# OSSIR
# Groupe Sécurité Windows

**Réunion du 2 avril 2007**

# Sécurité Windows Vista
# Premiers retours d'expérience


**Olivier REVENU**
**EdelWeb**
**olivier.revenu (à) edelweb.fr**


**Nicolas RUFF**
**EADS-IW**
**nicolas.ruff (à) eads.net**


**EdelWeb**

# Plan

- Introduction
- Principes de développement
- Revue des fonctions de sécurité
- Bilan
- Attaques connues
- Attaques possibles
- Conclusion

# Introduction

- **Vista : le système phare de Microsoft en 2007**
  - **A venir : Longhorn (2008), Vienna (2009), …**
- **Un système considérablement modifié**
  - **Vendu pour son interface graphique**
  - **Mais les changements sont sous le capot**
- **Des paradigmes de conception actuels**
  - **Sécurité (contre les malwares et le phishing)**
  - **DRM (contenu protégé et HD-DVD)**
  - **Lutte contre le piratage logiciel**
  - **Connexion permanente avec Microsoft**
    - **Ex. technologies P2P et IPv6 natives**
  - **Etc.**

# Principes de développement

- **Réécriture du code**
  - **Exemple de parties sensibles réécrites**
    - **Pile TCP/IP (double pile IPv4 / IPv6 native)**
    - **Protocole SMB (version 2, avec support IPv6)**
  - **Nouveaux protocoles développés from scratch**
    - **Ex. LLTD, PNRP, LLMNR, PNM**

- **Sécurité intégrée dès la conception**
  - **Secure Development Lifecycle (SDL)**
    - **Développeurs sensibilisés**
    - **Revue de code**
    - **Outils de développement sûrs**
    - **Surface d'exposition minimale par défaut**
  - **A prouvé son efficacité sur SQL Server 2005**
    - **Aucune faille connue à ce jour**

# Principes de développement

- **Limitation des privilèges "par défaut"**
  - **L'utilisateur n'est plus administrateur**
  - **Notion de "sudo" (comme sous Unix) : User Account Control (UAC)**

- **Niveaux d'intégrité sur les processus**
  - **User Interface Privilege Isolation (UIPI)**

# Revue des fonctions de sécurité (1/8)

- **Support des pages mémoire non exécutables**
  - **DEP : Data Execution Prevention**
  - **A fait ses preuves sous Linux et *BSD**
    - **Ex. PaX, W^X**
  - **Déjà présent dans Windows XP SP2**
    - **Mais désormais actif par défaut**

# Revue des fonctions de sécurité (1/8)

- **Limites**
  - **Nécessite un processeur récent (~ année 2005+)**
    - **Technologie NX chez AMD, XD chez Intel**
  - **Technique de contournement connue**
    - **"Retour dans la libc"**
  - **Peut être désactivé par l'attaquant**
    - **Simple bit dans le descripteur du processus**
    - **http://www.uninformed.org/?v=2&a=4**
  - **Automatiquement désactivé si le point d'entrée du programme n'est pas dans une section exécutable**
    - **Concerne une partie des protecteurs logiciel (packers)**

# Revue des fonctions de sécurité (2/8)

- **Espace mémoire "aléatoire"**
  - **ASLR : Address Space Layout Randomization**
  - **A fait ses preuves sous Linux et *BSD**
    - **Ex. GrSec**
  - **Limites**
    - **Nécessite une recompilation des exécutables avec Visual Studio 2005 SP1+**
    - **Nécessite que DEP soit activé**
      - **Aucune justification technique à ce fait**
    - **Aléa déterminé au boot**
    - **Entropie de 8 bits (256 essais au maximum)**

# Revue des fonctions de sécurité (3/8)

- **Pile (stack) protégée par le compilateur (/GS)**
  - **Déjà présent dans Windows XP SP2, Linux et *BSD (ex. StackGuard, ProPolice)**
  - **Limites**
    - **Nécessite une recompilation des exécutables avec Visual Studio 2002+**
    - **Exploitation possible si une exception est levée avant la sortie de la fonction**

# Revue des fonctions de sécurité (4/8)

- **Tas (heap) protégé par le système**
  - **Déjà présent dans Windows XP SP2, Linux (glibc récentes), *BSD**
  - **Limites**
    - **Entropie de 8 bits (256 valeurs possibles)**
    - **Ne protège pas les applications qui utilisent leur propre gestion du tas**
      - **Ex. Borland Delphi**

# Revue des fonctions de sécurité (5/8)

- **Exceptions protégées (SafeSEH)**
  - **Supporté par Windows XP SP2 mais rarement rencontré dans les binaires**
  - **Limites**
    - **Nécessite une recompilation des exécutables avec Visual Studio 2002+**
    - **Tous les binaires d'un processus (EXE + DLLs) doivent être protégés**
    - **L'utilisation d'un "trampoline" reste possible**

# Revue des fonctions de sécurité (6/8)

- **Fonctions traditionnellement dangereuses supprimées**
  - **Exemples**
    - **printf("%n") n'existe plus**
    - **strcpy() remplacé par safe_strcpy()**
  - **Limites**
    - **Nécessite une recompilation des exécutables avec Visual Studio 2005+**

# Revue des fonctions de sécurité (7/8)

- **Vérifications d'intégrité**
  - **CI.DLL en mode utilisateur**
  - **PatchGuard en mode noyau**

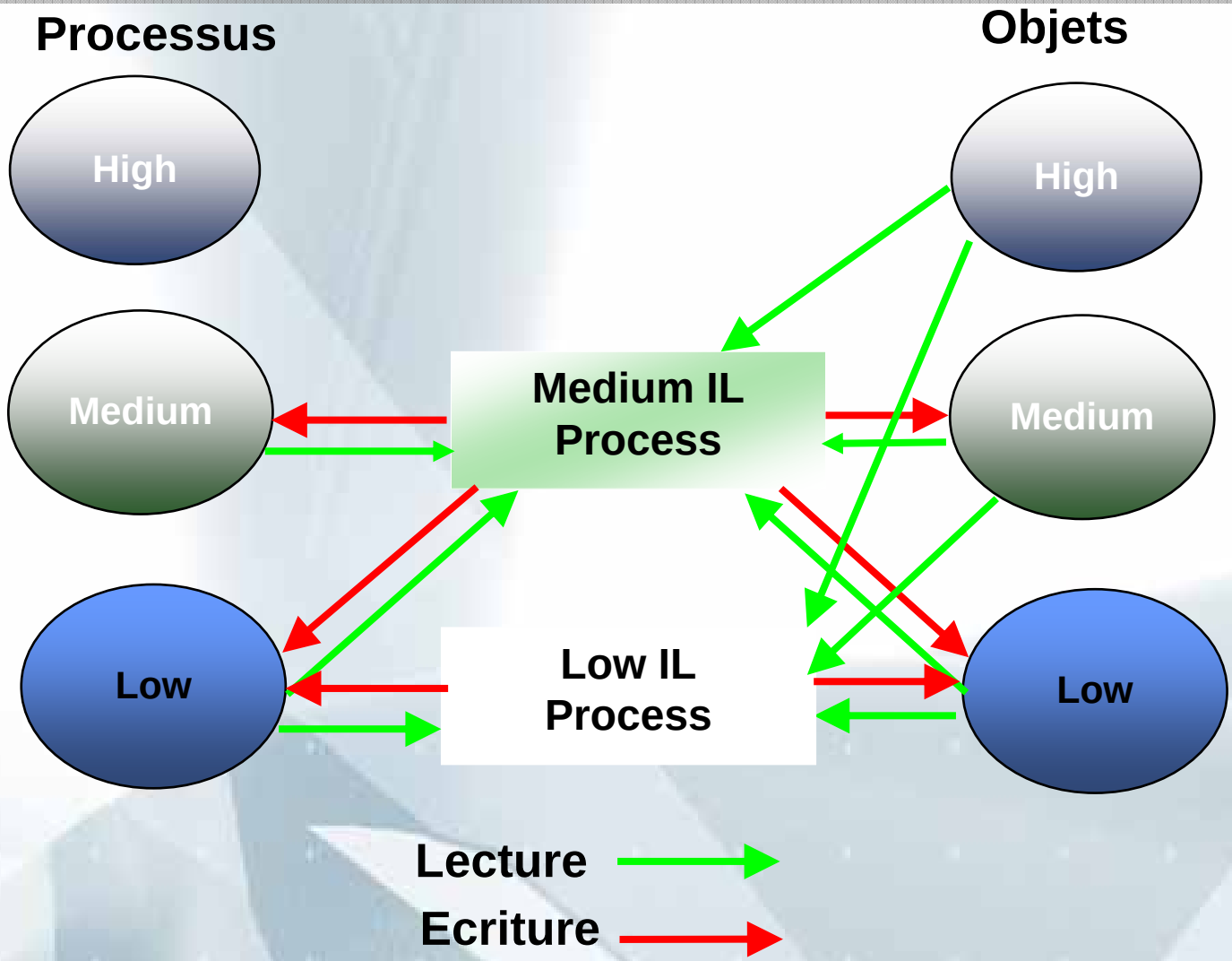
  - **Limites**
    - **N'est pas vraiment une fonction de sécurité**
      - **Imposé par les éditeurs de contenu multimédia**
      - **Améliore la stabilité du système en bloquant les patches du noyau**
    - **Non seulement PatchGuard est déjà contourné**
    - **Mais en plus il est possible de créer un malware indétectable grâce à PatchGuard !**
      - **http://www.uninformed.org/?v=6&a=1**

# Revue des fonctions de sécurité (8/8)

- **User Account Control (UAC)**
- **User Interface Privilege Isolation (UIPI)**

  - **Limites**
    - **"Ne sont pas des fonctions de sécurité"**
      - **Mark Russinovitch, Microsoft Corp.**
    - **Peut être désactivé par l'utilisateur … et les applications**
    - **Tout repose sur la décision finale de l'utilisateur (oui / non)**
    - **Tout programme contenant la chaine "setup" ou "install" ne peut être lancé qu'en mode administrateur**
    - **L'envoi de messages Windows vers un processus de niveau d'intégrité supérieur est autorisé**

# Revue des fonctions de sécurité (8/8)



# Bilan

- **Aujourd'hui le consensus est le suivant**
  - **Le nombre de failles "triviales" devrait être faible**
    - **Faille "triviale" = buffer overflow exploitable à distance sans authentification**
    - **... mais la faille "ANI" semble montrer que le code hérité va poser problème encore longtemps !**
  - **Chaque protection prise indépendamment peut être contournée**
    - **La combinaison des protections rend l'exploitation difficile**
    - **Cette combinaison ne se rencontre (actuellement) que dans les logiciels Microsoft récents**
      - **E.g. Vista, Office 2007**

# Bilan

- **Pour la plupart des failles, l'exploitation "universelle" sera difficile**
  - **C'est la fin des "vers" à la Blaster**
- **Microsoft a plusieurs années d'avance sur le reste des éditeurs**
  - **Ex. Oracle, Apple, etc.**

# Attaques connues

- **Code hérité**
  - **Exemple : faille "ANI"**
- **Problèmes complexes, non détectables à la compilation**
  - **Exemple : faille NtRaiseHardError() permettant d'obtenir les droits SYSTEM**
    - **Combinaison d'une fonction obscure, d'une fuite mémoire et d'un "double free"**
- **Problèmes conceptuels**
  - **Exemple : contournement de UIPI par envoi de messages WM_KEY**
- **Détournement de fonctions légitimes**
  - **Exemple : utilisation de la fonction "commande vocale" par une site Web malveillant, utilitaires d'accessibilité**

# Attaques connues

- **Applications tierces**
  - **Pour être pleinement protégée, une application tierce doit :**
    - **Etre compilée avec Visual Studio 2005 SP1+**
    - **Utiliser les options /GS, /SAFESEH, /DYNAMICBASE**
    - **Ne pas être protégée par un packer**
    - **Ne pas écrire dans les répertoires "Program Files", "Windows", …**
      - **Sinon les droits administrateur seront requis**

# Attaques connues

- **Applications tierces**
  - **Conclusion : l'écrasante majorité des applications Windows aujourd'hui restent attaquables sur Vista**
  - **Exemple présenté à la conférence RSA Security 2007**
    - **http://searchsecurity.techtarget.com/originalContent/0,289142,sid14_gci1242436,00.html**

# Attaques possibles

- **Les applications malveillantes**
  - **Une majorité des virus de messagerie arrive sous forme de pièce jointe exécutable**
    - **Seule nouveauté : le nombre de "oui" à cliquer (UAC)**

- **Les nouvelles fonctions**
  - **Très nombreuses**
    - **Découverte de la topologie réseau (LLTP)**
    - **P2P intégré**
    - **Gadgets de bureau, incluant de la publicité**
    - **Etc.**
  - **Peu de maturité**

# Attaques possibles

- **La connectivité totale**
  - **IPv6 natif ou encapsulé (tunnels) offre une visibilité globale sur Internet**
    - **Que se passe-t-il si l'utilisateur partage un répertoire … ?**
    - **Réponse partielle : notion de "profil réseau" (public / bureau / maison)**

- **Les failles noyau**
  - **Sujet de recherches intensives depuis 2005**
    - **Ex. série de failles dans les drivers WiFi**
  - **Le noyau n'a pas le même niveau de protection que les applications utilisateur**
  - **L'exploitation est délicate … mais pas impossible !**

# Conclusion

- **Avec toutes ses protections combinées, Vista devrait connaitre moins de failles critiques que ses prédécesseurs**
  - **Il ne faut pas en conclure que Vista est inviolable**
  - **D'ailleurs des failles critiques ont déjà été trouvées !**
- **De nouveaux risques sont à prévoir**
  - **IPv6 natif, P2P natif, gadgets de bureau, …**
- **Il reste à rendre plus sûr :**
  - **Les applications tierces**
  - **Les comportements utilisateur**
- **Et surtout à répondre à la question …**
  - **Vista est-il un OS pour l'entreprise, ou pour les particuliers ?**

# Démos