Les systèmes de commande face à la malveillance :

quelles solutions pour quelles menaces?

Yves Deswarte
LAAS-CNRS, Toulouse
deswarte@laas.fr

Nice, 10-11 mai 2006

Les systèmes de contrôle évoluent

- Ils profitent de l'évolution technologique :
  - Intranets d'entreprise
    - ➔ interconnexion avec d'autres systèmes d'information (commerciaux, financiers, management, …)
  - Ouverture directe/indirecte vers l'extérieur
    - ➔ partenaires, fournisseurs, clients, marketing, personnel
  - Web services, SOA, environnements de développement
- …pour réduire les coûts, améliorer la gestion, faciliter l'interopérabilité, l'adaptabilité, …
- …et parce que le contexte évolue
  - ouverture des marchés, dérégulation, concurrence

Vulnérabilités

- Autrefois : systèmes dédiés, fermés
  - Fautes de conception (fournisseurs), fautes d'opérateur (maladresse, malveillance)
- Avec l'évolution actuelle :
  - Plateformes génériques : nombreuses failles
  - Ouverture : interdépendance avec d'autres systèmes (fautes externes)
  - Interopérabilité : dilution de la responsabilité, facilité à modifier

Menaces

- D'internes :
  - Fournisseur, développeur (logique maligne)
  - Opérateur (maladresse, sabotage)
  - Utilisateur de systèmes interconnectés
- ➔ externes
  - Pollution d'Internet : script kiddies, vers, virus
  - Concurrence déloyale
  - Crime organisé, terrorisme, guerre électronique

Parades classiques

- Pare-feux, anti-virus/vers/spyware…, authentification forte, SSL/TLS, SOAP/OASIS, détection d'intrusions…
- Efficaces contre la pollution d'Internet
- Peu efficaces contre les attaques ciblées
  - Internes (abus de pouvoir)
  - Externes par des attaquants puissants

Coopération / concurrence

- Politiques / modèles de sécurité adaptés
  - Moindre privilège, responsabilité, intégrité, disponibilité
- Schémas d'autorisation
  - Multiples niveaux d'intégrité
  - Contrôle de flux entre les niveaux
- Mécanismes de contrôle d'accès
  - Grosse granularité : isolation, pare-feux
  - Fine granularité : labels, protection matérielle

Tolérance aux intrusions

- Diversification :
  différents types de plateformes, d'OS, de logiciels, avec les mêmes données

- Détection - recouvrement :
  - Détection par surveillance mutuelle, comparaison entre exécutions, recoupement, programmation défensive
  - Recouvrement par systèmes de secours, dégradation progressive, masquage
  - Multiples niveaux d'intégrité

Conclusion

- Ne pas se précipiter vers l'ouverture
  (effet de mode)

- Mettre en place des garde-fous
  - Systèmes de secours
  - Autonomie
  - Parades classiques

- Préparer l'avenir :
  - Politiques de sécurité
  - Tolérance aux intrusions
  - Multiples niveaux d'intégrité