Introduction

Sécurité et Administration des Systèmes Informatiques

Fabrice Legond-Aubry
Fabrice.Legond-Aubry@u-paris10.fr

Plan du cours

Plan du cours

Introduction

Concepts de sécurité

Administration machine

Administration réseau

Les services réseaux

Maintenance d'un parc

Conclusion: la sécurité

Introduction

Rôle de l'administrateur système

- Définir l'architecture d'un système
- Organisation des ressources
  - **SERVICES ,** Disque, CPU, capacité réseau, périphérique, mémoire
- Installation et configuration des machines
- Gestion des utilisateurs
  - Création/Suppression/Modification des comptes
  - Gestions des droits d'accès aux ressources
- Gestion des performances (optimisations ie « tuning »)
- Maintenir le bon fonctionnement et faire évoluer le parc
- Conseil les utilisateurs
- Sécuriser le système

Introduction

Différents niveaux d'administration

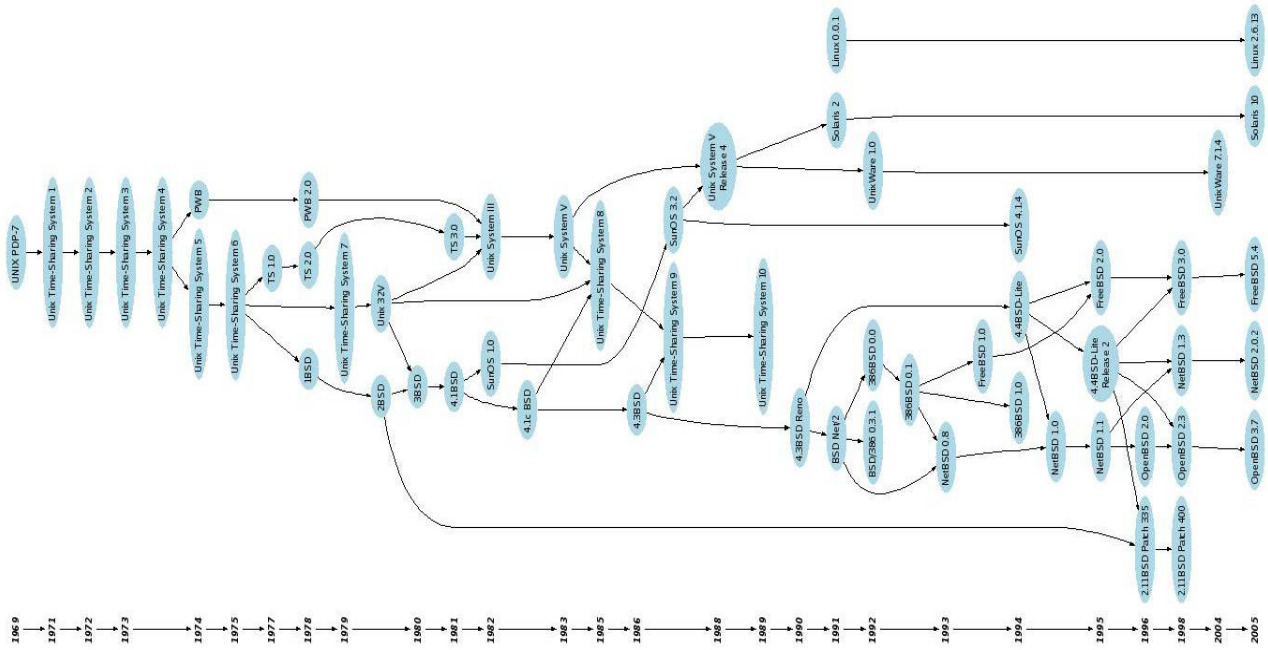
- Machines indépendantes
  - Peuvent être connectées au réseau mais reste indépendantes
  - Tous les services sont locaux à la machine
  - Plus facile à gérer (configuration unique)
  - Dédiée à un propriétaire ou une tâche
- Un parc de machines homogènes (clusters)
  - Distribution et partage de ressources
  - Configuration dupliquée
- Un parc de machines hétérogènes
  - Interopérabilité nécessaire
  - Complexité croissante (nombre de versions et de systèmes)
  - **Terminaux mobiles**
- Un site entier (serveurs + utilisateurs)
  - Recherche d'un équilibre en maintenabilité et utilisabilité
- **Interconnexion réseau**

Introduction

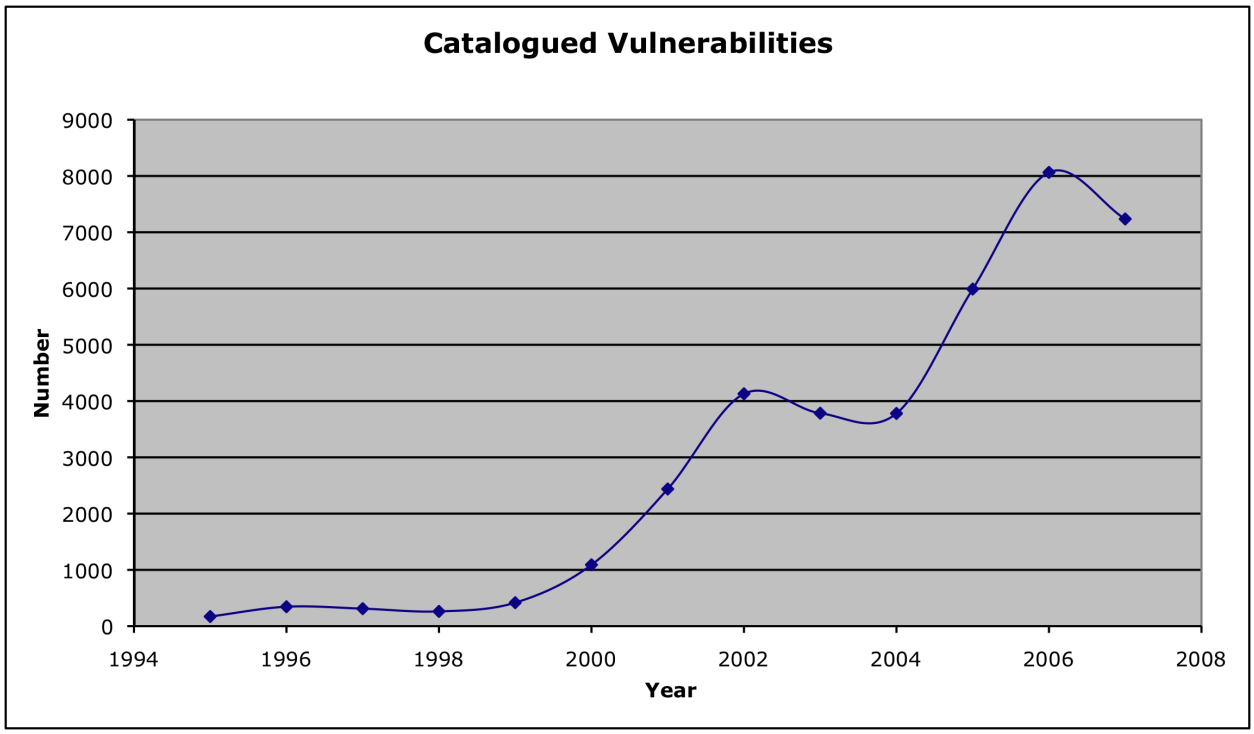
Les connaissances

- Profession généraliste assez peu connue mais recherchée.
- Assez peu de programmation. Essentiellement des scripts.
- Demande un panel important de compétences
- Connaître les OS
  - réseau, système (noyaux, cpu, mémoire), … [cours L et M1]
- Connaître l'environnement
  - Équipements (réseau), besoins utilisateurs, applicatifs, langages
- Outils de base :
  - Shells (bash, zsh, sh, tcsh), Scripts (python, perl)
  - Expressions régulières (regexp)
- Connaissances de sécurités

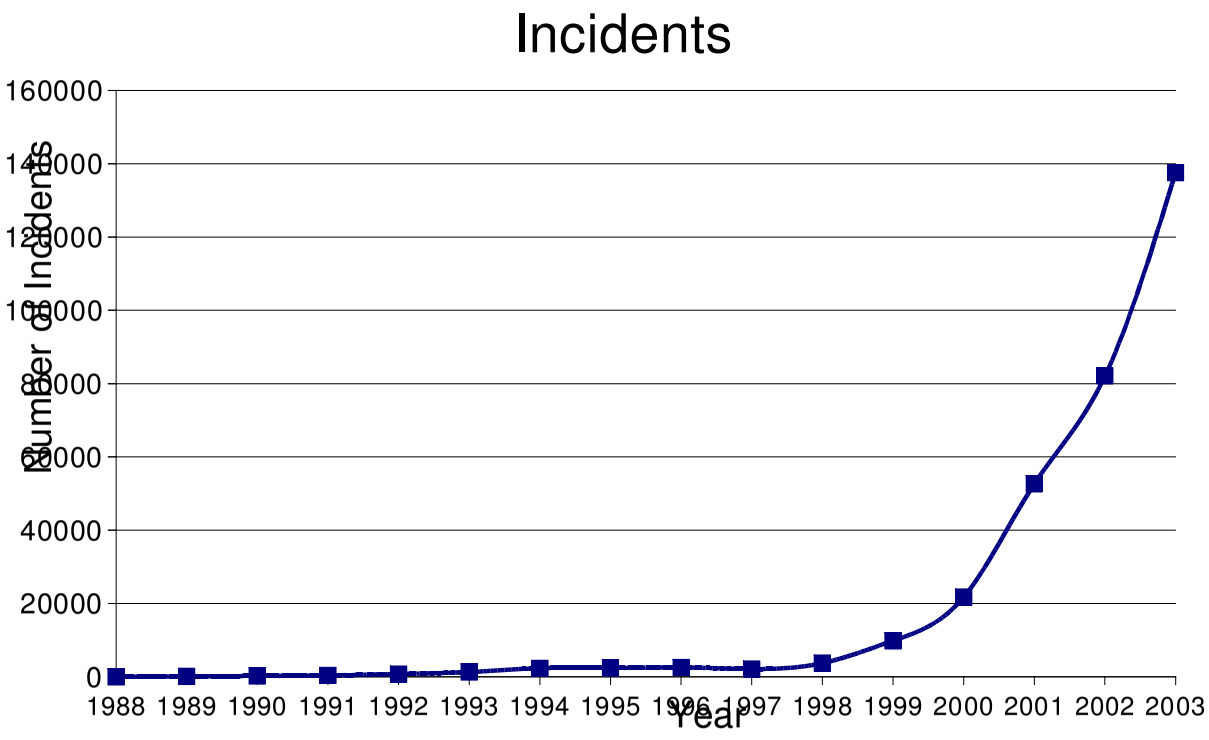
Histoire: les OS de type unix



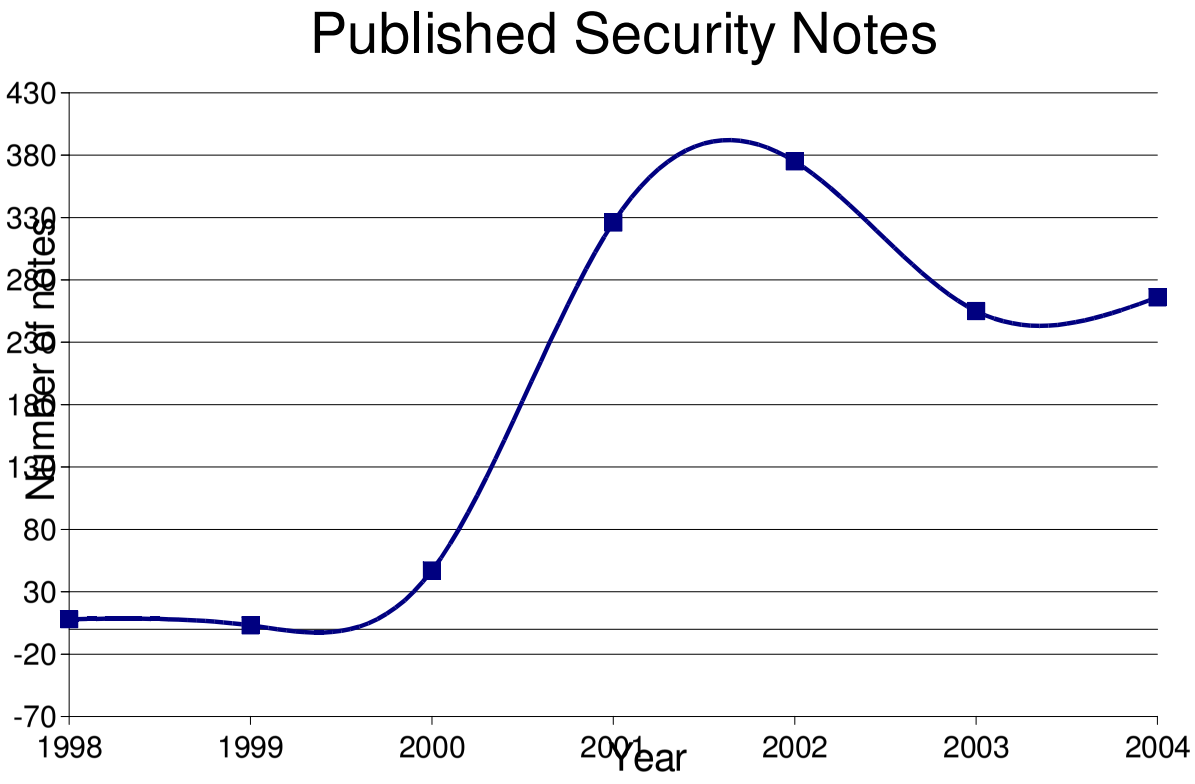
Statistiques



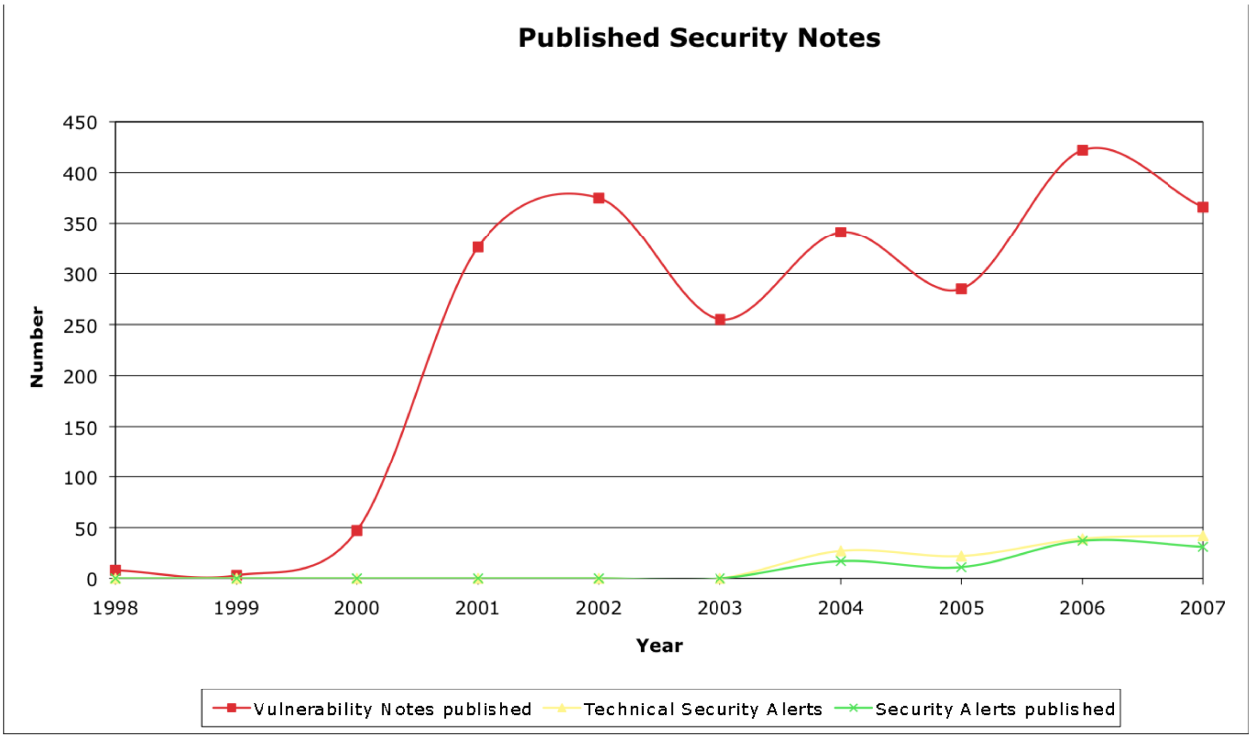
Statistiques



Statistiques



Statistiques



L'homme et l'ordinateur

- Importance croissante du rôle de l'ordinateur
  - Dans la diffusion de l'information
  - via des systèmes techniques de plus en plus complexes
  - dans des domaines de plus en plus variés
  - sur des terminaux de plus en plus variés
- Dans le passé, l'informatique était concentrée sur
  - les effets possibles d'une erreur de programmation
  - la validation de processus critique (transport, énergie…)
- Actuellement, on se concentre sur
  - le détournement possible des nouvelles technologies de l'information
  - la communication par soit des pirates / groupes étatiques / groupes industriels d'informations
- Faut-il craindre avec raison les effets pervers d'une informatisation trop rapide de la société?
  - OUI !!!!

Ce qui peut arriver à votre machine

- Refuser de faire quoi que ce soit (plantage)
- Faire trop tôt ou trop tard ce qu'il devait faire (mauvaise réactivité).
  - Problème sur les systèmes temps réels.
- Accomplir des actions différentes de celles attendues :
  - La destruction de vos données
  - La transformation de votre écran en une œuvre d'art minimaliste
  - L'inondation de la planète de messages pornographiques
  - L'espionnage de votre comportement et la vente de ces informations
  - L'utilisation de votre machine comme relai d'attaque
  - L'implantation d'un module de surveillance étatique

Conséquences

- Dans la majorité des cas, des conséquences assez bénignes:
  - "retaper" deux ou trois fois la même chose, suite à la « perte d'un fichier »
  - Perdre des emails, des photos, des textes
  - Subir de la publicité
  - Réinstallation d'une machine chez le particulier
- Mais pour une entreprise, des conséquences considérables:
  - la paralysie des serveurs Web,
  - le vol de sommes considérables,
- Dans le futur ?
  - l'échec d'un tir de fusée,
  - la création d'embouteillages monstrueux,
  - une panne de courant paralysant une métropole,
  - une panne paralysant les transports ferroviaires d'un grande capitale,
  - Votre jeux en ligne préféré qui ne fonctionne plus

Pourquoi est-ce si important ?

- Dommages potentiels importants
  - Indisponibilités des systèmes
  - Destruction/Manipulations des données/systèmes
- Coûts importants de remise en marche
  - Financiers (remise en marche, ventes manquées)
  - Temporels (remise en marche, configuration)
  - Humains (juristes, informaticiens)
  - Matériels (serveurs de sauvegarde, redondance, sécurité)
- Coûts importants de maintient en état
  - Analyses des données de surveillance
  - Analyses des machines

La sécurité : un problème critique !

- La sécurité des machines et des réseaux
  - Doit être la première préoccupation de toute entité utilisant l'informatique
    - ✔ Entité = gouvernement, entreprise, particulier, associations, …
    - ✔ Laisseriez-vous ouverte votre porte d'appartement ?
  - Si ignoré, des nombreux problèmes financiers
  - Doit dépendre d'ingénieurs spécialistes
- Nécessite une définition
  - Des risques de sécurité
  - D'un plan et d'une politique de sécurisation
    - ✔ architectures, droits, organisations, acteurs
  - D'un plan de réaction aux attaques

Sécurité : centres de préoccupations

- Sécurité locale (sur une machine)
  - Sécurisé l'OS
  - Sécurisé les services
  - Sécurisé l'accès à la machine (boot)
- Sécurisé réseau (services réseaux)
  - Topologie et architectures des serveurs
  - Les protocoles exploités
  - Le contrôle d'accès du réseau et des services
- **Les utilisateurs !!!!**
  - Education comportementale
    - ✔ Peur de l'ordinateur (ligne 14, régulateurs vitesses, …)
    - ✔ La non-compréhension des outils informatiques
  - Identifications des maillons faibles (personnes à risques)
- Le cadre juridique et sociale. Voir politique !

Conclusion

- Besoin en spécialistes en sécurité pour définir :
  - Quels machines et services déployés
  - Comment les interconnecter
  - Quels types d'attaques l'entreprise peut subir (points faibles)
  - Quels moyens de protections sont à mettre en place
  - Quels mesures (contre-mesures) utiliser en cas d'attaque
  - Quels sont les contrôles sont à effectuer et à quelle fréquence
- Il n'y a aucun système sûr à 100%
- Il faut savoir choisir son degré de protection en fonction de ses besoins
  - ADEQUATION DES MOYENS ET DES OBJECTIFS
  - C'EST UNE OBLIGATION JURIDIQUE

Conclusion

Il existe donc une probabilité raisonnable de pouvoir cohabiter et même collaborer avec les ordinateurs.

Il suffit de prendre le temps de savoir ce que nous voulons en faire et comment.

Lorsque le problème est bien posé, les solutions techniques existent déjà souvent et, dans le cas contraire, seront inventées.

Bibliographie

- S. Natkin, « *Protocoles de Sécurité de l'Internet* », Dunod, 2002
- B. Schneier, « *Cryptologie appliquée* », Thomson publishing, 2001
- J. Stern ,*« La science du secret »*, Odile Jacob Ed, 1998
- D. Stinson, « *Cryptologie: théorie et pratique* », Thomson publishing, 2003
- D. B. Chapman & E. D. Zwicky, *« La sécurité sur Internet — Firewalls »*, O'Reilly , 1996
- Microsoft Security Team, « *Sécurité Windows* », Microsoft Press, 2005
- Les livres de poches d'Isaac Asimov (« *les robots* »)
- S. Garfinkel & G. Spafford , *« Practical UNIX & Internet Security »*, seconde Édition, 1996

Bibliographie

- B. Schneier, « *Secrets and Lies, Digital Security in a Networked World* », J. Wiley and sons ed, 2000
- Richard Bejtlich, « The Tao of Network Security Monitoring: Beyond Intrusion Detection »,
- Stuart McClure, Joel Scambray, George Kurtz, « Hacking Exposed: Network Security Secrets and Solutions, Sixth Edition »
- Niels Ferguson, Bruce Schneier, Tadayoshi Kohno, « Cryptography Engineering: Design Principles and Practical Applications »

Sites WEB

- Commentcamarche : introduction
- Le site du cnam (G. Florin, S. Natkin) pour le module sécurité

  (de nombreuses informations sont extraites de ce cours)
- http://www.ssi.gouv.fr/ Serveur thématique sur la sécurité des systèmes d'information du Secrétariat Général de la Défense Nationale
- http://fr.wikipedia.org/ section sécurité
- http://www.cru.fr/ Comité Réseau des Universités
- http://www.urec.fr/ Unité Réseau du CNRS
- https://www.clusif.asso.fr/ Club de la Sécurité des Systèmes d'Information Français
- www.renater.fr, www.cert.org, www.securite.org, www.ouah.org, http://www.phrack.com/issues.html, www.securityfocus.org
- Cours sur le web :
  - Michel Riguidel (http://perso.enst.fr/~riguidel/UESecur)
  - Stephane Naktin au CNAM

Quelques indications sur les couleurs

- ***Pour ce qui est important***
  - ***J'utilise la couleur rouge***
- ***Pour ce qui concerne les noms de fichiers / répertoires***
  - ***J'utilise la couleur verte***
- ***Pour ce qui concerne les commandes***
  - ***J'utilise la couleur bleu***
- ***Pour ce qui concerne les fichiers de configuration ou de données***
  - ***J'utilise la couleur violette***