Nouveautés en matière de sécurité du Service Pack 2 de Windows XP

Microsoft Windows XP
Service Pack 2
with Advanced
Security
Technologies

Benoit HAMET
Ingénieur d'étude/Formateur
MVP
Concept Réseau

Microsoft

Sommaire

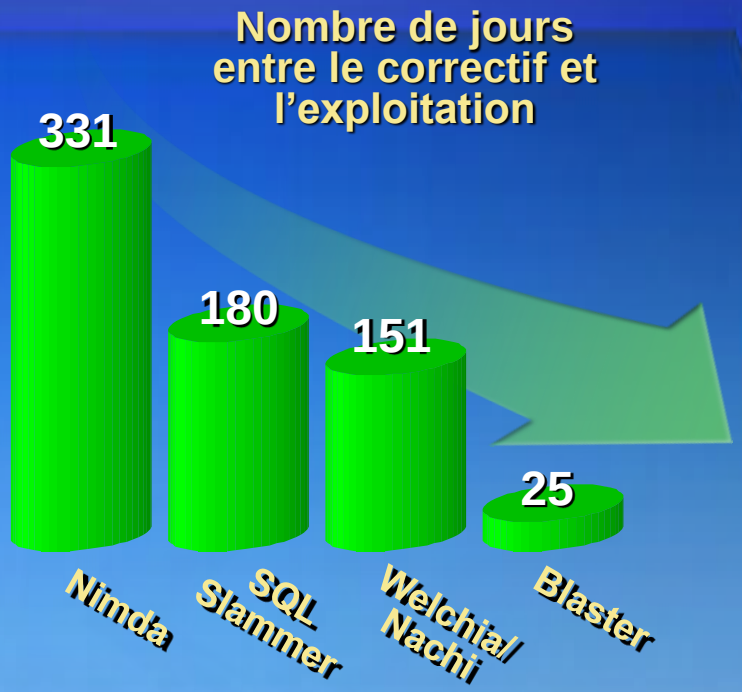
- Motivation
- Les 4 grandes classes
  - Protection réseau
  - Navigation Internet
  - Messagerie et messagerie instantanée
  - Protection mémoire
- Autres améliorations

Microsoft Windows xp
Service Pack 2
with Advanced
Security
Technologies

Constats

Octobre 2003

- Prolifération des correctifs
- Temps avant exploitation en baisse
- Exploitations plus sophistiquée
- L'approche classique n'est pas suffisante



La sécurité est notre priorité n°1
Il n'y a pas de remède miracle
Le changement nécessite des innovations

Réponses pour améliorer la sécurité

- Faire tendre vers 0 le nombre de vulnérabilités
- Améliorer la gestion des correctifs de sécurité
- Diminuer la vulnérabilité résultante, sans application de correctif
- Fournir des guides et formations
- Sensibiliser les utilisateurs

Windows XP Service Pack 2

- Cumulatif des mises à jour post SP1 http://go.microsoft.com/fwlink/?linkId=20403
- Pour autant, ce n'est pas un Service Pack classique
  - Ingénierie proactive plutôt que réactive en renforçant la sécurité par des moyens préventifs permettant de bloquer des classes d'attaques
    - Réduction de la surface d'attaque
    - Renforcement des capacités de défense en profondeur
    - Meilleure sécurité par défaut
    - Meilleure gestion des correctifs de sécurité
    - Diminution du fardeau des décisions de sécurité pour l'utilisateur
  - Approche bouclier pour diminuer les attaques possibles et faire en sorte que 7 correctifs sur 10 déployables à votre rythme

Windows XP Service Pack 2

- Focus sur 4 grands types d'attaque
  - Réseau (pare-feu amélioré / configuration réseau RPC DCOM renforcée)
  - Messagerie électronique et messagerie instantanée (pièces jointes)
  - Navigation Internet (ActiveX, pop-up)
  - *Mémoire* (protection de la mémoire améliorée contre les *Buffer overflows*)
- Autres améliorations liées à la maintenance de la sécurité

Protection réseau

- Pare-feu Windows
- RPC / DCOM

Pare-feu activé en permanence

Activé par défaut sur toutes les interfaces (LAN, modem, VPN, Wi-Fi,…)

Internet

Détecte automatiquement la connexion au réseau d'entreprise et utilise la configuration correspondante (profil du domaine vs profil standard)

Protection lors du démarrage avec règle statique par défaut (sauf si désactivé) : seuls DNS, DHCP et Netlogon sont autorisés jusqu'à ce que le pare-feu ait démarré

Réseau d'entreprise

Restriction de certains services au réseau local ou à une certaine étendue (adresses sources)

Pare-feu Windows

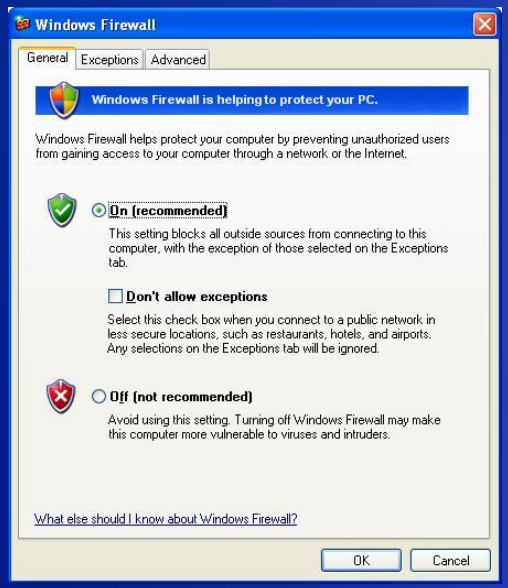
- 3 modes opérationnels
  - Activé (trafic entrant autorisé = exception)
  - Activé sans exception (plus de trafic entrant non sollicité, conservation des réglages)
  - Désactivé
- Configuration globale (réglage par interface possible)
- Liste d'exceptions
- Ouverture statique de ports
- Config d'options ICMP
- Simplification des réglages (ex : partage de fichiers)
- Journalisation des paquets rejetés et des connexions réussies
- Support de IPv6

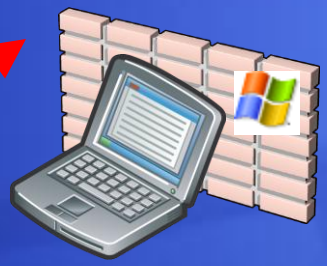
Gestion du pare-feu Windows

Interface utilisateur

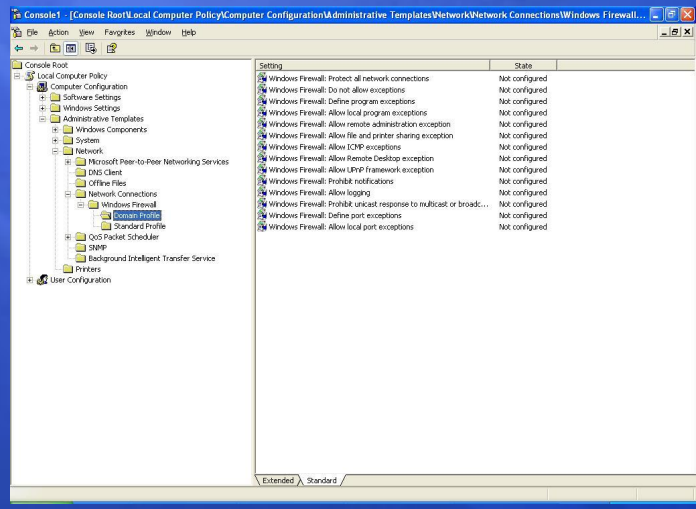
API

Fichier d'installation *unattended*





Stratégie de groupe

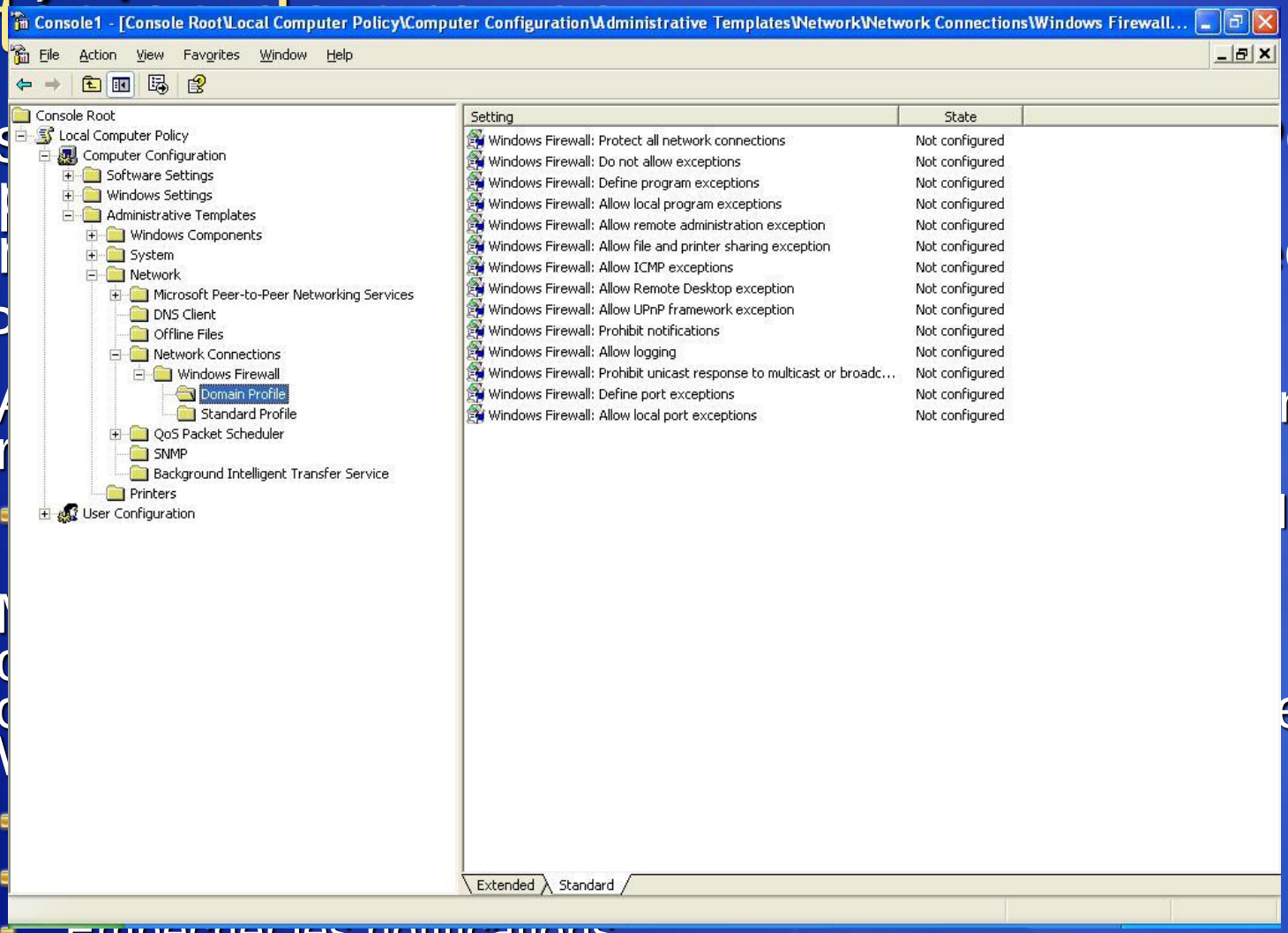


Ligne de commande (Netsh)

Pare-feu Windows

Stratégie de

- Mis
  dep
  par
- GP
  - A
    - Empêcher les notifications
    - …



Pare-feu Windows

- Liste des exceptions
  - Dans les versions précédentes, les applications devaient de[mander] l'ouverture d'un port (API)
  - Or, les ports [sont] connus à l'avance
  - Nouvelles fo[nctionnalité] application ajoutée à la liste ouvrira [automatiquement] quel que soit le contexte de [l'application]
  - La manipulation de la liste demande les privilèges administrateurs
  - Stratégies de groupe
    - Définir les exceptions de port
    - Autoriser les exceptions de ports locaux (permet aux administrateurs locaux d'ajouter des exceptions)

Pare-feu Windows

- Support broadcast et multicast
  - Les trafics de broadcast et de multicast sont différents de l'unicast car la réponse provient d'un hôte inconnu
  - La pare-feu autorise une réponse unicast pendant 3 secondes depuis n'importe quelle adresse source avec le même port que celui duquel le trafic a été émis
  - Stratégie de groupe : empêcher les réponses monodiffusion pour des requêtes multidiffusion ou diffusion

Pare-feu Windows

- Profils multiples
  - Chaque profil correspond à un paramétrage
  - L'un pour le réseau d'entreprise (domaine), l'autre pour les autres réseaux (ex : hôtel, hotspot)
    - Si aucun contrôleur de domaine sur le réseau : profil **standard**
    - **Sinon profil** domaine
  - Attention : nécessite un domaine (les machines en groupe de travail n'ont qu'un seul profil)
  - Recommandation : configurer les 2 profils


démo
Microsoft

Utilisateurs administrateurs locaux

- Si vos utilisateurs sont administrateurs locaux de leurs machines et si vous craignez qu'ils puissent installer le SP2 de leur propre chef, vous pouvez désactiver le pare-feu a priori en créant les clés de registre
  - HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\FirewallPolicy\DomainProfile\EnableFirewall=0 (DWORD)
  - HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\FirewallPolicy\StandardProfile\EnableFirewall=0 (DWORD)

Déploiement du pare-feu sans les stratégies de groupe

- Netfw.inf à l'installation
  - http://www.microsoft.com/downloads/details.aspx?familyid=cb307a1d-2f97-4e63-a581-bf25685b4c43&displaylang=en
- Script netsh après l'installation

```
netsh firewall set portopening UDP 1434 Slammer
```

Amélioration RPC / DCOM

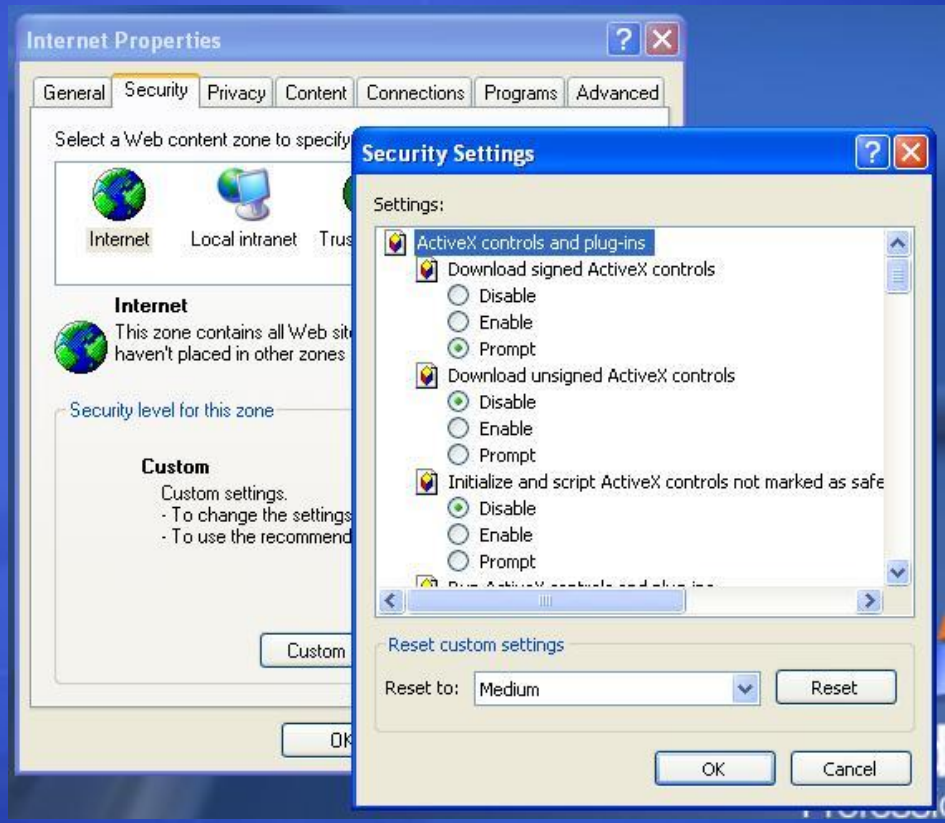
- Restriction RPC
  - S'exécute avec des privilèges moindre
  - Requière une authentification sur les interfaces par défaut (clé de registre RestrictRemoteClients)
  - Possibilité de restreindre à la machine locale par programmation
  - Désactivation de RPC via UDP par défaut
- Restriction DCOM
  - S'exécute avec des privilèges moindre
  - Contrôle d'accès plus stricte et paramétrable via le registre (accès, lancement, activation)

Navigation Internet plus sûre

Microsoft

Les zones de sécurité d'IE

- Zone Poste de travail
  - Non montrée dans l'interface utilisateur
  - Tout contenu HTML sur la machine locale
  - Niveau de sécurité Faible pour supporter les applications HTML
- Sites de confiance
  - Niveau de sécurité : Faible
- Intranet local
  - Machines dans votre domaine
  - Niveau de sécurité : moyennement bas
- Internet
  - Noms FQDN
  - Niveau de sécurité : Moyen
- Sites sensibles
  - Utilisé par les applications pour manipuler des e-mail HTML avec un niveau de sécurité Haut



Navigation plus sûre

- Verrouillage des zones Poste de travail et intranet
- Amélioration de la notification pour l'exécution et l'installation d'applications ou de contrôles ActiveX
- Éviter l'usurpation d'interface graphique
- Bloqueur d'éléments contextuels (pop-ups!)
  - Bloque les pop-ups non sollicités
  - Peut permettre des pop-ups pour certains domaines (ex: intranet)
  - Les fenêtres ouvertes par un clic de l'utilisateur ne sont pas restreintes


démo
Microsoft

Verrouillage de la zone Poste de travail

- Avant le SP2 : les fichiers de la machine locale et le contenu associé n'avaient pas de zone
- Désormais, tout le contenu local est dans le contexte de sécurité de la zone Poste de travail (afin d'éviter les tentatives d'élévation de privilèges)

Gérer les modules complémentaires

- Visualisation et contrôle des modules complémentaires chargés
- L'administrateur peut établir la liste des modules complémentaires autorisés et interdits
  - Attention : ces modules peuvent toujours être appelés par d'autres composants, d'où l'importance de gérer l'inclusion de modules complémentaires

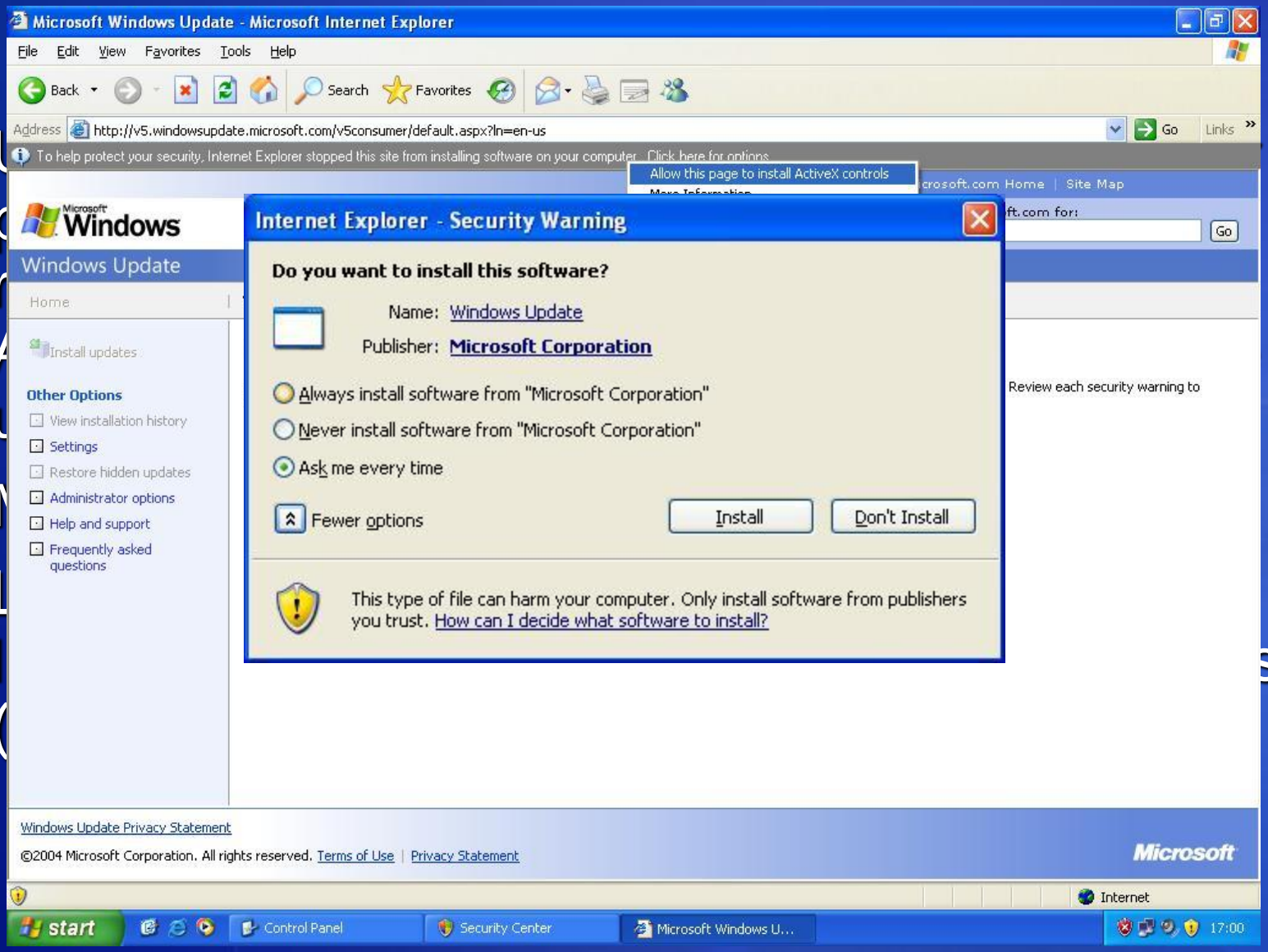
Comportements binaires; cache

- Comportements binaires
  - Composants qui encapsulent certaines fonctionnalités pour des éléments HTML
  - Préalablement non contrôlés, peuvent maintenant être restreints par zone
  - En particulier, Sites sensibles
- Mise en cache des objets
  - Auparavant : des objets pouvaient être mis en cache pour donner accès à des contenus d'une autre page Web (le navigateur affiche du contenu et des objets de 2 sites)
  - Problème : l'objet en cache (script) pouvait écouter des événements dans un autre *frame* (carte de crédit)
  - Erreurs « Accès refusé ». L'objet doit être remis en cache avant de pouvoir être accédé par script

Types MIME

- Le type MIME (*Multipurpose Internet Mail Extensions*) détermine la façon dont un contenu est manipulé
  - Ex : une image est affichée alors qu'un exécutable provoquera une boîte de dialogue de téléchargement
- Nouvelles règles pour éviter l'usurpation de type MIME
- Le MIME « sniff » déterminera si un fichier est un exécutable déguisé (signature de bits). Tous les fichiers ainsi détectés auront leur extension modifiée et seront enregistrés dans le cache
- Important : correspondance sur le sites des entêtes et des extensions

Éditeurs de confiance



Restrictions sur les fenêtres

- Interdictio pop-up sans la b de titre et la ba
- Inter nêtre par s e par l'utili

Blocage de l'élévation de zone

- Empêche la modification des paramètres de sécurité depuis un contenu qui s'exécute dans une zone inférieure
- Les pages Web qui appelles d'autres pages plus privilégiées échouent (une page dans la zone Internet ne peut pas naviguer vers une page de la zone Poste de travail)

En navigant d'une zone peu privilégiée vers…	*..IE aura le comportement suivant*
Poste de travail	Blocage
Sites de confiance	Demande
Intranet local	Demande
Internet	Autorisation
Sites sensibles	Autorisation

Nouvelles stratégies de groupe (GPO)

- Configuration utilisateur\Modèles d'administration\Composants Windows\Internet Explorer
  - Gestion des modules complémentaires : Mode
  - …
- Configuration utilisateur\Modèles d'administration\Composants Windows\Internet Explorer\Panneau de configuration de Internet\Onglet Sécurité
- Configuration utilisateur\Modèles d'administration\Composants Windows\Internet Explorer\Panneau\Fonctionnalités de sécurité
  - Internet Explorer, Tous les processus ou Liste des processus

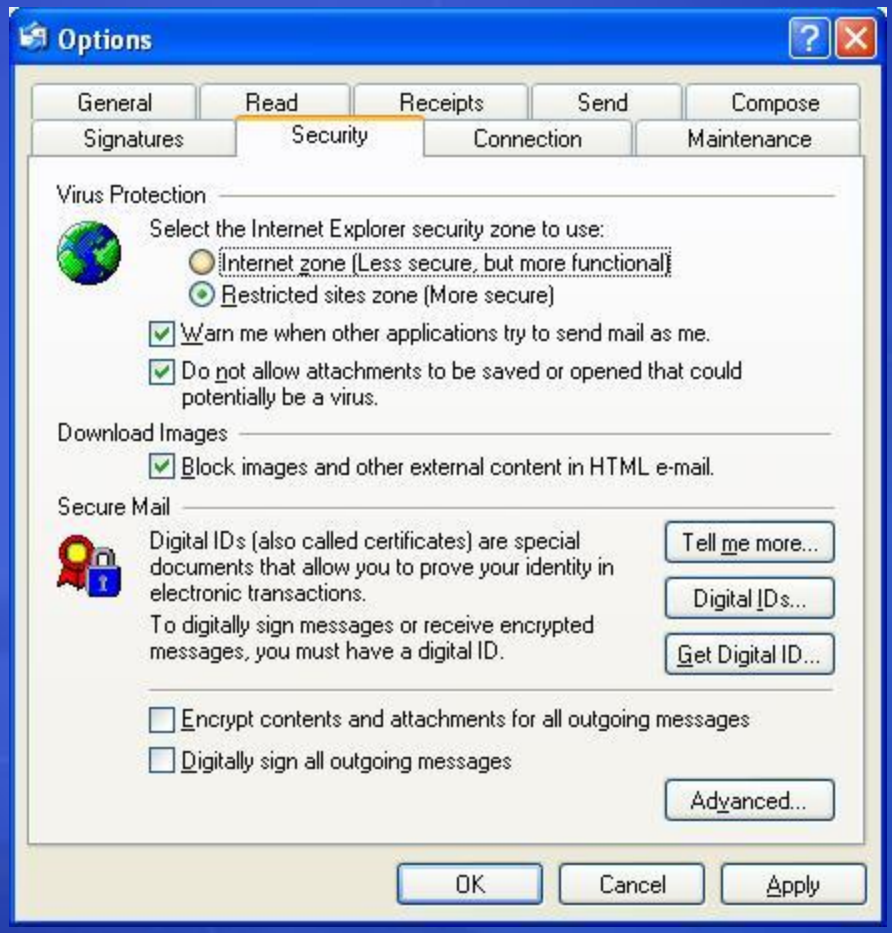

Messagerie et
messagerie
instantanée plus sûres
Microsoft

Pièces jointes

- Gestion des pièces jointes
  - Pour gérer en un point unique la notion de confiance en un type de pièce jointe
  - Pour permettre aux applications d'avoir un moyen cohérent de déterminer les pièces jointes dangereuses
- Création d'une API publique de gestion des pièces jointes (Attachment Execution Services) au niveau du système pour une gestion cohérente pour toutes les applications
- Par défaut : tout est considéré comme dangereux
- Outlook Express, Windows Messenger, Internet Explorer utilisent la nouvelle API
- Ouverture et exécution avec le minimum de privilèges

Outlook Express

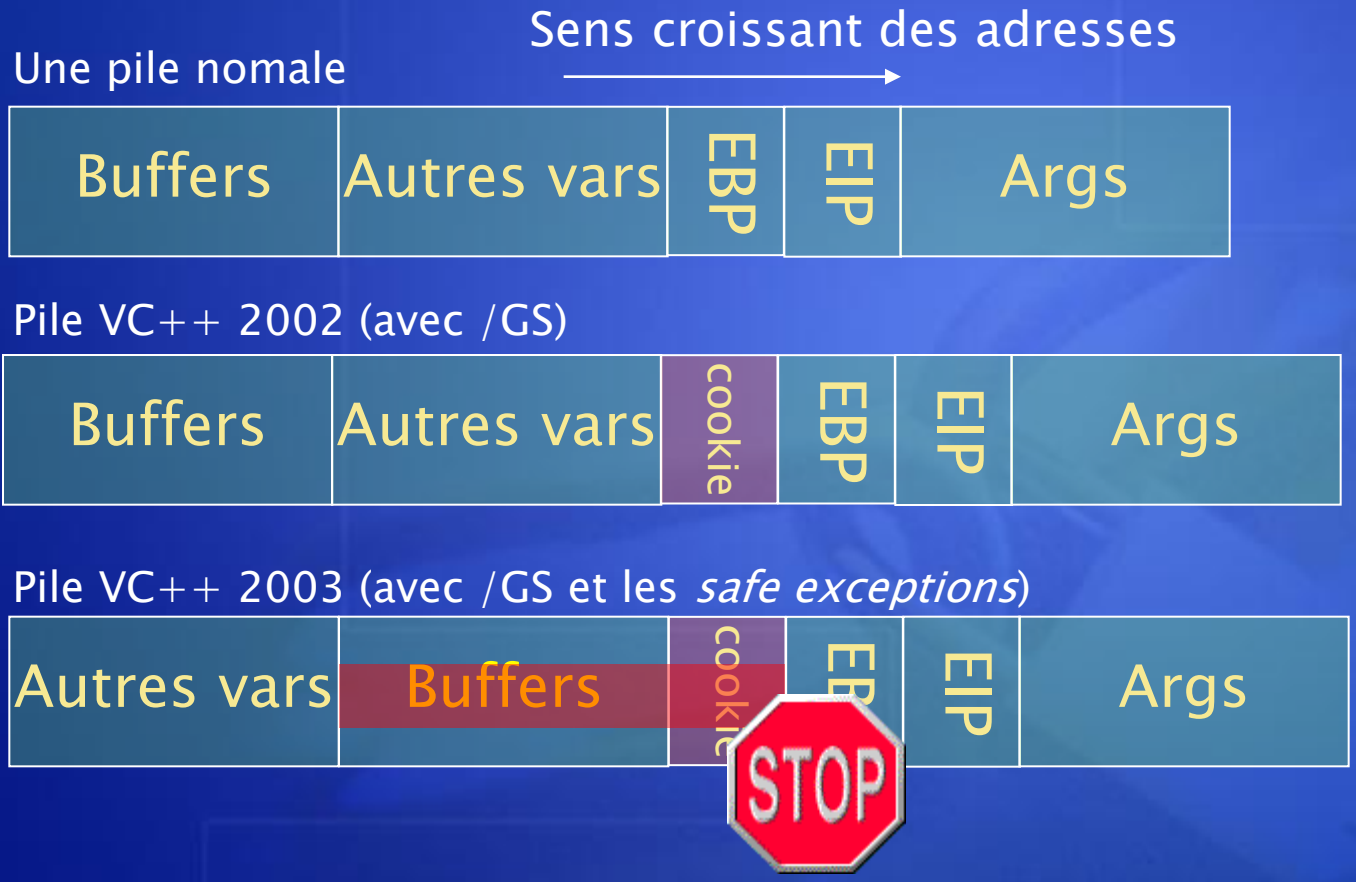
- Aperçu de message plus sûr
- Améliorations dans OE comparables à celles d'Outlook 2003
  - E-mail HTML en zone Sites sensibles
  - Non téléchargement du contenu HTML externe
  - Protection du carnet d'adresses
  - Protection contre le contenu exécutable



Protection mémoire

Réduction de l’exposition à certains *buffer overflows*

Compilation avec /GS (Visual Studio 2003)



Prévention de l'exécution des données

- Prise en charge de la protection matérielle contre l'exécution (NX : No Execute) des processeurs récents (AMD64 / Itanium)
  - Seules les régions de mémoire marquées explicitement pour l'exécution peuvent s'exécuter (mode noyau et mode utilisateur)
  - Activé par défaut pour les binaires Windows
  - Attention : applications de type compilateur juste à temps

Autres améliorations

Microsoft

Autres améliorations

- Mises à jour automatique
  - Écran modal lors de l'installation sauf si
    - "AutomaticUpdates=1" in the "[Data]" section of the UNATTEND.TXT
    - GPO
    - Déjà réglé pour installation planifiée
  - Client pour Windows Update Services (SUS2)
  - Gestion de la reprise du téléchargement d'un correctif interrompu ou incomplet
  - Note : son réglage n'est pas modifié par Sysprep
- Windows Update v5
- MSI 3.0

Autres améliorations

- Réduction de la surface d'attaque : désactivation du service Windows Messenger (pop-up Windows) et Alerter
- Autres
  - Windows Media Player 9
  - DirectX 9.0b
  - Bluetooth 2.0
  - Nouveau client WLAN universel

Centre de sécurité

- Outil de suivi des 3 étapes de protection des PC
  - Pare-feu
  - Mise à jour automatique
  - Antivirus à jour


démo
Microsoft

Conclusion

- Une étape dans le voyage vers des plateformes, applications et périphériques sécurisés
- Permettra une meilleure protection
  - Vous donnant du temps pour la gestion des correctifs de sécurité
  - Limitant l'impact des vers et des virus
  - Augmentant la difficulté pour les attaquants
- Large diminution de classes de vulnérabilités (vs correction ponctuelle)
  - Attaques réseau
  - Attaques d'ingénierie sociale
  - *Buffer overflows*
- Contrôle administratif des changements
  - Stratégie de groupe, scripts en ligne de commande, registre

Informations disponibles

- Preview
  - http://www.microsoft.com/sp2preview
- Changes to Functionality in Microsoft Windows XP Service Pack 2
  - http://www.microsoft.com/technet/prodtechnol/winxppro/maintain/winxpsp2.asp
- Deploying Internet Connection Firewall Settings for Microsoft® Windows® XP with Service Pack 2
  - http://www.microsoft.com/downloads/details.aspx?FamilyID=4454e0e1-61fa-447a-bdcd-499f73a637d1&DisplayLang=en

Informations disponibles

- Windows XP Service Pack 2 White Paper Overview
  - http://download.microsoft.com/download/6/6/c/66c20c86-dcbe-4dde-bbf2-ab1fe9130a97/windows%20xp%20sp%202%20white%20paper.doc
- How to Make Your Web Site Work with Windows XP Service Pack 2
  - http://msdn.microsoft.com/asp.net/using/understanding/security/default.aspx?pull=/library/en-us/dnwxp/html/xpsp2websites.asp

Informations disponibles

- Cours pour les développeurs
  - http://www.microsoft.com/france/msdn/technologies/technos/windows/info/info.asp?mar=/france/msdn/technologies/technos/windows/info/20040527-windowsxpsp2.html
- Comment activer le débogage distant sur Windows XP Service Pack 2
  - http://www.microsoft.com/france/msdn/technologies/technos/windows/info/info.asp?mar=/france/msdn/technologies/technos/windows/info/2004-06-02-xpsp2remotedebug.html

Merci de votre attention

Microsoft®

Microsoft® Windows® xp
Service Pack 2
with Advanced
Security
Technologies