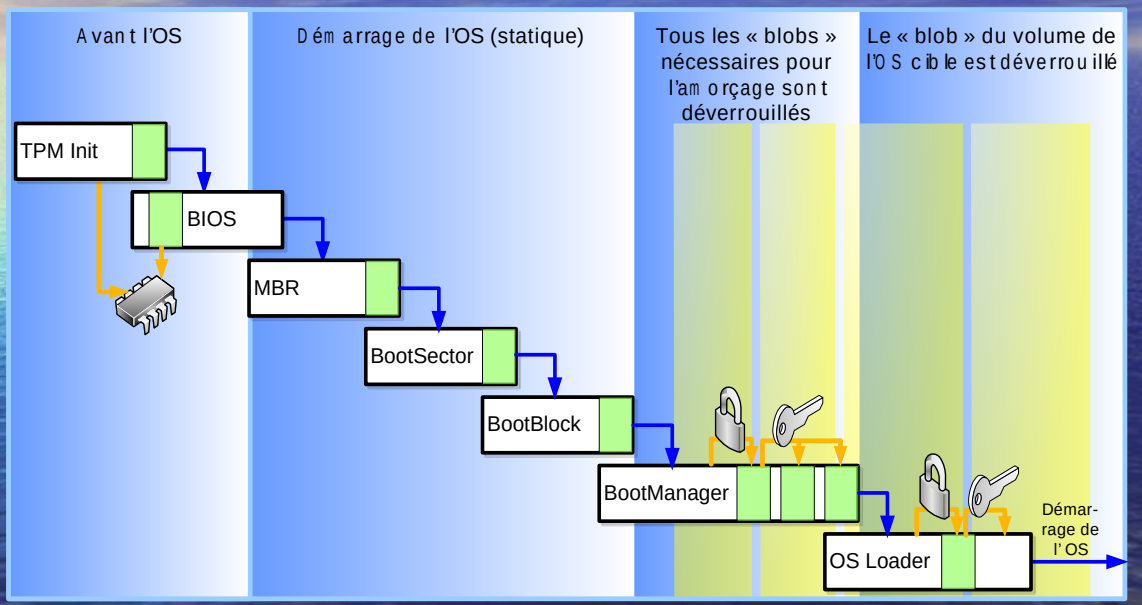
Spécification TPM 1.2 :
www.trustedcomputinggroup.org

Authentification du logiciel

- Résulte de la même étape simple répétée plusieurs fois
  - Le module n « mesure » (*hash*) le module n+1
  - Le module n enregistre (fonction « *extend* ») le *hash* du module n+1 dans le TPM
  - Le module n transfère le contrôle au module n+1
  - On « nettoie » et on recommence
- A n'importe quel moment, le TPM contient une « mesure » de tous les logiciels qui ont été chargés jusqu'alors
  - On ne peut desceller le contenu que si ces informations sont « correctes »

Architecture de *Secure Startup*

SRTM des premiers composants de l'amorçage

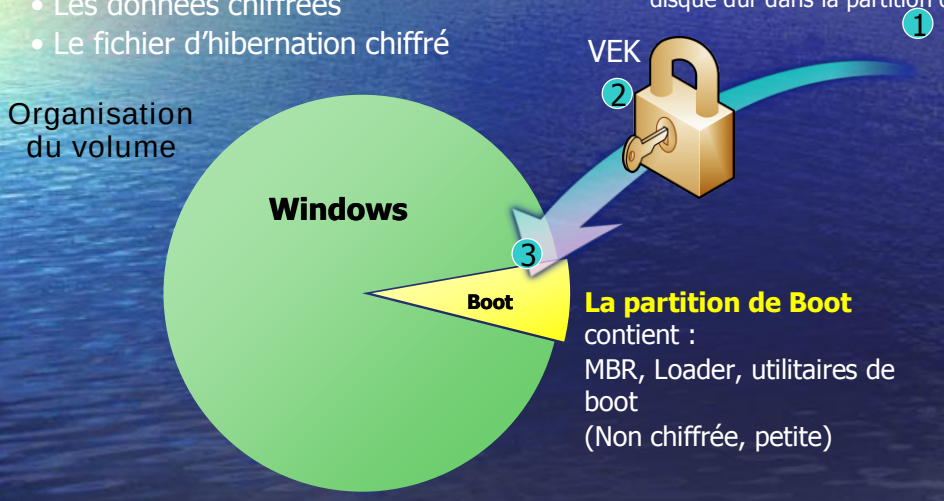


L'organisation du disque et le stockage des clés

La partition Windows contient
- Le système d'exploitation chiffré
- Le fichier de pagination chiffré
- Les fichiers temporaires chiffrés
- Les données chiffrées
- Le fichier d'hibernation chiffré

Où sont les clés de chiffrement ?

1. ***SRK*** (*Storage Root Key*) contenu dans le TPM
2. **La *SRK*** chiffre la ***VEK*** (*Volume Encryption Key*) protégé par TPM/PIN/Clé USB
3. **La *VEK*** est stockée (chiffrée par la ***SRK***) sur le disque dur dans la partition de **boot**



La partition de Boot contient :
MBR, Loader, utilitaires de boot
(Non chiffrée, petite)

Bitlocker™

Chiffrement de la partition

- Chiffrement secteur par secteur
  - Tailles 512, 1024, 2048, 4096, ou 8192 octets
- Avec une clé VEK (*Volume Encryption Key*)
  - 256 bits
  - Protégée par la SRK
- Méthode
  - AES 256 en mode CBC avec une diffusion supplémentaire (voir plus loin)


Bitlocker™ : pré-requis et
déploiement

Considérations générales sur le déploiement

- Bitlocker™ requiert une mise à jour software et hardware (optionnelle pour une mise en œuvre sans TPM)
  - Nécessite probablement une montée en puissance progressive, en démarrant par les ordinateurs les plus prioritaires
- Concerne essentiellement les portables
- Considérer également les ordinateurs de bureaux dans des environnements peu sécurisés (agence, usine, kiosque, …)
- Prévoir une gestion des clés dans l'entreprise (nécessite la mise en place de processus fiables)

Coexistence de systèmes d'exploitation

- Bitlocker™ chiffre des partitions : il ne sera donc pas possible de faire du *dual-boot* d'un autre OS sur la même partition
- Par contre, positionner d'autres OS sur d'autres partitions ne pose pas de problème
- Tenter de modifier la partition Windows protégée la rendra non *bootable*
  - Remplacer la MBR
  - Modifier ne serait-ce qu'un seul bit

Bitlocker™ ne peut pas stopper toutes les attaques

- Débogueurs Hardware
- Attaques online – Bitlocker™ est uniquement concerné par le processus de démarrage du système
- Attaques postérieures au logon
- Sabotage par les administrateurs
- Piètre maintenance de la sécurité
- …

Les besoins hardware de Bitlocker™

- Besoins matériels pour supporter BDE
  - *Trusted Platform Module* (TPM) v1.2
    - Permet les mesures d'intégrité de la plateforme et le *reporting*
    - Nécessite le support par la plateforme de l'interface TPM (TIS)
- *Firmware* (conventionnel ou BIOS EFI) compatible TCG
  - Etablit la chaîne de confiance avant le démarrage du système d'exploitation
  - Doit supporter la notion de *Static Root Trust Measurement* (SRTM) spécifiée par le TCG
- Fonctionnalités additionnelles rendues disponibles par la clé USB
- Au moins 2 partitions
  - Ces partitions doivent être NTFS

Bitlocker™

Le déploiement d'une machine unique avec un TPM

Installation de Windows Vista

- BDE est seulement disponible dans les versions Enterprise et Ultimate de Windows Vista
- BDE nécessite une partition séparée de la partition système de Windows Vista avec un espace libre minimum de 350(500) MO
- Pendant l'installation on contrôle que le système dispose bien d'une version correcte du TPM (v 1.2) et du BIOS via Plug and Play
- Les drivers TPM et BDE sont installés

Installation de BDE

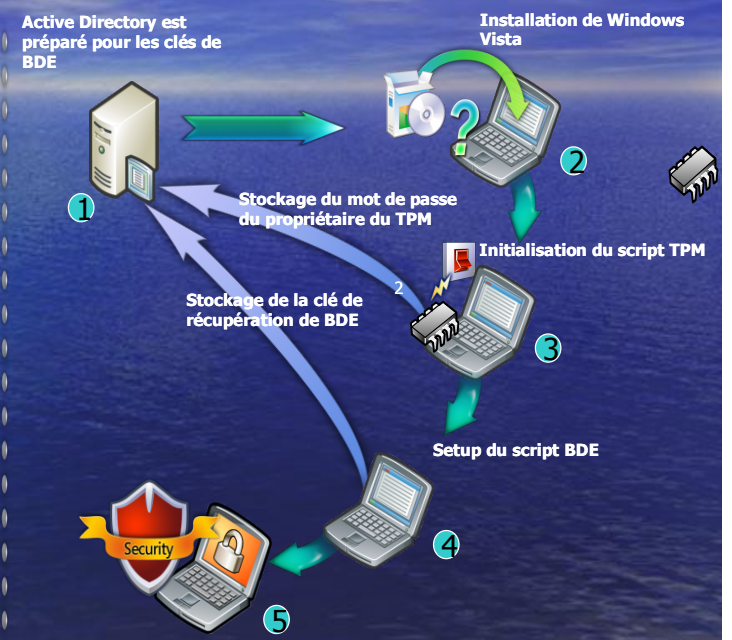
1. Lancer l'installation à travers le panneau de contrôle de BDE
2. L'installation vérifie l'organisation requise des partitions du disque. La partition cible doit être formatée NTFS et contenir une installation de Windows Vista
3. L'installation met en service BDE pour le volume Windows et vérifie que ce volume contient bien des versions de Vista Enterprise ou Ultimate
4. L'installation vérifie que le TPM a été initialisé
5. L'utilisateur choisit sa méthode de sauvegarde de clé de récupération et l'installation continue par le chiffrement du volume
6. L'installation affiche une barre de progression du chiffrement (réalisé en arrière plan) et notifie l'utilisateur quand BDE est prêt

Bitlocker™

Le déploiement d'une machine en entreprise avec un TPM

Installation de BDE

1. Active Directory préparé pour les clés de BDE
2. Installation de Windows Vista
   a. BDE est uniquement disponible avec les version Enterprise et Ultimate de Windows Vista.
   b. BDE nécessite une partition séparée de celle de la partition du système d'exploitation de Windows Vista avec un minimum de taille libre de 350 (500) MO
   c. Pendant l'installation on vérifie que le système dispose bien de la bonne version du TPM (v 1.2) et du BIOS via Plug and Play
   d. Les drivers TPM et BDE sont installés
3. Initialisation de BDE
   a. Initialisation via un script du TPM
   b. Le mot de passe du propriétaire du TPM est sauvegardé dans l'Active Directory
4. Exécution à distance du Script BDE
   a. La politique sauvegarde la clé de récupération dans l'AD
   b. Le système est chiffré
5. Inspection des journaux d'événement pour contrôler la bonne fin du chiffrement




Bitlocker™ : Comment ça marche ?

Quelques définitions du TCG

- TCG : *Trusted Computing Group* (https://www.trustedcomputinggroup.org)
- TPM : *Trusted Platform Module* (voir plus loin)
- RTM : *Root of Trust Measurement*
  - C'est une chaîne de confiance où, étant donné un point de départ du code digne de confiance, on peut déterminer la mesure de son intégrité et la maintenir pour chacun des blocs de code subséquents
- CRTM : *Core Root of Trust Measurement*
  - C'est une petite section de ROM non *flashable* d'un BIOS compatible TCG qui est exécutée avant tout autre code après le redémarrage d'une machine afin d'établir la RTM

Quelques définitions du TCG

- DRTM : *Dynamic Root of Trust Measurement*
  - C'est une chaîne de confiance qui démarre à un code digne de confiance et qui peut commencer après l'exécution d'une instruction spéciale du microprocesseur ; la chaîne de confiance est valide pour une instance spécifique du code dont l'intégrité est mesurée par le hardware et par un hyperviseur
- PCR : *Platform Control Register*
  - Registre d'un TPM
  - Ce registre est suffisamment grand pour contenir un *hash* (aujourd'hui seulement SHA-1)
  - Un registre ne peut être qu'« étendu », ce qui veut dire que son contenu est un hash « glissant » de toutes les valeurs qui y ont été chargées

Quelques définitions du TCG

- L'utilisation des registres PCR[0] à PCR[7] est prédéterminé par le TCG
- Les registres PCR[8] à PCR[15] sont utilisés par la SRTM et sont disponibles pour les systèmes d'exploitation
- PCR[0] à PCR[15] sont remis à zéro seulement lors du *boot*
- PCR[16] et au-delà sont utilisables par le DRTM

- *Seal* : un processus par lequel des données sont chiffrées et authentifiées par le TPM et appariées avec un ensemble de valeurs de PCR cibles, créant ainsi un Blob (*Binary Loadable Object*) chiffré
  - Les Blobs retournés par une opération *Seal* du TM ne sont pas stockés à l'intérieur du TPM ; ils peuvent être stockés n'importe où (sur le disque dur par exemple) puisque leurs données ne peuvent être révélées que par une opération *Unseal* subséquente

Quelques définitions du TCG

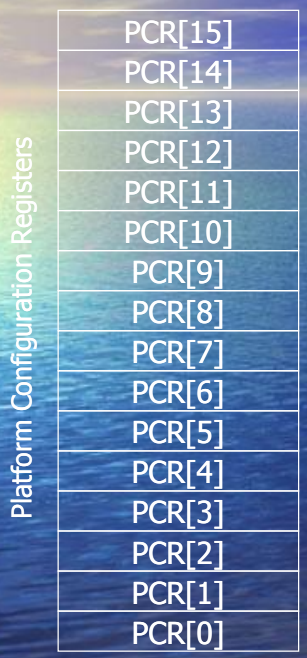
- *Unseal*
  - Le processus par lequel les données contenues dans un Blob scellé sont déchiffrées par le TPM pour révéler le secret originel
  - Ce Blob ne peut être descellé que lorsque les PCR du TPM sont identiques au PCR spécifiés dans le Blob ; si l'une quelconque des valeurs des PCR sont différentes, le TPM refusera de desceller les données et retournera une erreur

Chiffrement de disque avec Bitlocker™

Usage du TPM

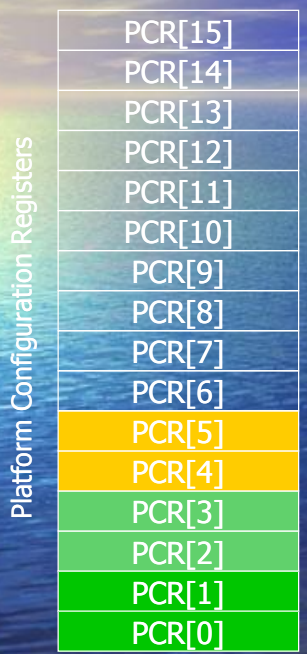
- Le démarrage sécurisé (*Secure Startup)* s'appuie sur le *Static Root of Trust Measurement (SRTM)* du TPM
- Fonction *Extend*
  - L'authentification de l'OS est établie par la constitution d'empreintes du code dans les PCR (*Platform Configuration Register*)
  - A la mise sous tension, les PCR sont initialisés à zéro
  - La fonction *Extend* permet d'enrichir un PCR du condensé (*hash*) de sa valeur actuelle et des nouvelles données en entrée :
    - Le code à authentifier
  - On « mesure » ainsi le code avant son exécution
  - Chaque PCR est affecté à la mesure d'un bout de code de démarrage
    - BIOS PCR
    - Boot Sector PCR, etc…
- Fonctions *Seal/Unseal*
  - *Seal* permet de chiffrer une donnée
  - *Unseal* permet de déchiffrer une donnée si et seulement si le jeu des registres PCR auquel est associée l'opération sont positionnés à la même valeur que lors du *Seal*
    - On ne peut desceller une clé qui si on a démarré le même OS

Mesure de l'OS à l'aide du TPM

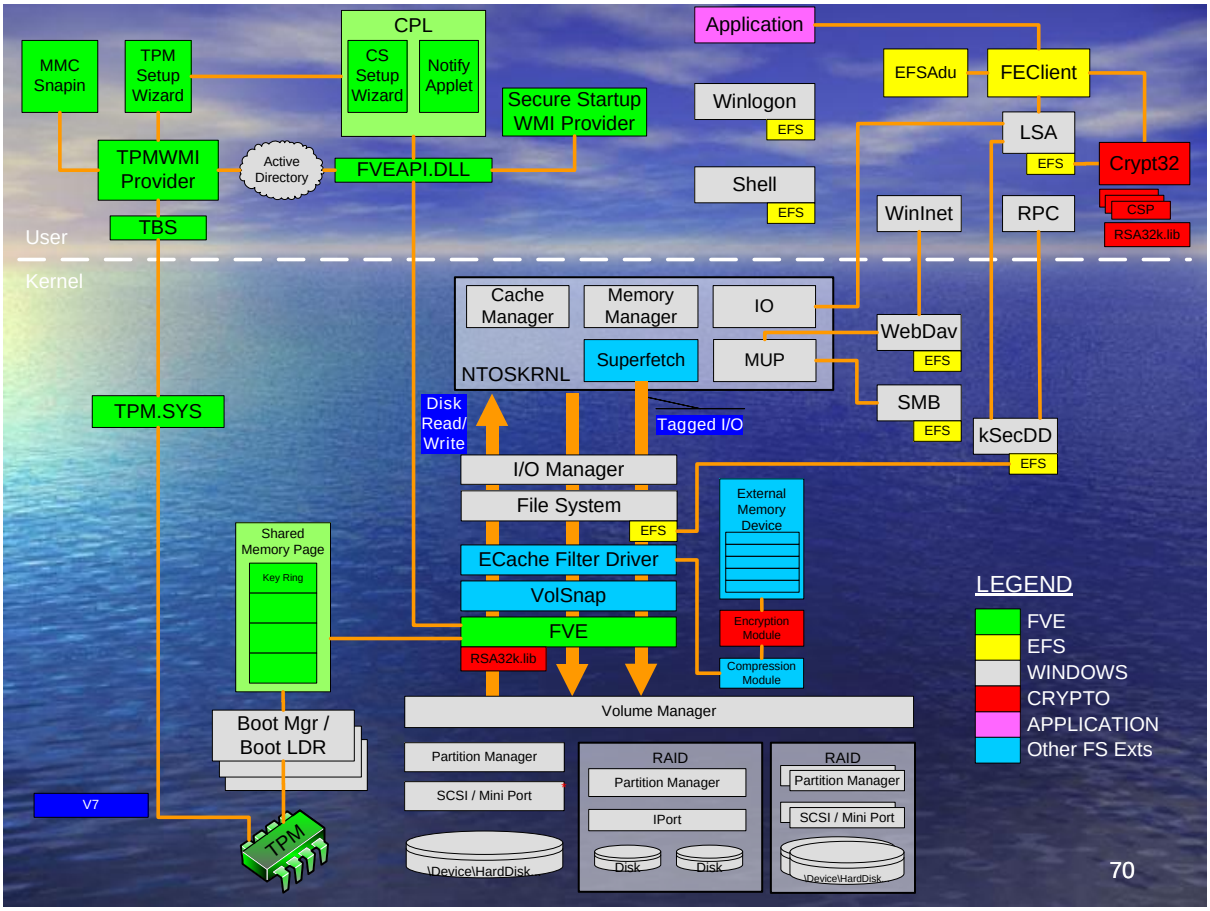


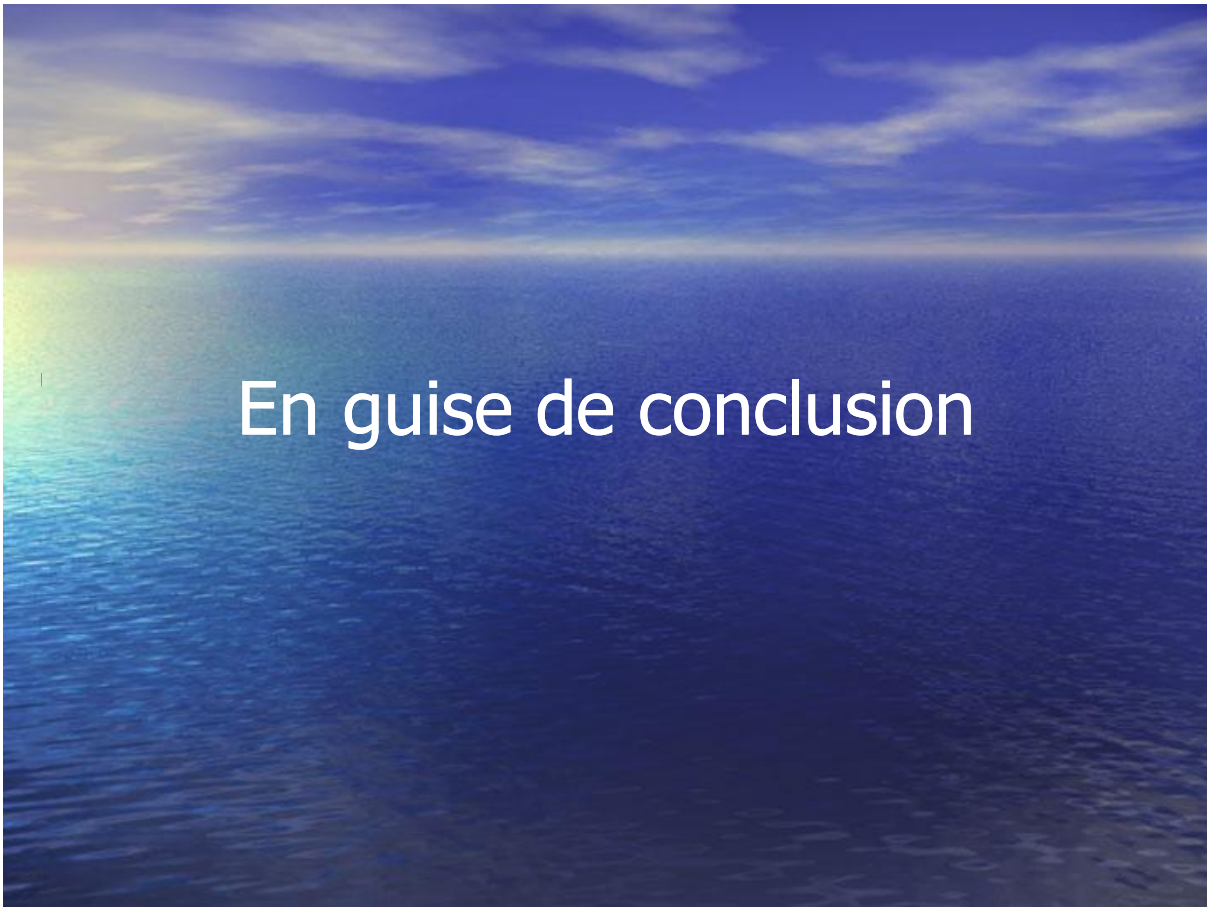
- Initialisation des registres et transfert de l'exécution au *Core Root of Trust Measurement*
- Mesure du *firmware* dans PCR[0] et des données dans PCR[1]
  - Test hardware et configuration
- Le code est d'abord mesuré, puis exécuté
  - Le PCR s'enrichit du SHA-1 du texte en entrée
- Option ROMs et données dans PCR[2] et [3]
- MBR dans PCR[4], table des partitions PCR[5]

Mesure de l'OS à l'aide du TPM

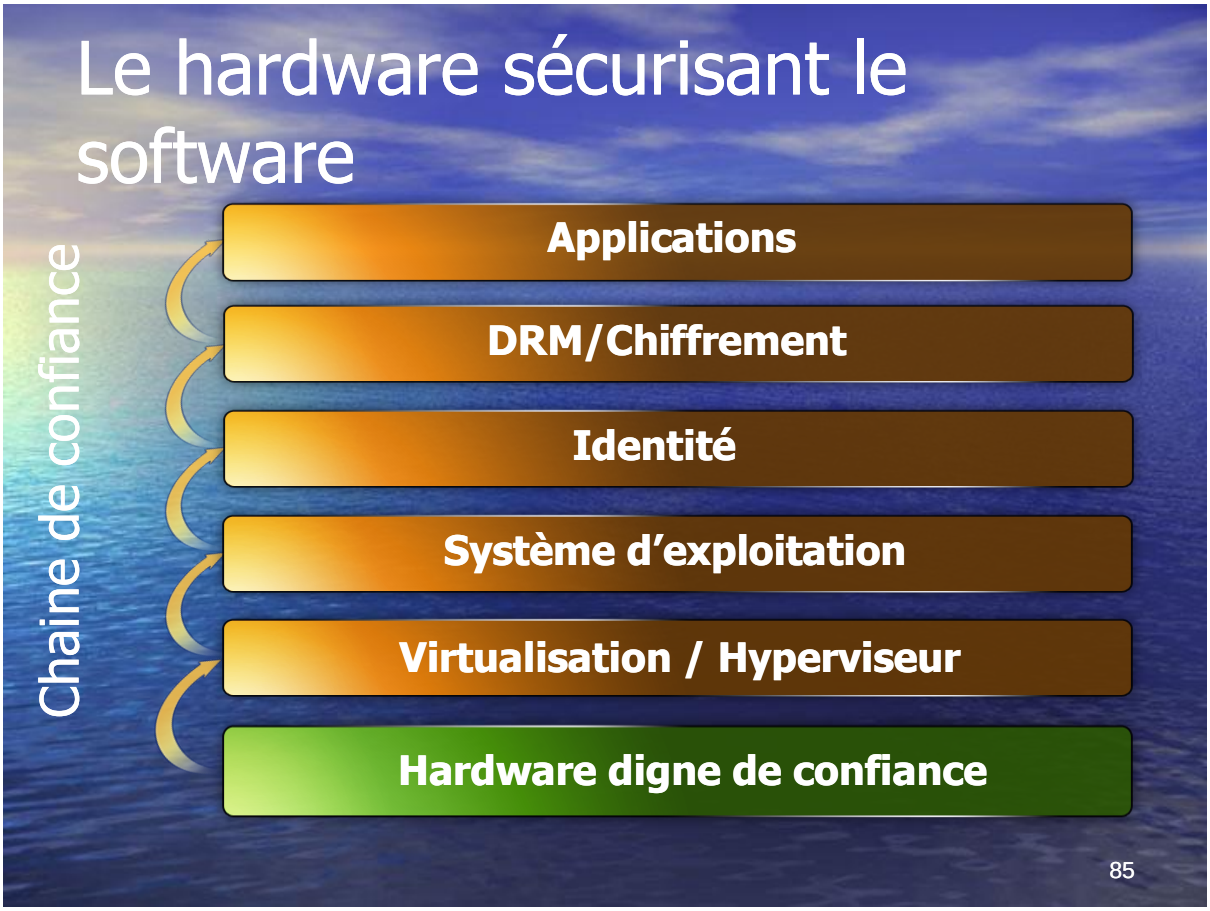


- MBR prend le contrôle; charge le premier secteur de la partition de boot active en mémoire; mesure les premiers 512 octets dans PCR[8]
- Le secteur de *boot* est mesuré dans PCR[9] puis exécuté
- Le code de BOOTMGR est mesuré dans PCR[10] puis exécuté
- Les applications de démarrage additionnelles doivent être chargées à partir de la partition Bitlocker™
- Finalement, BOOTMGR transfère le contrôle vers l'OS; l'OS vérifie alors l'intégrité des exécutables avant le transfert d'exécution


CPL
MMC Snapin
TPM Setup Wizard
CS Setup Wizard
Notify Applet
Application
EFSAdu
FEClient
Secure Startup WMI Provider
Winlogon
EFS
LSA
EFS
Crypt32
CSP
RSA32k.lib
TPMWMI Provider
Active Directory
FVEAPI.DLL
Shell
EFS
WinInet
RPC
TBS
User
Kernel
Cache Manager
Memory Manager
IO
NTOSKRNL
Superfetch
MUP
WebDav
EFS
SMB
EFS
kSecDD
EFS
TPM.SYS
Disk Read/ Write
Tagged I/O
I/O Manager
File System
EFS
External Memory Device
Shared Memory Page
Key Ring
ECache Filter Driver
VolSnap
FVE
RSA32k.lib
Encryption Module
Compression Module
LEGEND
FVE
EFS
WINDOWS
CRYPTO
APPLICATION
Other FS Exts
Volume Manager
Boot Mgr / Boot LDR
Partition Manager
SCSI / Mini Port
RAID
Partition Manager
IPort
RAID
Partition Manager
SCSI / Mini Port
V7
TPM
\Device\HardDisk
Disk
Disk
\Device\HardDisk
70

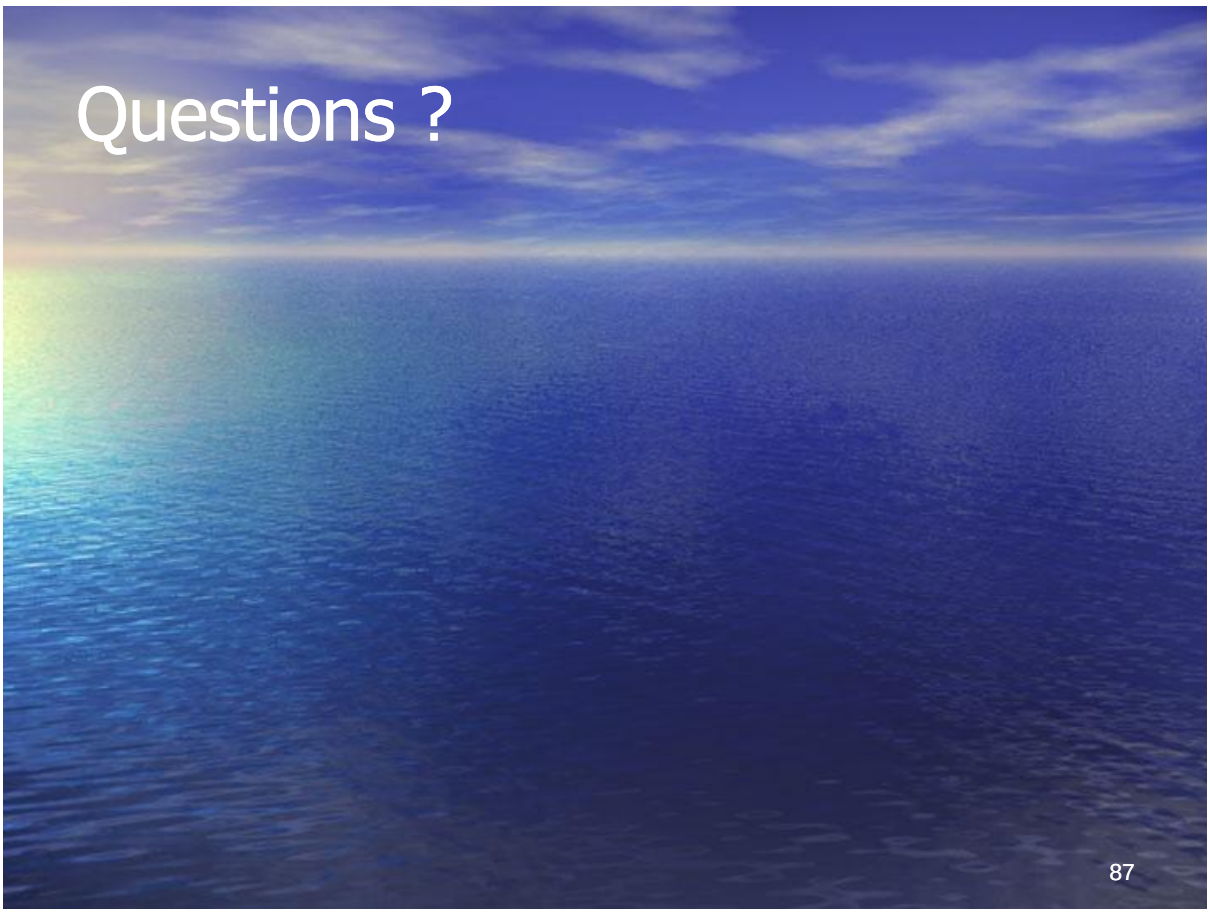

En guise de conclusion

Le hardware sécurisant le software



La suite…

- La virtualisation offre des perspectives intéressantes (cf. la présentation qui a été faite l'année dernière sur ce sujet lors des Journées Microsoft de la Sécurité)
- En particulier, si elle est assistée par le hardware sur le plan des performances et de la sécurité afin de garantir par le hardware que les partitions sont bien isolées
- C'est dans cette direction notamment qu'évolue NGSCB


Questions ?
87


Microsoft®
Votre potentiel, notre passion.™
Microsoft France
18, avenue du Québec
91 957 Courtaboeuf Cedex
www.microsoft.com/france
0 825 827 829
msfrance@microsoft.com
88