NeoValens

PMAS et le principe du moindre privilège

Marco Peretti
Managing Director

marco@neovalens.com

Agenda

- A propos de moi-même
- Définition du problème
- Vocabulaire
- Fonctionnement
- Le produit
- Démo

A propos de moi-même

- “Ancien” Fondateur & CEO de SecureWave
  - 35 Employés (LU, UK, US)
  - 200+ gros clients
  - 250k ordinateurs protégés
- Produits
  - Gestion centralisée de périphériques I/O
  - Alternative aux anti-virus
  - Protection contre le `buffer overflow` pour Windows 2000/XP

Définition du problème

Les privilèges administratifs sont souvent accordés aux utilisateurs car certains programmes ne fonctionnent pas autrement.

Examples:

- Legacy applications
- Installation des périphériques PnP
- Développeurs
- Outils systèmes tels que RegMon, FileMon, etc.

Conséquences

- Les membres du groupe Administrateurs ont tous les droits.
  - Installation d'applications
  - Modification de la configuration du PC
  - Plus vulnérable (virus, spyware, etc.)
  - Aucun contrôle sur les Administrateurs Junior
  - Etc.

NT Sys Admin top 10

- 10) Allows Malware to really *REALLY* hose the PC if it gets hit.
- 9) Allows users to mess up their settings royally.
- 8) Administrative nightmare to manage.
- 7) Must spend more time ghosting machines because of 10, 9, and 8.
- 6) Users get rather pissy about the loss of data stemming from 7
- 5) Any corporate software and mail policy can be easily broken
- 4) They can undermine anything administratively done to their machines
- 3) With only minor creativity in phrasing, local admin rights can easily violate Sarbanes-Oxley and other pseudo-security legislation.
- 2) Users can load -any- software, even illegal stuff...
- 1) Makes corporate security people laugh so hard, they can't effectively do their jobs

Solution

- Gérer les privilèges au niveau de chaque application plutôt qu'au niveau utilisateur
- Limiter l'appartenance au groupe Administrateurs à ceux qui en ont réellement besoin : les administrateurs réseau/système.
- Protéger les administrateurs réseau/système quand ils exécutent certains programmes tels que Internet Explorer, Outlook, etc.

PolicyMaker Application Security

- Policy Maker Application Security permet la gestion des privilèges (les groupes et les privilèges système) au niveau applicatif.
- Policy Maker Application Security est la seule solution sur le marché capable de changer le contexte de sécurité d'un processus. Les changements sont effectués dynamiquement au démarrage de l'application.

Vocabulary quick summary

Pour comprendre le fonctionnement de PolicyMaker Application Security nous avons besoins de revoir quelques termes : SID, ACE, ACL, Security Descriptor, Process, Privilege, Token

Vocabulary

- Security Identifier (SID)
  - (SID) A data structure of variable length that identifies user, group, and computer accounts. Every account on a network is issued a unique SID when the account is first created. Internal processes in Windows refer to an account's SID rather than the account's user or group name.
  - Example: S-1-5-32-544 (Administrators)

Vocabulary

- Access Control Entry (ACE)
  - An entry in an access control list (ACL). An ACE contains a set of access rights and a security identifier (SID) that identifies a trustee for whom the rights are allowed, denied, or audited.

Vocabulary

- Access Control List (ACL)
  - A list of security protections that applies to an object. (An object can be a file, process, event, or anything else having a security descriptor.) An entry in an access control list (ACL) is an access control entry (ACE). There are two types of access control list, discretionary and system.

Vocabulary

- Security Descriptor
  - A structure and associated data that contains the security information for a securable object. A security descriptor identifies the object's *owner* and *primary group*. It can also contain a DACL that controls access to the object, and a SACL that controls the logging of attempts to access the object.

Vocabulary

- Process
  - The security context under which an application runs. Typically, the security context is associated with a user, so all applications running under a given process take on the permissions and privileges of the owning user.

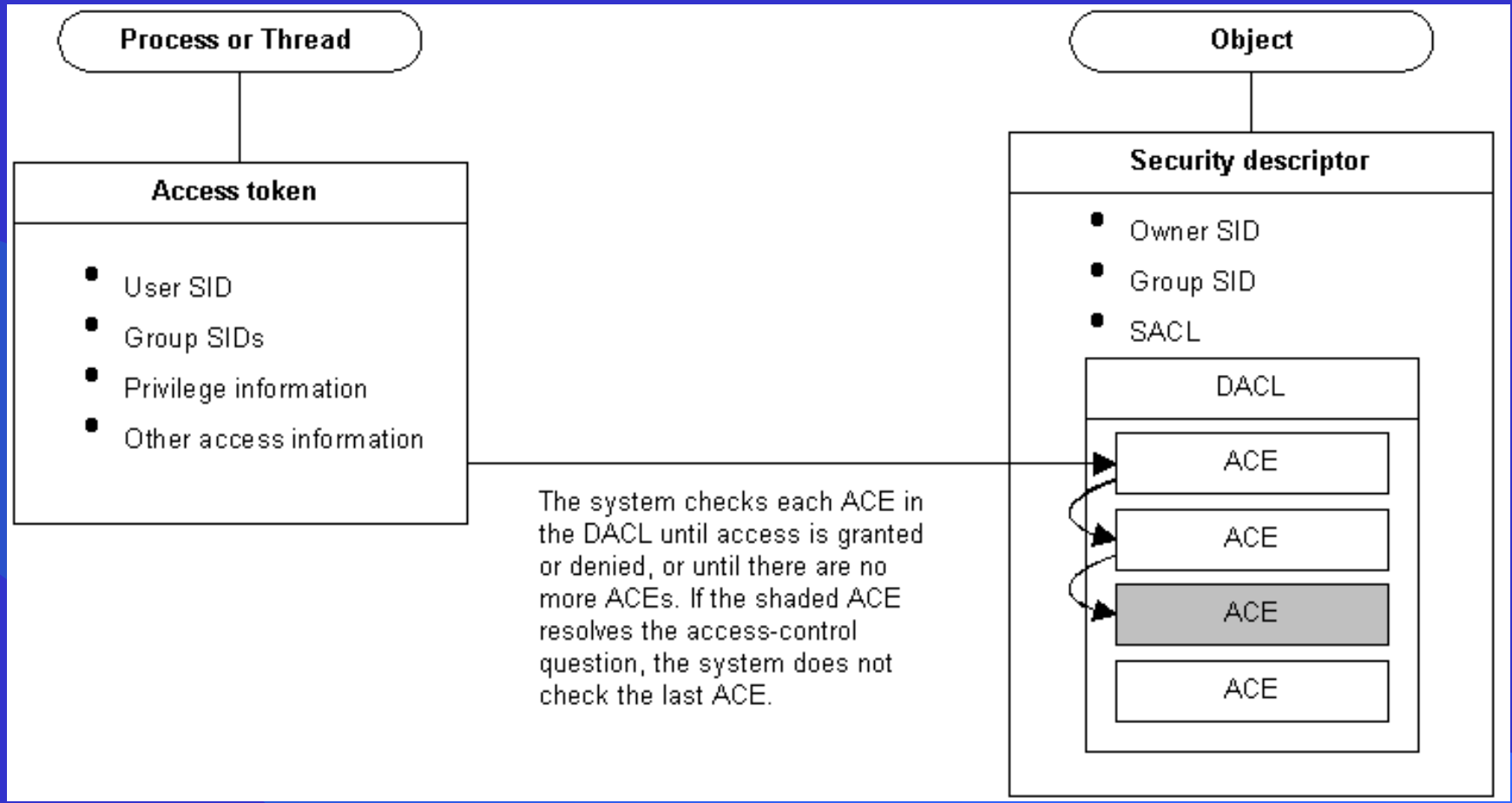
Vocabulary

- Access Token
  - An access token contains the security information for a logon session. The system creates an access token when a user logs on, and every process executed on behalf of the user has a copy of the token. The token identifies the user, the user's groups, and the user's privileges. The system uses the token to control access to securable objects and to control the ability of the user to perform various system-related operations on the local computer.

Vocabulary

- Privilege
  - The right of a user to perform various system-related operations, such as shutting down the system, loading device drivers, or changing the system time. A user's access token contains a list of the privileges held by either the user or the user's groups.

AccessCheck



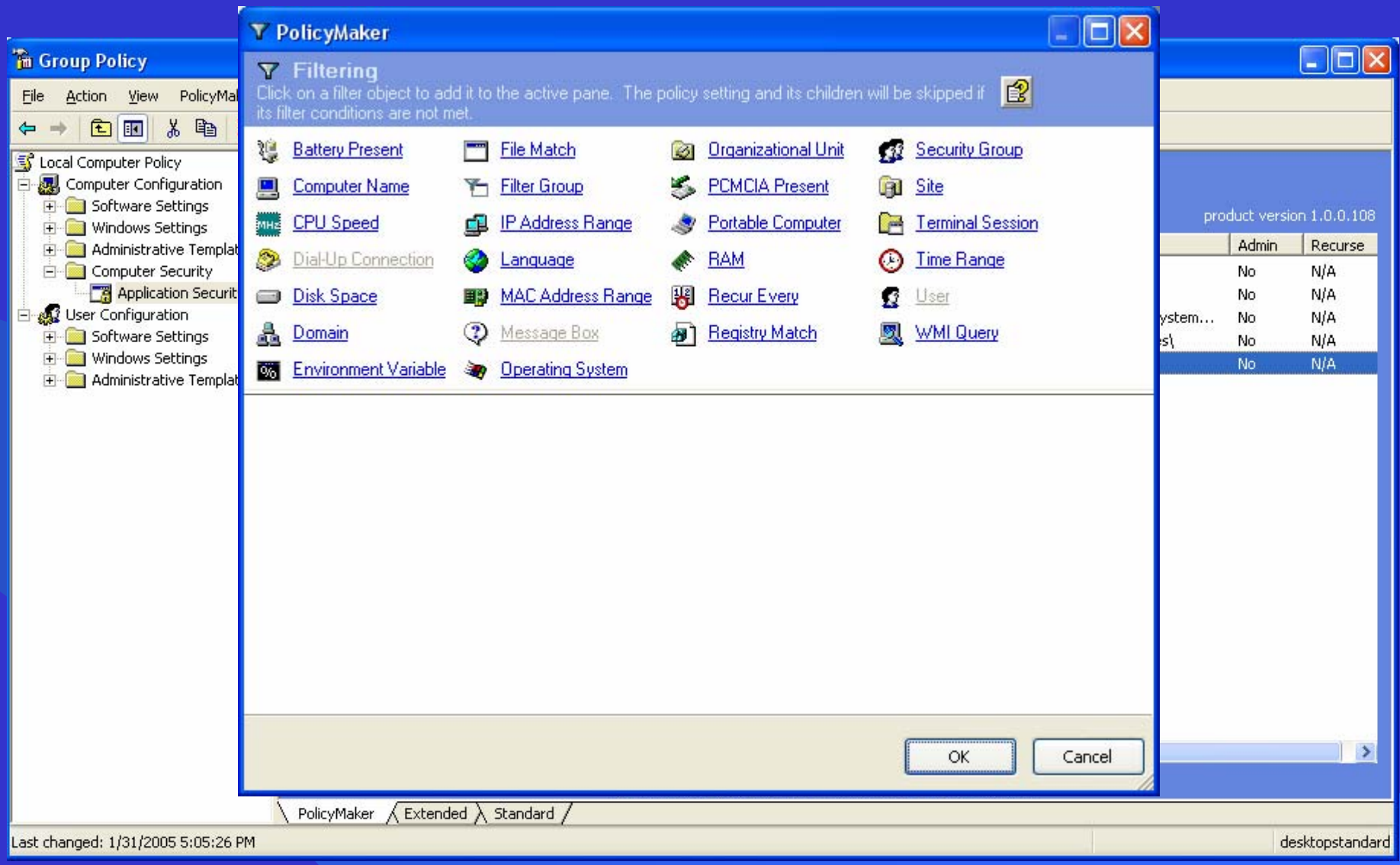
Fonctionnalités (1/2)

- Fonctionnalités principales
  - Gestion des groupes
  - Gestion des privilèges
  - Déploiement automatique des politiques
  - Interface MMC

Fonctionnalités(2/2)

- Meilleur interface (UI)
- Nouveau type de règle (Folder rule)
- Hiérarchie des règles (LSOUD)
- Import/ export des règles en XML
- Filtres très puissants (HW, OS, Langage, etc.)
- Résolution dynamique du Groupe -> SIDs
- Support technique / marketing / vente
- Etc.

PolicyMaker Application Security



Démo

- Exemples
  - Filemon
  - Regmon
  - DebugView
  - DumpTok
  - Explorer