Les enjeux de la sécurité informatique

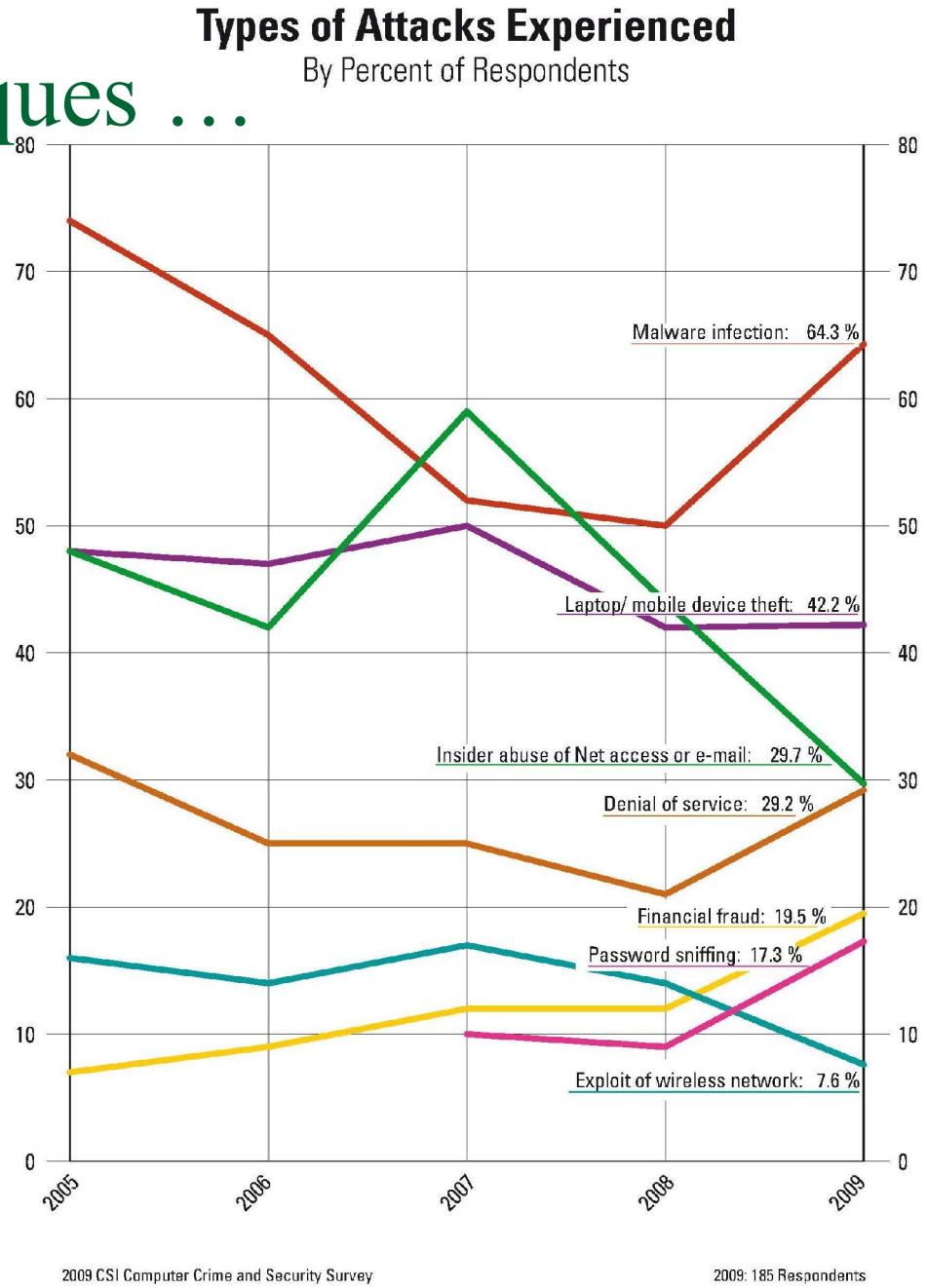
Jean-Marc Robert
Génie logiciel et des TI

Plan de la présentation

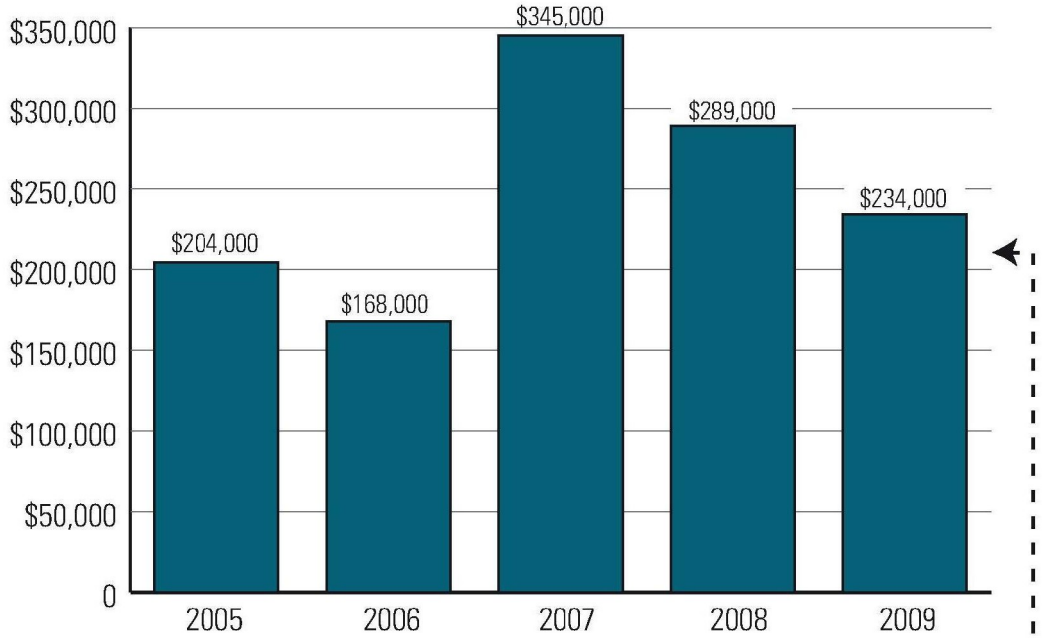
- Le constat est navrant …
- La sécurité informatique, ce n'est pas …
- Principal objectif de la sécurité
- Analyse de risque
- Approches
  - Pragmatique (infrastructure TI)
  - Holistique (logiciel)
- Conclusions

L'Internet un vaste terrain de jeu!

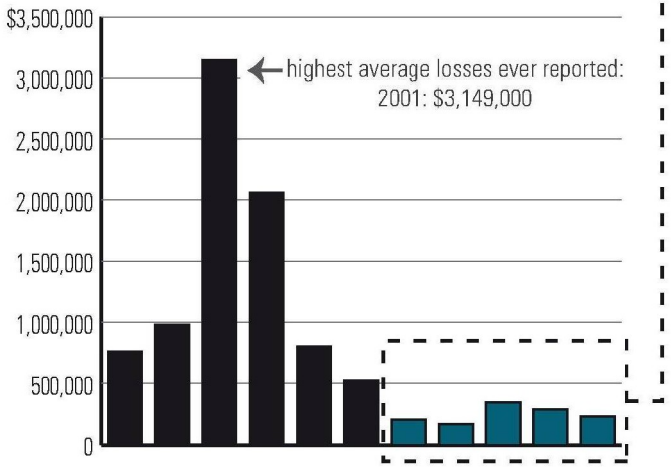
Les attaques …



… et leurs impacts financiers!



In 2005, respondents' reported losses dropped beneath the $500,000 mark. Losses haven't come anywhere near that amount, since then.



2009 CSI Computer Crime and Security Survey

2009: 102 Respondents

Motif des attaques

- Traditionnellement,
  - Prouver ces compétences techniques
  - Représailles envers un ancien employeur
  - …

- Nouveaux motifs
  - $$$$ – Extorsion (déni de service vers un site populaire)
  - $$$$ – Vol (carte de crédit, identité)
  - $$$$ – Vol sur une grande échelle (transactions bancaires)
  - $$$$ – Distribution de la publicité (SPAM)
  - Sécurité nationale

Les vulnérabilités – trop nombreuses!

- NIST – National Vulnerability Database (http://nvd.nist.gov/)
- 47059 CVE Vulnerabilities (19 juillet 2011)

C'est autant de possibilités pour des attaques.

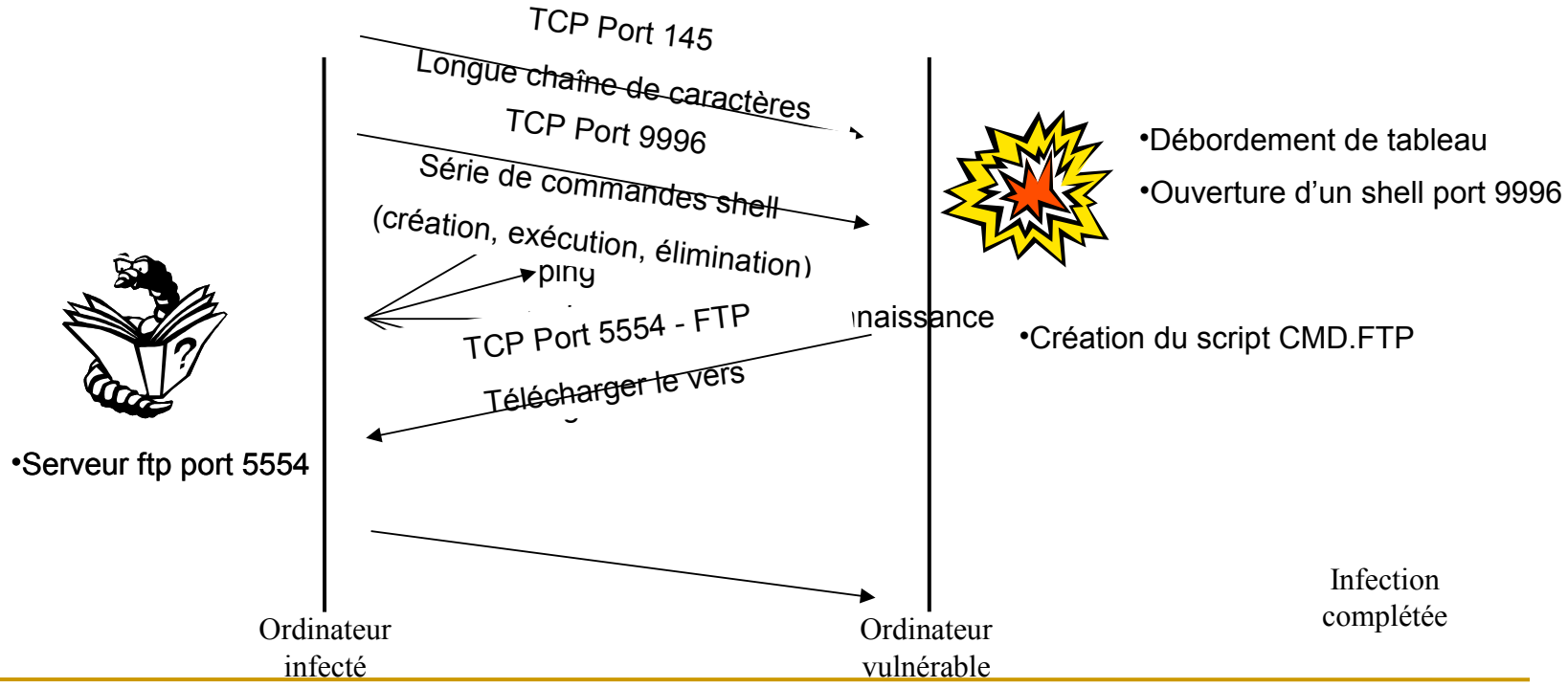
Les vulnérabilités – De l'annonce à l'exploit!

Nom	Annonce	Exploit	Intervalle
SQLsnake	27 novembre 2001	22 mai 2002	176
CodeRed	19 juin 2001	19 juillet 2001	30
Nimda	15 mai 2001	18 septembre 2001	126
Plusieurs vecteurs	6 août 2001		42
	3 avril 2001		168
Slapper	30 juillet 2002	14 septembre 2002	45
Scalper	17 juin 2002	28 juin 2002	11

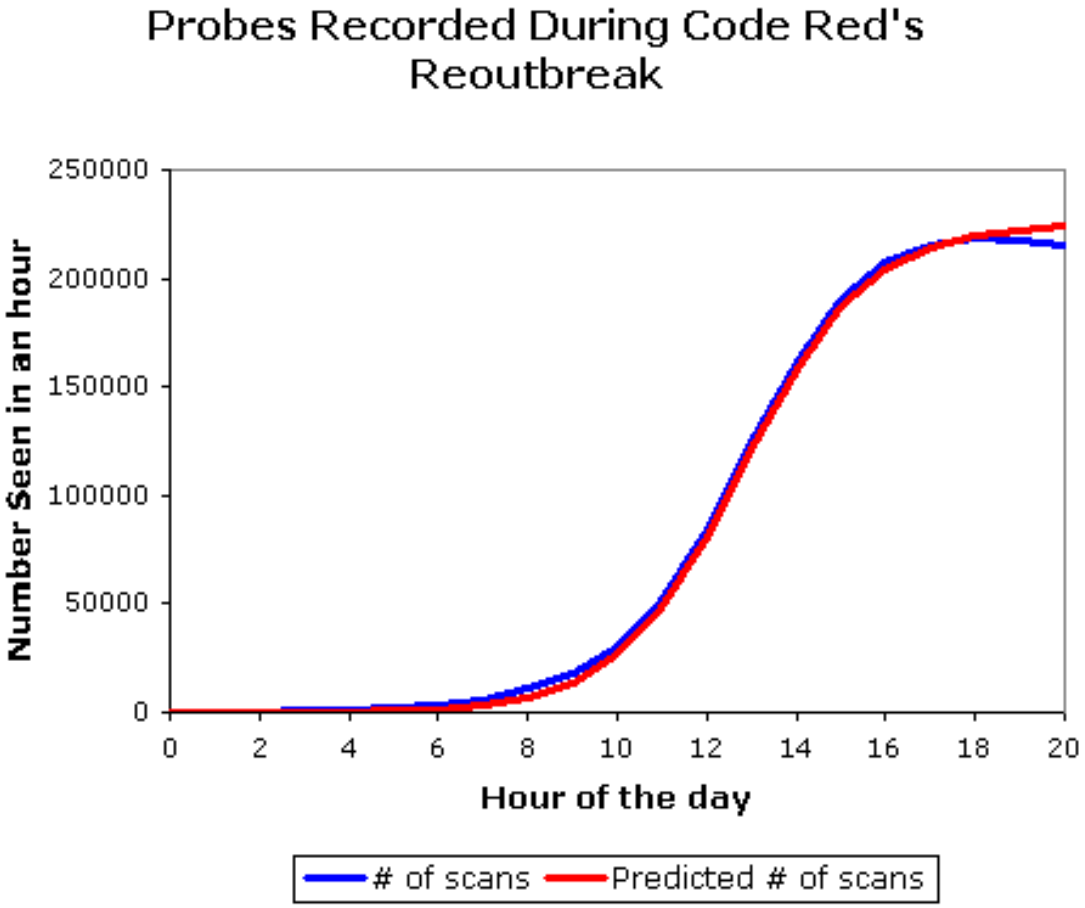
Adapté de J. Nazario, *Defense and Detection Strategies against Internet Worms,* 2004

Les vulnérabilités – la porte d'entrée

- **W32.Sasser.Worm – avril 2004**
  - Critique pour Microsoft Windows XP et Windows 2000.
  - Exploite un débordement de tableau dans l'application LSASS (*Local Security Authority Subsystem Service*).



Lent départ puis l'explosion exponentielle!



Ce comportement est classique et s'applique aussi bien à Sasser.

W32.Sasser.Worm – détection à la source

- Infection – le ver cherche à se reproduire.
  - 225 4.433584 **10.10.10.36** -> 10.10.4.97 ICMP Echo (ping) request
    226 4.435647 **10.10.10.36** -> 173.218.81.160 ICMP Echo (ping) request
    227 4.436819 **10.10.10.36** -> 10.179.239.146 ICMP Echo (ping) request
    228 4.438945 **10.10.10.36** -> 10.10.1.28 ICMP Echo (ping) request
    230 4.442799 **10.10.10.36** -> 103.83.48.240 ICMP Echo (ping) request
    …
- Connexions sur le port TCP 145 puis sur le port 9996.
- Connexion sur le port TCP 145 + signature de la chaîne de caractères utilisée pour le débordement du tableau.

W32.Sasser.Worm – détection à la destination

- Détection d'une attaque
  - Connexion sur le port TCP 145 ou le port 9996 initiée de l'extérieur.
  - Connexion sur le port TCP 145 + signature de la chaîne de caractères utilisée pour le débordement du tableau.
  - Connexion sur le port 5554 initiée de l'intérieur.
- Mauvaise gestion
  - Le pare-feu aurait dû fermer le port 9996.
  - Le pare-feu aurait dû fermer le port 145 ou en réduire l'accès.
- Réaction à l'attaque
  - Mise à niveau du logiciel corrigeant la vulnérabilité.
  - Règles d'accès ajoutées au pare-feu.

W32.Sasser.Worm – Leçons apprises ???

- Piètre qualité du logiciel
  - **Vérifier les bornes des tableaux (spécialement en C et en C++)!**
- Piètre gestion de l'infrastructure
  - **Mettre à jour les logiciels!**
  - **Limiter l'accès au strict minimum!**
  - **Surveiller le trafic entrant et sortant!**

La sécurité informatique, ce n'est pas …

- Pare-feu
  - Systèmes permettant de filtrer les flux de données entre deux domaines.
- Systèmes de détection ou de prévention d'intrusion
  - Systèmes permettant de détecter ou de prévenir les attaques informatiques.
- Logiciels antivirus
  - Systèmes permettant de détecter et d'éliminer les virus informatiques.

Des outils permettant de développer des solutions sécurisées.

La sécurité informatique, ce n'est pas …

- Contrôle d'accès
  - Authentification
    - Permettre d'identifier une entité.
  - Autorisation
    - Vérifier si une entité peut accéder à un service ou à de l'information.
  - Audit
    - Garder des traces de toutes les opérations effectuées.

Un outil permettant de développer des solutions sécurisées.

La sécurité informatique, ce n'est pas …

- Cryptographie
  - Confidentialité
    - Limiter la diffusion des données aux seules entités autorisées.
  - Intégrité
    - Vérifier que les données ne sont pas altérées lors de leur traitement.
  - Non-répudiation
    - S'assurer que les entités engagées dans une communication ne peuvent nier d'y avoir participé.
  - Anonymat et Domaine privé
    - S'assurer que les informations liées à l'identité ne sont pas divulguées.

Un outil permettant de développer des solutions sécurisées.

L'objectif de la sécurité informatique …

Information security is the ***protection*** *of information* [**Assets**] *from a wide range of threats in order* ***to ensure business continuity***, ***minimize business risks*** *and* ***maximize return on investment and business opportunities***.

Adapté de *Norme ISO 17799:2005*.

… si deux opinions valent mieux qu'une!

The purpose of information security governance is to ensure that [enterprises] *are proactively* ***implementing appropriate information security controls*** *to* ***support their mission*** *in a* ***cost-effective manner****, while* ***managing evolving information security risks****.*

As such, information security governance has its own set of requirements, challenges, activities, and types of possible structures. Information security governance also has a defining role in identifying key information security roles and responsibilities, and it influences information security policy development and oversight and ongoing monitoring activities.

Adapté de *NIST Special Publication 800-100 – Information Security Handbook: A Guide for Managers*

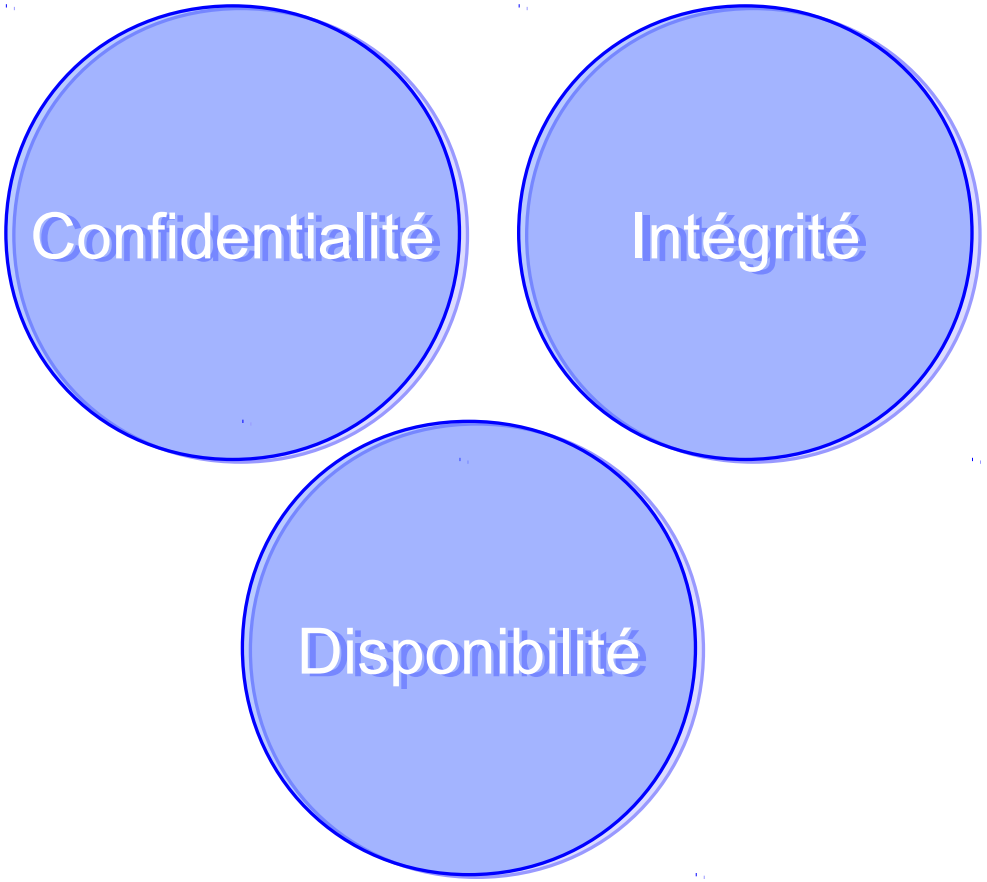
Les actifs …

Les actifs informationnels *représentent l'ensemble des données et des systèmes d'information nécessaires au bon déroulement d'une entreprise.*

- Base de données Clients
  - Vente et Marketing
- Base de données Employés
  - Ressources humaines
- Portail web
  - Vente directe ou indirecte
- Code source d'une application
  - Équipe de développement
- Base de données Usagers
  - Équipe des TI

… et leurs propriétés

Le trio du CID:



en anglais: CIA (Confidentiality, Integrity and Availability)

Confidentialité

Propriété d'une donnée dont la diffusion doit être limitée aux seules personnes ou entités autorisées.

- Menaces
  - Surveillance du réseau
  - Vol de fichiers
    - Fichiers de mots de passe
    - Fichiers de données
  - Espionnage
  - Ingénierie sociale
- Contre-mesures
  - Cryptographie
    - Chiffrement
  - Contrôle d'accès
    - Mot de passe à usage unique
    - Biométrie
  - Classification des actifs
  - Formation du personnel

Intégrité

Propriété d'une donnée dont la valeur est conforme à celle définie par son propriétaire.

- Menaces
  - Attaques malicieuses
    - Virus
    - Bombes logiques
    - Portes dérobées
  - Erreurs humaines
- Contre-mesures
  - Cryptographie
    - Authentification, signature
  - Contrôle d'accès
    - Mot de passe à usage unique
    - Biométrie
  - Système de détection d'intrusion
  - Formation du personnel

Si cette propriété n'est pas respectée pour certains actifs, cela peut avoir des impacts sur la confidentialité de d'autres actifs.

Disponibilité

Propriété d'un système informatique capable d'assurer ses fonctions sans interruption, délai ou dégradation, au moment même où la sollicitation en est faite.

- Menaces
  - Attaques malicieuses
    - Dénis-de-service
      - Inondation
      - Vulnérabilités logicielles
  - Attaques accidentelles
    - *Flashcrowd – Slashdot effect*
  - Pannes
    - Environnemental, logiciel, matériel
- Contre-mesures
  - Pare-feu
  - Système de détection d'intrusion
  - Formation du personnel

L'objectif de la sécurité informatique (reformulé)

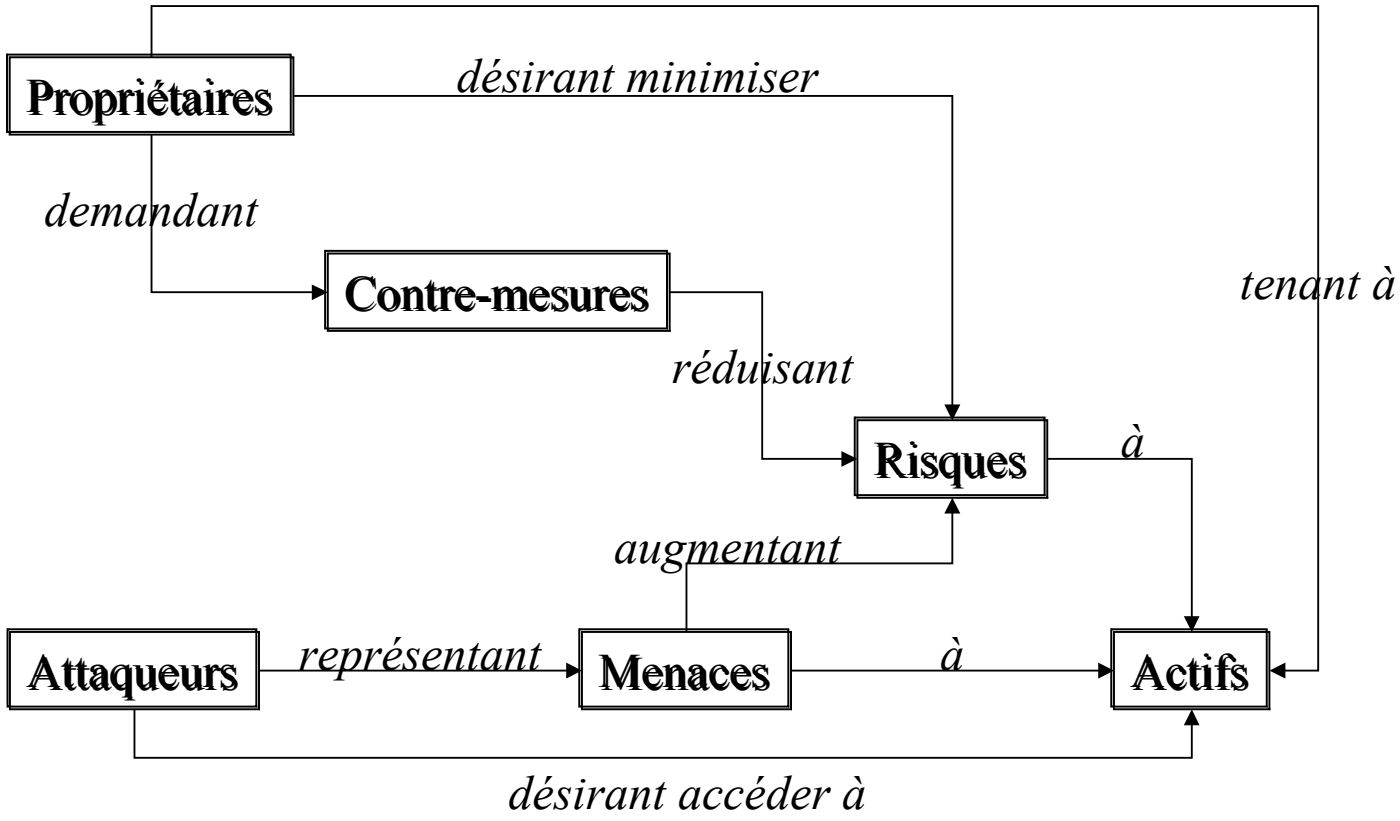
- La sécurité de l'information consiste à protéger les *actifs* informationnels afin d'assurer l'intégralité de leurs *propriétés*.

- Les actifs et leurs propriétés sont définis par les *objectifs d'affaire*.

L'analyse de risque – le premier pas

- Définir les besoins.
  - Déterminer les *actifs* à protéger et leurs *propriétaires*.
    - Quelles sont leurs valeurs? Quelles sont leurs criticités? Quelles sont leurs propriétés?
  - Déterminer les *menaces* représentant des *risques*.
    - Quels sont les *attaqueurs*? Quels sont leurs moyens? Quelles sont leurs motivations?
  - Déterminer les *objectifs* à atteindre.
    - Quelles sont les propriétés des actifs à protéger?
- Proposer un solution.
  - Déterminer les *contre-mesures* à mettre en place.
- Évaluer les risques résiduels.
  - Déterminer quelles sont les *vulnérabilités* toujours présentes.
  - Déterminer leurs *impacts* sur les objectifs initiaux.

L'analyse de risque – schématiquement



Adapté de *ISO/IEC 15408 – Common Criteria.*

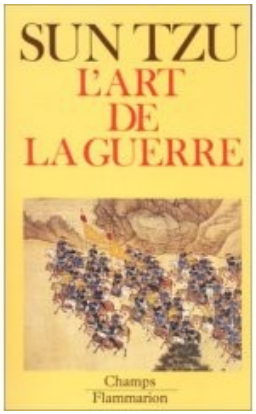
L'analyse de risque – une vieille histoire

Connais ton ennemi et connais-toi toi-même; eussiez-vous cent guerres à soutenir, cent fois vous serez victorieux.

Si tu ignores ton ennemi et que tu te connais toi-même, tes chances de perdre et de gagner seront égales.

Si tu ignores à la fois ton ennemi et toi-même, tu ne compteras tes combats que par tes défaites.

Sun Tzu, approx. 4ième siècle av.



Sécurité – approche traditionnelle

- Le rôle des responsables des TI
  - Se basant sur le fait que les systèmes informatiques sont intrinsèquement vulnérables (bogues de logiciel, mauvais design, …), les responsables des TI doivent mettre en place les moyens de résister aux diverses menaces afin de protéger les actifs de leurs entreprises.

Les objectifs techniques de la sécurité …

- Déployer une infrastructure adéquate résistant aux attaques et assurant l'intégralité des actifs (et leurs propriétés).
  - Prévention
    - Contrôle d'accès
    - Mise à jour des logiciels
    - Pare-feu, Systèmes de prévention d'intrusion (SPI)
  - Détection
    - Antivirus
    - Systèmes de détection d'intrusion (SDI)
    - Audit
  - Réaction
    - Pare-feu

Veille technologique à la recherche des vulnérabilités.
CERT , NIST, Virus Bulletin, Microsoft, Bugtraq…

… et les façons de les atteindre!

- Protéger le périmètre du réseau.
  - Pare-feu, SDI, SPI
- Protéger les serveurs publics.
  - Logiciels mis à jour régulièrement
  - Zones démilitarisées
- Partitionner le réseau interne.
  - Contrôle d'accès, pare-feu, SDI, SPI
- Protéger les serveurs internes et les usagers.
  - Logiciels mis à jour régulièrement
  - Antivirus

Mais l'enjeu est plus général!

- Il ne faut pas mélanger les besoins et les moyens utilisés pour répondre à ces besoins.
  - Quels sont les acteurs?
  - Quels sont les actifs?
  - Quels sont les objectifs?
  - Quelles sont les règles de gestion à mettre en place?
  - Quels sont les moyens opérationnels à mettre en place?
  - …

Politiques de sécurité

- Les *politiques de sécurité* sont des énoncés généraux dictées par les cadres supérieurs décrivant le rôle de la sécurité au sein de l'entreprise afin d'assurer les objectifs d'affaire.

- Pour mettre en œuvre ces politiques, une organisation doit être mise en place.
  - Définition des *rôles*, des *responsabilités* et des *imputabilités*

L'analyse de risque est à la base de cette activité

L'information est disponible – même trop !

- NIST –Département du commerce, É.-U.
  - SP 800-100 Information Security Handbook: A Guide for Managers
  - SP 800-97 Draft, Guide to IEEE 802.11i: Robust Security Networks
  - SP 800-94 Draft, Guide to Intrusion Detection and Prevention (IDP) Systems
  - SP 800-68 Guidance for Securing Microsoft Windows XP Systems for IT Professionals
  - SP 800-41 Guidelines on Firewalls and Firewall Policy
- ISO
  - ISO/IEC 17799:2005(E) – Code of Practice for Information Security Management.
  - ISO/IEC 21287:2002 – System Security Engineering – Capability Maturity Model.
- US-CERT – Software Engineering Institute de CMU
  - Defense in Depth: Foundations for Secure and Resilient IT Enterprises
  - Advanced Information Assurance Handbook
- Amazon.ca
  - 1229 livres sont proposés en utilisant les mots clé: *Information Security*.
- Google.ca
  - Ce que vous cherchez s'y trouve. Bonne chance!

Mais le problème demeure …

- L'industrie de la sécurité
  - En 2003, le marché de la sécurité réseau était évalué à 45 milliards USD.

Firme d'analystes IDC

- Constat
  - L'approche traditionnelle sécurisant le périmètre du réseau ne semble pas adéquate puisque nous avons toujours les mêmes problèmes.

- Raison
  - La qualité des logiciels.

Le produit intérieur brut du Québec était de 225 milliards CAD en 2006.

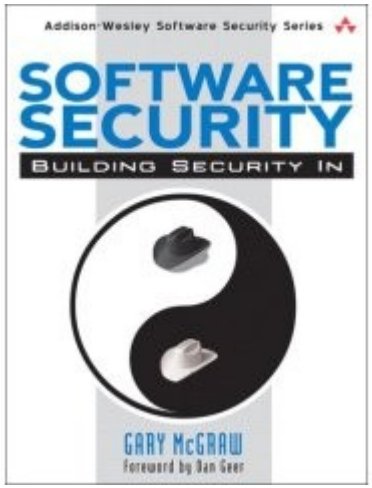
Une nouvelle approche holistique nécessaire

- La sécurité des logiciels est donc critique!
  - 50 % des vulnérabilités proviennent des erreurs de conception.
  - 50 % des vulnérabilités proviennent des erreurs d'implémentation.
    - Dépassement de mémoire et d'entier
    - Concurrence critique

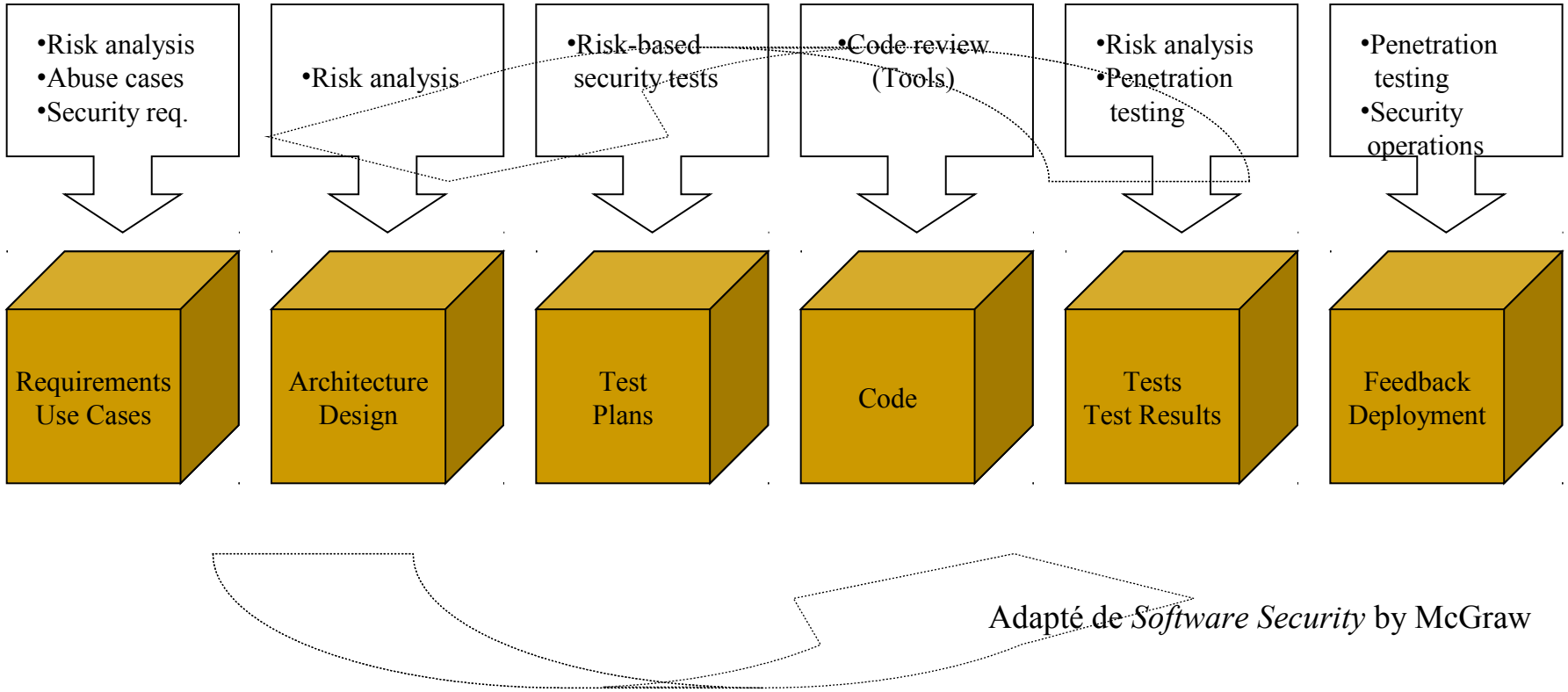
- *Microsoft's Trustworthy Computing Initiative*
  - Mémo de Bill Gates en janvier 2002 présente la nouvelle approche de Microsoft de développer des logiciels sécurisés.
  - Microsoft aurait dépensé plus de 300 millions USD.
  - *The Trusthworhty Computing Security Development Lifecycle.*

Sécurité ↔ Robustesse!

- Sécurité du logiciel – Robustesse
  - Gestion du risque
    - Actifs, menaces, objectifs, …
  - Cycle de développement du logiciel
  - Bases de connaissance



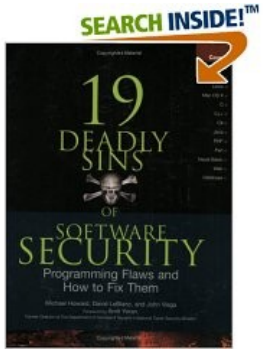
Cycle de développement du logiciel

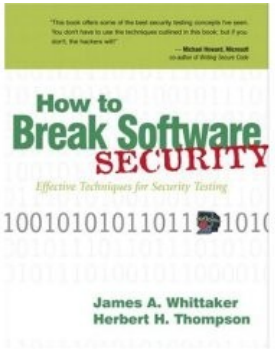


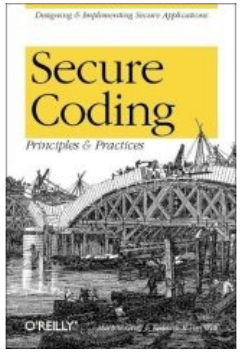
- Intégration d'activités propres à la sécurité du logiciel dans le cycle du développement (en ordre d'efficacité – subjectif)
  - *Code review, Risk analysis, Penetration testing, Security tests, Abuse cases, Security requirements, Security operations*

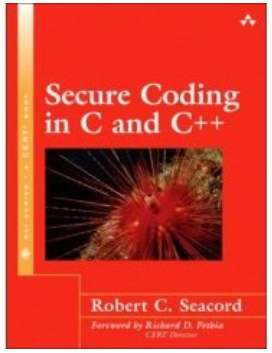
L'information est disponible

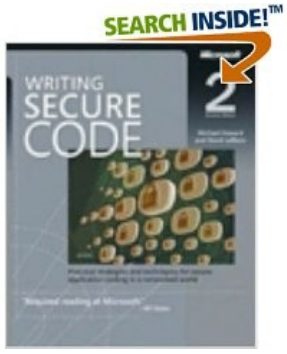
- Le domaine de la sécurité du logiciel est naissant et vaste. Il peut être difficile de s'y retrouver...

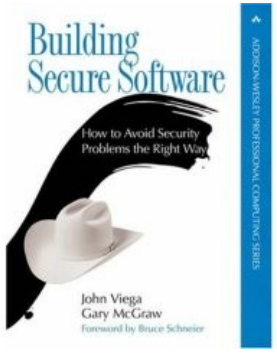


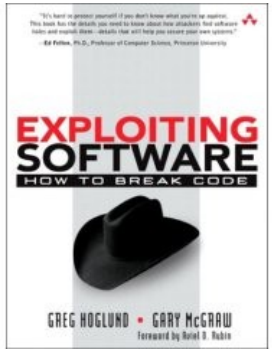












+ le site web

https://buildsecurityin.us-cert.gov/

Conclusions

- Connaissez-vous vous-même.
  - Déterminer les *actifs* qui doivent être protégés et leurs propriétés.
  - Déterminer les *objectifs* à atteindre.
- Connaissez vos ennemis.
  - Déterminer les *menaces* contre lesquelles ils doivent être protégés.
- Reposez-vous sur les épaules de géants.
  - Veille technologique, base de connaissances.
  - Principes, guides et règles connues.

Ne jamais dire: ceci est impossible, ils ne peuvent faire cela.