CONSTRUISONS ENSEMBLE
LA DÉFENSE DE DEMAIN

COURS
WINDOWS ET LA SÉCURITÉ

DGA

Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE

MINISTÈRE
DE LA DÉFENSE

MÉCANISMES DE PROTECTION

MÉCANISMES DE PROTECTION
Introduction

- Afin de réduire l'impact des erreurs de programmation dans les programmes et dans Windows lui-même, Microsoft a ajouté à Windows, au fur et à mesure des versions, des techniques de protection
- Exemple de fonctions de sécurité ajoutées:
  - Utilisation des protections des composants
  - Sécurisation des zones mémoire
  - Signature des binaires et des drivers
  - Sécurisation du démarrage
  - Chiffrement du stockage

MÉCANISMES DE PROTECTION

Techniques d'attaques (Rappel)

- Le dépassement de tampon (buffer) est la technique principale qui est la plus utilisée pour exploiter une faille
- Un dépassement consiste à écrire plus de données que l'espace qui a été réservé par le programmeur ou le compilateur
- Cela permet d'injecter du code, de modifier le flux d'exécution afin de faire réaliser une action par le programme

MÉCANISMES DE PROTECTION

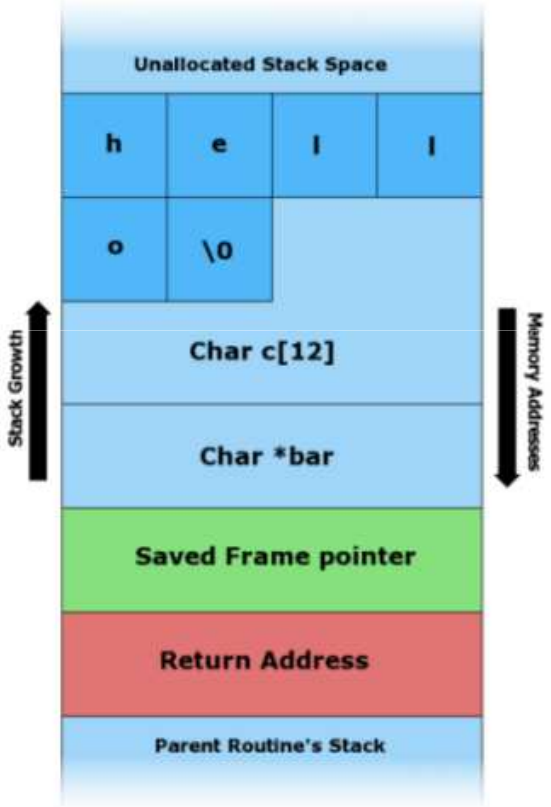
Cas du buffer overflow

- Les variables sont stockées dans la pile
- Lors de l'appel à une fonction par le processeur, l'adresse de retour de la fonction est aussi stockée dans la pile
- Dans la pile, la variable est avant l'adresse de retour
- Si on copie une valeur plus grande que l'emplacement prévu pour la variable, on risque d'écraser l'adresse de retour
- Si la valeur copiée est du code et que l'on modifie l'adresse de retour de la fonction pour pointer sur l'adresse du code copié, on a réussi à faire exécuter le code copié

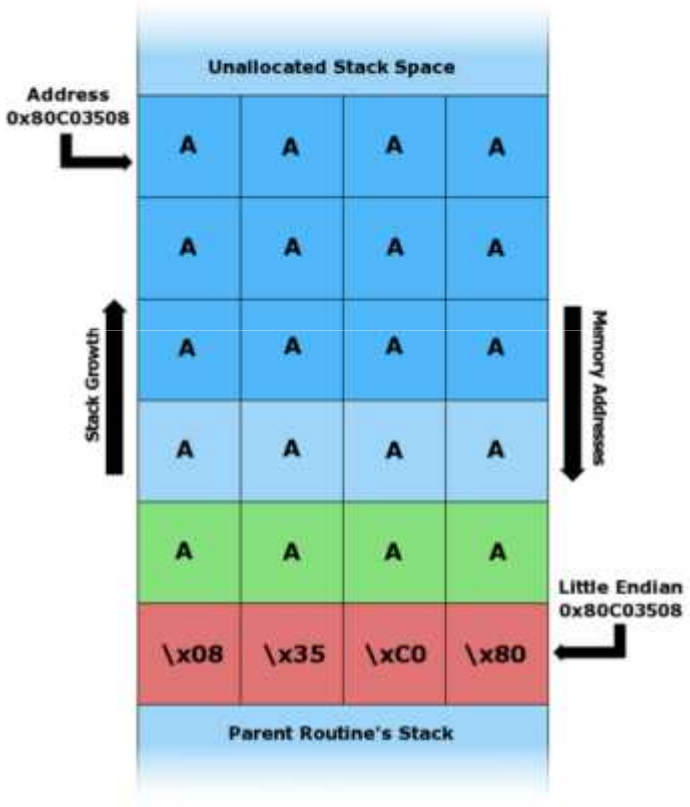
MÉCANISMES DE PROTECTION

Exemple de « Buffer overflow »

- Strcpy normal



- Dépassement de tampon



MÉCANISMES DE PROTECTION

Protection des zones mémoire

- Afin d'essayer de réduire l'impact d'un dépassement de buffer, le mécanisme « Bit NX » au niveau du processeur est apparu en 2003
- Bit NX (Never eXecute) chez AMD ou XD (eXecute Disable) chez Intel permet de définir des zones d'exécutions et des zones de données dans lesquelles le CPU ne pourra pas exécuter de code
- Depuis XP SP2 et Server 2003 SP1, Windows utilise au travers de la fonctionnalité de sécurité DEP (Data Execution Prevention) la technique du Bit NX

MÉCANISMES DE PROTECTION
DEP

- A cause d'incompatibilités de certaines applications, DEP a été activé pour le système et les services de Windows uniquement
- La fonction DEP est activable pour l'ensemble des applications tout en excluant certaines
- Des contournements à DEP sont possibles comme par exemple : ROP (Return Oriented Programming) consiste à modifier par dépassement l'adresse de retour de la fonction pour pointer sur un code d'une librairie qui est autorisé par DEP

MÉCANISMES DE PROTECTION
ASLR

- ASLR (Address Space Layout Randomization) permet de rendre l'attaque ROP très difficile
- Le principe consiste à distribuer aléatoirement l'espace d'adressage des programmes
- Un attaquant ne pourra pas prédire l'emplacement du code qu'il veut faire exécuter lors d'un dépassement
- La technique de distribution aléatoire nécessite une bonne entropie pour que l'emplacement ne soit pas prédictible (Privilégier un OS 64bits)

MÉCANISMES DE PROTECTION
SafeSEH & SEHOP

- Une autre technique d'attaque par dépassement consiste à modifier la structure du traitement des exceptions (SEH) d'un programme
- A partir de XP SP2, la protection SafeSEH (Safe Structured Exception Handling) a été intégrée et à partir de Vista SP1, SEHOP (Structured Exception Handling Overwrite Protection) est une amélioration de SafeSEH
- Ces protections vérifient l'intégrité de la structure SEH avant d'exécuter le gestionnaire d'exception

⇒L'attaque de la SEH devient difficile sur un système 64 bits avec les protections SEHOP + DEP + ASLR activées

MÉCANISMES DE PROTECTION

Signature des composants

- Afin d'améliorer le niveau de confiance du code exécuté sous Windows, Microsoft a introduit une fonction de signature par certificat (Authenticode)
- Le certificat peut être intégré, soit dans le PE, soit à un catalogue (.cab) qui contiendra tous les « hashs » et les signatures des binaires de l'application
- Lors du chargement d'un PE, Windows va vérifier le certificat ainsi que son intégrité
- L'usage de drivers signés est devenu obligatoire à partir de Windows 7 64bits.
- L'ensemble des PEs de Windows sont signés

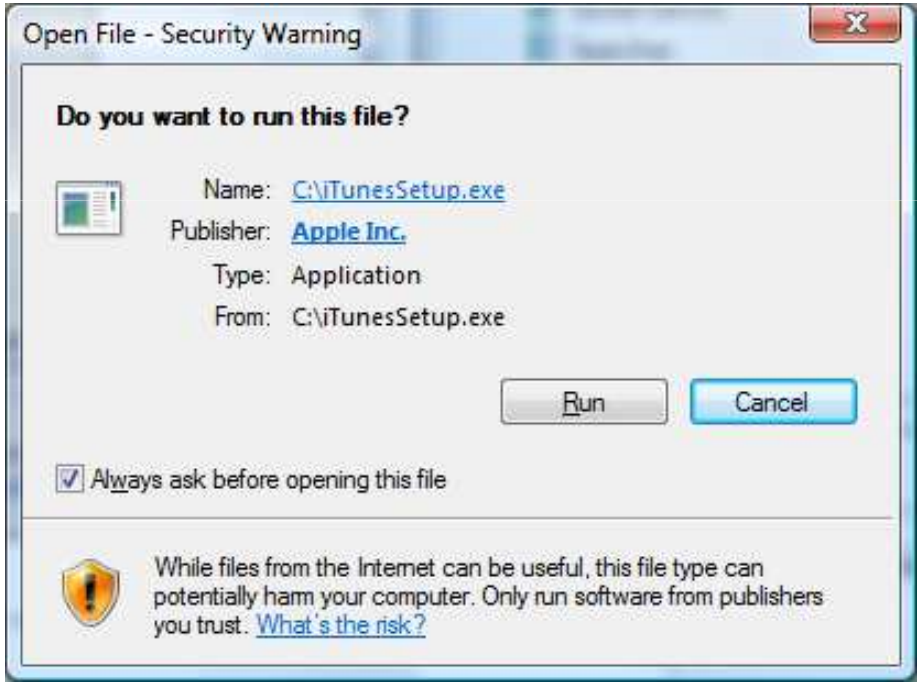
MÉCANISMES DE PROTECTION
Authenticode

- Une signature d'un PE ne garantit pas le bon fonctionnement, il garantit juste qu'il provient bien d'une personne donnée et qu'il n'a pas été modifié depuis sa signature
- Windows utilise un format PKCS contenant un certificat X.509 lié à un certificat d'autorité (CA)
- Un certain nombre de CA sont intégrés de base lors de l'installation de Windows

⇒Si un attaquant arrive à compromettre un CA, il pourra par exemple diffuser des binaires sous l'identité du CA

MÉCANISMES DE PROTECTION
La confiance des CA

- **Dans le cas où un PE est signé à partir d'un CA inconnu, un message avertit l'utilisateur :**



MÉCANISMES DE PROTECTION
Sudo sous Windows

- Pour permettre à un utilisateur sans privilège d'utiliser Windows et d'y installer ponctuellement et simplement des applications ou des drivers avec des privilèges élevés, Windows à partir de Vista propose la technologie UAC (User Account Control)
- Ressemble à sudo sous Linux
- Windows UAC permet :
  - De ne pas ouvrir une session Administrateur
  - De limiter par défaut les privilèges de tous les utilisateurs
  - De limiter l'ajout des privilèges à un seul programme
  - D'avertir l'utilisateur lors d'une modification du système par une application

MÉCANISMES DE PROTECTION
Windows UAC

- Exemple de deux programmes qui souhaitent avoir des privilèges plus élevés
  - Non signé
  - Signé par Microsoft

=> L'attaquant utilise souvent l'ingénierie sociale pour contourner cette protection

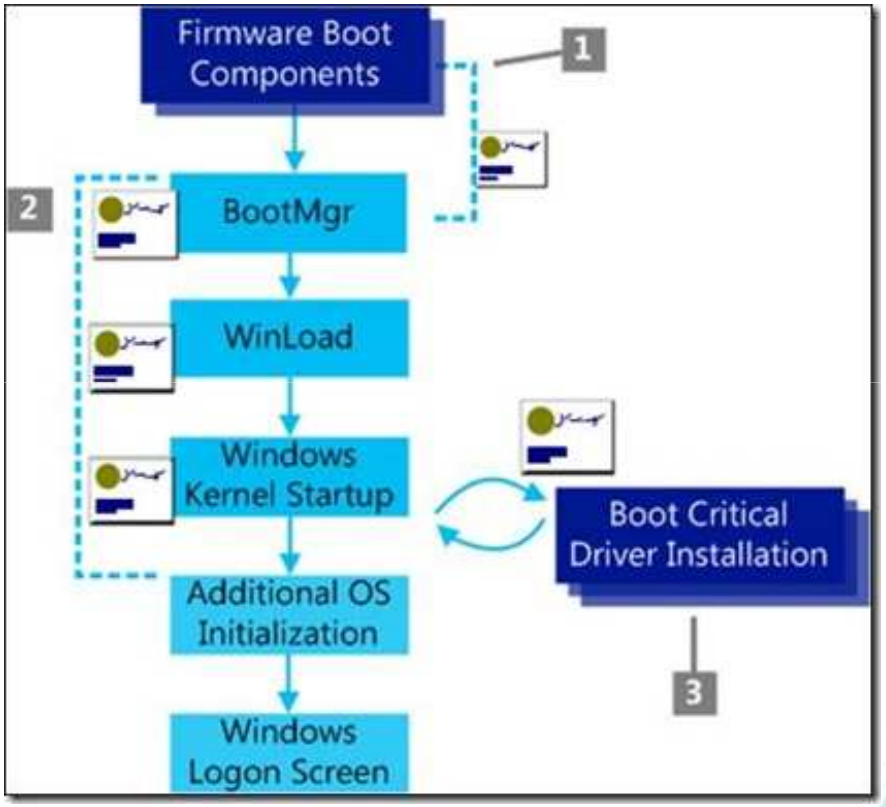
MÉCANISMES DE PROTECTION
Démarrage sécurisé

- La fonctionnalité « Secure Boot » permet de sécuriser le démarrage de Windows en vérifiant la signature de chaque code avant de l'exécuter
- L'ordinateur doit avoir au minimum un « bios » UEFI en version 2.3.1 Errata C (UEFI Class 2 ou 3)
- L'UEFI contient dans une « Secure Key Database » des « Secure Boot Keys » liées au constructeur du matériel et à Windows
- Si le « Secure Boot » est activé dans l'UEFI, les OS qui n'ont pas de signature valide ne peuvent pas démarrer

⇒Démarrage sur certains linux ou LiveCD bloqué

MÉCANISMES DE PROTECTION
Secure Boot

- 1 UEFI vérifie la signature du Boot Manager
- 2 Chaque étape du démarrage de Windows vérifie la suivante
- 3 Les drivers sont aussi vérifiés

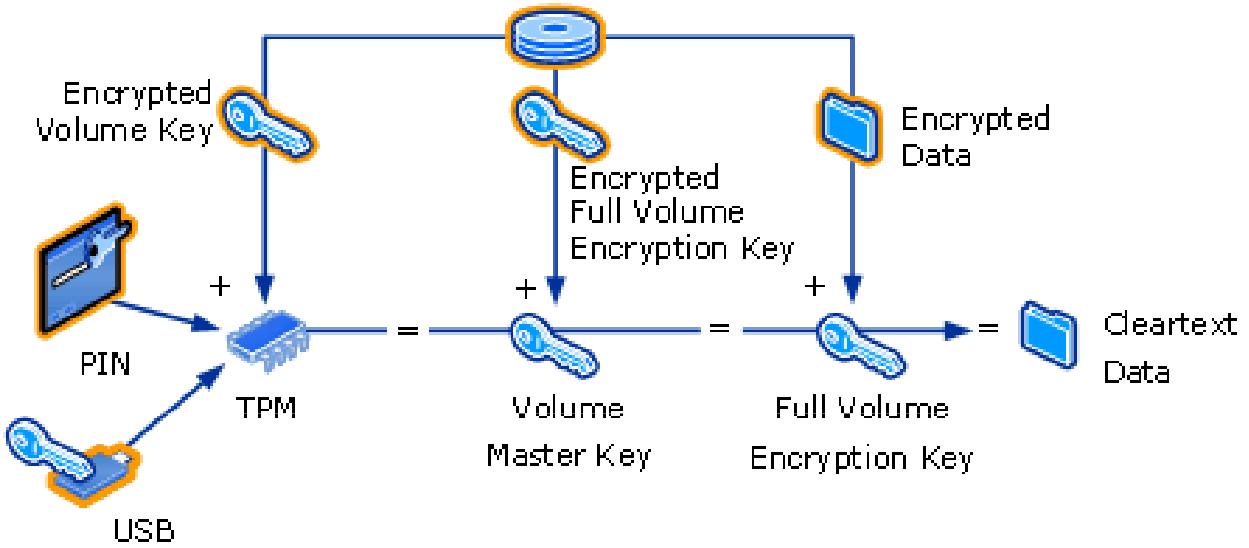


MÉCANISMES DE PROTECTION
Chiffrement de volume

- Depuis Vista, Windows propose une fonctionnalité de chiffrement de disque nommée BitLocker Drive Encryption
- Une clé « Master key » est stockée soit dans une puce TPM (Trust Platform Module) du PC soit dans une clé usb
- Cette « Master key » peut être protégée par un code PIN ou un mot de passe
- Lors du chiffrement du disque, Windows fournit une clé de récupération utilisable en cas de secours (TPM mort)
- Bitlocker To Go permet de chiffrer des supports amovibles (USB, Disque externe, …)

MÉCANISMES DE PROTECTION

Fonctionnement de BitLocker avec un TPM



- **Attention, sur Windows 10 la clé de récupération est stockée sur le compte Microsoft de l'utilisateur (US ?)**

⇒**Le but de l'attaquant est de récupérer soit la « Master Key » soit la clé de récupération**

MÉCANISMES DE PROTECTION

Les mises à jour

- Depuis Windows 98, Windows Update permet de mettre à jour Windows par internet ou par un serveur WSUS (Windows Server Update Services)
- Windows Update permet de garder Windows à jour afin de se protéger des failles connues
- Depuis Windows XP, des drivers et des mises à jour mineures ainsi qu'un outil de désinfection sont aussi proposés
- A partir de Windows 10, les mises à jour sont diffusées en mode P2P entre les utilisateurs

MÉCANISMES DE PROTECTION

Ce qu'il faut retenir pour la suite

- CPU Bit-NX + DEP + ASLR + SEHOP + 64bits => bonne protection contre les dépassements de tampon
- La signature des binaires est indispensable mais cela ne protège pas contre les failles et les sources malveillantes
- SecureBoot et Bitlocker permettent de garantir une protection du démarrage ainsi que des données
- UAC permet de se connecter avec des privilèges limités mais cela ne protège pas contre les failles humaines
- Mettre à jour, mettre à jour et mettre à jour !