La sécurité des S.I.

Alexis BONNECAZE
Polytech Marseille
alexis.bonnecaze@univ-amu.fr

Objectif et déroulement

Avoir conscience de l'importance de la sécurité et connaître le vocabulaire.
Il s'agit d'une vue d'ensemble plutôt orientée crypto.

5 cours et 5 TD, 5 TP
Tous les rapports de TP à rendre.
La note de TP comprend la participation,
la qualité des rapports rendus.
Les notes de TP représentent 20% de la note finale
L'évaluation écrite représente 80% de la note.
L'évaluation écrite comprend l'examen final et éventuellement
un (des) contrôle(s) court(s) en début de cours.
Des points bonus peuvent être donnés durant l'enseignement.

Quelques livres intéressants

COMPUTER SECURITY, A Hands-on Approach,
Wenliang Du, https://www.handsonsecurity.net

Computer and Information Security, handbook,
John Vacca, Morgan Kaufmann publishers, Elsevier

Computer Security, Principles and Practice,
Williams Stallings, Lawrie Brown

Encyclopedia of Cryptography and Security, Springer

Network security, know it all,
Morgan Kaufmann publishers, Elsevier

L'ère numérique

- L'information numérique
  - Peut être détruite, amputée, falsifiée, et modifiée de multiples manières
  - Pas d'original, ni des copies mais des clones où la reproduction est à l'identique
  - Prend peu de place
  - Se transporte facilement
- Comment signer, authentifier, dater, transmettre des données ?

Les enjeux de la sécurité

- Maîtriser le transport, le traitement et le stockage des informations
- Valoriser les contenus
  - Multimédia, logiciel, propriétés intellectuelles, …
  - Libre circulation des contenus
  - Disséminer les œuvres, rétribuer les auteurs
- Asseoir la confiance dans l'univers numérique
  - E-commerce, e-business, e-governement…
- Sécuriser les infosphères
  - L'individu : liberté, protection de l'intimité
  - L'entreprise : prévention des risques

Exemples

Connexion au site de ma banque

- S'agit-il bien de ma banque ?
- Un tiers peut-il lire les informations ?
- Un tiers peut-il modifier les informations ?

Vote électronique

- Le résultat reflète-t-il les votes ?
- Confidentialité, résultats partiels ?
- Les votants sont-ils des électeurs ?
- Ont-ils voté une seule fois ?
- Ont-ils voté dans la bonne plage horaire ?

Paiement par carte bleue

- S'agit-il d'une vraie carte ?
- Le montant débité sera-t-il égal au montant crédité ?
- Le code est-il bien protégé ?

Monnaie électronique

- Peut-on créer de la fausse monnaie ?
- Comment interdire de dépenser le même argent plusieurs fois ?
- Que faire si on a perdu sa clé privée ?
- Permet-elle d’acheter ou vendre anonymement ?

Bases de données sécurisées

- Qui est habilité à accéder à une vue partielle ?
- Comment vérifier qu'une personne est habilité ?
- Comment permettre l'accès à une vue ?
- Comment faire une mise à jour ?
- Comment marier sécurité et efficacité ?
- Comment préserver l'anonymat dans une BD statistique ?
- Peut-on être accusé à tort d'avoir modifié une donnée ?

Prise de contrôle à distance

- D'un ordinateur, smartphone
- D'une voiture
- D'un avion
- D'un dispositif médical (pacemaker,...)

Surf sur Internet

- Comment éviter la pub
- Traçage, anonymat

La criminalité informatique

- La criminalité informatique affecte
  - les individus,
  - la gestion et la vie des entreprises,
  - le fonctionnement des états

- Principales attaques
  - Virus, accès non autorisé, dénis de service, pénétration du système, vols d'informations, sabotage, fraudes financières…

Pluridisciplinarité de la sécurité

La sécurité couvre des aspects issus de plusieurs domaines

- Ethique
  - Vie privée, liberté de l'individu
  - Politique d'échange et de commerce
  - démocratie
- Législation
  - Lois sur la cryptographie, droits des sujets, autorisations, droit d'utiliser un service ou une application
  - Propriété intellectuelle, gestion des droits de distribution des œuvres, RGPD
- Réglementation
  - Contrôle et filtrage de contenus (contenus illicites)
- Technique
  - Mathématiques, traitement du signal, informatique, électronique
  - Ingénierie (des réseaux, architecture des systèmes…)
- Méthodologique
  - ITSec, critères communs
- Normes
  - Standards crypto (AES, DSA…), protocoles (IPSec,…)

Nouveaux systèmes numériques

- Il n'existe plus de systèmes isolés, fixes

Développement de l'informatique diffuse/ubiquitaire (pervasive computing)

  - L'informatique est omniprésente
  - Implique hétérogénéité
  - Mobilité (Manet, spontané, ...)
  - Systèmes distribués, tolérance pannes

- L'interconnexion rend chaque entité importante
  - Attaque à partir d'un portable, d'une tablette,...

Sécurité en général

Sécurité = protection des biens et des personnes

La sécurité dépend de la valeur des biens à protéger (coût d'une attaque réussie)

Difficulté de la sécurité : elle doit gérer en même temps

- de la technologie
- le facteur humain

Une définition de la sécurité informatique

Gollman : « La sécurité informatique s'occupe de la prévention et de la détection d'actions non autorisées, par les utilisateurs d'un système informatique. »

En fait, il existe 3 niveaux de protection

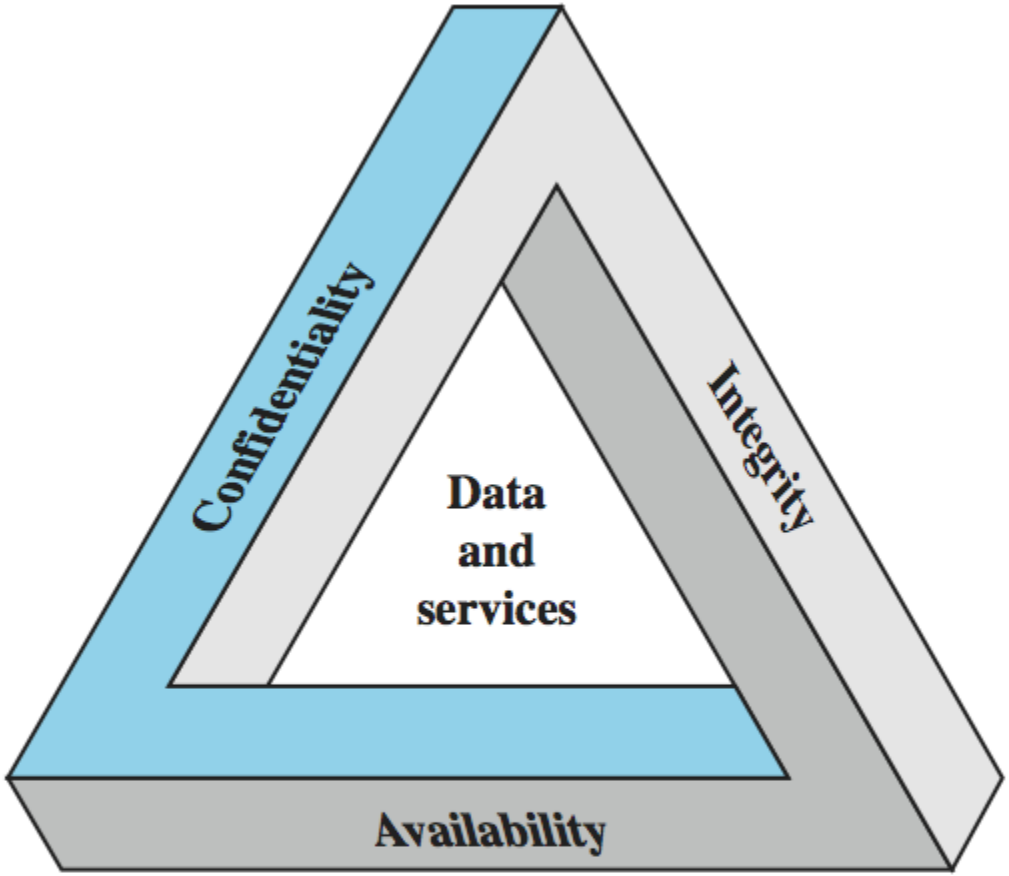
La prévention, la détection et la réaction

Sécurité informatique
Fips Pub 199

Protection apportée à un système d'information automatisé dans le but de lui assurer de préserver

1. Confidentialité
2. Intégrité
3. Disponibilité

Les concepts clé de sécurité



Sécurité informatique

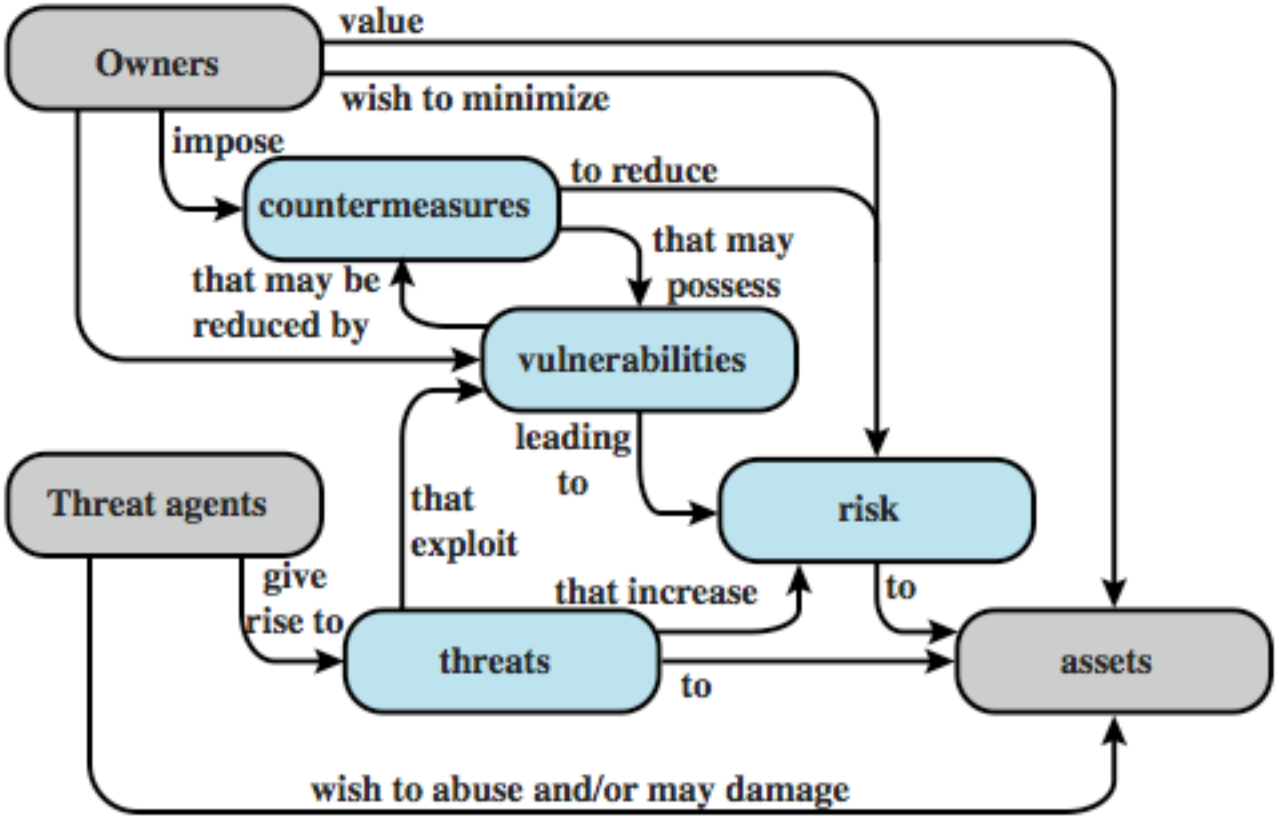
- Confidentialité : empêcher la révélation non autorisée d'information
- Intégrité : empêcher la modification non autorisée d'information
- Disponibilité : empêcher le blocage non autorisé à l'information ou à des ressources

Sécurité informatique

Cette liste doit être complétée :

– Authenticité : s'assurer de l'identité d'un utilisateur
– Responsabilité : attacher une identité à une opération
– Fiabilité : s'assurer du fonctionnement d'un système

Terminologie de la sécurité



Vulnérabilités et attaques

- Les ressources du système peuvent être
  - Corrompues (perte d'intégrité)
  - Espionnées (perte de confidentialité)
  - Indisponibles (perte de disponibilité)
- Les attaques peuvent être
  - Passives/Actives
  - Externes/Internes

Contre-mesures

- Moyens permettant de
  - Prévenir
  - Détecter
  - Récupérer
- Peut engendrer de nouvelles vulnérabilités
- Exemples : firewall, alarme, authentification biométrique, restriction physique d'accès,…

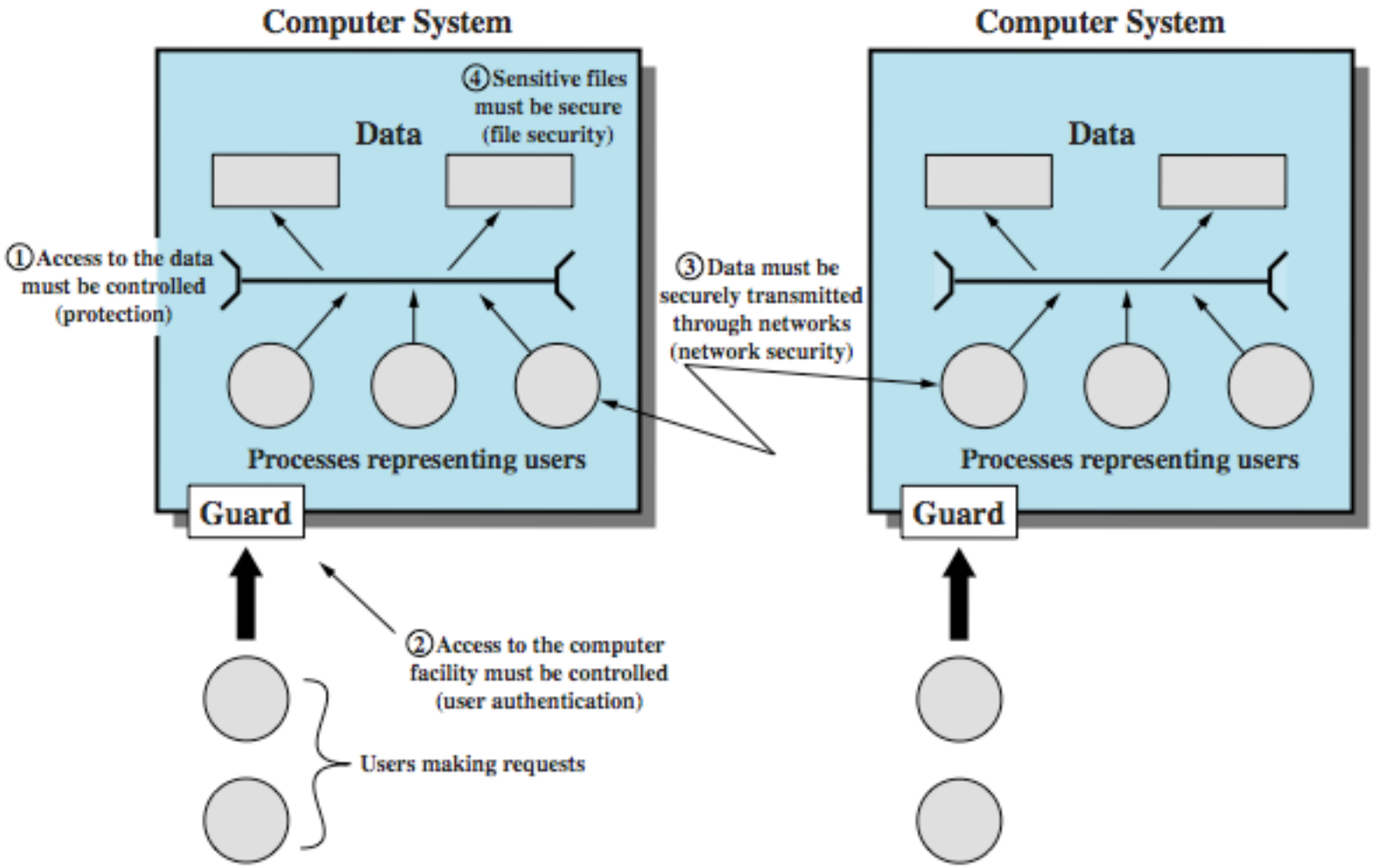
Conséquences des menaces

- Divulgation non autorisée
- Leurres
  - Masquerade, falsification, répudiation
- Désorganisation
  - Interruption du système, corruption, obstruction
- Usurpation
  - Prise de ctrle non autorisée d'une ressource
  - Amène le système à opérer une fct non sûre

Exemples de menaces

	Disponibilité	confidentialité	intégrité
hardware	Equipement volé, rendu inutilisable		
software	Prgm deleted, accès refusé à l'utilisateur	Copie non autorisée	Prgm modifié
données	Fichiers supprimés, accès refusé	Lecture non autorisée; une analyse révèle des données	Fichiers modifiés, fichiers créés
communication	Messages détruits communication non disponible	Messages lus Analyse du trafic	Messages modifiés, fabriqués

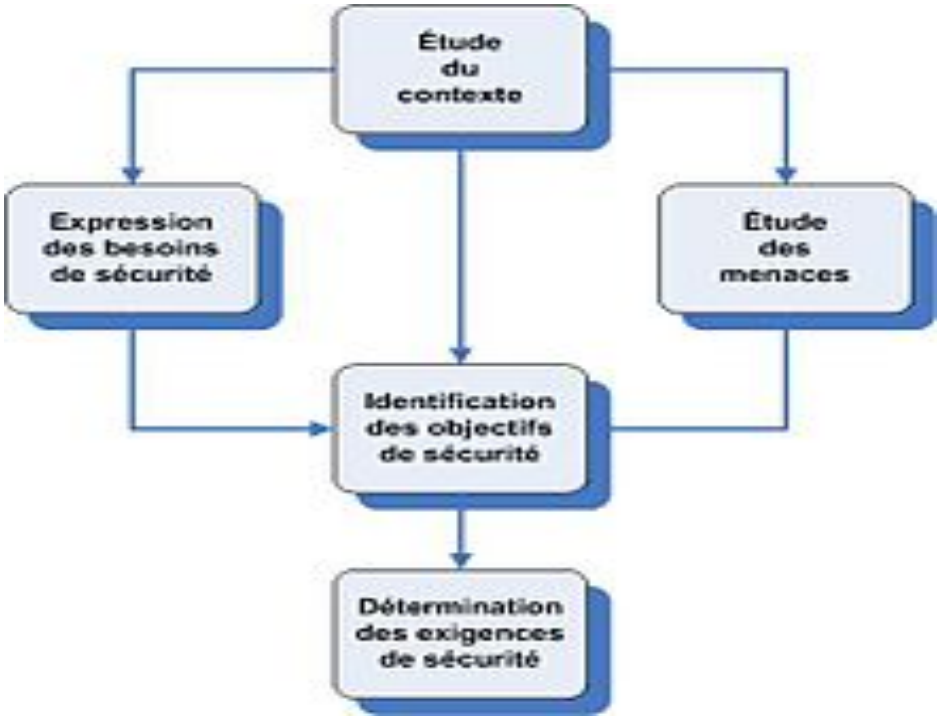
Cadre de la sécurité informatique



Evaluation des risques

Plusieurs méthodes pour évaluer les risques

Ex : EBIOS

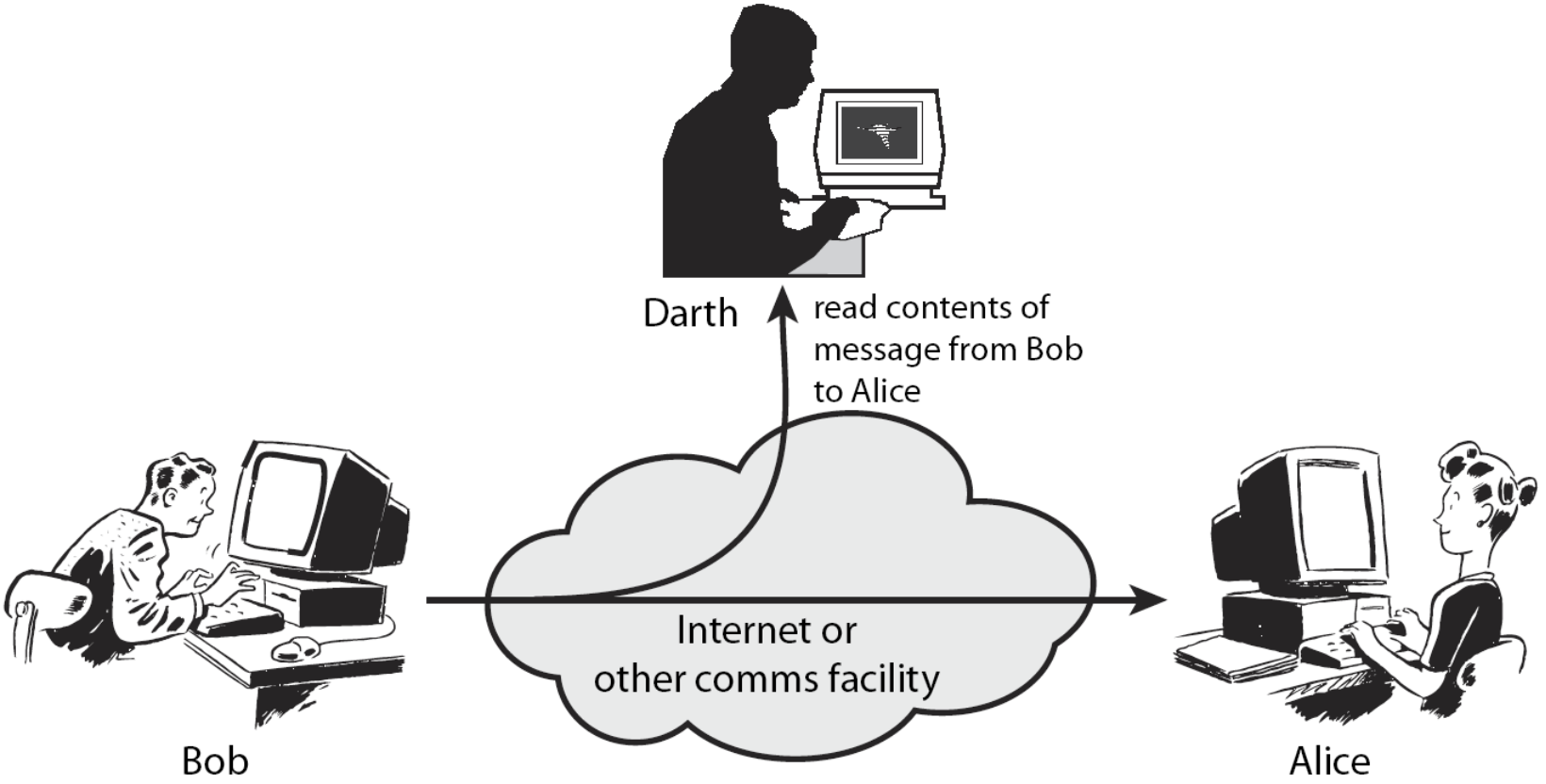


Le degré de protection d'un bien dépend de la valeur du bien

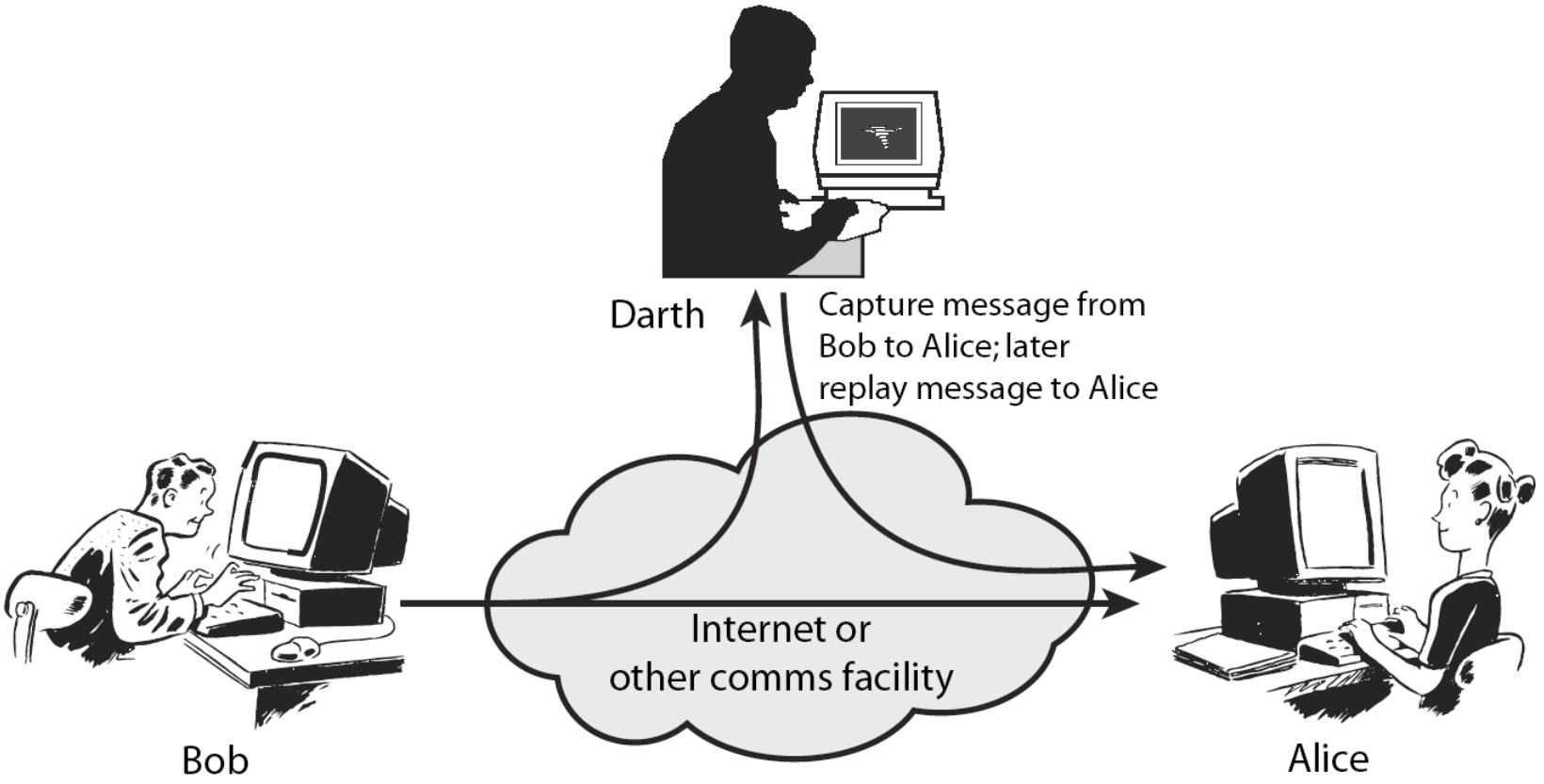
Les attaques en sécurité réseau

- Classifiées passives/actives
- Attaques passives : espionnage
  - Analyse de trafic
  - Vol de contenu
  - Difficile à détecter mais doit être anticipé
  - N'affecte pas les ressources du système
- Attaques actives
  - Masquerade, replay, modification, denial of service
  - Peut être détecté et (difficilement) anticipé

Passive Attacks



Active Attacks



X.800 Security Architecture

- X.800, *Security Architecture pour OSI*
- Recommandations définissant les exigences en matière de sécurité et caractérisant les approches pour les satisfaire
- Elles comprennent
  - Mécanismes de sécurité
    - Mécanisme permettant de détecter, prévenir ou réagir face à une attaque
  - Services de sécurité
    - Services permettant de contrer une attaque. Ils utilisent des mécanismes

Service de Sécurité

- Accroit la sécurité des SI et des transferts d'informations
- Permet de contrer les attaques
- Utilise un ou plusieurs mécanismes
- Imite souvent les opérations associées à des documents physiques
  - Signatures, dates, besoin de protection contre toute divulgation non autorisée, destruction ou modification;
  - Notarisation, licence,...

Services de Sécurité

- X.800:

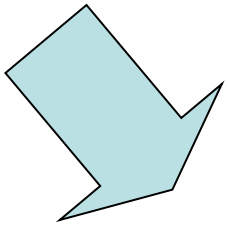
“a service provided by a protocol layer of communicating open systems, which ensures adequate security of the systems or of data transfers”

- RFC 2828:

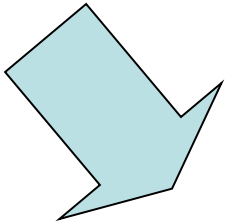
“a processing or communication service provided by a system to give a specific kind of protection to system resources”

Services de sécurité

Politique de sécurité



Service de sécurité



Mécanismes de sécurité

Security Services (X.800)

- **Authentication** - assurance that the communicating entity is the one claimed
- **Access Control** - prevention of the unauthorized use of a resource
- **Data Confidentiality** –protection of data from unauthorized disclosure
- **Data Integrity** - assurance that data received is as sent by an authorized entity
- **Non-Repudiation** - protection against denial by one of the parties in a communication

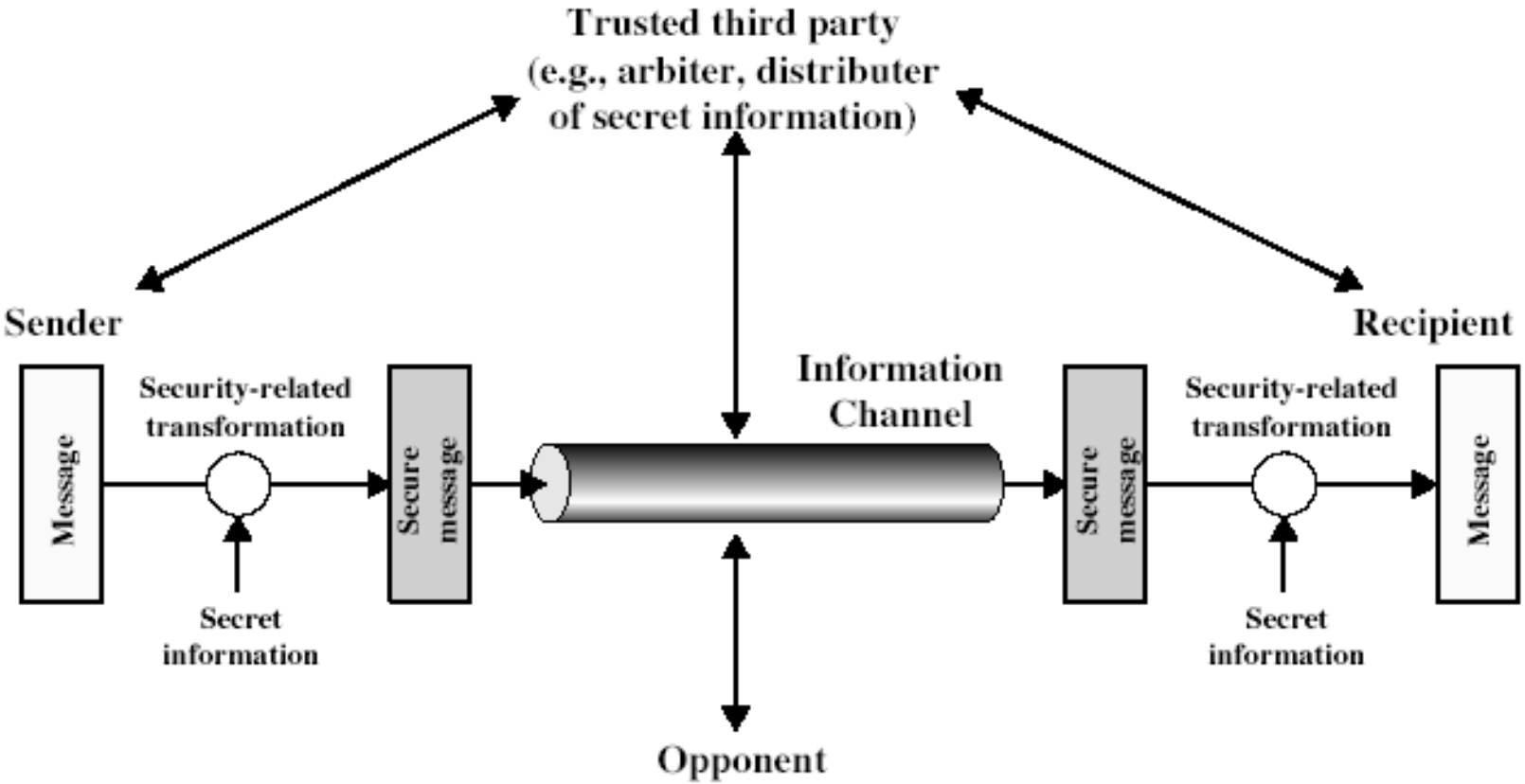
Mécanisme de Securité

- Permet de détecter ou prévenir une attaque ou réparer après une attaque
- Les services requierent plusieurs mécanismes différents
- Cependant, les **techniques cryptographiques** sont très souvent à la base des mécanismes de sécurité
- D'où l'importance de les étudier

Mécanisme de Securité (X.800)

- Les mécanismes spécifiques
  - encipherment, digital signatures, access controls, data integrity, authentication exchange, traffic padding, routing control, notarization
- Les mécanismes “pervasifs”
  - trusted functionality, security labels, event detection, security audit trails, security recovery

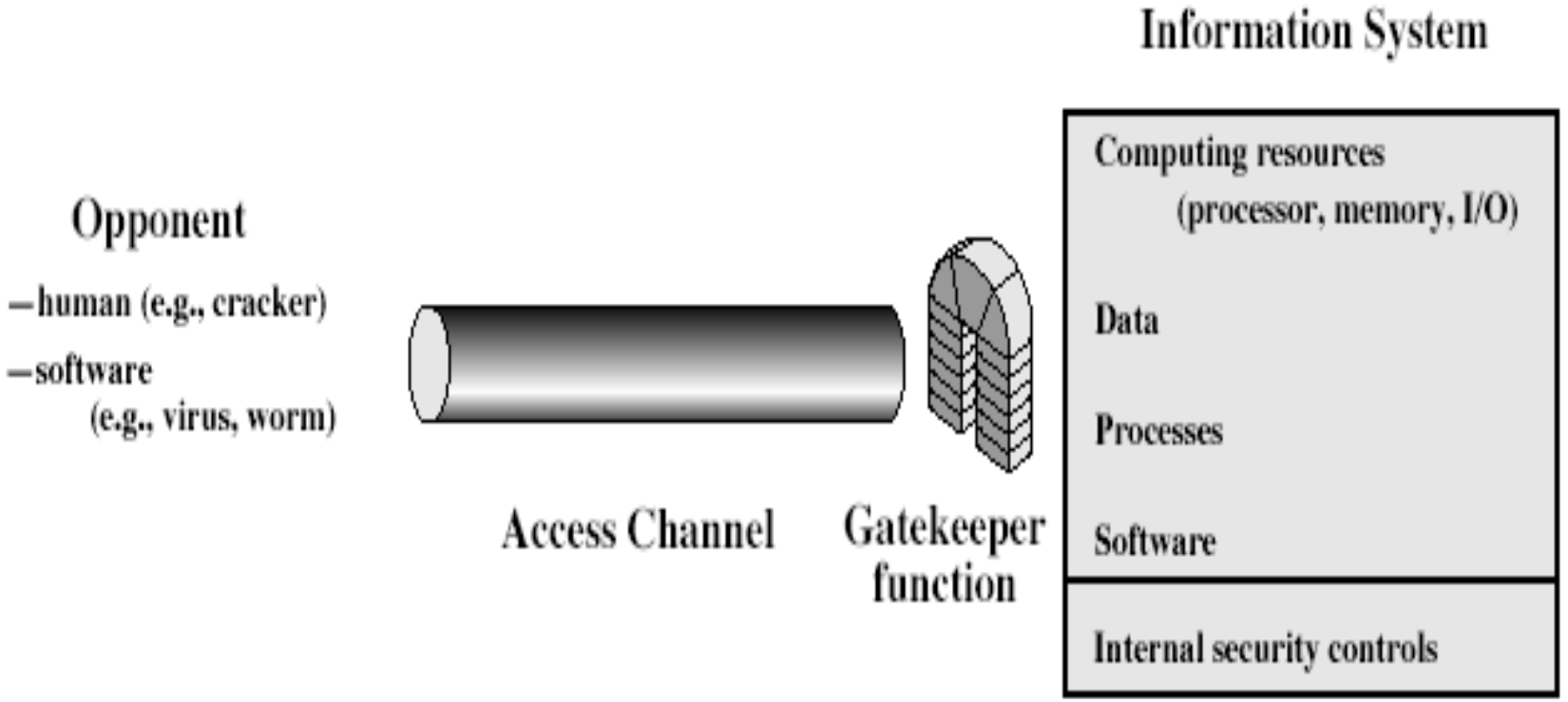
Modèle pour la sécurité réseau



Modele pour la sécurité réseau

- Utiliser ce modèle demande de :
  1. Trouver un algorithme adhoc
  2. Générer des clés (utilisés par les algorithmes)
  3. Developper des méthodes pour distribuer et partager le secret
  4. Spécifier un protocole permettant d'utiliser l'algorithme et le secret afin d'obtenir un service de sécurité

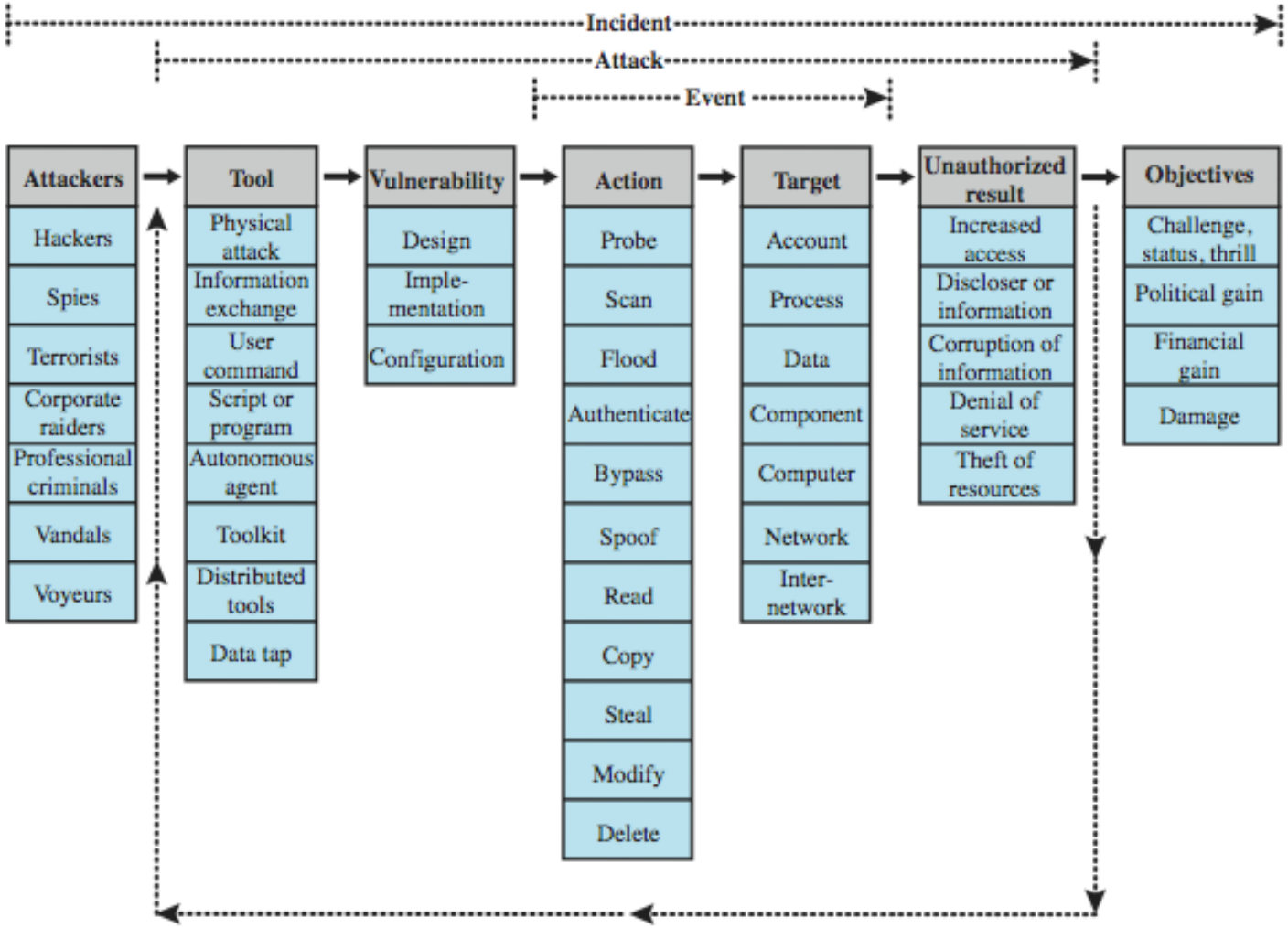
Modele de sécurité pour l'accès réseau



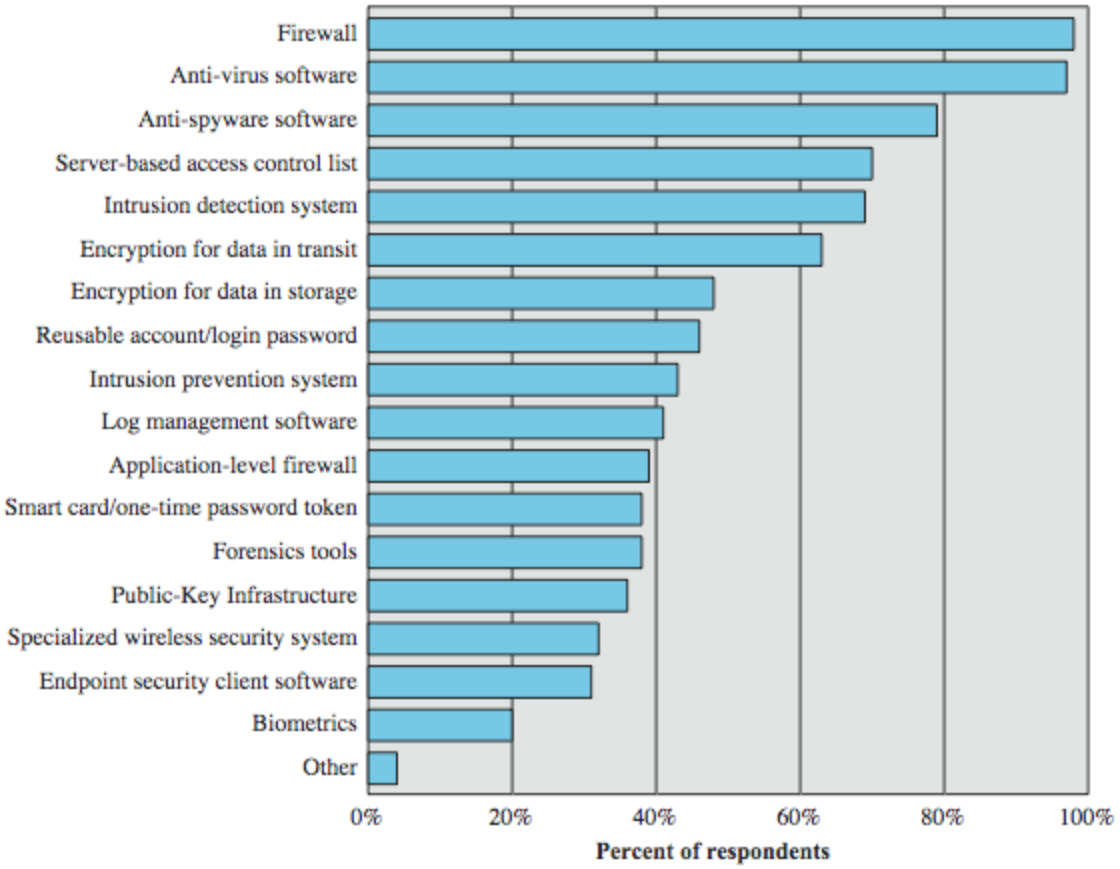
Modele de sécurité pour l'accès réseau

- Utiliser ce modele demande de :
  1. Selectionner les fonctions appropriées du "gatekeeper" pour identifier les utilisateurs
  2. Implanter des controles de sécurité pour que seuls les utilisateurs autorisés aient accès aux ressources

Security Taxonomy



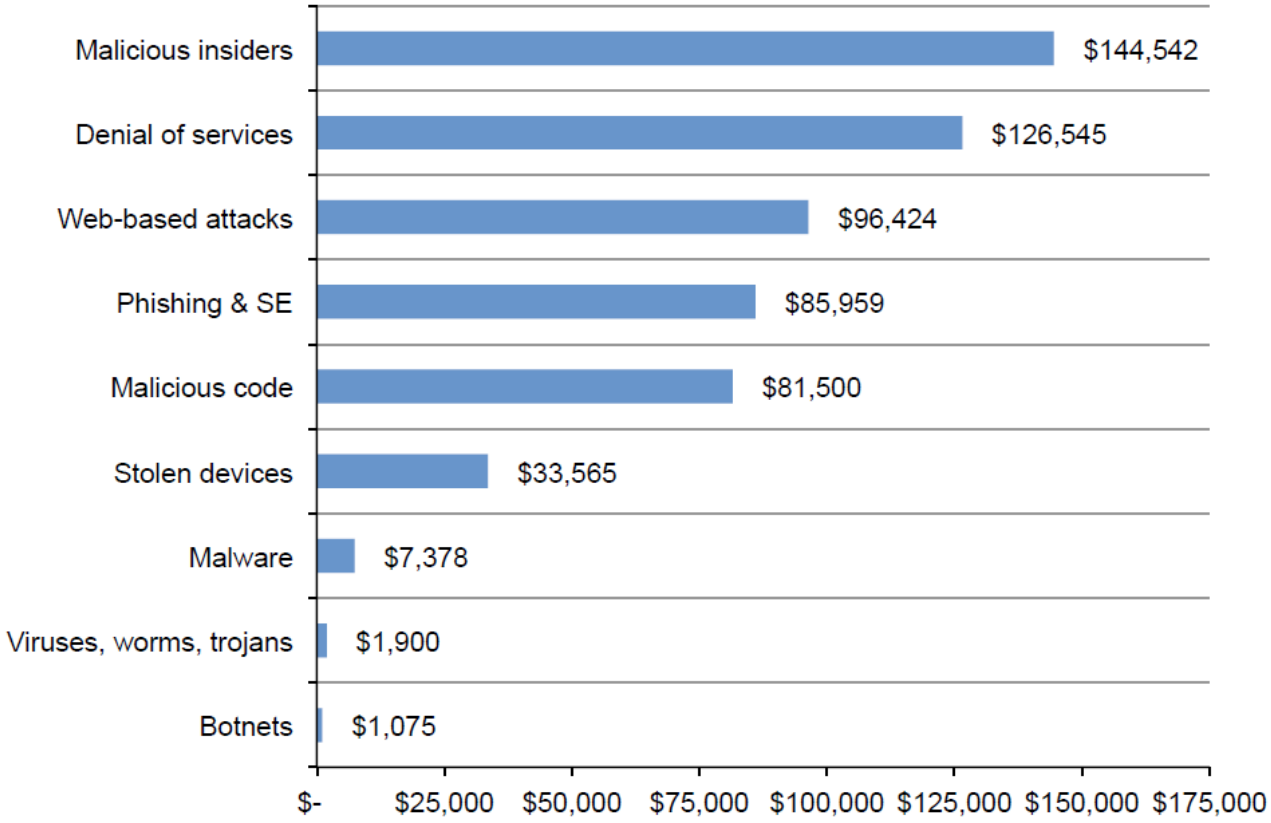
Technologies utilisées



Source: Computer Security Institute/FBI 2006 Computer Crime and Security Survey

Origines des attaques et coût pour les entreprises

Figure 11. Average annualized cyber crime cost weighted by attack frequency
Consolidated view, n = 252 separate companies



Stratégie de sécurité

- specification/politique
  - Qu'est ce que le schéma de sécurité est-il supposé faire?
  - Coder en règles et procédures
- implementation/mécanisme
  - Comment le fait-il?
  - prévention, détection, réparation
- exactitude/assurance
  - Est-ce que ça marche vraiment?
  - Degré de confiance en la politique, évaluation

Dilemme

Usagers : besoins en sécurité mais pas d'expertise

- L'analyste doit comprendre les besoins

Performance vs sécurité

- Les mécanismes de sécurité utilisent des ressources
- Changent les habitudes de travail
- Gestion de la sécurité
- La sécurité a un coût (vs coût d'une attaque ?)

En Résumé

- Concepts de sécurité
- Terminologie
- X.800 standard
- Attaques, services, mécanismes de sécurité
- Modèles de sécurité réseau

National Institute of Standards and Technology (NIST)

- Il a produit beaucoup de Federal Information Processing Standards Publications (FIPS PUBs)
- Très utiles pour gérer, implanter ou concevoir

Exemples :

- FIPS PUBs 199 : objectifs de sécurité pour les Systèmes d'Informations
- FIPS PUBs 200 : security requirements (exigences de sécurité)

Web sites

- http://sec.ietf.org/
- http://www.vtcif.telstra.com.au/info/security.html
- http://www.ieee-security.org/index.html
- http://csrc.nist.gov/
- http://www.securityfocus.com/
- http://catless.ncl.ac.uk/risks
- http://packetstormsecurity.org/
- http://www.isecom.org/
- https://www.clusif.asso.fr/fr/production/ouvrages/

Scope of computer security

- Action
- Target
- Event
- Tool
- Vulnerability
- Unauthorized result
- Attack
- Objectives
- incidents