Sécurité informatique : Introduction

Matthieu Amiguet

2006 – 2007

haute école arc ingénierie
neuchâtel berne jura saint-imier le locle porrentruy

Sécurité 2

- Dans l'expression "Sécurité informatique", le mot *sécurité* recoupe deux notions distinctes
  - La capacité à résister à /récupérer de problèmes accidentels et naturels (en : *safety*)
  - La capacité à résister à/ récupérer d'une attaque humaine malveillante (en : *security*)
- Le premier problème est avant tout un problème d'infrastructure
  - Sauvegardes, ondulateurs, sprinklers, . . .
- Le deuxième problème requiert non seulement ces mesures, mais fait également appel à de nombreux autres points techniques
  - C'est sur cet aspect-là que nous allons nous concentrer.

Sécurité. . . oui mais de quoi ? 3

- En informatique, la sécurité porte principalement sur trois points :
  - Confidentialité
  - Intégrité
  - Disponibilité
- À noter que les deux premiers points peuvent être à double sens, suivant si l'on se place du point de vue
  - de l'utilisateur ou
  - du distributeur (de contenu ou de logiciels).

Vocabulaire et concepts 4

Faille	caractéristique du système pouvant compromettre sa sécurité
Menace	possibilité d'exploitation d'une faille
Risque	probabilité qu'une menace soit réalisée
Gestion des risques	compromis, principalement, entre le coût d'une protection et le risque de ne pas la mettre en place
Exploit	programme ou méthode d'exploitation d'une faille, depuis la machine attaquée (exploit local) ou depuis une autre machine (exploit distant)

Vocabulaire et concepts – suite 5

Preuve de concept (PoC) exploit “gentil” visant essentiellement à mettre en garde contre la faille et à encourager sa correction

0-day exploit publié en même temps que – voire avant – la publication de la faille exploitée

Déni de service (DoS) attaque contre la disponibilité d’un système. L’attaque peut provenir d’une seule machine ou de plusieurs (déni de service distribué, DDoS)

Confiance la notion de sécurité informatique implique toujours une notion de confiance : si on assure la disponibilité/intégrité/confidentialité, on l’assure *pour quelqu’un*. La définition du cercle de confiance est cruciale dans une démarche de sécurité.

Attaquants et motivations 6

Criminels isolés ou organisés (mafia...), visant à obtenir des sous, des renseignements à rançonner, etc.

Espions industriels ou étatiques (voire presse...)

Soldats visant à la prise de contrôle ou à la destruction de l’infrastructure adverse

Terroristes visant à la déstabilisation d’un système (entreprise, gouvernement, ...)

Hackers (amateurs, académiques, ...) visant à une meilleure compréhension des mécanismes, à la publicité ou au *fun*

Responsables informatiques qui testent la résistance de leur réseau (ou de celui de leurs clients)

Irresponsables qui le font parce que que c’est possible et marrant...

...

Qui est concerné ? 7

- Un mythe courant est que seules les grandes entreprises doivent se poser des questions de sécurité informatique...
- ... et dans ces entreprises, seuls les responsables de la sécurité seraient concernés !
- Mais :
  - Il est difficile, voire impossible, d’assurer la sécurité d’un réseau informatique moderne sans la participation de ses utilisateurs
  - Les PME et même les particuliers sont aussi concernés !

Le particulier et la sécurité informatique 8

- “Pour ce que j’ai à cacher, tu vois...”
- Faux, parce que
  - Les ordinateurs personnels contiennent de plus en plus de données sensibles (n° de carte de crédit, ...)
  - Le jour où le disque dur sera effacé/crypté/... par un logiciel malicieux, ça pourrait changer les choses
  - L’ordinateur risque d’être ralenti ou de moins bien fonctionner s’il est trop attaqué
  - Un ordinateur individuel est une cible rêvée pour servir de “relais” à une autre attaque. Non seulement c’est embêtant en soi, mais en plus l’attaque aura l’air de venir de cette machine...
  - ...

La sécurité est un processus

- “The only truly secure system is one that is powered off, cast in a block of concrete and sealed in a lead-lined room with armed guards - and even then I have my doubts.” (Eugene H. Spafford)
- Un système n’est jamais inconditionnellement sûr. Il y a toujours un compromis entre enjeux, moyens à disposition, capacité des éventuels attaquants, . . .
- On observe souvent une “escalade” entre attaques et moyens de défense. La victoire (temporaire) revient au plus rapide. . .
- Une image courante compare la sécurité informatique à une chaîne : la solidité du tout est celle du maillon le plus faible. . .