au cœur de la société de l'information

Cours de Sécurité

Michel Riguidel Année 2006 - 2007

TELECOM PARIS
école nationale supérieure des télécommunications

get

Présentation

- Objectifs du cours
  - appréhender l'importance de la sécurité des technologies de l'information, de la communication et du multimédia
  - approfondir les concepts et nouveaux paradigmes
    - Quels sont les modèles de sécurité utilisés ?
    - Quelles sont les politiques de sécurité sous-jacentes ?
  - comprendre l'évolution parallèle des ingénieries
    - de la sécurité
    - de l'informatique et des réseaux
  - dresser un panorama technique des problèmes et solutions pragmatiques et opérationnelles en sécurité
- Interrogations en sécurité
  - comment développer, déployer et interconnecter des systèmes avec la sécurité adéquate ?
  - quelles solutions opérationnelles (modèles, architectures, produits, ...) ?
  - quelles sont les contraintes (coûts, formation, administration, certification) ?
- Que doit-on maîtriser techniquement ?
  - quelles technologies (informatique, sécurité, mathématique, ..) ?
  - quels composants (algorithmes, ...) ?
  - quels modules clés (piles protocolaires, ...) ?
  - pour quelle offre (équipements, produits, systèmes et services) ?

TELECOM PARIS
école nationale supérieure des télécommunications

Sommaire

- Généralités : la sécurité à l'ère numérique
- Les enjeux de la sécurité
- Les définitions
- La confiance dans la sécurité des systèmes numériques
- La sécurité des réseaux et des systèmes d'information à l'ère numérique
- Les nouvelles menaces
- L'état des lieux de la sécurité
- La sécurité des réseaux
- La sécurité des architectures
- La sécurité, à l'ère numérique, dans un monde mobile
- Sécurité plurielle, Confiance versatile, Intelligence Ambiante
- Les verrous de la sécurité dans les années 2000
- Quelques rappels sur les techniques cryptographiques
- Pare-Feu & Filtre de Confiance
- Les Cyber-attaques
- La Biométrie
- Les virus informatiques
- Les aspects légaux contre le piratage informatique
- La sécurité des documents électroniques
- L'intimité numérique (« privacy »)
- La protection des infrastructures critiques

Généralités

La sécurité à l'ère numérique

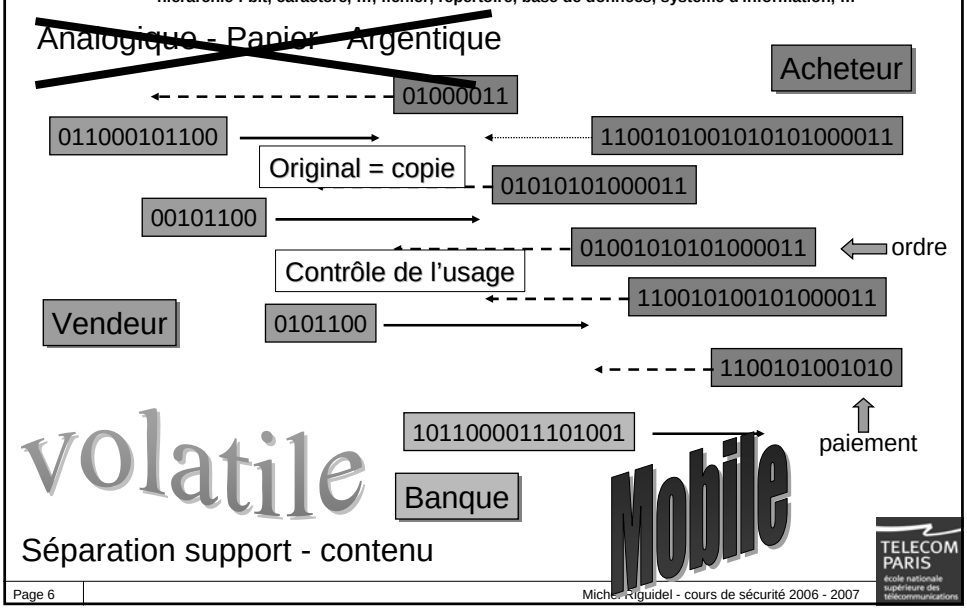
La Planète numérique est un Village Virtuel Violent

- La volatilité du numérique
  - Numérisation des échanges et de l'information
  - Dématérialisation des contenus
- Les réseaux interconnectés
  - Routage, aiguillage
- La transmission de l'information
  - Fibre optique
  - Ressource radio
- Moteur de recherche
  - Navigation
  - Fouille de données

- Mais peuplé d'êtres anonymes dans des endroits virtuels
- Un village avec de la violence
- Une urbanisation digitale, reflet de la vie réelle de notre société

L'ère et le nouvel Ordre Numérique

hiérarchie : bit, caractère, …, fichier, répertoire, base de données, système d'information, …



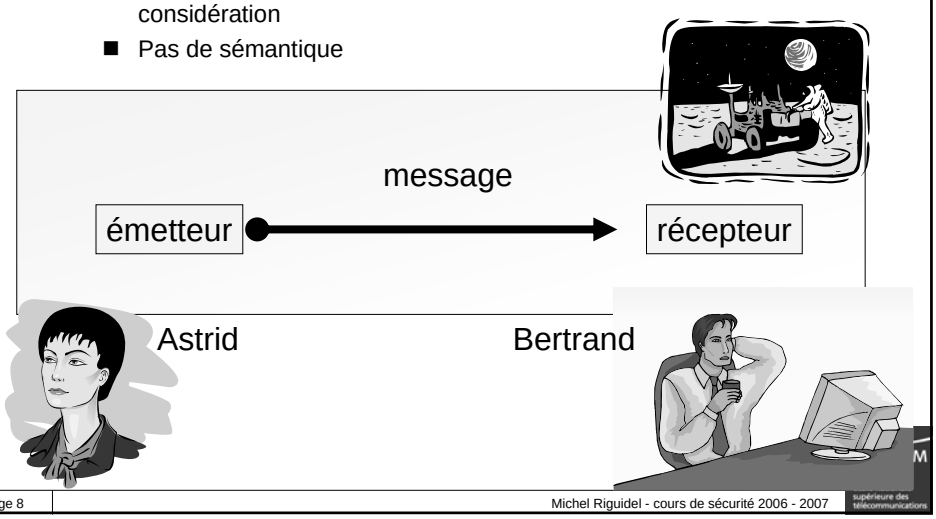
Séparation support - contenu

Ère numérique

- L'information numérique est **vulnérable**
  - Peut être détruite, amputée, falsifiée, confisquée, plagiée et modifiée de multiples manières
  - Pas d'original, ni des copies
  - Seulement des clones où la reproduction est à l'identique
- L'information numérique est **volatile**
  - Peut être ajustée et personnalisée
    - Une lettre générique peut être particularisée pour un destinataire spécifique
    - Un logiciel général peut être ajusté selon le contexte ou peut être ciblé à un usage spécifique

Modèle de C E Shannon & Weaver (1949)

- Modèle de communication unidirectionnel et linéaire
- Ni la relation entre les interlocuteurs ni le contexte ne sont pris en considération
- Pas de sémantique



Orthogonalité de la sécurité au nouveau contexte

- La généralisation du numérique
  - vulnérabilité essentielle des organisations
  - mobilité de l'information
  - tous secteurs : patrimoine, monétique, documents administratifs
- L'ouverture des systèmes
  - limitations des systèmes propriétaires
  - la banalisation des accès
  - les logiciels sur étagère
  - la non maîtrise des SI par les personnes responsables
- L'interconnexion des systèmes
- La convergence Multimédia, Communication, Informatique
- La mondialisation
  - tous les systèmes se ressemblent (reproductibilité des méthodes et techniques)
  - uniformisation des méthodes d'administration

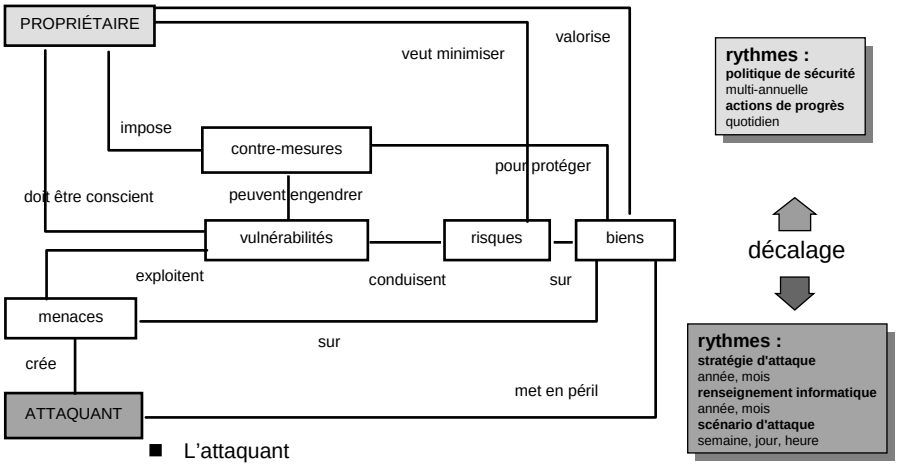
La sécurité : l'art de partager un secret

- Secret
  - Le cycle de vie du secret
    - Création, Stockage (archivage, sauvegarde), Distribution, Exploitation, Obsolescence, Destruction
      - Secrets éternels
        - ➔ périlleux de fonder une sécurité sur un unique secret statique, « inviolable » (?)
      - Secrets éphémères, jetables (one-time password, …)
        - ➔ attention que la gestion et la circulation des secrets ne soient pas une nouvelle vulnérabilité ou un obstacle dans les communications (une clé par message)
  - Stockage sécurisé
    - Dissimulé dans un coffre-fort
      - S'il n'existait pas de huis clos tangible dans un univers numérique, tous les secrets seraient des secrets de Polichinelle
  - Transport protégé
    - Protégé par chiffrement
      - ➔ nécessité d'un autre secret : « nous voilà au rouet » (M de Montaigne)
      - ➔ le quantique résout cette récursivité
  - Exploitation en secret : Alchimie des secrets
    - Cryptographie, stéganographie, tatouage, …
- La relation spatiale entre le secret et l'objet à sécuriser
  - Le secret absolu, statique, éternel, à conserver dans un coffre inviolable
    - Ancrage qui appartient à l'architecture de sécurité
      - ➔ À l'abri
  - Le secret qui accompagne l'objet
    - Étiquette, label, tagguage, sceau, signature
      - ➔ À découvert
  - Le secret qui est incrusté intimement dans l'objet
    - Tatouage, aquamarquage, filigrane électronique
      - ➔ À la merci (Écrin fragile)

Architecture de sécurité

- **Instiller la sécurité** dans le système, puis la maintenir
  - Entités de confiance forte
    - Amorce de confiance
  - Liaisons des entités
    - Sécurité inconditionnelle entre entités par protocoles cryptographiques
  - Entités de services de sécurité
    - Dispositif matériel et/ou logiciel pour audit, détection d'intrusion, pare-feu, …
- **Accrocher cette sécurité** aux Applications & Individus dans un système d'information
  - Identification
    - Certificats, authentification
  - Autorisation, privilèges, droits et devoirs, contrôle d'accès
    - Protocoles, certificats, tickets, …
  - Sécurité des applications et du système dans la durée
    - Outils matériel (carte à puce, pare-feu, système de détection d'intrusion, boîtier de chiffrement, …) et logiciel (protocole, …)
  - Assurance de sécurité
    - Garantie de construction, d'installation, d'exploitation, …
  - Formation, sensibilisation

Le modèle général de sécurité (protection / attaque)



- L'attaquant
  - Prend connaissance du Système d'Information (SI)
  - Décide d'un degré maximum de détectabilité avec un certain risque
  - Décide d'un degré de compromission avec le SI

Les modèles opérationnels de sécurité

- La protection
  - Cryptographie : Cacher le contenu sémantique et esthétique d'un message
  - Stéganographie : Transmettre un message caché de manière subliminale en utilisant le support d'une communication banale
- La dissuasion
  - Tatouage : Couvrir le corps d'un message avec un filigrane électronique qui est un autre message clandestin, en clair mais indétectable et indélébile
- La survie, le huis clos, le cloisonnement
  - Sélection et isolement des fonctions et des informations cruciales
  - Repli ou retrait dans un huis clos (bunker, quarantaine) : Architecture sans communications pendant une attaque
  - Le cloisonnement : Diviser l'organisation en segments disjoints et contrôler les flux
- La traçabilité, l'audit
  - Marque, empreinte, trace : Retrouver les marques, repérer les empreintes et les traces laissées par les sujets et les objets sur les lieux
  - Poursuivre les cyber-criminels
- La prévention
  - La sensibilisation (vis à vis des utilisateurs légitimes)
  - Le renseignement (vis à vis des attaquants potentiels)
- La désinformation
  - Leurre, "pots à miel" : Créer des chimères, des simulacres pour piéger les attaquants ou retarder leur avance
  - Le silence, la furtivité, la discrétion : Supprimer les messages intempestifs à l'extérieur qui signalent une présence
- L'attaque
  - Réagir, en temps réel, pour contrer un adversaire

Exemple générique pour l'attaquant d'un Système d'Information (SI)

- L'attaquant veut être un utilisateur légitime : qu'est ce qui est licite/illicite?
  - identification (comment rester anonyme? pseudonyme?)
  - authentification (mot de passe, carte à puce, quelle sécurité?)
  - contrôle d'accès (liste d'autorisation, privilèges, …)
  - utilisation d'une application sur un équipement connecté (savoir utiliser, ergonomie, …)
  - connexion à un serveur (autorisation? est-ce le bon serveur? les opérations sont-elles surveillées?)
  - va-t-il être surveillé sur la ligne, le réseau? va-t-on enregistrer son opération?
- L'attaquant veut atteindre les Services du SI
  - applications des utilisateurs
  - les applications de l'administrateur «système et réseaux» pour la gestion du service avec maintien du bon service (les protocoles qui gèrent le réseau, les applications systèmes)
- L'attaquant veut connaître et atteindre les Services de Sécurité
  - les services de sécurité mettent en application la politique de sécurité en vigueur : fonctions classiques de sécurité et notaire électronique (management des clés, des éléments secrets, ...). Comment les attaquer discrètement?
- Quelles sont les opportunités d'attaques? (intrusion, virus, cheval de Troie)
  - sur l'utilisateur? (menaces sur le PC, sur le réseau, ...), quel rôle ? (simple usager, administrateur)
  - sur le SI, fournisseur de services ? lorsqu'il présente ses services sur le réseau
- Comment s'opère la surveillance? Quelles sont les méthodes de défense, de contre-attaque?

La confiance

- La sécurité est en relation avec la confiance
  - Il n'existe pas de curseur de 0 à 1, allant d'une politique de sécurité laxiste à une politique sévère
    - La confiance est un treillis
      - en général, on ne peut pas comparer deux politiques
- Sentiment de la confiance
  - Réel
    - Par construction
      - formelle
    - Par empirisme
      - après observation du comportement, …
      - Acculturation, réputation
    - Par consentement, reconnaissance
      - parrainage, lettre de recommandation
  - Symbolique
    - Dissuasion, désinformation, leurre
  - Imaginaire
    - Mascarade, séduction, importance

Les principes de sécurité

- Ouverture
  - infrastructures à clé publique PKI (Public Key Infrastructure) encore peu déployées
  - Services de sécurité peu ouvert, convivialité décevante
- Transparence
  - L'administration des réseaux doit être ouverte aux usagers
  - Le contenu qui transite dans les réseaux doit être régulé
  - Une infrastructure ne doit pas affaiblir les autres réseaux
  - Ces constructions ne doivent abriter des économies parallèles
- Éthique
  - Contrôle du contenu, de l'origine, de la destination, et éventuellement du chemin
  - L'imputabilité est une fonction essentielle des futures infrastructures, pour qualifier une dérive d'un quelconque acteur de la chaîne de communication
- Subsidiarité et autonomie
  - Les communautés doivent pouvoir définir elles-mêmes leur politique de sécurité
  - Elle doit pouvoir s'adapter aux législations et aux cultures locales, tout en restant compatibles avec les objectifs de sécurité
- Réactivité
  - Traitement dans l'urgence pour réagir rapidement face à une agression
  - Des organismes dûment désignés doivent être capables de répondre à des situations de crise
- Discrétion
  - Les dispositifs de sécurité ne doivent pas être provocants
  - Pour ne pas agresser ou tenter l'appétence vorace du pirate devant un défi ludique

Le périmètre de la sécurité:
fiabilité et confiance

- Sûreté de fonctionnement (dependability)
  - Fiabilité, …
  - Propriétés des systèmes critiques (embarqués, …)
  - Réflexion sur notre dépendance vis à vis des technologies
    - addiction à Internet pour les entreprises et au téléphone portable pour les individus
- Sécurité (security)
  - Sécurité des valeurs
    - Biens immatériels (contenus et services dématérialisés)
    - Biens matériels en relation avec les TICs
  - Confidentialité, intégrité, disponibilité
    - Identification & Authentification, Non-répudiation
    - Contrôle d'accès, Audit
    - Identité virtuelle, anonymat
- Innocuité (safety)
  - Sécurité des personnes physiques et des biens tangibles
  - Ingénierie de la gestion et maîtrise des risques

La sécurité est pluridisciplinaire

- La sécurité couvre des aspects issus de plusieurs domaines
  - Éthique
    - vie privée, liberté de l'individu
    - bonne gouvernance: commerce et échange entreprise
    - démocratie : république numérique
  - Législation
    - lois sur la cryptographie, autorisations, droits des sujets, droit d'utiliser un service, une application
    - propriété intellectuelle, gestion des droits de distribution des oeuvres
  - Réglementation
    - Contrôle et filtrage de contenus (contenus illicites)
  - **Technique**
    - Mathématique, traitement du signal, informatique, électronique
    - Ingénierie
      - des réseaux, des architectures de systèmes
  - **Méthodologie**
    - ITSEC, Critères Communs (CC)
  - **Normes**
    - Standards cryptographiques (AES), protocoles (IPSec, …), …

Les Instruments

- Cryptologie
  - Chiffrement, Signature
  - Protocole cryptographique
  - Mise en œuvre matérielle / logicielle
- Stéganographie
  - Tatouage audiovisuel
  - Marquage sémantique
- Ingénierie des TICs
  - Réseaux, Informatique, Systèmes
  - Preuves, certification
  - Architecture de confiance : IGC
  - Biométrie
  - Intelligence économique
- Usages
  - Éducation, formation
  - Éthique, Sociologie
  - Arsenal juridique, Cybercriminalité

Les chapitres de la sécurité

- Les menaces, les objectifs de sécurité
- Les architectures de sécurité
  - Les Infrastructures de Gestion de Clés (IGC), les VPNs sécurisés
- Les fonctions de sécurité
- L'assurance de sécurité
- Les mécanismes de sécurité
  - La cryptologie (chiffrement, signature électronique)
  - La stéganographie (tatouage)
- Les solutions de sécurité
  - Protocoles cryptographiques (SET, SSL, IPSec, …)
  - Les infrastructures de confiance (PKIs, MPEG21, …)
  - Les produits de sécurité (pare-feu, boîtiers de chiffrement, identification biométrique)
- L'évaluation de la sécurité
  - Les critères communs, les ITSEC
- Les aspects sociologiques, éthiques (usage)

La sécurité à travers les âges

- La sécurité militaire (transmissions et communications)
  - de la Grèce antique à la 2ème guerre mondiale
    - Brouillage, Cryptage
  - utilisation de la la cryptologie pour chiffrer les messages
    - Chiffrement (C Shannon)
- La sécurité des systèmes d'exploitation
  - Le livre Orange (TCSEC)
- La sécurité de l'informatique répartie
  - Kerberos au MIT
- Les avancées en cryptologie
  - La généralisation du DES (symétrique), puis le RSA (asymétrique)
- La sécurité des grands réseaux
  - Les protocoles cryptographiques (PKI, SSL, …) et architectures (firewalls, VPNs, …)
- La sécurité des contenus
  - Tatouage, DRM (Digital Right Management)
- La sécurité des grandes infrastructures
- La sécurité en 2007
  - La cryptologie évolue (AES, courbes elliptiques)
  - La promesse du quantique
  - La sécurité de la vie privée et des réseaux hétérogènes
  - Transmission et stockage de contenus (information, services)
  - Sécurité de la production et de la distribution des contenus et services (DRM, …)
  - Sécurité des Calculs (Grille, Routage sur réseaux, …)
  - Sécurités des systèmes ouverts mobiles

Les enjeux de la sécurité

Les enjeux de la sécurité

- Maîtriser le Transport, le Traitement et le Stockage du Patrimoine Numérique Industriel, Intellectuel et Culturel
  - ➔ Politique (souveraineté)
  - ➔ Technologie maîtresse : cryptologie
- Valoriser les Contenus
  - – Multimédia, Logiciel, «Intellectual Properties», Base de Données…
  - – Assurer la libre circulation des contenus en toute confiance
  - – Disséminer les oeuvres, Rétribuer les auteurs, Essaimer le savoir-faire
    - ➔ Économique
    - ➔ Technologie maîtresse : tatouage et cryptologie
- Instaurer (ou Restaurer) la confiance dans l'univers numérique
  - – e-commerce, e-business, e-content, e-government, e-vote, e-democracy
    - ➔ Social (usage, lutter contre la fracture numérique)
    - ➔ Technologie maîtresse : infrastructure de confiance (distribuer des secrets et des certificats)
- Sécuriser **les infosphères**
  - – L'individu (liberté, intimité) : protéger
  - – L'entreprise (banques, transport, santé…) : prévenir
  - – Les infrastructures critiques et leurs interdépendances (effet de cascades des catastrophes en chaîne) : poursuivre la cyber-criminalité
    - ➔ Liberté, droits élémentaires, civilisation
    - ➔ Technologies maîtresses : ingénieries matérielle, biométrique, informatique, des réseaux, …
- Éviter le Syndrome sécuritaire
  - – Ne pas entretenir une spirale infernale
  - – Gérer les crises
    - ➔ Paix, valeurs européennes
    - ➔ Technologies maîtresses : modèles de sécurité (attaques et défenses) et de décision, politique de sécurité

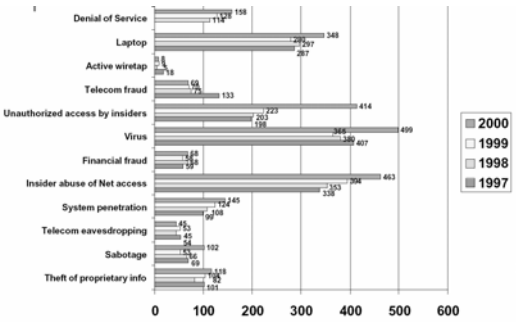
Les enjeux de la sécurité

- Vulnérabilité de la société de l'information et de la connaissance
  - – La société de l'information interconnectée est de plus en plus complexe et fragile
    - Interdépendances
      - énergie (centrale nucléaire, centrale électrique, ...)
      - transport (trafic aérien, port, trains, routes, …)
      - information (TV, radio, presse) et communication (téléphone, informatique)
      - santé (hôpitaux), éducation et loisirs
      - défense, administration
      - système bancaire, commerce électronique futur
  - – La civilisation de la rentabilité, du contact et de la spontanéité
    - Vies trépidantes et entreprises agiles à "flux tendus"
      - Réactions en chaînes et/ou décisions automatiques hasardeuses
      - Discontinuité dans le comportement des systèmes et organisations (rupture de stock, déficit de temps, phénomène de disette) aux conséquences inattendues
- Pour un ordre numérique sur la planète ?
  - – La sécurité est difficilement compatible avec un monde libertaire, fluide et non contrôlé
    - Intérêts contradictoires à divers niveaux
  - – Donner des grands principes (d'éthique, de responsabilité, de transparence, d'ouverture, d'autonomie, de subsidiarité, …) pour mettre en vigueur des règles du jeu réalistes
    - applicables par l'ensemble de la communauté internationale et
    - acceptées
      - localement par les utilisateurs et
      - globalement par des reconnaissances mutuelles

La criminalité informatique

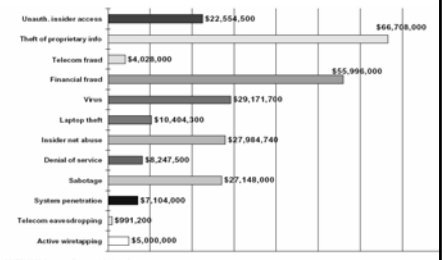
- Les réseaux de communication sont le nerf de l'économie des pays développés
  - La criminalité informatique est un fléau des sociétés développées qui affecte
    - le quotidien des individus, la gestion et la vie des entreprises, le fonctionnement des états
  - Le cyber-terrorisme est une menace fondamentale des sociétés modernes
  - l'interconnexion internationale des réseaux et le développement de l'informatique donne au crime informatique un caractère multiple, dangereux et international
- **20 000 attaques** réussies par mois dans les années 2000 dans le monde

Typologie des attaques et des fautes détectées



CSI/FBI 2000 Computer Crime and Security Survey
Source: Computer Security Institute

Cyber-Criminalité: les pertes



CSI/FBI 2000 Computer Crime and Security Survey
Source: Computer Security Institute

La sécurité des ordinateurs et des réseaux

- Vision selon l'homme de la rue
  - Les Attaques
    - Les virus
    - Les pirates sur Internet ("hackers ludiques")
    - Le "spam" (publicité sauvage) via la messagerie
  - Les protections
    - Les mots de passe
    - En France
      - Les cartes bancaires (carte à puce)
    - En Europe
      - La carte SIM du téléphone portable
    - Les pare-feu (firewalls)
    - La cryptographie (le chiffrement de messages)
- Vision plus large
  - Les Attaques
    - Guerre de l'information et de la connaissance
      - **Intelligence économique**
      - **Espionnage industriel**
    - Fragilité des systèmes complexes
      - Attaques réelles, symboliques, "gratuites" de déstabilisation
  - Les protections
    - La protection de la vie privée
      - Protéger les données personnelles
      - Pas d'observation ni de liens
      - Pas d'inscription dans des fichiers
    - La protection du patrimoine numérique
      - Protéger les contenus et les services
    - La protection des infrastructures critiques

Les défis de la sécurité des TICs

- Des Infrastructures résistantes
- Des Réseaux protégés
- Des Systèmes d'Information sécurisés
- Des Applications & Données immunes

- Un label de Qualité de fabrication
  - Fabrication des logiciels

- Innocuité des agressions de toute nature
  - Attaques physiques

Les définitions

Sécurité, Confiance, Protection, Dissuasion

- Sécurité (Security)
  - Quête d'indépendance vis à vis d'un péril, d'une peur, d'un piège, d'une menace, d'un risque, d'un doute, d'une crainte
  - Confidentialité, Intégrité, Disponibilité
- Protection (Protection)
  - Ensemble de mécanismes et de politiques nécessaires (pas suffisantes) pour atteindre la sécurité
- Dissuasion (Deterrence)
  - Ensemble de mécanismes et de politiques nécessaires (pas suffisantes) pour décourager un adversaire potentiel
  - Défense fondée sur la crainte de ripostes que le propriétaire peut faire subir à des agresseurs éventuels
  - Inciter un attaquant potentiel à abandonner son projet
- Innocuité (Safety)
  - Défense physique de la personnes et des biens
- Sûreté de fonctionnement (Dependability)
  - Fiabilité d'un système (par exemple avec des redondances)

Sécurité des technologies de l'information et du multimédia

- confidentialité
  - prévention d'une divulgation non autorisée de l'information
    - confidentialité d'un texte, d'une image (=> cryptographie)
    - confidentialité des flux d'information dans un réseau (=> bourrage)
  - ⌦ fuite d'information confidentielle, écoute ou lecture illicite
  - ⌦ information sensible à protéger
  - ⌦ niveau de classification d'information : SD > CD > DR, niveau d'habilitation des individus
  - ⌦ cloisonnement des projet A # projet B => droit d'en connaître (need to know)
- intégrité
  - prévention d'une modification non autorisée de l'information
    - intégrité d'une conversation, d'un programme informatique,
    - intégrité d'une image transmise (MPEG2) : non altération du contenu visible par l'œil humain (=> stéganographie, tatouage électronique)
  - ⌦ falsification d'un document, ajout d'un virus, d'un cheval de Troie, manipulation d'une séquence vidéo, écriture illicite
- disponibilité
  - prévention d'un déni non autorisé d'accès à l'information ou à des ressources
    - disponibilité d'un serveur informatique, d'un réseau
    - rétention de données, saturation d'un réseau par flux intempestif, brouillage de communication radio

La sécurité multimédia étend le spectre des fonctions de sécurité

- Confidentialité
  - le chiffrement global et systématique de l'information n'est pas indispensable, ni souhaité (performance)
    - On ne chiffre qu'une partie significative d'un document
    - Exemple : masquage des visages sur une photo, de tableaux commerciaux dans une réponse à Appel d'Offre
- Intégrité
  - ne se pose plus en terme d'exactitude de réplication
    - flux compressés : pas d'exactitude au bit près
    - la contrefaçon est plus délicate à détecter
- Disponibilité / Contrôle d'usage
  - le multimédia introduit une généralisation de l'usage autorisé d'un objet :
    - droit d'utiliser une version d 'un logiciel pendant un certain temps sur un PC dans un certain lieu
    - autorisation de recopier un certain nombre de fois un produit sous certaines conditions

Biens, menaces, risques et contre-mesures

- Bien, valeur (asset)
  - importance exprimée en terme de dommages consécutifs à la réalisation de menaces
  - dommages conséquence directe ou indirecte de la divulgation, la modification illicite, la destruction ou le détournement des informations
- menace (threat)
  - action ou événement susceptible de porter préjudice à la sécurité
  - menaces délibérées (des attaques) ou involontaires (erreurs ou défaillances)
- risque
  - les informations doivent être protégées contre les menaces qui peuvent induire des conséquences néfastes pour les biens
  - augmente avec l'importance des dommages éventuels et la probabilité de la réalisation des menaces
  - pour réduire les risques, des contre-mesures spécifiques sont choisies
- contre-mesures
  - par nature physiques, liées au personnel, organisationnels ou techniques
  - contre-mesures techniques : fonctions et mécanismes dédiés à la sécurité d'un système

Cible et vulnérabilité

- cible de sécurité (évaluation de la sécurité)
  - spécification de la sécurité qui est exigée d'une cible d'évaluation et qui sert de base pour l'évaluation
  - la cible de sécurité doit spécifier les fonctions dédiées à la sécurité de la cible d'évaluation
  - elle spécifie les objectifs de sécurité, les menaces qui pèsent sur ces objectifs ainsi que les mécanismes de sécurité particuliers qui sont employés
- vulnérabilité
  - faiblesse de la sécurité d'une cible d'évaluation (défaut dans l'analyse, la conception la réalisation ou l'exploitation
- estimation de la vulnérabilité
  - aspect de l'estimation de l'efficacité d'une cible qui recouvre la mesure dans laquelle des vulnérabilités connues pourraient compromettre en pratique sa sécurité telle qu'elle est spécifiée

Politique de sécurité

- politique de sécurité
  - spécifie l'ensemble des lois, règlements et pratiques qui régissent la façon de gérer, protéger et diffuser les informations et autres ressources sensibles au sein d'un système spécifique
  - une politique de sécurité identifie les objectifs de sécurité
  - les menaces prises en compte par une combinaison de fonctions dédiée à la sécurité implémentée dans une cible de sécurité et également des moyens physiques relatif au personnel et à l'organisation
- politique de sécurité d'un système
  - ensemble des lois, règles et pratiques qui régissent la façon dont l'information sensible et les autres ressources sont gérées, protégées et distribuées à l'intérieur d'un système spécifique
- administrateur
  - personne en contact avec la cible d'évaluation qui est responsable de son maintien en exploitation

Politique de sécurité (informatique)

- Une politique de sécurité
  - Ensemble des lois, règlements et pratiques qui régissent la façon de gérer, protéger et diffuser les biens, en particulier les informations sensibles, au sein de l'organisation
  - un ensemble de règles qui spécifient les autorisations, interdictions et obligations des sujets (agents)
    - (notion qui inclut à la fois les utilisateurs et les applications)
  - qui peuvent accéder au système informatique
- Une politique de sécurité
  - doit permettre d'exprimer des exigences
    - de confidentialité (pas de consultation illégale d'information)
    - d'intégrité (pas de création, de modification ou de destruction illégale d'information) et
    - de disponibilité (ne pas pouvoir empêcher que les autres agents puissent avoir un accès légitime à certains services ou ressources du système).

Fonctionnalité

- exigences de sécurité pour maintenir la confidentialité, l'intégrité, la disponibilité d'un système ou d'un produit
- mise en place de mesures techniques (fonctions dédiées à la sécurité)
  - Identification et authentification, contrôle d'accès, protection des données
  - Audit, protection des mécanismes de sécurité
  - Reprise sur incident, "zone de survie", etc
- Ne pas confondre
  - objectifs de sécurité
    - pourquoi la fonctionnalité est voulue ?
    - objectif de sécurité d'un système
      - réduire, pour l'organisation concernée, à un niveau acceptable de risques résiduels, les risques associés
  - fonctions dédiées à la sécurité
    - pour atteindre les objectifs de sécurité
    - quelle fonctionnalité est réellement fournie ?
  - mécanismes de sécurité utilisés
    - pour implémenter des fonctions dédiées à la sécurité
    - comment la fonctionnalité est fournie ?
    - mécanisme de sécurité: logique ou algorithme qui implémente par matériel ou logiciel une fonction particulière dédiée ou contribuant à la sécurité

Les Classes de Fonctionnalités

- Audit de la sécurité
- Communication
- Protection des Données utilisateurs
- Identification et Authentification
- Intimité ("privacy")
- Protection et Confiance des fonctions de sécurité
- Utilisation de ressources
- Accès à la cible
- Chemin de confiance

- FAU Security Audit
- FCO Communication
- FDP User Data Protection
- FIA Identification & Authentication
- FPR Privacy
- FDT Protection of Trusted Security Functions
- FRU Resource Utilization
- FTA TOE Access
- FTP Trusted Path

Identification et Authentification

- fonctions destinées à établir et vérifier une identité annoncée
- exigences pour la détermination et le contrôle des utilisateurs qui sont autorisés à avoir accès aux ressources contrôlées par la cible
  - implique d'établir l'identité annoncée par un utilisateur
  - vérifier que cet utilisateur est bien la personne qu'il prétend être (le sujet fournira à la cible une information que la cible sait être associée au sujet en question)
    - fonctions: ajouter de nouvelles identités, éliminer, invalider d'anciennes identités
    - permettre à des utilisateurs autorisés de contrôler les informations nécessaires pour vérifier l'identité d'utilisateurs
    - fonctions pour assurer l'intégrité des informations d'authentification
    - limiter la possibilité d'essais répétés d'établissement d'une fausse identité

Contrôle d'accès

- exigences pour garantir que les utilisateurs (et les processus qui agissent pour le compte de ceux-ci) sont empêchés d'accéder aux informations et aux ressources auxquelles ils ne sont pas autorisés à accéder ou auxquelles ils n'ont pas besoin d'accéder
  - exigences concernant la création ou la modification (y compris la suppression) non autorisées d'informations
  - fonctions destinées à contrôler les flux d'informations entre utilisateurs, processus
  - cela inclut l'administration (l'octroi ou le retrait) des droits d'accès et leur vérification
  - fonctions servant à établir et entretenir les listes et règles qui régissent les droits d'effectuer différents types d'accès

Autres fonctions (1)

- imputabilité
  - exigences pour garantir l'enregistrement des informations pertinentes sur les actions soit d'un utilisateur, soit d'un processus agissant pour le compte de celui-ci, de façon que les conséquences de ces actions puissent être ultérieurement associées à l'utilisateur en question et qu'on puisse le tenir pour responsable
- audit
  - exigences pour garantir que sont enregistrées suffisamment d'informations sur les événements (courant et exceptionnels) pour qu'un examen ultérieur puisse déterminer s'il y a effectivement eu violation de la sécurité, et dans ce cas, quelles informations ou autres ressources ont été compromises
    - fonctions destinées à déceler et à examiner les événements susceptibles de constituer une menace pour la sécurité
- réutilisation d'objet
  - exigences pour garantir que les ressources (mémoire centrale et zone disque) peuvent être réutilisées tout en préservant la sécurité
    - fonctions destinées à initialiser les objets supports de données non alloués ou à effacer ceux qui sont réalloués.

Autres fonctions (2)

- fidélité
  - exigences pour garantir que les relations spécifiques entre les différentes données sont correctement maintenues
- fiabilité de service
  - exigences pour garantir que les tâches critiques en temps sont exécutées au moment voulu
  - exigences pour garantir que l'accès aux ressources est possible quand on en a besoin, et que les ressources ne sont pas sollicitées ou conservées inutilement
  - fonctions destinées à garantir que les ressources sont accessibles et utilisables à la demande d'une entité autorisée et à prévenir ou à limiter les interférences avec les opérations critiques en temps
- échange de données
  - exigences pour la sécurité des données pendant leur transmission à travers des canaux de communication

Evolution of Security Functions

- Integrity is of paramount importance
  - Integrity of its own PC configuration, integrity of user's data, integrity of Information System, of the network, all integrity of any piece, at any scale is decisive. Classical danger against integrity is virus aggression. Electronic signature is the conventional answer to counter this risk.
- Confidentiality is, relatively speaking, less crucial as it used to be in the past, when only sensitive and confidential data were digital
  - Today, a large amount of our PC data are not secret. However, data confidentiality will be still in the future at the heart of security issues. Cryptography is the logical response to work out this challenge.
- Availability tends to be more considered as availability of network resources, due to new ways of working
  - Security measures have to be taken to avoid saturation of servers, firewalls, routers, network bandwidth and cache storage. Current threats are saturation attack to networks, to portals, to base station and to firewalls.

Evolution of Security Functions

- Access control, authorization
  - Because systems are interconnected and data or programs are freely circulating, it is necessary to re-consider the access control functionality and mechanisms. Firewall are bottlenecks in Information Systems and networks. Access control lists and authorization servers are difficult to manage in an open world.
- Identification and authentication
  - These functions are essential in virtual worlds, where people and machines are connected across networks. It is necessary to identify the physical individuals or groups, but also their representatives on the networks, which are executables, threads, agents, sessions launched by them. The entity, who is fully responsible of these actions, can produce possible damages on the whole Information System. He or she must be accountable of the consequences and traced by an audit system. Their content objects (image, video, Web pages) have to be identified and authenticated, whether stored in databases or transmitted via packets. The user attribute definition, using biometrics, steganography, and the specification of secrets, using cryptography, have to be designed carefully. The same applies to the link between a physical person and all the items running on the Information System on his behalf. This can be done through the use of digital signature and certificates.
- Communication security, Non-repudiation of origin and of receipt, Accountability must evolve
  - New tracability algorithms are yet to be investigated.

Evolution of Security Functions

- Privacy
  - Anonymity or pseudonymity are probably not enough considered in the current cryptographic protocols. Unlinkability and unobservability are more tricky to be guarantied and are in conflict with tracability and audit of actions.
- User content protection and security
  - A huge R&D effort is under way for Information flow control policy and functions, Access control policy and functions, Content authentication, integrity, confidentiality, either stored, exported/imported or transferred. Cryptography and steganography have to mutualize their capability to solve the issue of content life cycle across networks and in the hand of several actors.
- Security audit
  - More automatic response, analysis and review are needed to track accidental security events.
- Security management is the keystone of security architecture
  - Management of security policies along time and space, management of security functions, attributes, data, management of roles are part of the security officer's current duties. Cryptographic key and certificate management are yet to be validated at larger scale (e.g. european), for a larger spectrum than electronic commerce. Trusted path/channels are the major issues to supply confidence between the various distributed entities.

Assurance, conformité, efficacité

- assurance
  - confiance qui peut être accordée à la sécurité fournie par une cible d'évaluation
- conformité
  - propriété d'une représentation d'une cible d'évaluation qui fait qu'elle reflète exactement la cible de sécurité
- efficacité
  - propriété d'une cible qui représente la mesure dans laquelle elle assure la sécurité dans le contexte de son exploitation réelle ou prévue
- pertinence
  - pour réellement contrer les menaces envers la sécurité
- cohésion (binding)
  - aspect de l'estimation de l'efficacité qui recouvre la capacité à coopérer pour former un ensemble intégré et efficace
- facilité d'emploi
  - la cible ne peut pas être configurée ou utilisée d'une manière non sûre

Assurance

  - une confiance appropriée à ces fonctions est nécessaire : assurance
- confiance dans la conformité
  - de la réalisation des fonctions et mécanismes dédiés à la sécurité (développement et exploitation)
    - estimer si les fonctions et mécanismes dédiés à la sécurité sont implémentés correctement
  - degré croissant de confiance dans la conformité E0 à E6 (ITSEC, critères européens)
- confiance dans l'efficacité des fonctions
    - estimer si les fonctions et les mécanismes dédiés à la sécurité satisfont effectivement les objectifs déclarés
  - pertinence de la fonctionnalité
  - cohésion de la fonctionnalité (si les fonctions opèrent en synergie)
  - efficacité : les conséquences de vulnérabilités connues et découvertes
  - facilité d'emploi
  - capacité des mécanismes à résister à une attaque directe (3 niveaux de résistance élémentaire, moyen, élevé)

La Confiance dans la sécurité des systèmes numériques

Méthodologie
Évaluation
Certification

La confiance dans la sécurité

- La confiance dans les modèles fondamentaux
  - Modèle de sécurité
    - Modèle de protection
    - Modèle de dissuasion
    - Modèle d'anticipation, de prévention, précaution
  - Modèle d'attaque
    - Guerre de l'information
- Politique de sécurité
  - Spécification de catalogues de politiques de sécurité
  - Offre de kits personnalisés de sécurité pour les communautés
- La confiance dans les outils qui fabriquent la sécurité
  - La sécurité de la cryptologie
    - Cryptanalyse
  - La sécurité dans le tatouage
  - Les outils informatiques
    - La vérification formelle

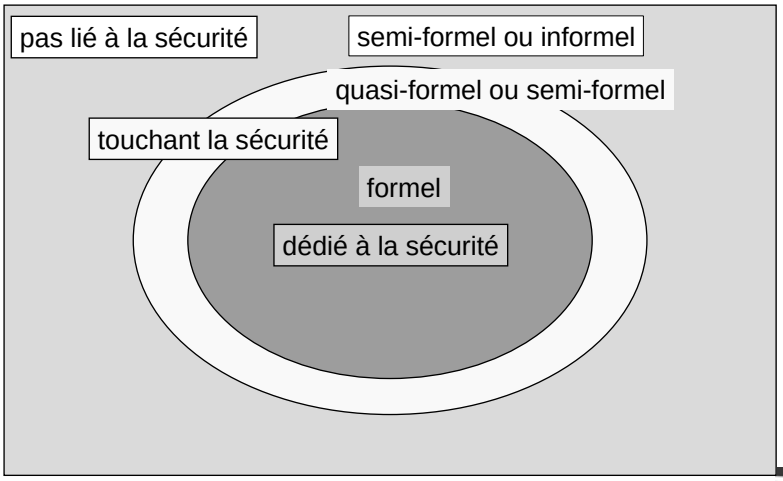
La confiance dans la sécurité

- Quelle confiance avoir dans la sécurité
  - d'un produit, d'un équipement, d'un système, d'un service, d'un SI
    - propriétés de sécurité :
      - Confidentialité
      - Intégrité
      - Disponibilité
    - ITSEC :
      - assurance d'efficacité et de conformité
- Méthodologie
  - Conception
  - Validation
  - Certification
- Menaces induites par les produits non évalués
  - Pas d'assurance de sécurité
  - Failles de sécurité
    - intentionnelles (chevaux de Troie, ...)
    - non intentionnelles (bugs, ...)
  - Fiabilité
  - Limitation des fonctions de sécurité offertes

TCSEC (le livre Orange), ITSEC et les Critères Communs

- Trusted Computer System Evaluation Criteria
  - orange book du DoD des US (ou livre orange)
  - évaluation de la sécurité des systèmes d'exploitation publié en 83
  - maintien de la confidentialité des informations classifiées au niveau national
  - classes D, C1, C2, B1, B2, A1
  - politique de sécurité, imputabilité, assurance, documentation
  - B2 contrôle d'accès réalisé par moniteur de référence
    - résistant à l'intrusion
    - systématiquement mis en œuvre
    - petit (soumis à des analyses et à des tests dont la complétude doit être assuré
- ITSEC
  - France, Royaume Uni, Pays bas, Allemagne : version 1.2 Juin 91
- Critères Communs
  - USA, Canada et Europe : version 2.0 Décembre 97

Les 3 parties d'un système



L'assurance vue par les ITSEC

Efficacité

- construction
  - pertinence et
  - cohésion des fonctionnalités
  - résistance des mécanismes
  - vulnérabilités de construction
- exploitation
  - facilité d'emploi
  - vulnérabilités en exploitation

... analyse utilisant la documentation fournie pour l'évaluation de la ...

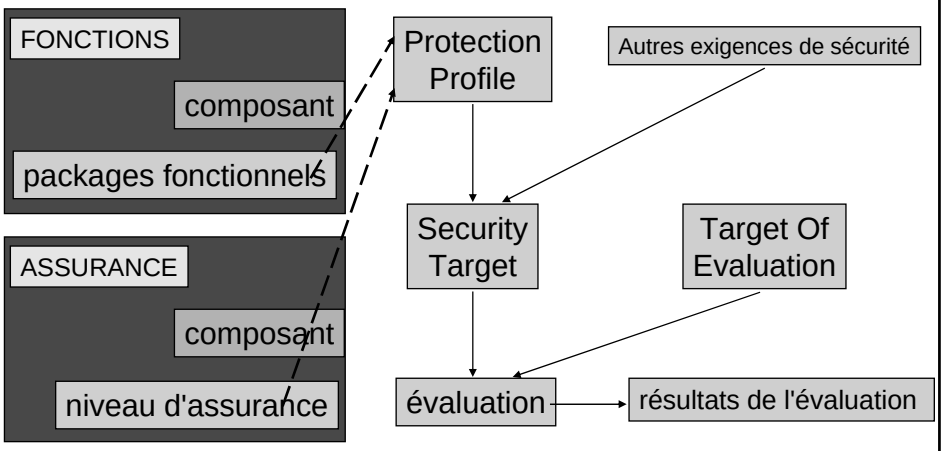
Conformité

- niveau de confiance E1 à E6
- développement
- environnement de développement
- exploitation

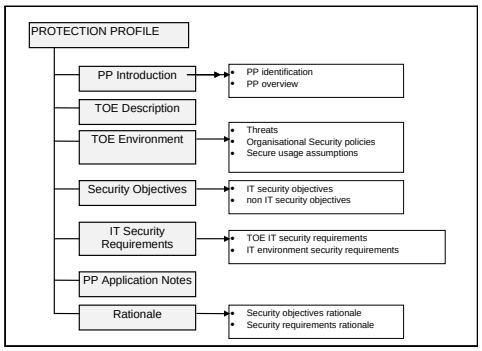
ITSEC: Niveaux d'assurance

- E6
  - Style formel pour la conception générale et les fonctions dédiées à la sécurité (politique de sécurité)
- E5
  - Correspondance entre conception détaillée et code source
- E4
  - Modèle formel de politique de sécurité
  - Conception générale et détaillée semi-formelle
- E3
  - Code source
  - Preuves des mécanismes
- E2
  - Conception détaillée informelle
  - Documentation de tests
  - Gestion de configuration
- E1
  - Conception générale informelle
  - Documentation de tests optionnelle

Concepts Clés des Critères Communs



Critères Communs: Profil de Protection



Modèle formel de Politique de Sécurité

- Modèle sous-jacent de politique de sécurité exprimé en style formel
  - présentation abstraite des principes de sécurité importants que la cible doit faire respecter
    - modèle de Bell-LaPadula
      - modèle des exigences de contrôle d'accès caractéristiques d'une politique nationale de sécurité pour la confidentialité
    - Clark et Wilson intégrité des systèmes transactionnels commerciaux
    - Brewer-Nash exigence de contrôle d'accès visant à assurer la confidentialité pour le client
- Objet O
  - entité passive qui contient ou reçoit des informations
  - objet de stockage (comporte des accès en lecture et écriture)
- Sujet S
  - entité active (une personne, un processus ou un équipement)
  - profil, rôle
- Opération licite T
  - un sujet S autorisé effectue l'opération licite T sur l'objet O
- Canal caché
  - utilisation d'un mécanisme non prévu pour la communication pour transférer des informations d'une manière qui viole la sécurité

Niveaux ITSEC

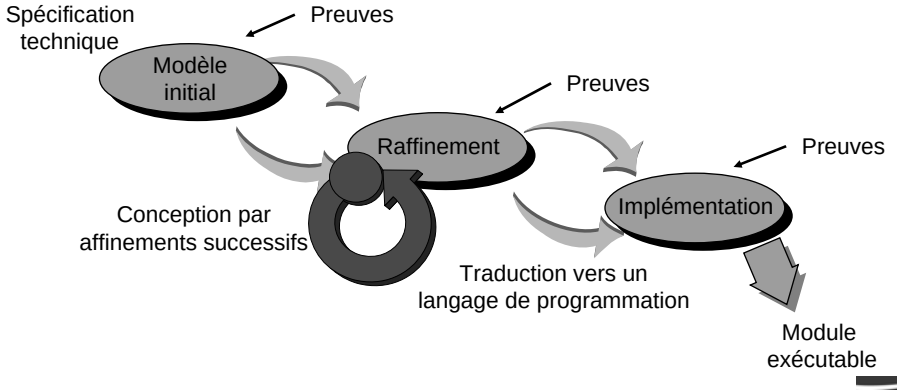
	Modèle Formel	Fonctions de Sécurité			Conception générale			Conception détaillée		Source schémas	Doc. de tests	Sources des Bib. et Routines système
		Informel	Semi-formel	Formel	Informel	Semi-formel	Formel	Informel	Semi-formel			
E6												
E5												
E4												
E3												
E2												
E1												

: Exiger pour le niveau

: Expliquer
: Décrire
: Présenter

La méthode B (Jean-Raymond ABRIAL)

Approche fonctionnelle de la programmation :
"Le logiciel conçu fonctionne correctement"



La méthode B

Mécanisme de base : la machine abstraite et ses invariants

Machine = données encapsulées & services

Ensemble
Relation, fonction
Suite, arbre

Pseudo-code en définition formelle
non exécutable

ni séquencement, ni boucle

mais précondition (logique) -> action (instantanée)

Invariant = Lois statiques

Génération des obligations de preuves

Méthode B pour les protocoles

- Spécification du protocole en ignorant temps et espace
  - on définit les invariants globaux du système tel qu'un observateur doit toujours le voir
- Raffinements
  - on spécialise par étapes en démontrant que
    - étape (n+1) = raffinement étape (n)
  - les protocoles sont définis sous forme de commandes gardées (à la Z: when ... then ...)
- Preuves
  - l'absence de deadlock est prouvée par intersection formelle des gardes
  - les invariants sont démontrés à chaque étape de raffinement
  - l'accessibilité est démontrée

Propriétés & champ d'applications

- Les politiques de sécurité
  - sont définies (existence, légitimité, cohérence, complétude, …) et
  - doivent être mises en application (sensibilisation, simplicité dans la définition et dans l'implémentation)
- Les politiques de sécurité modernes
  - ne doivent pas être statiques, mais dynamiques
    - c'est-à-dire configurables et personnalisables selon des profils d'utilisateurs, selon les flux, dépendant du contexte et de la localisation des acteurs en jeu.
- Elles s'appliquent et sont mises en vigueur dans le cadre :
  - de la convergence des domaines Télécom, Informatique, Multimédia,
  - de la convergence réseaux fixes et mobiles,
  - de l'Internet du Futur, de l'avènement de la génération 3G, de l'émergence du 4G.
- Elles doivent également prendre en compte les nouveaux besoins de protection des systèmes intégrant des logiciels embarqués
  - sécurité des communications entre le système et son environnement (en particulier, sécurité des nouveaux protocoles de communication sans fil) et
  - de l'accès à ces systèmes par des utilisateurs qui ne sont pas nécessairement de confiance (passager d'un avion, par exemple, …)

La problématique de la Politique de sécurité

- Définition du système à sécuriser, à protéger
  - Définition des biens à protéger
  - Les acteurs autorisés
  - Les actions autorisées
  - Les services et les contenus autorisés
  - Notion de secret, de partie privée, relation public /privé,
  - Monde ouvert/fermé, Mobilité
- Les premières questions
  - Quel est le périmètre ?
    - Système avec des frontières
    - Notion de domaine
  - Quelles est la taille du système ?
  - Quel sont les objectifs de sécurité ?
  - Quels sont les attaquants potentiels ?
  - Quels sont les biens à protéger ?
  - Quelles sont les vulnérabilités ? (bugs, accidents physiques)

Objectifs de sécurité, menaces

- Quelles sont les objectifs et les menaces ?
  - Politique de sécurité d'un individu
    - Intimité numérique : confidentialité
  - Politique de sécurité pour une entreprise
    - Intégrité du système d'information
  - Politique de sécurité pour une grande entreprise multi site
    - Disponibilité du réseau
  - Politique de sécurité d'une grande organisation (administration, état, etc)
    - Disponibilité du système
  - Politique de sécurité vis à vis d'Internet
    - Contenus illicites
    - Politique de contrôle d'accès des flux entrants
  - Politique d'accès à des contenus
    - Filtrage

Le point de vue de la sécurité sur le système

- Quelle granularité choisir ?
  - Utilisateurs, applications, paquets IP ?
- Définition de sujets, d'objets et d'opérations des sujets sur les objets
  - Identification des sujets : personnes, applications, …
  - Problème de l'anonymat dans un milieu ouvert
  - Problèmes des rôles : non pas la personne mais le rôle qu'elle joue
  - Identifications des objets
  - Identifications des opérations
- Mettre en place des contre-mesures
  - Législation, Organisation, Mesure technique
  - Les fonctions de sécurité
    - Audit : enregistrement de l'histoire du système d'information
    - Authentification
    - etc
  - Problème de la responsabilité : imputabilité
    - En informatique (protocoles) : tout ce qui n'est pas interdit, est autorisé …

L'environnement, le milieu, le contexte, l'ambiance

- L'environnement, le milieu (le temps, l'espace géographique)
  - Les bâtiments privés (la maison, le bureau), publics (l'aéroport, le campus, la mairie, …)
  - Les espaces privés, publics (la gare, l'aéroport)
  - Le déplacement privé (en voiture), public (en car, en train, en avion)
- Le contexte
- La politique de sécurité est unique (?) variant avec le temps, l'espace, le contexte (les derniers événements)
  - Dans un monde mobile, dans un périmètre il existe plusieurs politiques de sécurité qui se côtoient et vont rivaliser
  - Il faut protéger la vie privée
  - Compromis entre respect de la liberté de l'individu (CNIL) et sécurité du reste de la société

La politique de sécurité
dans les environnements spécifiques

- La confiance dans un monde de défense
  - Autorité centrale
  - Sujets habilités et droit d'en connaître
    - Niveaux de sécurité
    - Système multi-niveaux (MLS)
- La confiance dans le monde de la santé
  - Droit et devoir du médecin
    - Les médecins ne veulent pas diffuser l'information …
      - non pas que l'information soit nécessairement confidentielle, mais parce leur prestation pourrait être contestée (compétition entre hôpitaux, attaque possible devant la justice, etc)
  - Droit et devoir du personnel médical (infirmières, …)
  - Droit et devoir du patient
    - Les patients exigent de l'information qu'on ne veut pas leur donner …

La politique de sécurité spatio-temporelle

- La politique de sécurité en fonction du temps
  - Autorisation les jours ouvrés, entre 7 h et 20 h
  - Sur demande, le nuit ou les week-ends
  - Sur événement
- La politique de sécurité en fonction de l'espace
  - A la maison, au bureau, en déplacement à l'étranger
  - A l'extérieur chez un client, mais connecté au bureau
- Politique de sécurité dépendant de l'espace et du temps
  - Authentifier, autoriser un utilisateur en fonction de sa position, de sa situation
    - Du point de vue de l'utilisateur
      - Obligatoire
        - ➔ accès à un service selon un certain périmètre
      - Discrétionnaire
        - ➔ On restreint soi-même pour une certaine période l'utilisation de son portable : utilisable à partir de telle zone (configurée auparavant en secret avec son opérateur de télécoms ou son responsable de sécurité)
    - Du point de vue de l'interlocuteur
      - Création de protocole cryptographique pour sceller l'identité de l'utilisateur avec l'identité du lieu (de la station de base en GSM)
  - Notion d'état de l'environnement (paix, conflit, etc) vis à vis de la confiance
  - Notion de prise de risque plus ou moins élevée en fonction de l'état réel

La sécurité des réseaux et des systèmes d'information à l'ère numérique

Les tendances profondes
de l'informatique et des réseaux

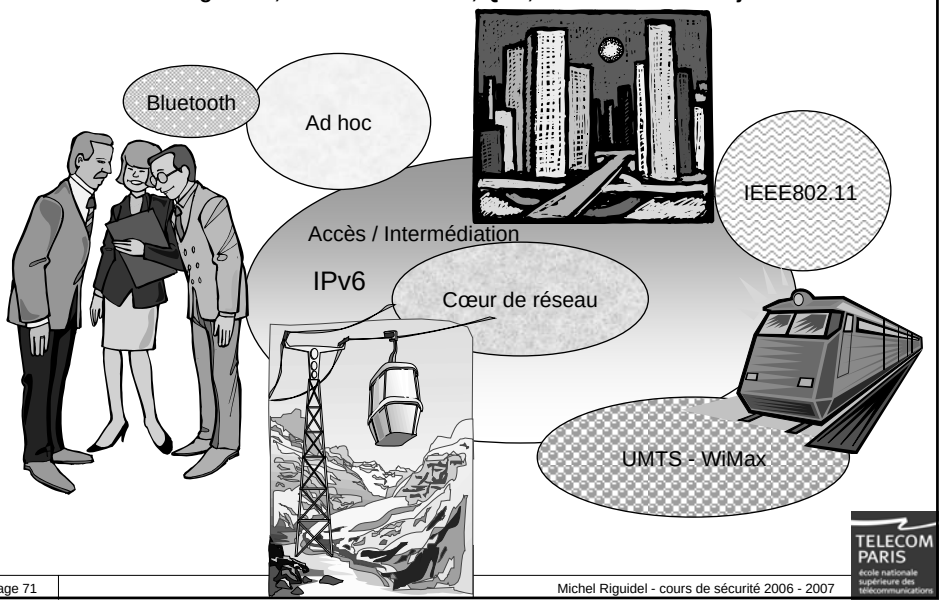
- Abandon de l'informatique à la Bill Gates
  - Toute l'information et toutes les applications sont sur mon disque dur
  - Les applications gargantuesques, engendrées par la Loi de Moore et la voracité de éditeurs de logiciels à versions, cancérisent les mips
  - Sentiment de sécurité (de possession ?)
- Utilisation du réseau pour l'interconnexion avec le monde et l'accès à l'information
  - Communiquer quand je veux avec qui je veux, où que je sois et télécharger la bonne et unique application configurée, personnalisée
  - La répartition spatiale est une vulnérabilité
- Utopie ou idéologie ou feuille de route : Ambiance, Informatique caméléon, Intelligence et ubiquité
  - Là où je suis
    - je vais récupérer l'information dont j'ai besoin, en toute convivialité
    - les applications, les contenus et les services vont se colorer selon mon contexte
  - L'intelligence des systèmes en support est une menace

Sécurité de l'urbanisation des systèmes numériques

- Il n'existe plus de systèmes isolés
  - Un système est plongé dans un milieu ambiant composé d'autres systèmes
    - La vulnérabilité de l'urbanisation : renseignement, observation
    - Les politiques de sécurité multiples
  - Transcender l'hétérogénéité ouverte
    - Nécessité de "roaming" vertical et horizontal
      - Le partage et la distribution des secrets à travers les frontières
- Le milieu numérique de la communication & du calcul
  - Informatique diffuse (objets déplaçables communiquant)
    - «pervasive computing»
    - Sécurité : sécurité du lien (couche 2) avec authentification mutuelle
  - Informatique de grille (nappe de calculs répartis à géométrie variable)
    - «Grid initiative»
    - Sécurité : Sécurité de la répartition, des intergiciels (bas de la couche 7)
  - Informatique mobile
    - radio cellulaires, réseaux ad hoc, réseaux spontanés
      - Sécurité gérée par un opérateur "juge et partie" : centralisée, totalement prise en charge sous le contrat client opérateur (carte SIM, etc)
      - Sécurité gérée par un service d'intermédiation : rétablir l'équilibre entre services et client
  - Informatique fixe (qui est parfois virtuellement mobile)
    - architecture d'égal à égal (Peer to Peer)
      - Sécurité des liens dynamiques entre acteurs
- Le Patrimoine numérique: la distribution des contenus
  - DRM (Digital Right Management)

Versatilité dans les réseaux d'accès

Hétérogénéité, Itinérance Globale, QdS, Services à Valeur Ajoutée

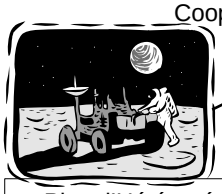


La construction sur la planète d'un milieu numérique urbanisé

- Urbanisation numérique des infrastructures, des architectures, des structures des TICs
  - Hétérogénéité à toutes les échelles de temps et de l'espace
    - Sécurité de bout en bout: difficile à gérer
  - L'expansion du monde numérique, l'effet d'échelle
    - La taille des édifices numériques et leurs interopérabilités font peur
    - Le diamètre de ce monde ne fait que croître
      - passage à des architectures moins fiables
        - ➔ Du client/serveur, puis intermédiation, puis d'égal à égal (P2P)
  - Gestion de la complexité et conduite du changement
    - Évolution selon les affrontements politico-économiques
      - tectonique des plaques Informatique (Intel-Cisco-Microsoft) - Télécoms (les Opérateurs) - Audiovisuel (Hollywood)
      - basculement de mondes "sûrs" (le téléphone, la télévision) vers le monde informatique à la réputation non sûre
    - Standards (protocoles, formats, …)
      - en retard par rapport à la technologie
      - absence de standards dans le marquage, les certificats, etc
    - Convergence lente mais inéluctable
- Naissance d'une Intelligence Ambiante
  - 3 entités sont en présence
    - L'environnement
    - L'intelligence ambiante
      - Murs, capteurs, actuateurs qui aident les systèmes et les individus à agir et évoluer
      - Équipements au service des individus
    - La cible de l'étude: le système informatique et son réseau
      - Le système n'est plus seul

Interconnexion globale « sans couture »

Hétérogénéité, Multimédia, macroMobilité



Enterprise

LANs

Interconnection of Local Networks

Telecom Operators & Internet

Internet Connections

Private

Cooperation

Cooperative Work

Remote Access

Mobiles

Public Networks Connections

Global Roaming

- Plus d'Hétérogénéité
  - Interopérabilité à travers différents réseaux
    - ✓ Pas d'espéranto : W-Corba, JavaRMI, J2EE, agents, … ne conviennent pas
    - ✓ M2M (middleware to middleware)
    - ✓ Sélectivité, Gestion de ressource, …

Évolution des paradigmes informatiques : vulnérabilité croissante

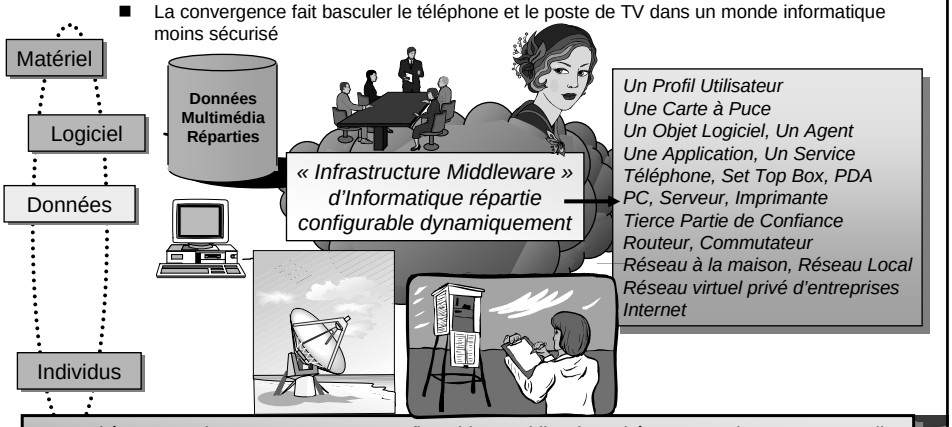
- Avant 1980 :
  - l'informatique appartient à des fiefs
- 1980: **Tout est fichier**
  - Instruments: Unix et Langage C (âge d'or des «informaticiens»)
    - Unix réunit matériel et logiciel
    - Un fichier: suite de caractères manipulables par le langage de programmation C
    - Une imprimante est un fichier (/dev/lpr), la Corbeille (/dev/null) aussi
- 1990: **Tout est document**
    - l'informatique pour toute l'entreprise
  - 1990: Sur le bureau (Microsoft)
  - 1995: Sur le réseau (Internet)
    - tout est document disponible sur le réseau, lisible par tous (HTML) ou exécutable partout (Java), pour le communicant
- 2000: **Tout est programme**
    - l'intelligence ambiante
      - Concept Jini : une imprimante est un programme Java (qui diffuse ses «méthodes Java» à ses proches voisins)
      - Réseau actif : un paquet IP a une entête qui est un programme Java qui s'exécute sur les routeurs du réseau
      - Architecture intentionnelle : un nom d'adresse est un programme qui va servir à la découverte
- 2010 : **L'architecture est un programme**

Évolution des paradigmes informatiques

- Avant 1980 : l'informatique appartient à des fiefs
  - Différence de J Von Neumann entre matériel et logiciel
  - Tout est parchemin ou feuille de calcul propriétaire, peu de flux
- 1980 : **Tout est fichier**
  - Un fichier : suite de caractères manipulables par le langage de programmation C
  - Une imprimante est un fichier (/dev/lpr), la Corbeille (/dev/null) aussi
  - Instruments: Unix et Langage C (âge d'or des « informaticiens »)
    - Unix réunit matériel et logiciel
- 1990 : **Tout est document**
  - recul de l'interopérabilité et de la transparence mais accessibilité aux non-informaticiens
  - l'informatique pour toute l'entreprise
  - 1990 : Sur le bureau (Microsoft)
    - Un disque dur est un tiroir où sont répertoriés des dossiers dans lequel résident des documents
    - Le monde de Microsoft : on perçoit par la fenêtre (Windows) de l'ordinateur le disque qui est à l'image des dossiers et documents sur le bureau
  - 1995 : Sur le réseau (Internet)
    - tout est document disponible sur le réseau, lisible par tous (HTML) ou exécutable partout (Java), pour le communicant
    - Internet : ce qui est sur le réseau est à l'image du disque dur qui est à l'image des documents sur le bureau
      - On appauvrit la sémantique (langage à balise HTML fruste) des documents (page html), l'architecture des systèmes d'information (un site Web est un ensemble de pages html que l'on feuillette) et des protocoles (http)
      - Privilège de l'accès à l'information : kiosque, serveur
      - Victoire de Java et XML : espérantos pour un langage de programmation et un méta-langage à balise
- 2000 : **Tout est programme**
  - Concept Jini : une imprimante est un programme Java (qui diffuse ses « méthode Java » à ses proches voisins)
  - Réseau actif : un paquet IP a une entête qui est un programme Java qui s'exécute sur les routeurs du réseau
  - Architecture intentionnelle : un nom d'adresse est un programme qui va servir à la découverte
- 2010 : **L'architecture est un programme**
  - Les ADL (Architecture Description Languages) sont exécutables

Le Paradigme de l'informatique ubiquiste

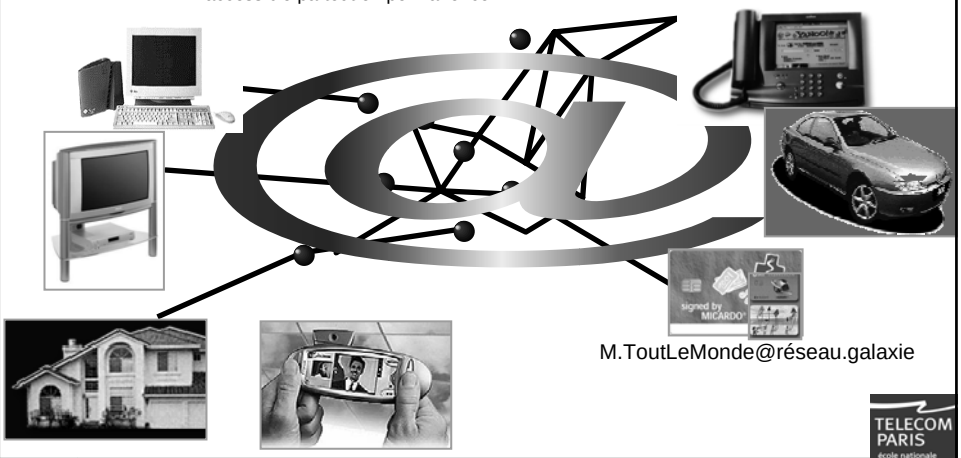
- Vers une Convergence Télécoms - Multimédia – Informatique
- Pour une Informatique mobile, configurable, sans couture, en zéro-administration dans un monde hétérogène
- La convergence fait basculer le téléphone et le poste de TV dans un monde informatique moins sécurisé



Des entités communicantes, autonomes, configurables, mobiles, branchées automatiquement entre elles autour d'une infrastructure interopérable, sécurisée, en Plug & Play, ajustable dynamiquement
Le Tout est managé de manière répartie par différents Acteurs, selon leurs divers points de vue

Le réseau, propice aux attaques (virus, saturation) ubiquité, « pervasive » computing (informatique diffuse)

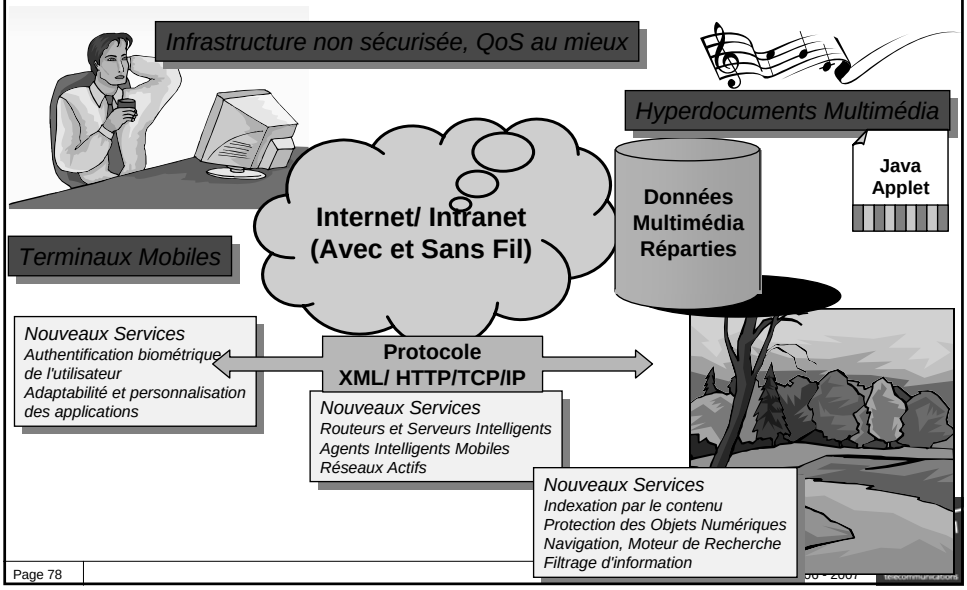
- Tout entité est connectée aux réseaux
  - Organisation et urbanisation du réseau de manière à s'articuler autour du réseau
  - Tous les objets numériques personnels (mobiles ou non) sont connectés à un réseau accessible partout en permanence



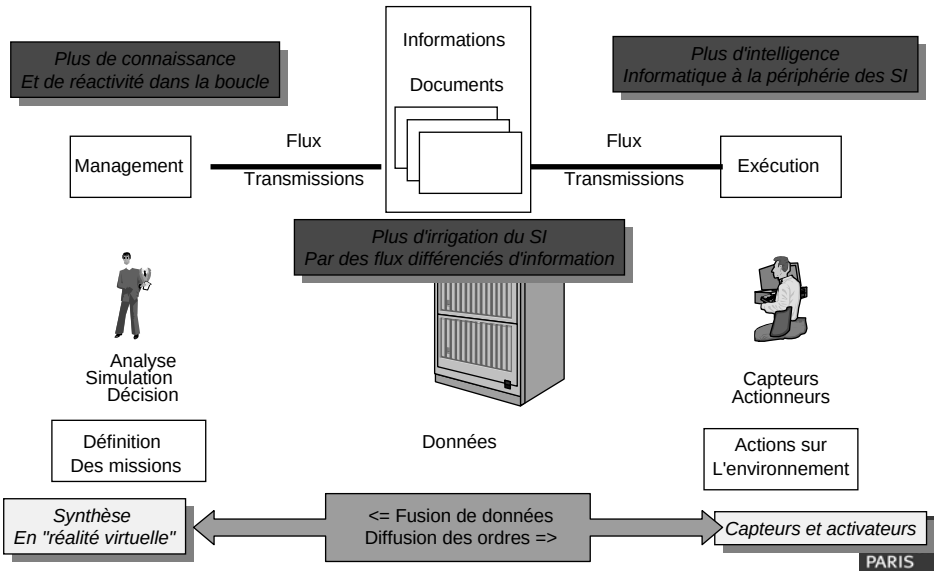
M.ToutLeMonde@réseau.galaxie

Infrastructure d'un Système Information

Intranet & Multimédia



Les Flux d'Information : Streams, DCN, Caches, …



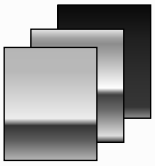
Monde numérique ouvert et/ou fermé ?

Ruban de Möbius

- Les systèmes sont devenus des rubans de Möbius !
  - Ils sont ouverts et fermés : pas d'intérieur, ni d'extérieur
  - Communauté ouverte et dynamique : des entrants, des sortants
- Le refuge du club fermé dans espace confiné au périmètre minimum
  - Site connexe
    - In vitro (pour éviter les fuites, les conséquences imprévisibles d'une expérience)
    - Coffre-fort à serrure savante : carte à puce avec un cœur de cryptographie
    - Cage de Faraday : silence électromagnétique
    - Bac à sable : Machine virtuelle Java, calcul inoffensif, interdiction de toucher aux fonctions essentielles de l'ordinateur
  - Sites non connexes
    - Tranchées numériques : VPNs pour rétablir la contiguïté du partage de l'information
- L'hospitalité des formes semi-ouvertes : le campus, la gare, le café, l'avion
  - Une communauté virtuelle semi-privée
    - Des permanents, des habitués, des gens de passage, des étrangers
    - Des entrants et des sortants
  - Coopération entre personnes aux politiques de sécurité différentes et avec des confiances mutuelles différentes
- La tolérance de l'agora, espace ouvert au cœur de la cité
  - Des anonymes, des "étrangers"
    - Serveurs Web
  - Situation différente suivant l'environnement
    - temps de paix, « vigipirate », « rue des snipers », …
    - objectifs de sécurité d'une entreprise (valeur, image de marque, …)

Les Systèmes à Logiciel Prépondérant :

l'architecture intervient dans tous les compartiments du SI

Diffusion & Accès	Nouvelles Couches OSI	Architecture Système
information & documents  Multimédia vidéo, image, code mobile, hyperdocument	coopération : télétravail, vidéoconférence, négociation temps réel applicatifs : configurables, téléchargeables distribution & services : Middleware, Corba & Code mobile communication convergence IP & ATM transmission : avec et/ou sans fil	performance sécurité répartition mobilité interopérabilité sûreté de fonct. maintenabilité

L'espace d'information : le fond ("logos") & la forme

La morphologie des systèmes et leur sécurité

- 1990 : Forme saillante
  - Ovoïde (cocon, forteresse, …)
    - Surface spécifique minimum
    - Partie privée importante: organe indépendant
    - Partie publique minimum: des contacts avec l'extérieur mais son «âme» est à l'intérieur
  - Fonction de sécurité
    - Politique de **contrôle d'accès**: protection maximum aux frontières du périmètre et pare-feu (contrôle des flux entrants et sortants)
    - Sécurité du type « ligne Maginot »
- 2000: Forme prégnante
  - Feuille, ramures, réseau capillaire
    - Surface spécifique maximum
    - Partie importante en contact avec l'extérieur: son «âme» est ailleurs
    - Infrastructure de communication: occupe un domaine maximum (un pays) avec un volume minimum (routes, voies ferrées, infrastructure GSM, ..)
  - Fonction de sécurité
    - Protection aux confluents par contrôle de flux, système d'écluses, audit, métrologie avec capteurs pour relever des mesures de terrain (systèmes de **détection d'intrusion**, mesure de trafic, …)
    - Sécurité du type « KGB » (chacun espionne l'autre)
- 2010: La poussière intelligente ("smart dust")
  - Autonomie des grains invisibles de technologie
  - Fonction de sécurité
    - **Traçabilité**: tagguer, surveiller

Complexité, Granularité des systèmes

- Conception et développement de nouveaux modèles de sécurité pour résoudre les problèmes de sécurité dans un monde ouvert à trois échelles d'espace :
  - 1. le milieu des très grands systèmes
    - administration nationale, transnationales, etc,
  - 2. le milieu de l'entreprise et/ou la personne morale et
  - 3. le milieu privé de la personne physique.
- La couverture des fonctions de sécurité en fonction de la granularité
  - Audit de la sécurité
  - Identification et Authentification
  - Communication
  - Protection des Données utilisateurs
  - Intimité ("privacy")
  - Protection et Confiance des fonctions de sécurité
  - Utilisation de ressources
  - Accès à la cible
  - Chemin de confiance

Les cibles selon la taille des infosphères : les édifices numériques

- Infrastructures transfrontières, fragiles, ouvertes à tout le monde
  - Aujourd'hui
    - Internet, infrastructure de téléphonie mobile, de diffusion de télévision numérique, les autoroutes de l'information
  - Dans le futur
    - e-X (commerce, justice, démocratie, vote, …)
  - Sûreté de fonctionnement et interdépendance
  - Sécurité souvent conflit avec le respect de l'anonymat
- La Protection des Infrastructures critiques en France (et en Europe)
  - Menaces
    - déni de service, (en général anonyme => Cyberterrorisme)
    - les attaques indirectes
  - Solution
    - Modélisation des systèmes complexes
    - Réduction des vulnérabilités par la robustesse
    - Gestion des crises
    - Définition de zone de survie, de mode de reprise, de modes dégradés
    - Surveillance et Justice planétaire?

Les cibles selon la taille des infosphères : les écosystèmes numériques, la personne morale

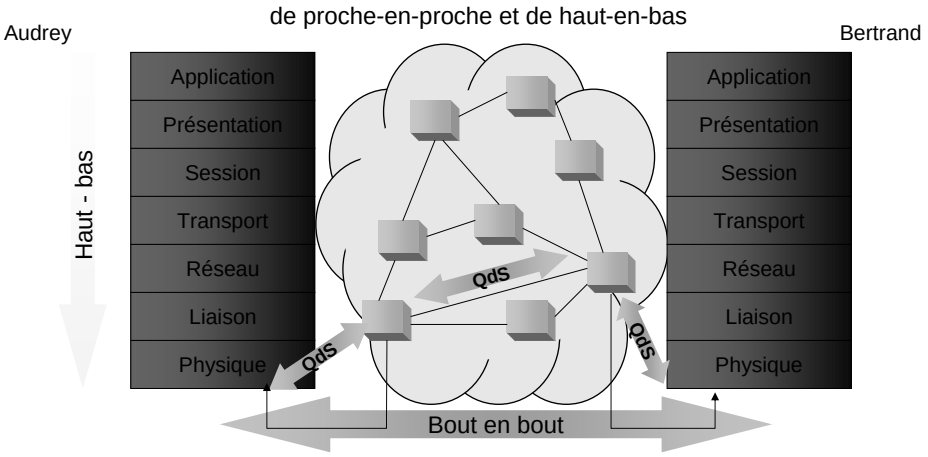
- Les écosystèmes numériques en réseaux (contenus et services)
  - Aujourd'hui: Business to Business, Business to Consumer, B2x
    - Sécuriser les entreprises multi-sites, les réseaux, les systèmes, les contenus
  - Demain: sécurité des applications et du business process
    - Entreprises à flux tendus
    - Les entreprises agiles
      - Adaptivité, contraire à la sécurité
    - Flottes de capteurs mobiles
      - Sécurité de la mobilité ou du nomadisme, difficile à mettre en œuvre
    - Communautés virtuelles, grilles
      - Fragile (déni de service)
      - Service d'intermédiation (tiers de confiance)
- La sécurité des écosystèmes
  - Menaces
    - Espionnage industriel
      - Guerre économique, intelligence économique ("kill xxx")
  - Solution
    - Système de renseignement, d'observation, de détection
      - Le contrôle minimum qui ralentit la configuration dynamique mais qui apporte un confort de fonctionnement
    - Système de détection d'intrusions installé en coupure sur les réseaux

Les cibles selon la taille des infosphères : l'individu physique et son attirail électronique

- Protéger la liberté de l'individu, sa vie privée, son intimité numérique
  - Confidentialité des données personnelles, de la localisation (mobilité)
  - Anonymat, pseudonymat
    - Préserver l'anonymat dans les achats, les déplacements, les activités
  - L'intimité numérique
    - Les données nominatives dans les différents fichiers (ses caractéristiques physiques, intellectuelles, morales, intimes, ses convictions politiques, religieuses)
    - Les traces de sa carte bancaire, de son téléphone portable, de ses connexions Internet
    - Messagerie électronique dans les entreprises
- La sécurité de la personne
  - Menaces
    - vis à vis de l'individu
      - L'atteinte à sa liberté, sa vie privée, son intimité
        - ➔ Écoutes et localisations illégales
        - ➔ Observabilité, Chaînabilité, Croisement des bases de données diverses
    - individu "pirate" vis à vis des autres individus
      - Profiter de la faiblesse des surveillances personnelles pour attaquer
  - Solutions
    - Sécurité souvent conflit d'objectif avec la sécurité des organisations (état, entreprise)
      - Entité de confiance personnelle (dispositif intelligent portable)
    - Biométrie
      - Identification de la personne

Les Couches OSI (modèle de Zimmerman)

de proche-en-proche et de haut-en-bas



- Du haut en bas et de proche en proche de Audrey à Bertrand
- Modèle à 7 couches : isotrope, pas de temps, pas d'espace
- Homologie des couches pour gagner l'interopérabilité des entités du réseau : gestion de l'espace – **génie logiciel horizontal**
- Ingénierie protocolaire : gestion du temps – **génie logiciel vertical**
- Moudre tout contenu en paquets, en datagrammes, en unités et finalement en bits
- Détruire la sémantique

L'ubiquité informatique

- L'ubiquité de calcul : couche 7 des applications
  - XML : métalangage pour trouver de l'interopérabilité
    - Permet de décrire des politiques, des intentions, d'interfacer des mondes hétérogènes, etc
  - Le métacalcul: Des nappes d'ordinateurs qui coopèrent (Le M2M, P2P)
    - Toboggan du 7ème étage : la socket : port + adresse IP
    - Il faut enrichir cette socket pour donner de l'épaisseur (QdS, Sécurité, Priorité)
    - Le génie logiciel horizontal : les intergiciels
      Au 7ème étage, les gens qui possèdent la sémantique s'agitent
- L'ubiquité d'accès : couche 2 des liens
  - Arrivée de l'Internet haut débit pour vaincre la fracture numérique
  - Dialectique des usages : construction d'un manteau d'Arlequin, d'un patchwork (Internet, GPRS, 802.11, 802.15)
  - Génie logiciel vertical
    - Au 2ème étage, les messagers qui transmettent les nouvelles s'agitent sur le perron (problème du dernier kilomètre ou du dernier centimètre, verrou de l'ATM, …)
- L'articulation des 2 ubiquités
  - IPv4 ou IPv6 ? Non pas seulement
- L'ubiquité du stockage (bientôt)
  - Delivery Content Network
  - Storage Area Network

L'écologie des réseaux

- Le prisme déformant de l'actualité
  - Internet
    - réseau d'accès à l'information, structurée en pages qu'il faut feuilleter
      - succès mais interconnexion trop rapide au détriment de la qualité, de la sécurité
  - Téléphonie GSM
    - infrastructure propriétaire pour un service unique : la voix
      - succès mais construction (trop) rapide d'une infrastructure
- Le tassement de la R&D
  - Essoufflement de l'IETF
    - Prisonnier de leur idéologie : « no votes, rough consensus and running codes, … »
  - Freins dans les télécoms
    - Trop de différences entre les rythmes
      - de modèles de rentabilité des entreprises et
      - de standardisation, déploiement des infrastructures
- Les besoins des utilisateurs
    - Avec la convergence, on est en train de remodeler le monde des communications
    - Accès à l'information, partage de la connaissance, mise au diapason, mise en communication, en coopération

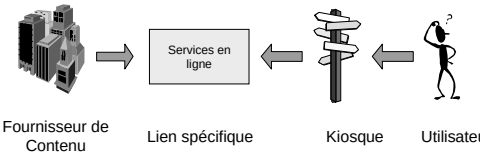
L'écologie des réseaux

Nature des interconnexions, contenus, nœuds
évolution spatio-temporelle

- Réseaux sociaux
  - Qui connaît qui => Réseaux virtuels privés
- Réseaux de connaissance
  - Qui connaît quoi => Gestion de la connaissance (knowledge management)
- Réseaux d'information
  - Qui informe quoi = > « à la Internet »
- Réseaux de travail
  - Qui travaille où => collecticiel (groupware)
- Réseaux de compétence
  - Quoi est où => connaissance dans l'espace et dans le temps
- Réseaux inter-organisationnel
  - Liens organisationnels => interopérabilité sémantique

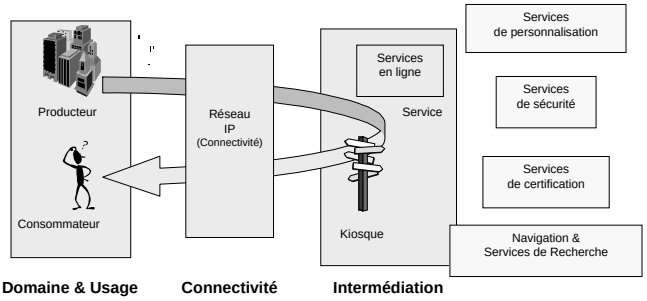
La Rupture de L'Internet du Futur

Modèle Traditionnel
Producteur - Consommateur



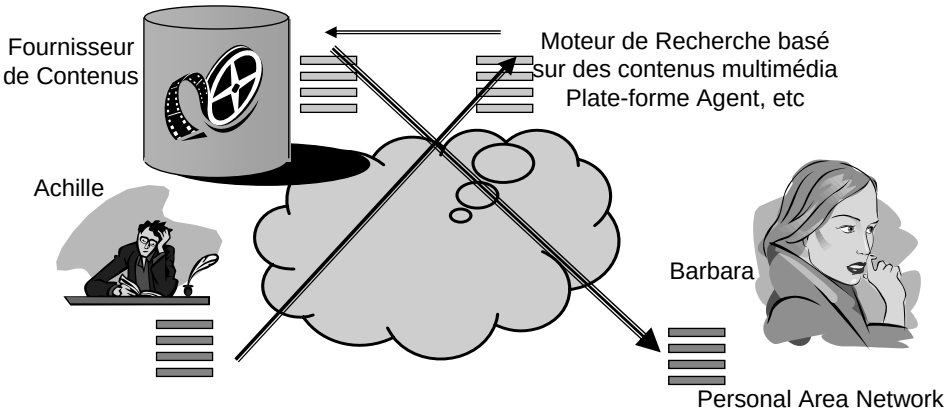
Nouveau modèle

Introduction d'un monde standard et d'Intermédiation



Nouveaux Services & Contenus

Intergiciels & Fournisseurs de services réseaux
Client –serveur => architecture d'intermédiation => architecture P2P



- Plus de Contenus : Contenus Riches et Contenus croisés
  - Voix sur IP, "QdS" temps réel, flux critiques, flux audio-vidéo
  - Traitement du contenu (recherche, découverte, …)

« QdS »

Des sphères gigognes
les différentes granularités

- La sphère privée de la personne physique : « privacy »
  - Corps humain : réseau biologique, prothèse numérique (dans le futur)
  - Mes objets personnels : carte bancaire, téléphone portable, assistant numérique, ordinateur personnel
  - Menaces & vulnérabilités
    - Utilisation frauduleuse de carte bancaire, vol de téléphone portable
    - Viol de l'intimité numérique (liberté, confidentialité)
    - Atteinte à l'intégrité: intrusion (virus, …)
  - Mes relations avec mes proches (famille, amis, collègues)
- La sphère privée de la personne morale : imputabilité, responsabilité
  - Intrusion dans les locaux d'une entreprise, dans le système d'information, …
  - Saturation malveillante de ressources
    - réseaux engorgés, serveurs à bout de souffle, imprimante avec gaspillage de papiers, télécopieur saturé, pare-feu ou détecteur d'intrusion enregistrant des événements anormaux truffant le disque
- La sphère ouverte des anonymes : renseignement, audit
  - Confiance a priori dans les citoyens, les contribuables, les usagers
    - Problème de la gestion des crises : perturbations sociales, terrorisme, …
  - Protection des infrastructures critiques
    - Interdépendances de ces structures géantes et fragiles
      - Informatique et électricité, Transport et Entreprises à flux tendus, …

La sécurité des systèmes : méthodologie

- Établir la bonne granularité
  - Identifier les **Ontologies** selon la politique de sécurité et le domaine (défense, santé, commerce)
    - En communication : session, circuit virtuel, paquet IP, etc
    - En informatique
      - Matériel: terminaux, station, routeur, fibre des réseaux,
      - Logiciel: logiciel de base, application, répertoire, fichier
- Statiques : diviser l'ensemble et protéger les parties
  - Identifier les **Sociologies**
    - La structure et l'architecture du système est la première chose à protéger
      - Décomposition en fragments, en domaines, en classes, en rôle, et politique pour chaque segment et contrôle aux interfaces
  - C'est l'irrigation du système qui crée la vulnérabilité (protocoles, données en transit)
- Mobiles et/ou Configurables : maîtriser le mouvement
  - Identifier les **Éthologies**
    - Il faut protéger la configurabilité : le mouvement et les états de transition

Les nouvelles menaces

Les nouvelles menaces et vulnérabilités

- Les attaques
  - Sur l'individu
    - Quelques attaques au hasard sur l'individu lambda
    - Les attaques de masse sur l'individu standard
      - Téléphones portables, cartes bancaires, (bientôt PDAs) : fraude (racket,…)
      - Ordinateurs : endommager les contenus (Virus) et contrarier l'activité normale
  - Sur l'entreprise et l'État
    - Le cyberterrorisme, plutôt du côté de l'état, de l'entreprise
    - L'intelligence économique
    - Embargo économique sur des versions de matériel, de logiciel
- Le statut des pirates
  - Vénérable : déférence vis à vis de l'attaquant ludique
  - Imperturbable : difficulté d'influencer l'attaquant / défenseur idéologique
    - Il considère son risque comme nul
      - Kamikaze / Bouclier humain : la vie ne vaut rien devant la "valeur" de la cible ou la cause qu'il défend
  - Mafieux : organisation clandestine des cyberpirates en réseaux furtifs mobiles, réfugiés dans des paradis numériques
    - Cyber-attaques massives prévisibles
    - Sites idéologiques (intégrisme religieux, racisme)
- L'éthique des contenus
  - Existence et Accès
    - Contenus pour adulte (sexe, violence, …)
    - Contenus illicites (racisme, pornographie, …)
  - Filtrage et Classement (rating, contrôle parental)

L'Après 11 septembre 2001

Avant : les pirates – les corsaires
- Attaque discrète pour obtenir un gain tangible **(marchandise)**
- Sécurité en relation avec la valeur/sensibilité à protéger

Après : cyber-guerre / violence - terrorisme
- Attaque vitrine sur des **symboles** visibles
- Perte de confiance de l'ensemble de la communauté
  - Attaque sur le sens et les valeurs
- Déni de service des réseaux pour rompre le nerf de l'économie

- Nouvelle sécurité : la résistance
  - Défense & Anticipation & Dissuasion
  - Protection des grandes infrastructures

La nouvelle situation: plus de dissuasion

- Autrefois
  - Attaque non détectable, discrète, pour gagner ou mettre en péril le bien d'autrui
  - Sécurité : Gestion du risque
    - Coût de la sécurité en rapport avec la valeur ou la sensibilité du bien
      - La sécurité contrecarre le péril sur les biens
      - La protection est en rapport avec le risque de perdre le bien
- Aujourd'hui
  - Les nouvelles menaces
    - les attaques fréquentes et faciles
      - déni de service pour rompre le nerf de l'économie (les réseaux)
    - les attaques inédites
      - préparer la guerre de l'information : on attaque directement le sens
    - les attaques gratuites
      - déstabiliser, faire perdre confiance à l'ensemble de la communauté
    - les attaques symboliques (et médiatiques): spectacle
      - attaques de vitrine (visibles) : le gain est au niveau du symbole
        - Tours du World Trade Center, entarter un personnage connu devant des caméras de télévision
        - Pénétrer dans un réseau avec retentissement, altérer un site Web, …
  - Sécurité
    - nécessité de revenir à la sécurité de base: audit (mesure, renseignement informatique), imputabilité (authentification)

L'état des lieux de la sécurité

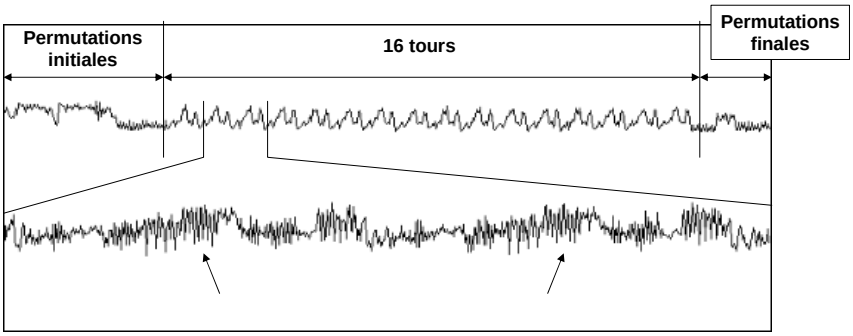
La crise
Les problèmes
Les percées potentielles
Les dérives à l'horizon

La crise de la sécurité

- Le manque de confiance dans la société de l'information
  - L'usage n'est pas passé dans les mœurs
    - La relation physique garde son importance dans le contact, les échanges et le commerce (échec relatif du e-commerce, du e-travail, etc)
    - Ne pas confondre
      - confiance dans les échanges et sécurité des paiements électroniques
    - Comment se sentir à l'aise dans un monde virtuel?
      - monde technologique, anonymat, virtualité de la géographie
  - Même avec une fibre optique au perron de porte des foyers domestiques et des PMEs, la fracture numérique existe : générationnelle, sociale, géographique
    - Comment faire des affaires dans un monde virtuel?
  - La sécurité du matériel vacille
- Les technologies existantes ne se diffusent pas
  - La signature électronique a du mal à s'implanter
  - Les PKIs (IGCs) ne prospèrent pas (trop compliquées, pas interopérables, pas de confiance supplémentaire, difficilement évaluables)
  - La carte à puce ne se répand pas en dehors de la France (hormis la carte SIM du GSM)
    - Difficultés des fabricants de cartes à puce
  - Comment sécuriser l'informatique répartie?
  - Donner une structure conceptuelle, nouvelle à la sécurité
    - en dehors de la sécurité du client serveur (Alice & Bob qui communiquent, cryptographie classique, SSL)
- Les technologies récentes ont du mal à s'enraciner
  - Certificats: SPKI
  - Heuristique: Protection de cd-roms
  - Usage de la Biométrie

La carte à puce : un coffre translucide

- Calcul DES sur carte à puce
  - Extraction d'une clef secrète en quelques heures avec un équipement standard



R Pacalet ENST

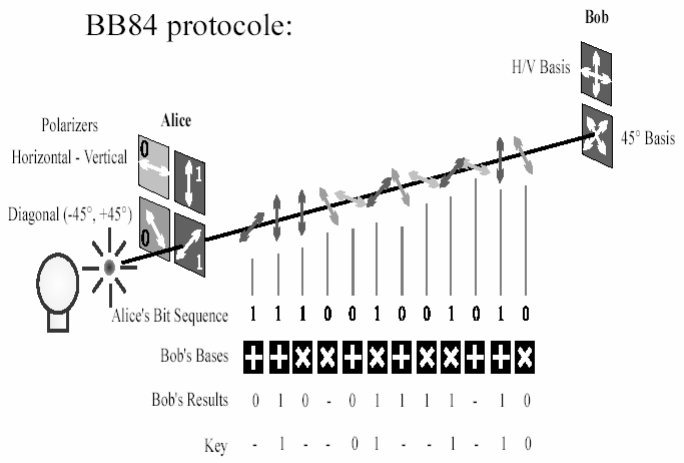
Les facteurs de vulnérabilité des systèmes

- La complexité
  - Les ontologies et leur structuration
  - L'hétérogénéité
    - La taille, le nombre et la diversité des acteurs, des entités et des actions
  - L'architecture
    - la sémantique et la forme des composants et des liens, à toutes les échelles
    - Les différents styles canoniques ont des vulnérabilités intrinsèques
  - Le virtuel (l'abstraction)
    - La fabrication de simulacres numériques pour fonctionner comme si c'était réel (machine, réseau, système d'exploitation, entreprise, …)
- La répartition
  - L'ouverture
  - La scalabilité
  - Les protocoles et les échanges
- La sensibilité
  - La valeur tangible
  - L'image de marque (agression symbolique, médiatique)
- Le mouvement
  - La mobilité
  - La configurabilité

La communication quantique

- Cryptographie quantique (Université de Genève)
  - La sécurité de la cryptographie quantique est basée sur les fondements de la physique quantique
    - Pour espionner un "canal de communication quantique", Ève doit effectuer des mesures sur des quanta individuels (pulses à un photon)
      - Mais, la mécanique quantique dit
        - toute mesure perturbe le système quantique
        - Ainsi, "lire" le "signal quantique" réduit la corrélation entre les données d'Alice de Bob
      - Alice et Bob peuvent donc détecter l'intervention de toute tierce personne en comparant (à l'aide d'un canal de communication classique) un échantillon de leur "signal quantique"
    - Le "canal de communication quantique" n'est pas utilisé pour transmettre un message (information), seule une "clé" est transmise
      - S'il s'avère que la clé est corrompue
        - Alice et Bob l'ignorent tout simplement (pas de perte d'information)
      - Si la clé passe le test avec succès
        - Alice et Bob peuvent l'utiliser en toute confiance
      - La confidentialité de la clé est contrôlée avant que le message ne soit envoyé
- Infrastructure quantique : réseau quantique de confiance
  - État de l'art en 2007
    - Échange de photons à débit lent sur des dizaines de km (expérience sous le lac Léman)
  - Projet intégré au 6ème PCRD (Secoqc)
    - Réseau de confiance (participation ENST pour l'infrastructure du réseau)
- Perspective: rupture en sécurité
  - La fabrication des secrets est aujourd'hui centralisée
  - L'infrastructure sécurité serait alors largement réticulaire et décentralisée
    - Distribution de secrets à la porte des utilisateurs finaux
    - Application dans les télécoms pour atteindre les utilisateurs par capillarité

La cryptographie quantique



Université de Genève

Les dérives potentielles des solutions universelles fermées de sécurité

- L'inquiétude sur l'identification universelle des PCs : L'inquisition, "Big Brother" de retour …
  - **TCPA (Trusted Computing Platform Alliance) / TCG**
    - Intel, IBM, …
    - La puce Fritz sur les Pentium IV après la tentative échouée de tatouage des Pentium III
  - Projet Microsoft Palladium / Microsoft Passport
    - Entité de confiance intégrée et scellée à l'ordinateur Intel-Windows
      - Identifier une machine par une puce (Fritz) contenant des clés de chiffrement
      - Module logiciel intégré dans Windows pour créer une zone de confiance
      - Signature numérique de logiciels "dignes de confiance"
        - Gestion de droits (DRM) avec des serveurs tiers
      - Contrôle d'accès obligatoire
        - Document étiquetés "secret"
    - Perte du contrôle de sa machine par l'utilisateur
  - Mort annoncée de la carte à puce européenne
    - Généralisation sur les PDAs, les portables téléphoniques
  - Fin de la "menace" du logiciel libre et Linux pour B Gates
- L'identification universelle IPv6
  - Adresses fixes : comment les rendre confidentielles pour éviter le harcèlement ?
  - Adresses permanentes ("toujours connecté")
- Trouver le bon compromis pour les entités intangibles
  - entre le "bourgeois bohémien", le "SDF nomade hors la loi" et "l'esclave moderne"
    - Être correct éthiquement et politiquement sans perdre son libre arbitre
      - Choisir sans obligation des standards vraiment ouverts sur des infrastructures libres
    - Être clandestin, sans papier et sans abri
      - PC autonome avec adresse intermittente (possibilité de chaparder des fichiers MP3, …)
    - Être esclave et subordonné à un monopole propriétaire fermé
      - Terminal personnel lié à l'infrastructure imposée par le monopole, à la merci de ceux qui le "manipule"
- Rétribuer loyalement les ayants-droits
  - Droit sur les copies (copie privée, une fois, plusieurs fois, …)

La cryptologie

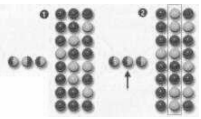
- Chiffrement symétrique
  - L'AES et ses suites
  - Haut niveau de sécurité, vitesse, coût faible
- Chiffrement asymétrique
  - Amélioration
- Chiffrement du haut débit
  - Gigabit/s
- Applications
  - Les protocoles cryptographiques
  - Les produits grand public
    - sur les entités de confiance personnelles
      - Authentification
      - Paiement universel, transaction mobiles sécurisées, micro-paiement
    - Protection des droits (DRM, …)
  - Sécurité des réseaux

La stéganographie, le tatouage

- Tatouage Multimédia
  - Faiblesses et failles dans les technologies de tatouage
    - Limites théoriques du tatouage multimédia
      - Voix, son, image fixe ou animée, document audio-visuel, graphiques
    - Difficultés
      - Résistance à la compression, à la transformation géométrique
      - Robustesse du marquage dans la chaîne de distribution
      - Nombreux algorithmes dépendant
        - ➔ de la nature: MPEG2, MPEG4, images JPEG, dessins 2D/3D, …
        - ➔ du contenu esthétique et de sa perception
        - ➔ humaine via les yeux ou oreilles ou
        - ➔ machine via des algorithmes de traitement de signal (lessivage des tatouages,…)
  - Intégration et industrialisation dans les DRM
    - Absence de standards et d'infrastructures générales
    - Nécessité de coupler stéganographie, cryptologie et PKI
  - Dialogue nécessaire entre académiques, industriels, pouvoirs publics, opérateurs
    - Verrouillage d'Hollywood et mésentente des industriels du multimédia
- Autres tatouages
  - Tatouage sémantique de texte en langage informatique
    - Tatouage et signature sémantique de logiciels (ENS, ENST)
    - Marquage de puce informatique (IPR des SoCs)
  - Tatouage d'architectures ou de textes structurés
    - Marquage de séquences de paquets protocolaires IP (pare-feu, etc)

Promesses de nouvelles ruptures

- Le XXIème siècle sera sans fil et mobile (2010)
  - Les objets communiquant dans des Ambiances Intelligentes
  - L'informatique omniprésente et enfouie (envahissante?)
  - Les grilles de calcul, de contenus, de communication
    - Danger : le syndrome des robots et de l'apprenti-sorcier
- Le XXIème siècle sera quantique (2020) : intrication, téléportation
  - L'informatique quantique (David Deutsch, 1985), la communication quantique
  - Décadence des transistors, des 0 et 1, des pixels, des lignes de télévision
    - Retour des grains de la photo et arrivée des photons
  - Le règne de l'incertitude (qubit : 0, 1, 01, 10) et de la décohérence
    - L'incertitude d'Heisenberg nous rassure
    - Le quantique pourrait contrarier la cryptographie (Peter Shor, 1994)
    - Attaque : gerbes venimeuses de photons, ouragan quantique …



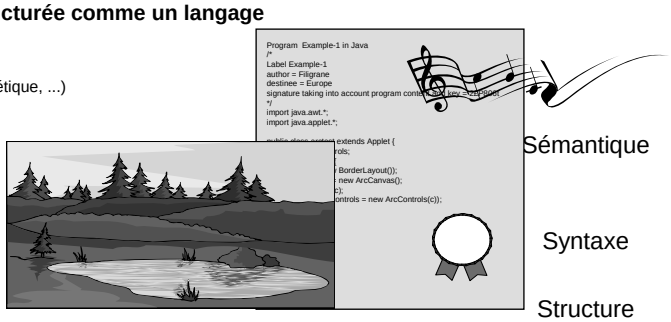
- Le XXIème siècle sera nano-technologique et génomique (2020)
  - La société de l'information fait place à la société nano-industrielle
  - Ingénierie du vivant (clone, culture des cellules) et du nanoscopique
  - La marchandise numérique intangible de Turing et Shannon est remplacée par du nano-matériel à l'échelle des molécules (machine mécanique, …) et du nano-vivant à l'échelle de l'ADN
    - Danger : le mythe prométhéen de Mary Shelley (1818)
      - Frankensteins lilliputiens clonés
    - Sécurité et confiance dans des machines invisibles
      - Tagguer et tracer les éléments

La sécurité des réseaux

La sécurité, c'est l'art de partager un secret

Elle est structurée comme un langage

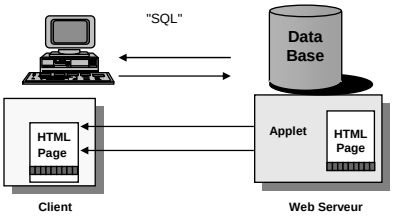
- Document
  - contenu (discours, esthétique, ...)
    - certification
  - Structure
- Route
  - hétérogénéité
    - protocole
    - management



Sémantique

Syntaxe

Structure



Architecture

Pragmatisme

La sécurité des contenus dans un monde en clair

Tatouage et Traçage des objets numériques

Les sanglots longs
des violons
de l'automne
bercent mon cœur
d'une langueur
monotone

```
Program  Example-1 in Java
/*
Label Example-1
author = Filigree
destine = Europe
signature taking into account program content and key = 2EP806t
*/
import java.awt.*;
import java.applet.*;

public class arctest extends Applet {
   ArcControls controls;
   public void init() {
      setLayout(new BorderLayout());
      ArcCanvas c = new ArcCanvas();
      add("Center", c);
      add("South", controls = new ArcControls(c));
   }
...
end
```

La sécurité des réseaux

- Babelisation des réseaux : Internet, GSM, etc
- Qui est à l'extrémité du réseau ?
  - Est ce que le protocole fait confiance à l'émetteur ?
  - Adresse des réseaux peuvent être contrefaites, maquillées
- Est ce que quelqu'un écoute, espionne (eavesdropping) ? beaucoup de technologies de diffusion
  - Des stations sur le réseaux peuvent surveiller le trafic, capturer le trafic et l'analyser
  - Les réseaux sans fil : avec le fil, il faut être connecter physiquement avec une ligne (fibre), ce n'est plus le cas avec le sans fil (802.11)
  - WAN : satellite, micro-onde qui est gérée par d'autres organisations (mise sur écoute – wiretapping)
    - D'où le problème de confidentialité des réseaux
- La saturation des réseaux
  - empêcher les gens de travailler

La place du marché

- Une réunion avec unité de lieu, de temps et d'action
- Des individus en chair et en os sont présents avec des marchandises tangibles et de la monnaie sûre et convertible

Acheteur
Vendeur
Banquier
Notaire

Échange
Transfert
Transaction
Interactivité

La confiance est donnée (ou non) in vivo

La définition de la confiance : une relation binaire

- La confiance est une variable
  - Non réflexive : ⌉(a ℜ a)
    - Attention
      - aux menteurs « faites moi confiance »
      - aux hâbleurs : « j'ai confiance en moi »
    - Un logiciel ne peut prouver seul son immunité ou son bon fonctionnement
    - A la racine, c'est souvent une haute autorité qui instille la confiance (conseil de l'ordre, Administration, …)
      - DCSSI : certification de systèmes selon les critères communs
      - Défense : habilitation suite à des enquêtes de voisinage
  - Non symétrique : a ℜ b #> b ℜ a
    - Alain fait confiance à Bénédicte mais ce n'est pas réciproque
  - Non transitive : a ℜ b et b ℜ c #> a ℜ c
    - « les amis de mes amis ne sont pas toujours mes amis »

La confiance est un treillis
une relation d'ordre partiel

- En règle générale
- on ne peut pas comparer deux politiques de sécurité
  - Exemple: filtrage sur un pare-feu, …
- Parfois il est possible de dire :
- « j'ai plus confiance en A qu'en B »
  - A ou B est une personne, un groupe de personnes ou une application informatique
    - preuve mathématique à partir d'un modèle formel
    - preuve statistique à partir de multiples expériences
    - preuve par parrainage: "des entités dignes de confiance m'ont certifié que je pouvais faire confiance à A«
  - "la politique de sécurité P1 est plus sévère que P2"
    - preuve à partir d'un modèle

Le huis clos : *la confiance de « droit divin »*

- milieu confiné
  - on est «à l'abri»
- toutes les informations pertinentes sont présentes
  - on peut distinguer les informations publiques des informations privées

- la confiance est intrinsèque
  - elle est décrétée par une instance supérieure (Administration)

- En général, un Système d'Information très protégé est de ce type
  - Cage de Faraday, Carte à puce
  - Bac à sable : « Sand box model » en Java
  - Antivirus : "Quarantaine"

L'éther : *« la confiance perdue »*

- le milieu est infini
  - on est "à découvert"
  - Internet, monde gratuit
  - avec une idéologie libertaire où cipherpunks, hackers naviguent dans un cyberespace
  - où on peut être anonyme et être placé virtuellement

- toutes les informations pertinentes ne sont pas "sous la main"
  - il faut surfer pour les trouver, les filtrer, les authentifier et quantifier leur degré de vérité
- la confiance n'est pas établie a priori
  - la confiance est perdue (chevaux de Troie des éditeurs de logiciels, ...)

- Les secrets de Polichinelle
- La confiance est rétablie par des tranchées numériques
  - VPNs, Tunnels

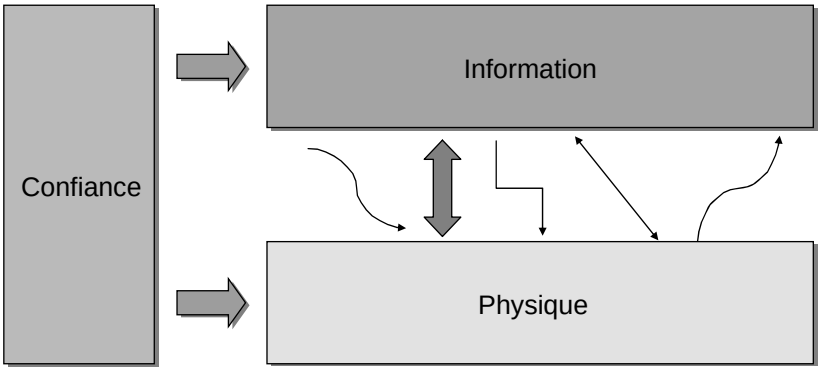
Le négoce : *« la confiance mesurée »*

- le milieu est hétérogène mais hiérarchisé en grappes
- les informations pertinentes sont dans leur propre environnement et à l'extérieur
- la confiance est une variable qui se mesure rationnellement avec vigilance à tous les instants
- la confiance est répartie et inter opérable (Tiers de Confiance, ...)

- une politique de sécurité variable dans le temps et l'espace existe et est configurable: $P = f_m(t,x)$
- la politique est ajustée en fonction des menaces, des vulnérabilités résiduelles et de la valeur des biens à protéger
- les politiques sur les différents sites sont négociées, médiatisées par des agents intelligents authentiques
- le risque est maîtrisé

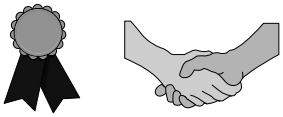
La Place de Marché Virtuelle :
rétablir la confiance

- La confiance doit lier les deux plans physique et logique

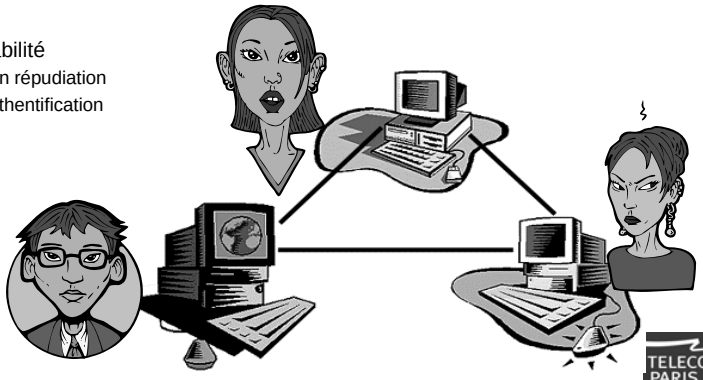


La sécurité des communications en réseau

- Un réseau d'acteurs capable de communiquer, transférer, échanger des objets (informations, documents, flux, opérations et ordres)

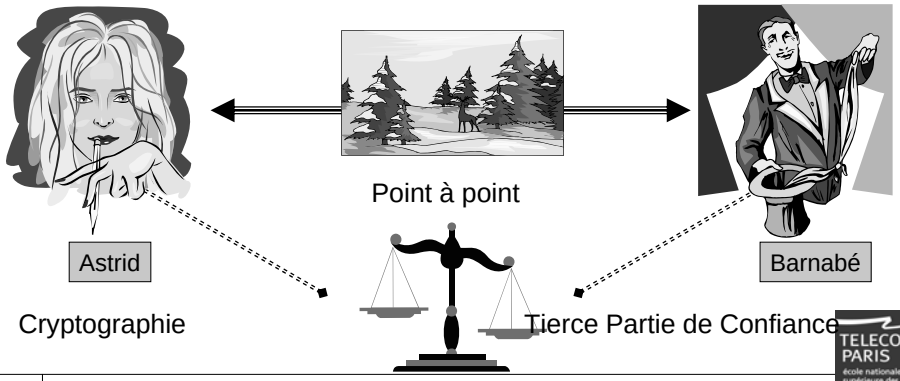


- Imputabilité
  - non répudiation
  - authentification



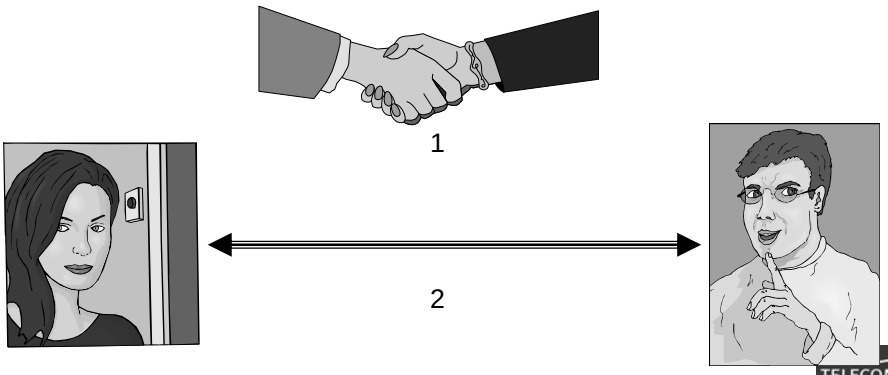
Claude Shannon (1916 – 2001) :
la théorie de la communication (1948)

- Les protocoles cryptographiques
  - SSL, IPSec
- Les infrastructures à clés publiques, les certificats (X509), pare-feu
- Le modèle de sécurité de la cryptographie peut être utilisé
  - Astrid et Barnabé partagent un secret pour
    - Chiffrer un message (cryptographie)
    - Incruster une marque subliminale dans un contenu afin de laisser une trace (tatouage)



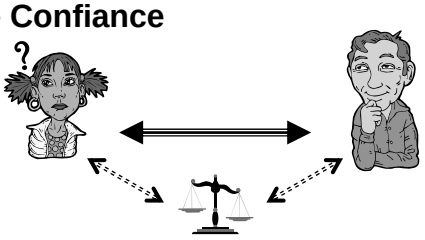
Scénario 1 : La Cryptographie symétrique

- Audrey et Basile se connaissent
  1. ont une réunion préalable et s'échangent un secret
  2. communiquent entre eux de manière sécurisée

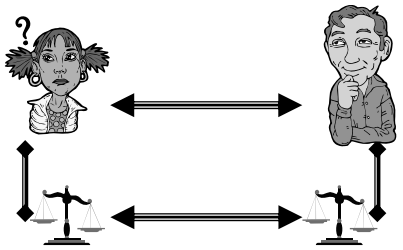


Scénario 2 : Le Tiers de Confiance

- Achille et Bérengère ne se connaissent pas
  - Tiers de Confiance
    - Achille et Bérengère font appel à un tiers Colin



  - Tierces Parties de Confiance interopérables
    - Achille fait confiance à Agathe
    - Bérengère fait confiance à Bertrand
    - Agathe et Bertrand se font confiance mutuellement



Scénario 3 : La Toile de Confiance se tisse

- Astrid & Boniface ne se connaissent pas mais vivent dans des sphères qui se croisent
  - Fabrication d'un réseau de confiance, non centralisé
    - lettre de recommandation, parrainage, etc.
- PGP (Pretty Good Privacy - Zimmermann)
  - Astrid a beaucoup d'amis, en particulier Charles
    - Boniface connaît Charles
  - Boniface a beaucoup d'amis, en particulier Chloé
    - Astrid connaît Chloé
  - Astrid va envoyer du courrier avec des signatures électroniques de Charles
  - Boniface va envoyer du courrier avec des signatures électroniques de Chloé
  - Au fil du temps, Astrid gagnera la confiance de Boniface

Scénario 4 : La Cryptographie asymétrique

- Arthur ne connaît pas Blandine, Céline, Delphine, Élodie

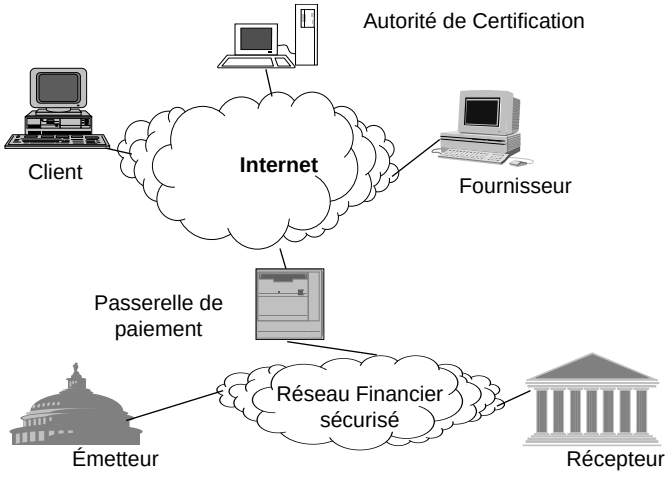
- Cryptographie asymétrique
  - Arthur protège sa clé privée
  - Arthur publie sa clé publique
  - Blandine, Céline, Delphine, Élodie, … enverront une clé secrète chiffrée par cette clé publique à Arthur

Autres Scenarii

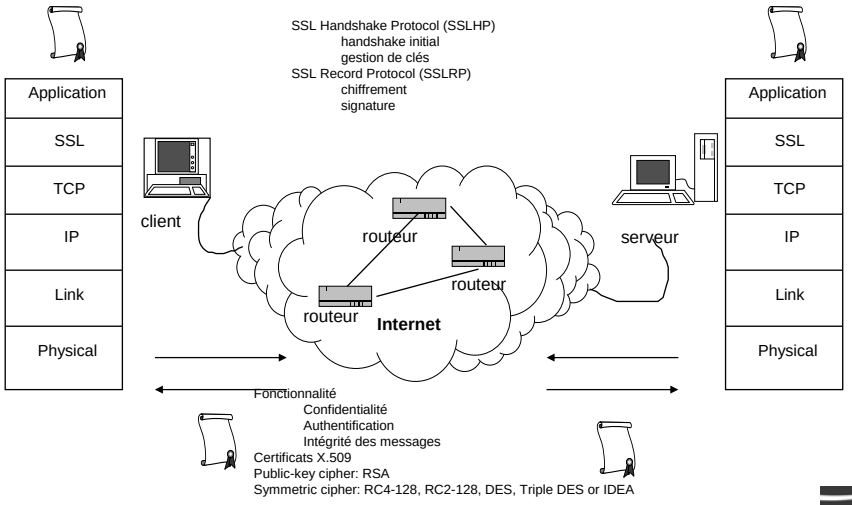
- Scénario 5 : Monde Fermé de gens qui se connaissent
  - Protocoles cryptographiques à inventer

- Scénario 6 : Monde Ouvert de gens qui ne se rencontrent que sur le réseau
  - Protocoles cryptographiques à inventer

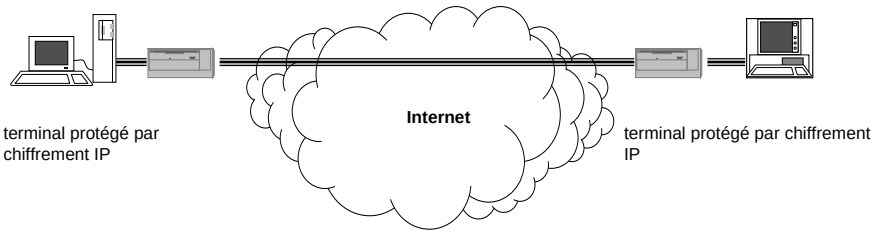
Modèle fonctionnel SET



SSL : Secure Socket Layer

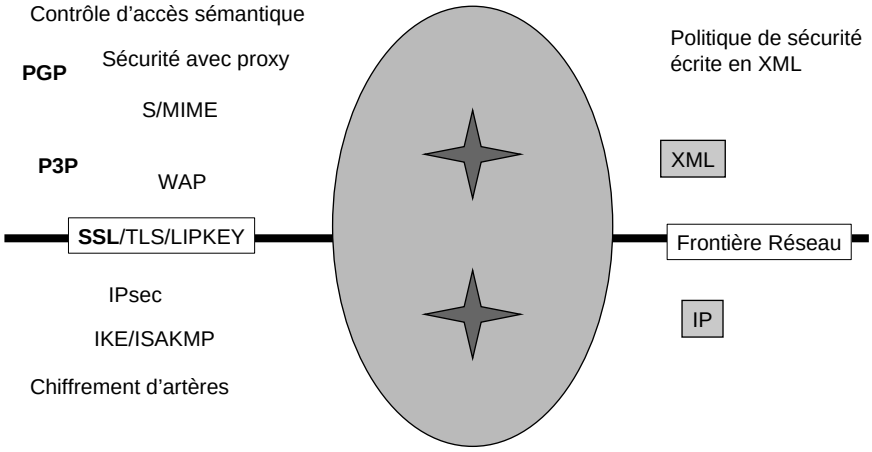


VPN, Tunnels, Chiffreurs IP



- Un VPN (Virtual Private Network) ou réseau virtuel privé est un moyen de simuler un réseau privé sur un réseau public comme Internet.
- Un VPN crée des connexions temporaires ou tunnels entre 2 machines, ou une machine et un réseau, ou 2 réseaux.
- Protection du transfert de données

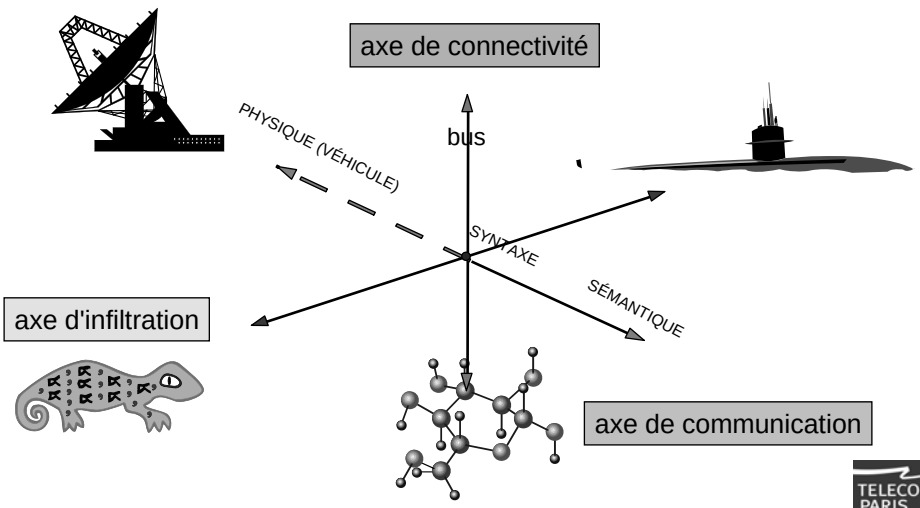
Les Solutions de Sécurité



- Beaucoup de solutions standards, d'utilisation souvent complexe
- Un protocole n'élimine pas toutes les menaces

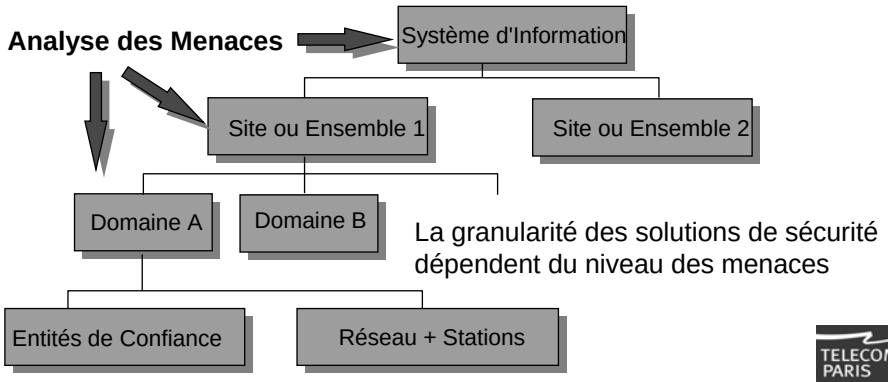
La sécurité des architectures

Les Dimensions d'Attaque / Défense d'un Système



Principe de cloisonnement en sécurité

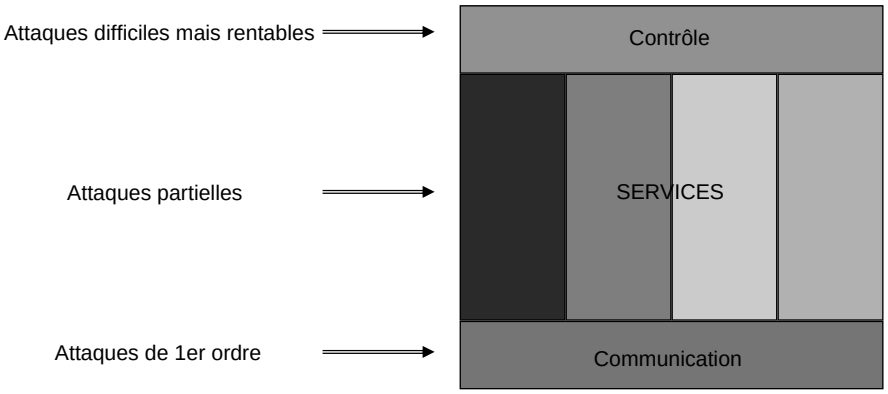
- Segmenter le SI en composants de sécurité homogène (domaines de confiance mutuelle)
- Contrôler l'accès des flux d'information échangés entre les composants (en respectant la politique de sécurité en vigueur)



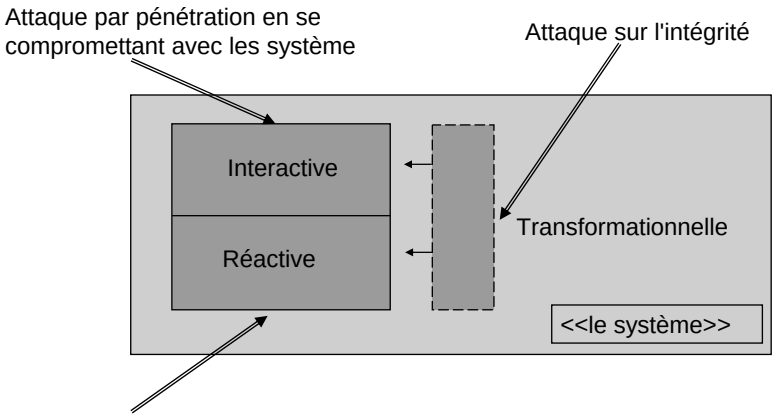
La granularité des solutions de sécurité dépendent du niveau des menaces

Les sous-ensembles d'un système

Structures d'un réseau et de ses équipements



Les sous-ensembles d'un système



Systèmes à logiciels prépondérants

- Validité
  - le système est utilisable et fait ce qu'on attend de lui
- Robustesse
  - même dans des conditions anormales
- Coût
  - et ce, pour un prix que le client peut et veut bien payer
- Extensibilité
  - le système est adaptable facilement aux changements de spécifications (simplicité de l'architecture, décentralisation, modules autonomes) => conception
- Réutilisabilité
  - une partie du système peut s'expatrier => bibliothèque de composants
- Compatibilité
  - le système peut être combiné avec d'autres => protocoles d'accès standard
- Efficacité
  - bonne utilisation de l'énergie informatique
- Fiabilité d'utilisation
  - accueil favorable de l'utilisateur
- Interopérabilité
  - intégration dans l'univers propre de l'utilisateur (système ouvert)
- Administrabilité
  - intégration dans l'univers organisationnel du client
- Vérifiabilité
  - bonne préparation de procédures d'acceptation et certification
- Évolutivité
  - adaptation à l'évolution informatique (hw & sw)
- Maintenabilité
  - adaptation à l'épreuve de la durée
- Intégrité
  - bonne protection des composants

Exigences d'un système & Architecture

L'Architecture est l'expression des contraintes sur les exigences

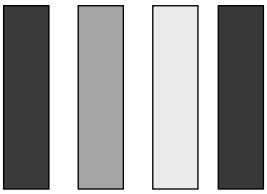
spécification

- les exigences fonctionnelles
  - F1, ..., Fn
  - performance (espace, temps)
- les exigences non fonctionnelles
  - sur la cible
    - E1, ..., Ep (SdF, interop., ...)
  - sur la fabrication de la cible
    - D1, ..., Dq (délai, coût, ...)
- les contraintes
  - les adhérences avec l'existant et l'environnement
    - patrimoine (ré-ingénierie, réutilisation)
    - COTS

architecture

- les composants
  - matériel ou logiciel ou données
  - C1, ..., Cn
- les liens (ou connecteurs)
  - L1, ..., Lp (p < n^2)
- les contraintes
  - flexibilité de F1, F2
  - indépendance de C1 et C2
  - disponibilité de F4
  - évolutivité de L3
  - L1 à L4 respectent les standards

Les Architectures

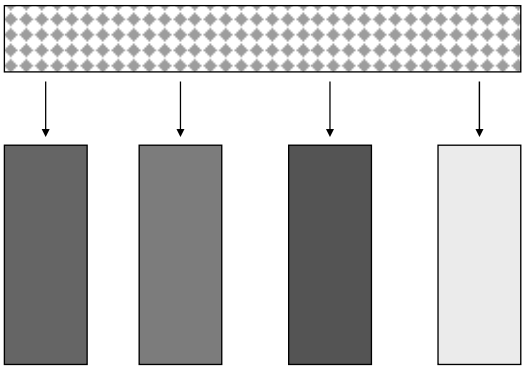


architecture en tranches :
services utilisateurs
ergonomiques (=> standard)
flexibles (=> modularité)
interopérable (=> protocole multimédia)

architecture en couches :
services de communication
interopérabilité (=> homologie)

Architectures en Grappes

Management hiérarchique

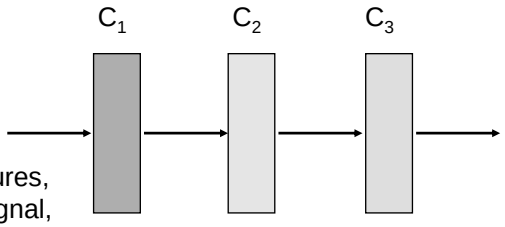


simplicité "overhead"

Fédération d' applications reconfigurables

- Architecture canonique
  - centralisée
- Attaque
  - Vulnérabilité de la tête de l'architecture
- Défense
  - Protéger la tête et éviter les remontées par un service

Architecture en Tubes & Filtres



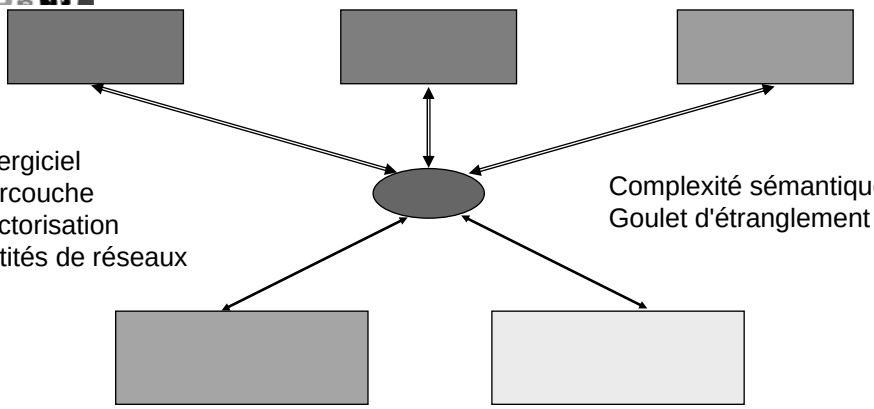
Collecticiels, Circuit de signatures, Traitement de Signal, ...

Simplicité
Autogestion
Pas flexible

n Composants => n liens

- Architecture canonique
  - Autogestion sans flexibilité
- Attaque
  - Déni de service d'un membre ou saturation d'un lien
- Défense
  - Contrôle des flux à l'entrée

Architecture en Passerelle



Intergiciel
Surcouche
Factorisation
Entités de réseaux

Complexité sémantique
Goulet d'étranglement

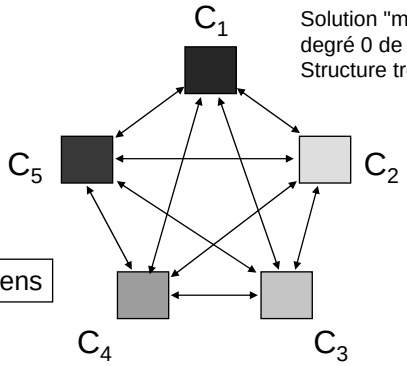
- Architecture canonique
  - Passage obligé et centralisé par un contrôle de flux entrant et sortant
  - Très vulnérable
- Attaque
  - Déni de service ou saturation de la passerelle
- Défense
  - Contrôle des flux

Architecture en Bus

Solution "miracle" de l'informaticien
degré 0 de l'architecture
Structure très vulnérable

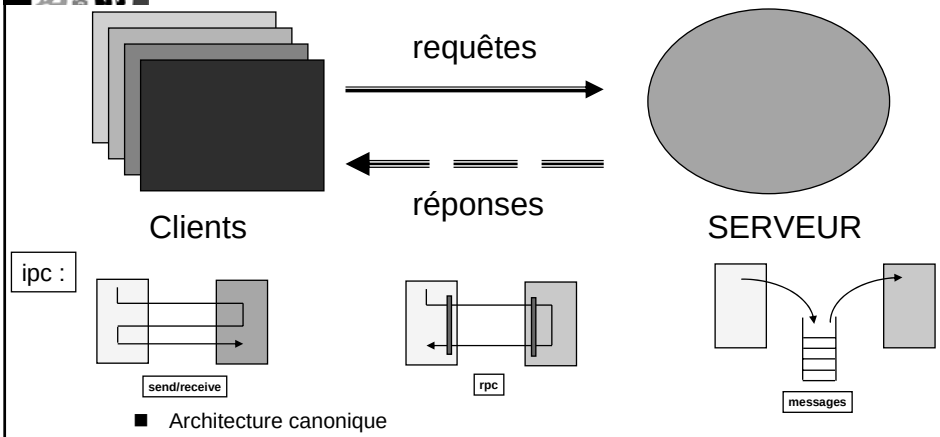
Corba,
Suites intégrées,
...

C_i # C_j => n x (n-1) liens



- Architecture canonique
  - Diffusion systématique de toutes les informations aux membres de la communauté
  - Très vulnérable
- Attaque
  - Écoute pour la confidentialité
- Défense
  - Protection des communications

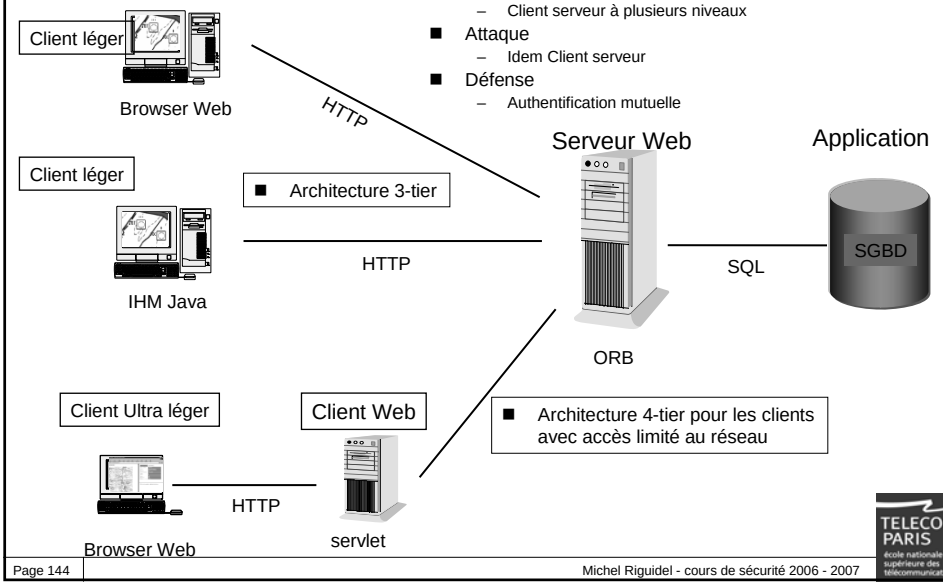
Architecture Client-Serveur



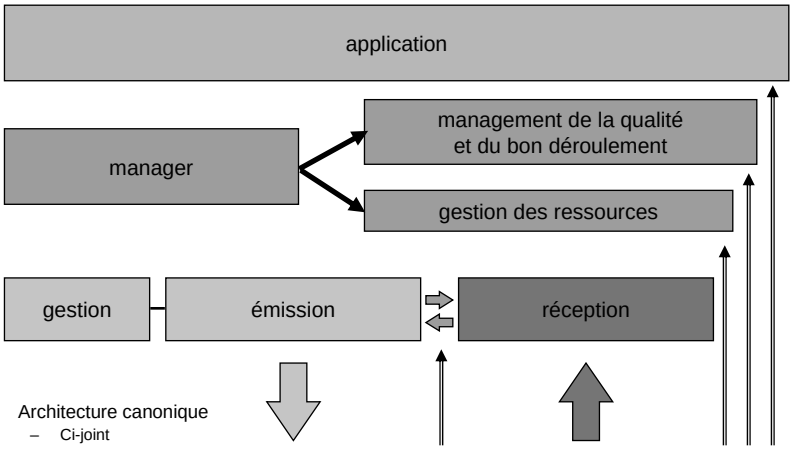
- Architecture canonique
  - Liaison point à point
- Attaque
  - Écoute pour la confidentialité, attaque par le milieu, rejeu
- Défense
  - Authentification mutuelle

Architecture en tiroirs ("n-tiers)

- Architecture canonique
  - Client serveur à plusieurs niveaux
- Attaque
  - Idem Client serveur
- Défense
  - Authentification mutuelle



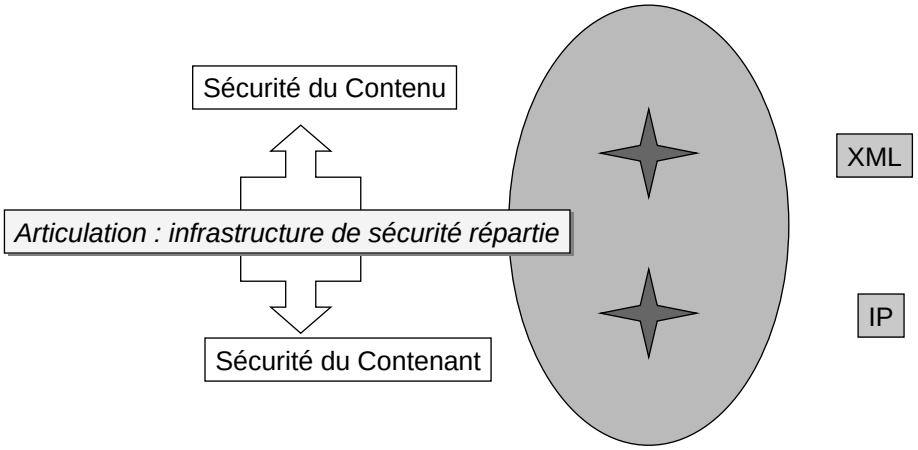
Structure d'une couche, d'un protocole



- Architecture canonique
  - Ci-joint
- Attaque
  - Perturbation par la réception pour atteindre les piles émission ou réception ou le management du protocole ou l'application
- Défense
  - Dans la sémantique du protocole

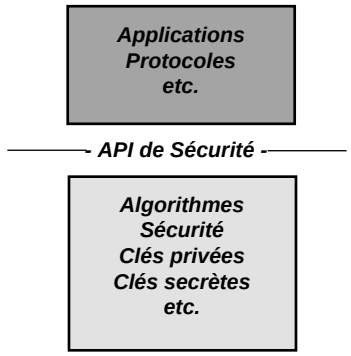
Attaque essentielle par la réception

Le besoin de sécurité d'architecture



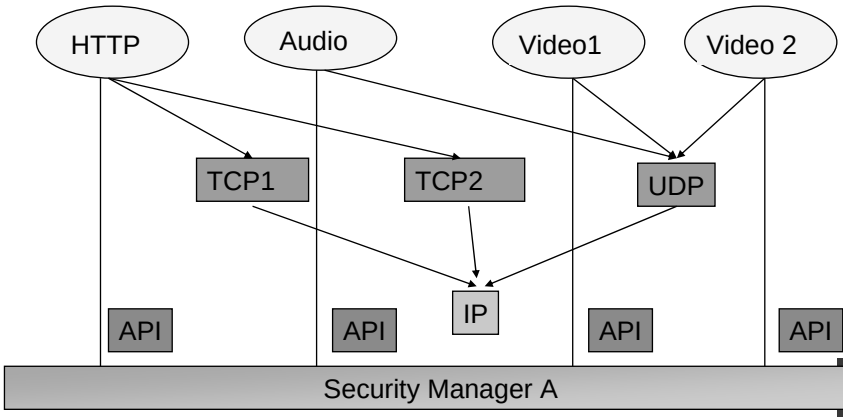
APIs de sécurité :
pour permettre le raccourci du Plug & Play

- Services avec APIs classiques
  - APIs bas niveau pour accès aux fonctions cryptographiques
  - APIs haut niveau pour traiter les certificats
- Le catalogue des APIs disponibles existant est large
  - GSSAPI
  - Microsoft CryptoAPI
  - PKCS #11
  - Cryptographic Interface (CI)
  - Security Services API (SSAPI)
- Interfaces avec le matériel



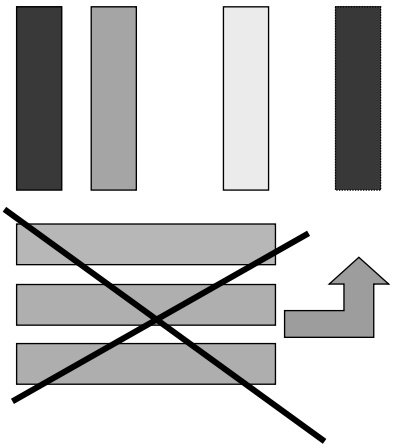
Adaptation : conception croisée à travers les couches

- Exemple : Communication point à point
  - Il faut fournir aux applications les APIs
    - SSL sur TCP
    - Sécurité sur UDP sans utiliser TCP
      - (environnements ad hoc pour les players)



Changement dans les Architectures

- La communication, la configuration, …, sont des services comme les autres ! ?



Architecture en Tranches
architecture (« Plug & Play ») :
Services utilisateurs
convivialité (=> standard)
flexible (=> modularité)
interopérable (=> protocole multimédia)

Architecture en Couches :
services communication
interopérabilité (=> homologie)

La sécurité en environnement dynamique

- La sécurité doit être interopérable et ajustable selon les objectifs de sécurité
  - en environnement hétérogène,
  - mobile
  - entre les différents acteurs
- La communication entre les entités de réseaux doit être sécurisée
  - visibilité
  - authentification
- Administration de la sécurité
  - annuaires
  - répartition

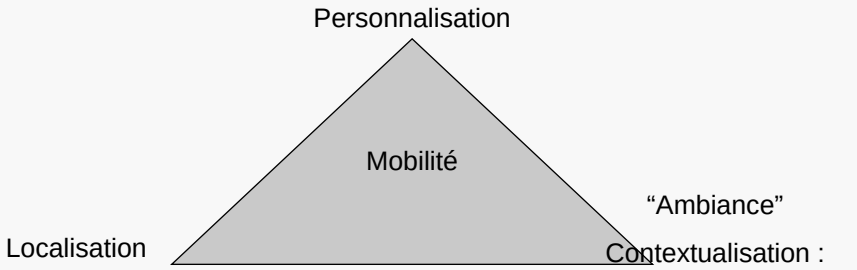
La sécurité, à l'ère numérique, dans un contexte mobile

L'intelligence ambiante et la mobilité sont des vulnérabilités redoutables

- Les modèles classiques de sécurité sont intemporels, sans tropisme et n'envisage pas le monde numérique comme un milieu
  - Il est essentiel d'enrichir les vieux modèles, les politiques et les protocoles pour appréhender la mobilité en les dotant de propriétés spatio-temporelles et contextuelles
  - Il est important de dévoiler des concepts de **traçabilité** car la mobilité est en relation avec **l'histoire** (le temps, la durée) des milieux et des êtres qui y sont hébergés et qui y vivent le long de trajectoires.
  - La **mémoire** du système et le souvenir des événements dans le milieu sont des gages pour sécuriser l'ensemble.
- La morphologie des systèmes est intimement liée avec leur protection et leur sécurité.
  - On peut fabriquer virtuellement des formes numériques et des architectures adaptées à la politique de sécurité, on peut engendrer des êtres abstraits virtuels nouveaux, comme par exemple des machines virtuelles ou des réseaux virtuels privés dynamiques qui relient des sites distants.
- Restaurer la confiance dans un monde numérique nécessite de briser l'informatique plate d'Internet, de rompre avec le virtuel infini et l'anonyme, et de réinvestir les mondes numériques avec des preuves pour les êtres en chair et en os, avec des matières tangibles, de la géographie et du temps incompressible.
  - Si l'on veut sécuriser cet univers, on peut avoir recours à des **alibis** pour prouver qu'ici et maintenant, il existe les **témoins** d'une histoire.
  - Il reste à identifier des **invariants** spatio-temporels **dignes de confiance** dans les architectures : positions des stations de base d'une infrastructure de communication, horloge de confiance, etc.
  - Il reste à créer des gages (coupons de fidélité dans un voisinage).
- Par ailleurs, la mobilité peut avoir des avantages
  - Elle crée de la liberté : déplacement de l'intelligence et de l'information, là où il faut
  - Elle crée du désordre: on peut s'en servir pour créer de l'aléatoire et du secret (cryptographie mobile)

Contexte mobile & monde numérique

- Plus de Mobilité
  - Les utilisateurs mobiles (réseaux cellulaires, réseaux sans fil Bluetooth, Ethernet radio)
    - Individus nomades (à pied ou en véhicule) avec des terminaux (PC, PDA, téléphones)
  - Les infrastructures mobiles (réseaux ad hoc, les satellites défilant)
  - Les services mobiles (caches, etc) et les contenus mobiles (DCN)
    - Téléchargement d'applications, agents mobiles, logiciel liquide, VHE, …



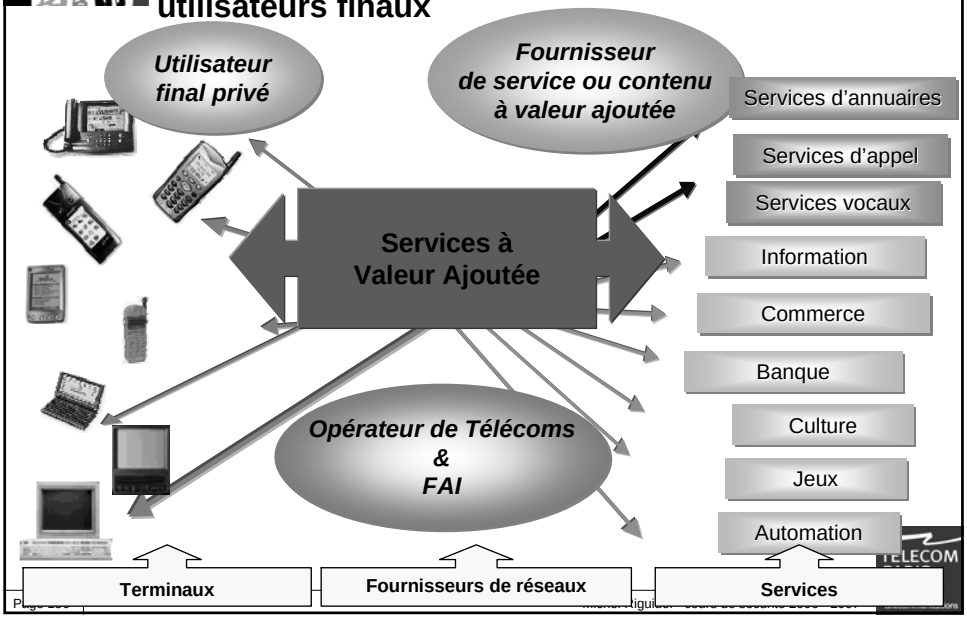
Monde numérique statique/mobile

- Le monde numérique n'est pas statique. Ce n'est pas :
  - un amas statique d'applications protégées dans un Système d'information
  - un musée Grévin qui se démultiplie à l'infini dans des miroirs selon des clones
- Le monde numérique est composé de :
  - Rubans de Turing pour les programmes
    - ce sont des entités vivantes (programmes Java)
  - Rubans de Shannon pour les contenus et les données
    - ce sont des séquences de 0s et de 1s (message, flux MPEG2, fichier MP3, …)
- C'est un monde paramétrable, programmable, adaptable, configurable en fonction des circonstances
  - Configuration, Personnalisation, Profilage, Adaptation à l'environnement, Optimisation des ressources
- Nouvelle informatique grâce aux réseaux
  - aller chercher le bon contenu, télécharger le bon service au bon moment

Mobile & Nomades

- Nomade, déplaçable, ambulant, migrant
  - Terminal nomade
    - Autonome et transportable, connectable par intermittence
  - Routeur déplaçable
    - Déploiement rapide d'infrastructures, avec routeur reconnectable
    - Adaptation rapide au trafic et à l'utilisation
  - Service ambulants, application migrante
    - Déplacement ou duplication des applications pour être au plus près des utilisateurs
    - « Agents mobiles » : en fait, agents ambulants qui transportent leur intelligence
- Mobile
  - Connexion dynamique maintenue
    - Infrastructure dynamique: Satellites défilant
    - Handover : radio cellulaires (passage du terminal d'une cellule à l'autre)
    - Réseaux ad hoc : flotte de capteurs, de véhicules qui sont connectés dynamiquement
- Adaptable, configurable
  - Services et applications personnalisés selon le contexte, le profil de l'utilisateur

Fourniture dynamiques de services à des utilisateurs finaux

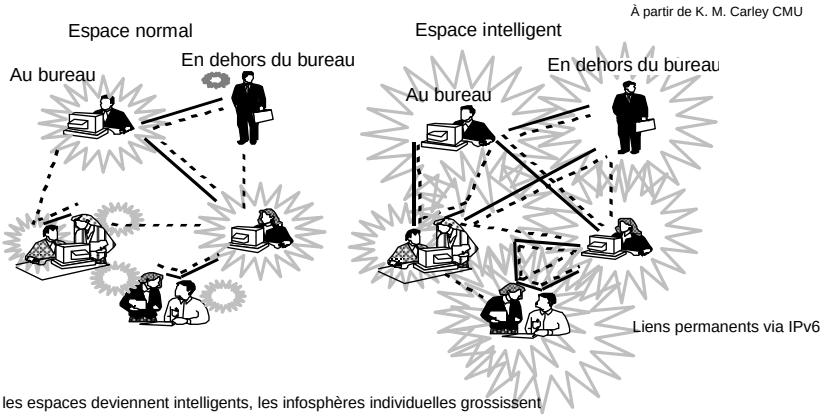


PAN-Bluetooth-WLan-UMTS-Internet

Mobilité & Infosphères

évolution des espaces : normal & intelligent

À partir de K. M. Carley CMU



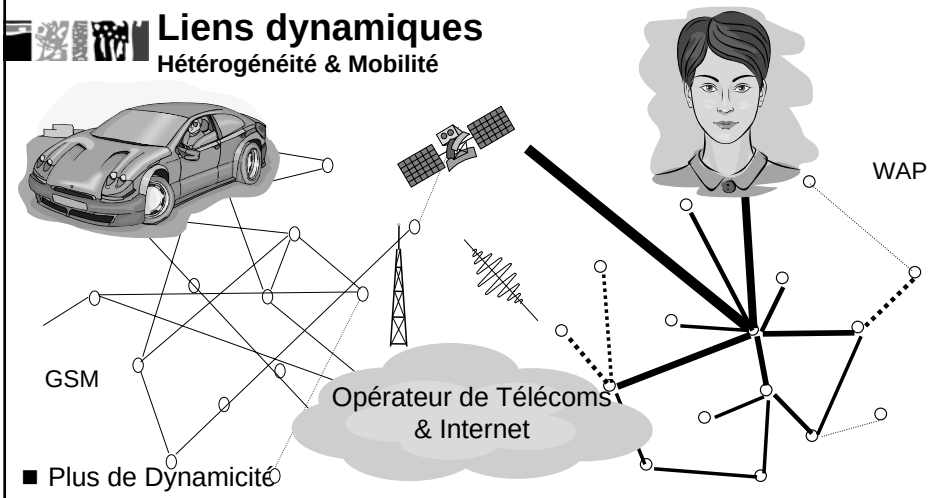
A mesure que les espaces deviennent intelligents, les infosphères individuelles grossissent

Infosphères : cercles
Interaction : lignes en gras
Réseau de connaissance : lignes pointillées

La localisation

- Le monde en réseau : comment localiser
  - Les sujets : Nomades, Services
  - Les objets : les contenus
- Les problèmes de localisation
  - Peut on situer quelqu'un en France ? Peut localiser sa voiture ?
- Authentification de confort
  - Suivant que je suis ici ou là , je me donne les autorisations qui vont bien (politique discrétionnaire)
  - Selon que je suis ici ou là, mon entreprise m'autorise à faire ceci et pas cela (politique obligatoire)
- Peut on localiser un service ?
  - Où se trouve les plus proches hôtels ? garages ?
  - Qui est autorisé à découvrir ces services ?
- L'urbanisation et l'environnement compte
  - On peut trouver le numéro de téléphone de quelqu'un dans l'annuaire (sauf liste rouge)
  - le secret utilisé donne des possibilités de localiser les personnes

Liens dynamiques
Hétérogénéité & Mobilité



- Plus de Dynamicité
  - Les changements dépendent
    - ✓ Politique, Trafic, …
    - ✓ Opportunité, positions, contexte, ressource

Itinérance Globale

La Mobilité :
une vulnérabilité redoutable

- Le périmètre de sécurité
  - Pas de système ouvert ou fermé
    - ruban de Möbius, politique de contrôle d'accès restreinte: pas de pare-feu efficace
  - Les vieux schémas de sécurité ne sont pas applicables
    - En dehors du temps et de l'espace: Monde virtuel, non incarné
- Un monde mobile a une histoire
  - Les empreintes des ontologies (sujets, objets, opérations)
  - Les traces laissées par les trajectoires des êtres
  - Les témoins qui assistent à ces déplacements
  - Les cycles de vie des objets numériques s'accélèrent (formats, …)
- Sécurité
  - Établir et tisser une Confiance « ici et maintenant »
  - Recomposer la cinématique pour des enquêtes futures, authentifier les scènes
  - Enregistrer en filigrane les parties saillantes du film des nomades
  - Une économie de la sécurité ouverte
    - Interopérabilité des politiques de sécurité (pas de sécurité dans l'obscurité)
    - Protéger ou sécuriser les contenus
    - Nouvelles attaques sur les biens intangibles : attaque symbolique

Les Alibis

- Confiance dans un monde géo-historique
  - Construire des relations de confiance entre l'infrastructure et le sujet/objet qui se déplace
    - Protocoles cryptographiques (d'usage, de confort)
  - Trouver des témoins dignes de confiance
    - Donner des gages (partager des secrets éphémères)
- Sécurité in situ
  - Briser la virtualité du monde numérique
  - Surmonter l'anonymat
  - Utiliser l'intelligence (sémantique)
    - chez les êtres qui habitent cet espace
    - de l'espace qui les abrite
  - Politique de sécurité
    - Fonction du temps et de l'espace
    - Configurable en fonction du contexte, de l'ambiance

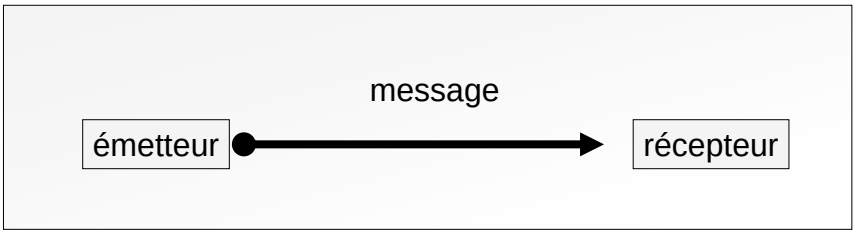
Retrouver la sémantique

- Modèles de sécurité
  - Abandonner (ou enrichir) les modèles universels fondés sur les 1s et 0s des textes et sur les pixels des images
  - Bâtir de nouveaux modèles de communication, de conservation en y incluant la sécurité fondés sur
    - L'esthétique
    - La sémantique, etc
  - Alliance cryptographie et stéganographie
- Sécurité de logiciels mobiles
  - Tatouage sémantique de logiciels (Cousot & Riguidel)
    - Brevet (pas une signature électronique mais sémantique)
  - Protection de contenu sur Cdrom (jeux vidéo, encyclopédie, …)
    - Fondé sur la sécurité configurable fonction du comportement de l'utilisateur
    - Heuristique de désinformation, de leurres contre les pirates

Modèle de communication
inspiré de Roland Barthes / Jacques Lacan

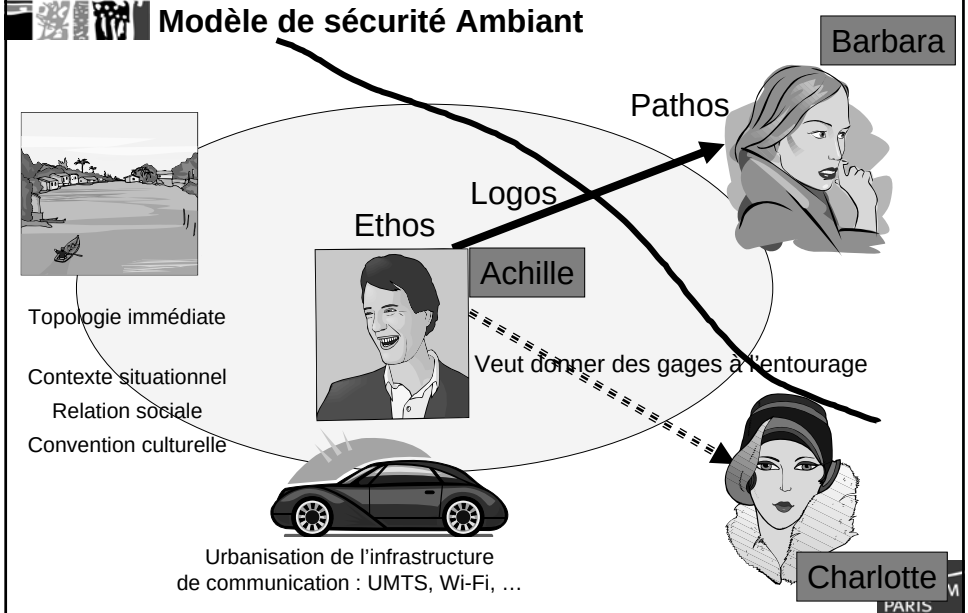
- **Restituer la sémantique**
  - Critique de J Lacan (séminaire II, 1954) sur le modèle de Shannon
  - Roland Barthes relit Aristote et propose un nouveau modèle de communication (vers 1960)

Ethos | Logos
Réel & Subliminal & Rhétorique | Pathos



Mobilité : ajouter la sécurité du canal

Modèle de sécurité Ambiant



Un Contenu, hors d'un huis clos, en clair

- Un contenu en clair peut être cloné
  - Un texte se lit, une image se voit, une musique ou une voix s'entend, un programme s'exécute en clair
- Un contenu est créé, édité, packagé, distribué, …, consommé et non détruit (donc réutilisable)
  - Chaîne d'acteurs: auteur, éditeur, producteur, distributeur, consommateur et (pirate).
- Un contenu numérique n'est ni une denrée périssable, ni un produit jetable
  - Modèle de communication : problème résolu
  - Modèle de conservation & destruction : problème à résoudre
    - La voix, les conversations
    - Les données, le patrimoine
    - Les contenus riches, les logiciels (jeux, etc)
  - Politique de sécurité et modèle économique
    - Recréer l'obsolescence: Produire un contenu dégradable avec le temps, la copie, etc

La traçabilité

- Fonctions de sécurité essentielles en mobilité
  - Identification/authentification : oui (les traces)
  - Contrôle d'accès : non
  - Protection des données : non
  - Protection de la gestion des secrets : secrets éphémères
  - Audit : oui
  - Imputabilité : oui
- Instaurer une confiance ad hoc
  - Sécurité configurable avec des seuils, statistique, …
  - Tisser de la confiance à partir des voisins
  - Protocoles d'authentification dans la couche 2 du modèle OSI

Protéger / Sécuriser des info-sphères

- Protéger ou sécuriser les contenus (commerce en ligne)
  - Pendant le transport : oui, facile
  - Pendant la conservation : oui, difficile, mais à résoudre
  - Pendant le travail (présentation, calcul, …) : pas forcément, approche classique
    - En direct, pendant le déplacement (« handover », …)
- Relaxer les contraintes pour l'informatique diffuse: réseau personnel, « pervasive »
  - Désynchroniser l'acte de sécurité de l'action elle-même
  - Faire fonctionner la sécurité sur des êtres en veille
    - Pendant le travail : du luxe …(SSL, etc)
    - Avant : si c'est possible, inonder l'entourage avec des secrets, intimité numérique (« privacy »)
    - Après : si on ne peut pas faire autrement (détection d'intrusion, …)
  - Ne pas tout recommencer
    - Économiser l'énergie numérique, Confiance mesuré au fil du temps

La sécurité dans un monde mobile

- Quitter le monde virtuel, infini, abstrait et anonyme
- Réinvestir le monde numérique avec les êtres et les actes
  - Laisser des marques, des empreintes, des traces : Mettre en mémoire
  - Avoir des témoins /enregistrer des preuves
    - Savoir les mettre en valeur le moment venu
  - Définir pragmatiquement les modèles, personnaliser et enrichir les modèles
  - Ne pas évacuer la sémantique
- Utiliser l'arsenal des architectures et structures invariantes pour projeter cette information sur toute la structure
  - Projeter la spécification de la politique de sécurité sur tout le continuum support / infrastructure / utilisateur
    - Identifier les bonnes ontologies
    - Protocole cryptographique ontologique, éthologique
    - Signature historique, Tatouage sémantique
    - Témoins (de confiance) et preuves : partage de sens, d'habitudes avec ses voisins

Sécurité plurielle, Confiance versatile, Intelligence Ambiante

vers une évolution des Critères Communs ?

Évolution des méthodologies d'évaluation

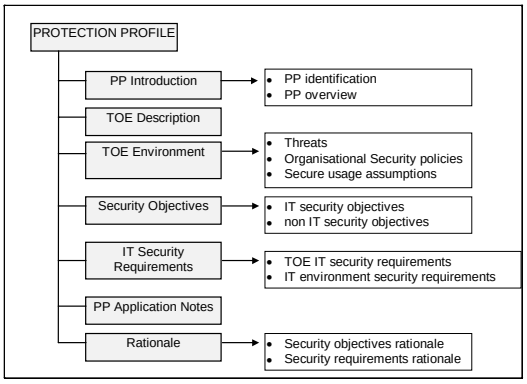
- La sécurité dans une intelligence ambiante
  - Pour des méthodologies adaptées à l'époque
    - Livre Orange
      - Sécurité des systèmes d'exploitation
    - ITSEC
      - Apparition de la notion de systèmes
    - Critères canadiens
      - Notion de profil
    - Critères Communs
      - Synthèse profonde, mais pas d'avancées selon les paradigmes informatiques
  - Une nouvelle méthodologie ?
    - Les contenus et services en clair, publiques, distribution gratuite
    - Le système et son image médiatique
    - La mobilité, la configurabilité
    - L'ambiance (informatique)
    - La grille, l'informatique diffuse
- Critères Communs : Profil de Protection
  - Manichéisme entre
    - La cible de sécurité (ToE) et son environnement
    - La partie informatique (IT) et le reste (non IT)
  - Vers un nouveau découpage
    - Les cibles de sécurité et l'environnement
      - Sa relation avec l'environnement
        - ➔ Produit
        - ➔ Service
        - ➔ Système
      - Les hypothèses
        - ➔ Prises en charge par
        - ➔ l'environnement, l'organisation
        - ➔ la législation, la réglementation
    - Les cibles, l'ambiance, l'environnement
      - Les cibles dans l'ambiance
      - L'ambiance dans l'environnement

La sécurité des systèmes : méthodologie

- Établir la bonne granularité
  - Identifier les Ontologies
    - En communication : session, circuit virtuel, paquet IP, etc
    - En informatique
      - Matériel: terminaux, station, routeur, fibre des réseaux,
      - Logiciel: logiciel de base, application, répertoire, fichier
- Statiques : diviser l'ensemble et protéger les parties
  - Identifier les Sociologies
    - La structure et l'architecture du système est la première chose à protéger
      - Décomposition en fragments, en domaines, en classes, en rôle, et politique pour chaque segment et contrôle aux interfaces
  - C'est l'irrigation du système qui crée la vulnérabilité (protocoles, données en transit)
- Mobiles et/ou Configurables : maîtriser le mouvement
  - Identifier les Éthologies
    - Il faut protéger la configurabilité : le mouvement et les états de transition

Critères Communs : Profil de Protection

- Manichéisme entre
  - La cible de sécurité (ToE) et son environnement
  - La partie informatique (IT) et le reste (non IT)

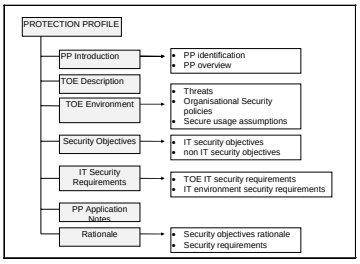


Vers un nouveau découpage

- Les cibles de sécurité et l'environnement
  - Sa relation avec l'environnement
    - Produit
    - Service
    - Système
  - Les hypothèses
    - Prise en charge par
      - L'environnement, l'organisation, la législation, la réglementation
- Les cibles, l'ambiance, l'environnement
  - Les cibles dans l'ambiance
  - L'ambiance dans l'environnement

Les nouvelles politiques

- La politique de sécurité
  - Sujets, objets, opérations des sujets sur des objets
  - Les attributs
    - Le contexte, le temps, l'espace
- Le côtoiement des politiques
  - Chaque sujet, chaque objet, chaque lieu a une politique de sécurité
  - Pour une scène:
    - Négociation
      - En temps réel ou non
      - Solution positive ou négative
    - Règle de décision : a priori
- La criticité des attaques
  - Politique de sécurité classique
    - Suivant la valeur des biens
  - Politique de sécurité médiatique
    - Affichage, gestion des crises
    - Leurres, désinformation
- La traçabilité de l'éphémère
  - La précarité des situations, des actions, …
    - Protocoles complexes, opérations fugaces
  - L'immuable
    - Surveillance, redondance



La sécurité du monde intangible : le logiciel

- Menace
  - Les erreurs et/ou imperfections de spécifications, de conception, d'exploitation de ses programmes légitimes
  - Les inconnues des logiciels sur étagères (COTS)
    - Perte de confiance dans ses disques cancérisés par des bibliothèques
    - Le loup dans la bergerie
      - porte dérobée, pare-feu avec cheval de Troie, connexion intempestive pour vérifier le paiement des licences, etc
  - Les méfaits des autres programmes parasites
    - virus, "cookies", …
- La sécurité des propriétés fonctionnelles : y = f(x)
  - "f fonctionne correctement" conformément à une spécification et à une documentation lisible fournie à l'utilisateur
    - Difficile à démontrer …possible pour du logiciel embarqué écrit en langage formel
  - "f n'est pas vulnérable et f est docile vis à vis de son entourage"
    - Pas facile non plus …
- La sécurité des propriétés non fonctionnelles
  - Configurabilité, mobilité, évolutivité, etc
- Technologies
  - La sémantique des langages informatiques
  - La spécification formelle (des protocoles, des fonctions)
  - La vérification logicielle, la preuve formelle
  - La certification

La typologie de la sécurité (1)

- Sécurité dans un huis clos
  - Bac à sable, Carte à puce, Communauté fermée pour les calculs répartis
  - Un logiciel
    - Propriété intellectuelle
    - Correction du logiciel
    - éthique
  - Des données
    - Confidentialité, intégrité, disponibilité
  - Une horloge
    - Intégrité
  - Des ressources
    - Disponibilité

La typologie de la sécurité (2)

- Le logiciel tourne dans une ambiance
  - Dans une ambiance
  - Dans un espace réparti
  - Dans un temps éclaté
  - Avec des collègues, pour des collègues

Les verrous de la sécurité (en 2002)

Groupe RNRT sécurité

Animé par M Riguidel et D Bois

Avec RNTL, académiques et industriels

Sept Priorités en Recherche

1 Sécurité des composants matériels
- entités de confiance, informatique envahissante (pervasive)
- méthodologie de conception, optimisation de l'interface hw/sw

2 Politiques de contrôle des accès aux services
- mécanismes d'identification, fédération des solutions
- outils de gestion des données et droits d'accès aux services comme aux contenus

3 Robustesse des réseaux : disponibilité, QoS
- modélisation des risques, détection des intrusions, protection des éléments critiques du réseau
- application aux réseaux émergeants: hauts débits, ADSL, Bluetooth, HiperLAN, …

Sept Priorités en Recherche

4 Services de confiance communautaires
- sécurité multi-acteurs pour des groupes ouverts et dynamiques
- modèles d'établissement et de maintien de la confiance
- simplification des infrastructures de gestion de clés

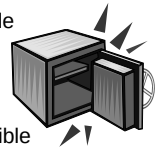
5 Protection et filtrage des contenus
- dans le réseau, au niveau des stockages ou caches
- données personnelles, vie privée, œuvres audiovisuelles

6 Expérimentations de solutions; Plates-formes
- validation: passage à l'échelle, acceptabilité, usages
- thèmes possibles: biométrie, réseaux domestiques ou personnels, réseaux sans fil, services communautaires

7 Outils et modèles
- mise en œuvre, critères communs

Le déficit de la sécurité matérielle

- Certitude d'une sécurité fondée sur le matériel ?
  - L'entité de confiance personnelle : sûre, configurable
  - Certification difficile du logiciel : méthode, outils
    - Le matériel est conçu avec du logiciel
    - Complexité, coût, délais, cycle de révision
  - L'informatique envahissante («pervasive») : coût faible



- Le Quantique : rupture à quel horizon ?
  - Distribution des secrets, Communications sécurisées
  - Passage à l'échelle, échéancier
- Biométrie : intégration dans la chaîne de confiance
  - Plates-formes : expérimentation - usages

Le nouveau paysage des systèmes urbanisés

- Les systèmes ouverts/fermés
  - L'intelligence, la complexité sont des vulnérabilités
  - Difficulté de construire des architectures
  - Défi incertain d'une mobilité sûre
  - Cloisonnement : périmètre de survie, points de reprise

- La pathologie de la sécurité logicielle
  - Le mythe d'une sécurité absolue a disparu
    - Impossibilité d'éradiquer les bugs, les virus

Politique de Contrôle d'accès

- Accès aux services & contenus
  - Identification & Authentification
  - Fédérations des solutions pour transcender l'hétérogénéité
  - Pare-feu : goulets d'étranglement
    - Signature électronique, graffiti sur paquets
- Autorisation, Délégation
- Outils de Gestion des Droits

Des Réseaux robustes

- Disponibilité & QoS
  - Modélisation des risques
  - Détection d'intrusion
  - Protection des éléments critiques du réseau
- Applications aux réseaux émergents
  - Haut débit, ADSL, Bluetooth, Hiperlan, …
  - Ouverts, Hétérogènes, Dynamiques, Multimédia, Mobiles
- Sécurité des protocoles
  - IPv6
  - Introduire de la sémantique des services dans les réseaux pour marquer, filtrer, tracer

Lourdeur de la gestion de la sécurité

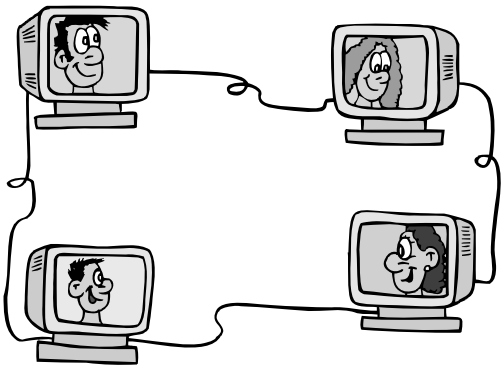
- Bureaucratie des IGCs universelles
  - Confiance insuffisante pour un usage courant
  - Utilisation & intégration pas satisfaisantes
  - Interopérabilité partielle entre PKIs
- Projets
  - Simplification des infrastructures de confiance
  - Service d'Intermédiation à Valeur Ajoutée de sécurité
    - certificat, autorisation, tatouage, preuve…

Expérimentation & Usages d'IGCs pour des métiers & domaines particuliers (notaires, santé, éducation, …)

IGC : Infrastructure de Gestion de Clés – PKI : Public Key Infrastructure

Services de Confiance communautaires

- Sécurité multi-acteurs pour des groupes ouverts & dynamiques
- Modèles d'établissement & maintien de la confiance

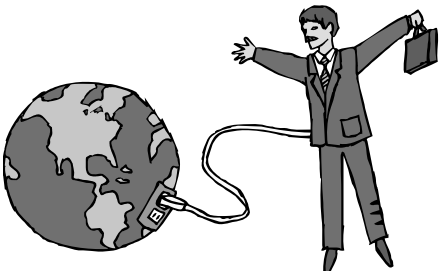


Protection & Filtrage des Contenus

- Éthique des Contenus
  - Sur le réseau, le Web
    - Contenus illicites
    - Données volatiles des caches
  - Métacomputing, Grilles de Calculs
    - Éthique des calculs sur les nappes d'ordinateurs
- Vie privée
  - Confidentialité des données
  - Intimité
    - protection, pas d'observation, pas de liens
- Protection des Œuvres
  - Audiovisuelles (IPR, DRM)
  - Logiciels, CD-Roms, …

Expérimentation de solutions, Plates-formes

- Validation de solutions
  - Acceptabilité, usages
- Déploiement
  - Passage à l'échelle
- Expérimentation
  - par exemple
    - Biométrie
    - Réseaux domestiques, personnels
    - Réseaux sans fils
    - Services Communautaires



L'assurance de sécurité

- Enjeu économique de la certification
  - La sécurité devient un métier de haute technologie informatique
  - Fabriquer des produits certifiés
    - Produits sur étagère, Modules Standards
  - Méthode, organisation, charte
  - Les Critères Communs
- Projets
  - Nouveaux modèles de sécurité
  - Nouveaux outils pour accroître la productivité
  - Mise en œuvre des Critères Communs

La structuration de la recherche

- Technologies de base
  - Algorithmes, outils matériels et logiciels
  - Méthodes formelles, modèles
  - Méthodologie
- Les modules
  - Crypto-processeurs, capteurs, modules logiciels (IPSec, …), simulateurs
- Les briques
  - Carte a puce, dispositif biométrique, carte crypto, intergiciels de sûreté et sécurité (protocoles, …)
- Les dispositifs et systèmes intégrés
  - VPN, pare-feu, serveur de sécurité, système de détection d'intrusion (IDS)
- Les infrastructures et solutions de sécurité
  - PKIs, CIPs (Critical Infrastructure Protection)

La structuration de la recherche

- Les infrastructures de sécurité
  - PKIs, CIP, MPEG21, …
- La sécurité des réseaux (~ travaux IETF)
  - Sécurité des architectures
  - Sécurité des protocoles
  - Détection d'Intrusion
- La sécurité de la couche application
  - Sécurité des contenus et des services
    - Les techniques de tatouage
    - Les DRMs, "IP"
- Les technologies de base pour la sécurité
  - La cryptologie, les protocoles cryptographiques et les méthodes formelles
  - Les modèles et les politiques de sécurité
    - Sécurité mobile, configurable, …
    - Les modèles d'attaque, les leurres, …
- La biométrie
- La sécurité matérielle
  - Dispositifs matériels : Carte à puce, crypto haut débit
  - Architecture matérielle sécurisée: crypto-processeur

Feuille de route de la R&D en sécurité

- Les technologies de base pour la sécurité
  - La cryptologie, les protocoles cryptographiques et les méthodes formelles
  - Les modèles et les politiques de sécurité
  - Certification et méthodologie d'évaluation
- Les infrastructures de sécurité
  - Modéliser les grands domaines ouverts publics
    - PKIs (à déployer par subsidiarité pour l'usage)
    - MPEG21 (à industrialiser et standardiser)
    - Quantique (à développer)
    - Infrastructure critiques (à modéliser)
  - Modéliser la protection de la vie privée
    - Infosphères personnelles, PET (Privacy Enhanced Technologies)
- La sécurité des propriétés non fonctionnelles
  - La mobilité : sécurité 802.11x, réseaux ad hoc, …
  - La configurabilité : intergiciels personnalisables, logiciels téléchargeables, agents mobiles
  - La répartition : sécurité des grilles, machines virtuels, systèmes d'exploitation répartis
  - Les architectures
- La sécurité de la couche application (contenus et des services)
  - Les DRMs, "IP" (Intellectual Properties)
  - Les techniques de tatouage
  - Les protocoles cryptographiques dédiés à des usages
- La sécurité des réseaux (~ travaux IETF)
  - La sécurité des multi-services (GPRS, UMTS, …)
  - Sécurité des protocoles (AAA, DNSSec, IP mobile, …)
  - Détection d'Intrusion, leurres, …
- Les dispositifs matériels
  - Entité de confiance personnelle (Carte à puce nouvelle génération)
  - Architecture matérielle sécurisée: crypto-processeur configurable, crypto haut débit
- La biométrie

Quelques rappels
sur les techniques cryptographiques
(confidentialité et intégrité mais pas disponibilité)

Mécanismes de sécurité

- Mécanisme de base
  - Les protocoles de sécurité fournissent grâce à des algorithmes cryptographiques des services de sécurité
    - la confidentialité, l'authentification, l'intégrité et la non répudiation
- Cryptographie
  - Principes : algorithmes et clés
  - Chiffrement
  - Signature

Algorithmes de cryptographie

- Cryptosystèmes symétriques (DES, TripleDES, IDEA, AES)
  - Une seule clé secrète pour chiffrer et déchiffrer
  - Les entités en communication doivent partager cette clé secrète
  - La base des services de confidentialité
- Cryptosystèmes asymétriques (RSA, …)
  - avec un couple de clés appartenant à un propriétaire
  - Clés publique et privée, une pour chiffrer, l'autre pour déchiffrer
  - La clé privée est gardée secrète par le propriétaire
  - La clé publique est rendue publique à tous les intervenants de la communication
  - La base des services d'intégrité, d'authentification et de non répudiation
- Algorithmes de hachage à sens unique
  - Utilisés pour produire des condensés
  - Utilisés pour des empreintes
  - Utilisés avec un cryptosystème asymétrique pour calculer des signatures électroniques

Les services de sécurité

- Confidentialité
  - préserver le secret d'une information
  - protection de l'information lors de sa conservation, du transfert ou du calcul
- Intégrité
  - préserver contre les modifications, sauf autorisation
  - vérifier la non altération frauduleuse
- Disponibilité
  - Garantir la possibilité d'accéder aux services
  - Éviter les interruptions, les obstructions
  - Pas de modèle de disponibilité (infrastructures)
- Autorisation
  - identification (nom) et authentification (garantir l'identité)
  - contrôle les droits d'accès, rendre un service de sécurité
- Authentification
  - Identification, contrôle d'accès, non répudiation

Tout système est vulnérable

- Exemple enfantin (puéril ?)
  - pot de confiture opaque, fermé, avec étiquette, posé en haut sur une étagère
    - La grand mère peut
      - lire l'étiquette « confiture de fraise » (pas confidentiel pour elle)
      - ouvrir le pot et prendre de la confiture (pas intègre)
      - saisir le pot (disponible, prêt à l'emploi)
    - Les enfants ne sont pas autorisés à manger la confiture
      - ne savent pas lire l'étiquette écrite en français
        - ➔ (confidentiel pour les enfants, bien que ce soit écrit en clair; ce ne serait pas confidentiel si la grand mère avait dessiné des fraises)
      - ne peuvent pas ouvrir le pot pour en manger
        - ➔ (intègre, la grand mère a bien fermé le pot)
      - ne peuvent pas atteindre le pot sur l'étagère
        - ➔ (pas disponible pour des petits enfants)
        - ➔ Attaque possible : monter sur un tabouret

Système numérique :
indépendance du contenu et du support

- Moyens de transmission en croissance
- Patrimoine numérique en hausse
- Clonage
  - duplication quasi infinie et falsification indétectable

- En 2007, la cryptographie est finalement « peu » (!?) utilisée
  - Internet est en clair à 9x %
    - rien à cacher ?
  - Le GSM
    - seule la portion sans fil (à la station de base) est chiffrée
- Il faut encore attendre l'ère du e-X
  - X = business, administration, commerce, formation, etc
  - le B2B, le B2C, e-démocratie, …
  - les services de personnalisation
  - le patrimoine industriel et commercial en ligne (service payant)

Cryptographie

- Avant 1945
  - sécurité dans l'obscurité
    - algorithme secret
  - chiffrement des caractères et des textes écrits
    - redondance, etc
- Après 1945 : C Shannon
  - liaison forte avec la théorie de l'information (codage, etc)
  - secret dans le codage (pas dans la sémantique)
  - les algorithmes chiffrent des nombres (machine numérique)
  - on chiffre la voix, l'écrit, l'image, la vidéo, etc
  - La cryptographie s'oriente vers les systèmes dont les algorithmes de codage et de décodage sont connus par tous comme le (DES, AES, RSA, …)
  - Seule, une clé permet d'assurer la confidentialité

Définitions - Terminologie

- **Cryptologie**
  - Science des messages secrets. Elle se décompose en deux disciplines
    - la **cryptographie** et la **cryptanalyse** indissociable pour la sécurité
  - **Cryptographie** (du grec κρυπτος: caché et γραφειν: écrire)
    - Art de transformer un message clair en un message inintelligible par celui qui ne possède pas les clefs de chiffrement
  - **Cryptanalyse**
    - Résistance des algorithmes, mesure de la sécurité
    - Art d'analyser un message chiffré afin de le **décrypter**
    - recherche exhaustive, cryptanalyse différentielle, linéaire
- **Tatouage, Stéganographie** (du grec στεγανος: couvert et γραφειν: écrire)
  - Ne pas rendre le message inintelligible, mais le **camoufler** dans un support (texte, image, etc.) de manière à masquer sa présence
- **Autres définitions**
  - **Chiffre**
    - Ensemble de procédés et ensemble de symboles (lettres, nombres, signes, etc.) employés pour remplacer les lettres du message à chiffrer
  - **Code**
    - Ensemble de procédés et ensemble de symboles (lettres, nombres, signes, etc.) employés pour remplacer les mots du message à coder
  - **Décryptement**
    - Restauration des données qui avaient été chiffrées à leur état premier ("en clair"), sans disposer des clefs théoriquement nécessaires
  - **Déchiffrement**
    - Opération inverse du chiffrement
    - Obtenir la version originale d'un message qui a été précédemment chiffré en connaissant la méthode de chiffrement et les clefs

Cryptologie : 2 branches

- Symétrique
  - DES, …, AES, …
    - rapide
    - empirisme et prolongement de l'histoire
    - clef symétrique (clef secrète) distribuée lors d'une réunion préalable
    - issue de Shannon (1942-1948)
  - gestion des clés en n^2
  - confidentiel : un secret partagé , chiffrement-déchiffrement
- Asymétrique
  - RSA, …
    - lent
    - conjecture sur la factorisation des nombres premiers
    - clef asymétrique (publique, connue de tous)
      - 1976 : Whitfield Diffie et Martin Hellman
    - propriétaire
      - le seul a pouvoir déchiffrer avec sa clé privée connue de lui seul
  - gestion des clés en n

Crypto asymétrique

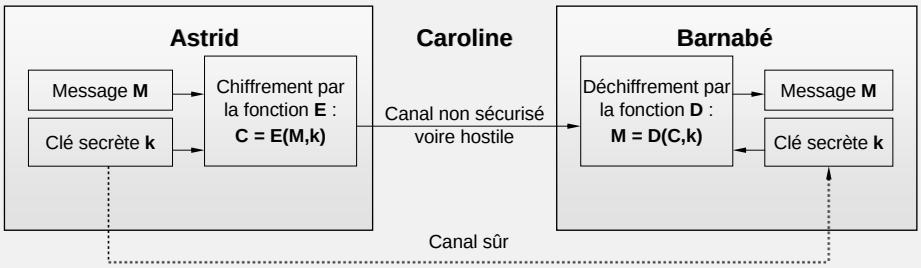
- asymétrie forte
  - 2 types d'opérations
    - chiffrement et vérification de signature
    - déchiffrement et signature
- Exemple
  - Pour envoyer un document chiffré à Astrid
  - Pour déchiffrer une signature (un message court : nom, prénom, fonction)
    - Barnabé, Charlotte, David, Élodie, Fabien utilise la clé publique d'Astrid
  - Pour déchiffrer un document venant de Barnabé, Charlotte, David, Élodie et/ou de Fabien
  - Pour envoyer une signature chiffrée à Barnabé, Charlotte, David, Élodie et/ou à Fabien
    - Astrid utilise sa clé privée

Système de chiffrement symétrique

- C et C^{-1}
- Algorithme réversible

- Chiffrement par bloc
  - Bloc de taille fixe (64 bits)
  - Souvent entrée et sortie de même taille
- Chiffrement par flot
  - Génération d'une suite pseudo-aléatoire de blocs
  - Changer la clé à chaque message

Cryptosystèmes à clé symétrique



protocole d'une transmission chiffrée par cryptosystème à clé symétrique

1. Astrid et Barnabé choisissent un cryptosystème, par exemple le DES.
2. Astrid engendre une clé, et en donne une copie à Barnabé (ou bien ce peut être Barnabé qui engendre la clé, ou bien, c'est Astrid et Barnabé qui conviennent ensemble d'une clé commune)
3. Astrid chiffre son texte en clair à l'aide de l'algorithme choisi, avec la clé sélectionnée et l'envoie.
4. Barnabé déchiffre le texte avec le même algorithme, la même clé, et finalement lit le message.

DES (Digital Encryption Standard)

- Le plus étudié et le plus utilisé
  - Standard américain et de facto
  - Genèse en 76 - 77 (origine IBM)
  - Aujourd'hui TripleDES
    - 3 fois le DES avec des clés différentes
- Le DES est un code à blocs de 64 bits
- Le fichier clair est donc découpé en plusieurs blocs de 64 bits
  - déchiqueter l'information en suite de 8 octets
- Clé de 56 bits transformée en 16 sous-clés de 48 bits

DES

- Le DES est un code dont l'idée vient de Shannon
  - combine simultanément diffusion et confusion qui sont des méthodes peu sûres quand on les utilise séparément
  - leur combinaison permet d'atteindre un niveau de sécurité assez considérable
    - La diffusion utilise ici des permutations dont le but est d'éclater dans le fichier la redondance présente dans le fichier clair
    - La confusion qui a pour but de compliquer la liaison entre le fichier chiffré et les clés secrètes, utilise des substitutions, non linéaires, de façon à produire un système cryptographique qui résiste à toute cryptanalyse mathématique
- Difficile de démontrer l'inviolabilité d'un tel produit
  - mais l´aspect aléatoire du produit des bits chiffrés rend la tâche très difficile à tout cryptanalyste

DES : Algorithme

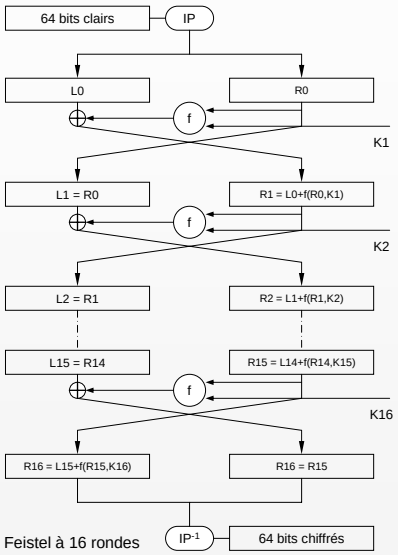
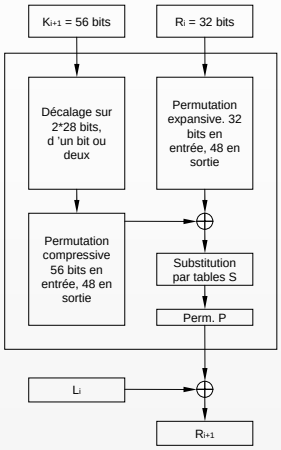


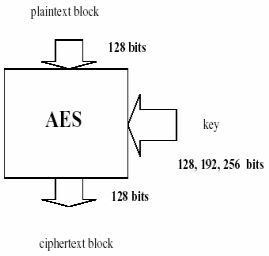
Schéma de Feistel à 16 rondes



Fonction f (R_i,K_{i+1})

Advanced Encryption Standard:
l'algorithme des années 2000

- Les anciens standards sont devenus trop faibles
- En janvier 1997, le NIST (National Institute of Standards and Technologies) lance un appel d'offre pour l'élaboration d'un algorithme :
  - Robuste aux différentes attaques actuelles
  - Facile à l'utilisation
  - Rapide (utilise les instructions de base du microprocesseur)
  - Utilisable dans les cartes à puce
  - Permettant de chiffrer de blocs de différente taille



AES : Rijndael

- un standard, libre d'utilisation, sans restriction d'usage ni brevet
  - un algorithme de type symétrique (comme le DES)
  - un algorithme de chiffrement par blocs (comme le DES)
- supporte différentes combinaisons [longueur de clé]-[longueur de bloc]
  - 128-128, 192-128 et 256-128 bits
    - il supporte également des tailles de blocs variables, mais cela n'est pas retenu dans le standard
- sécurité ou l'effort requis pour une éventuelle cryptanalyse
- facilité de calcul
  - cela entraîne une grande rapidité de traitement
- besoins en ressources et mémoire très faibles
- flexibilité d'implémentation
  - cela inclut une grande variété de plates-formes et d'applications ainsi que des tailles de clés et de blocs supplémentaires
- hardware et software
  - il est possible d'implémenter l'AES aussi bien sous forme logicielle que matérielle
- simplicité
  - le design de l'AES est relativement simple
- l'algorithme Rijndael http://www.esat.kuleuven.ac.be/~rijmen/rijndael/

Rijndael versus DES

- En termes décimaux:

  3.4×10^{38} clés de 128-bit possibles
  6.2×10^{57} clés de 192-bit possibles
  1.1×10^{77} clés de 256-bit possibles
- 10^{21} fois plus de clés 128 bits pour l'AES que de clés 56 bits pour le DES
- En supposant que l'on puisse construire une machine qui pourrait craquer une clé DES en 1 seconde (donc qui puisse calculer 2^{55} clés par seconde), cela prendrait encore 149 mille milliards d'années pour craquer une clé AES
- Pour donner un ordre d'idée plus concret, l'univers est vieux de 20 milliards d'années au maximum
- NIST Computer Security Division - http://csrc.nist.gov
- ADVANCED ENCRYPTION STANDARD (AES)
  http://annu.cryptographie.free.fr/

Rijndael: Algorithme

Rijndael Cypher**AES**(*data_block*, *key*) {
in *State*, *RoundKeys*

State ℜ *State* xor $RoundKey_0$
for *Round* = 1 **to** *Nr*
SubBytes(*State*)
ShiftRow (*State*)
If not(last Round) **then** *MixColumn*(*State*)
State ℜ *State* xor $RoundKey_{Round}$
out *State*

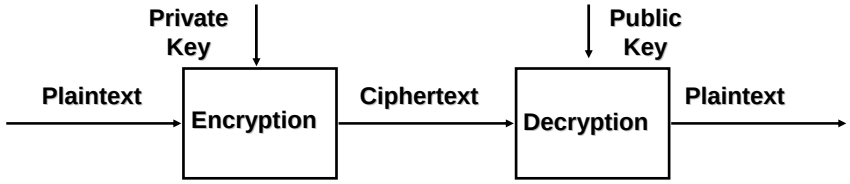
}

- BYTE_SUB (Byte Substitution) est une fonction non linéaire opérant indépendamment sur chaque bloc à partir d'une table dite de substitution
- SHIFT_ROW est une fonction opérant des décalages
- MIX_COL est une fonction qui transforme chaque octet d'entrée en une combinaison linéaire d'octets
- le OU exclusif (XOR)
- Ki est la ième sous-clé calculée par un algorithme à partir de la clé principa

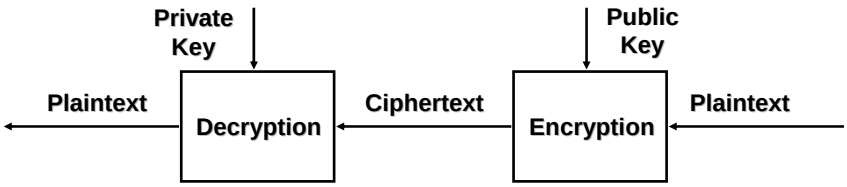
Asymmetric Algorithms

- RSA (Rivest, Shamir & Adleman)
  - most widely known & used asymmetric cipher
  - can be used to encrypt data in *both directions*
  - varying key sizes (512 bits, 1024 bits, …)
- DSA (Digital Signature Algorithm)
  - Digital Signature Standard (DSS) - NIST standard
  - key size 512 to 1024 bits
  - cannot be used for encryption; just for *digital signatures*
- KEA (Key Exchange Algorithm)
  - based on the Diffie-Hellman key exchange algorithm
  - cannot be used for encryption; just for *key exchange*

Asymmetric (Public-key) Algorithms

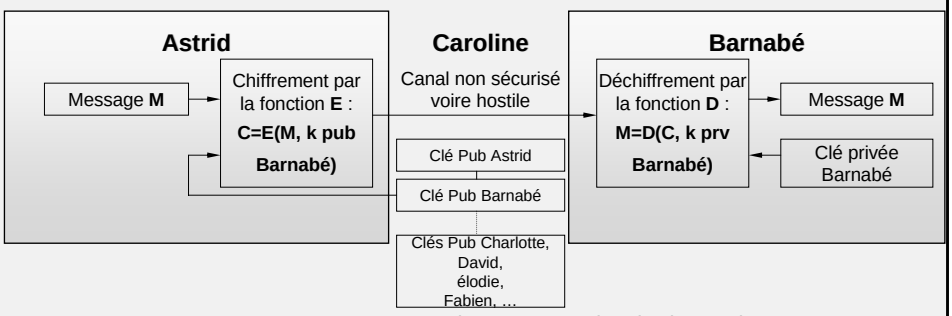


- Allows anyone to check origin/integrity of data



- Used in reverse to send secret data to the key owner

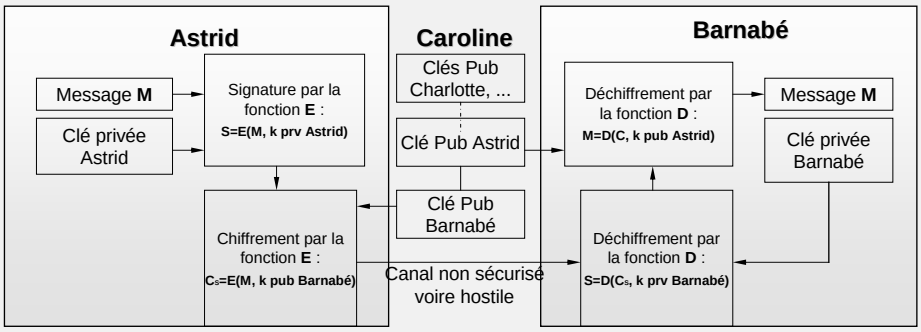
Cryptosystèmes à clés asymétriques



Protocole d'une transmission chiffrée par cryptosystème à clés asymétriques

1. Barnabé fabrique une paire de clés (publique + privée) à l'aide d'un algorithme de génération de clés asymétriques
2. Il donne sa clé publique à Astrid. Peu importe le moyen et le canal
3. Astrid chiffre un message en utilisant la clé publique de Barnabé, et envoie le message
4. Barnabé récupère le message et le déchiffre avec sa clé privée. Il est le seul à pouvoir le faire

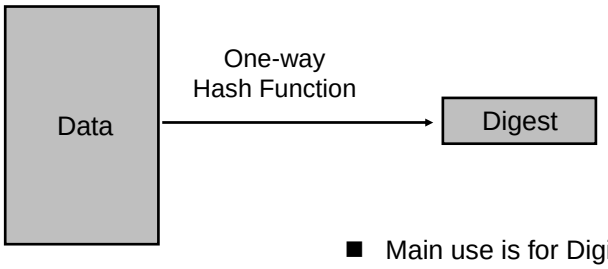
Cryptosystèmes à clés asymétriques



Protocole d 'une transmission signée puis chiffrée par cryptosystème à clés asymétriques

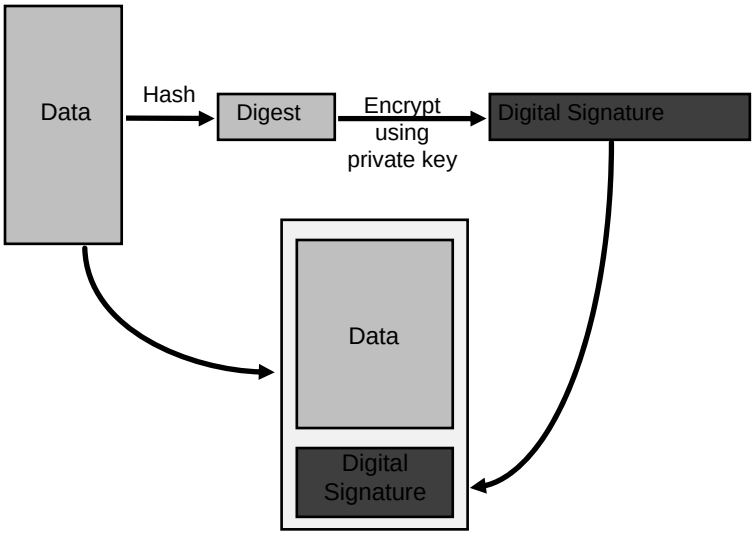
1. Astrid chiffre son message avec sa propre clé privée. Cette étape est la signature.
2. Elle chiffre le résultat avec la clé publique de Barnabé, et envoie le tout à Barnabé
3. Barnabé déchiffre le message avec sa clé privée. Il obtient le message qui a été chiffré avec la clé privée d'Astrid.
4. Il déchiffre le message avec la clé publique d'Astrid.

Hashing Algorithms

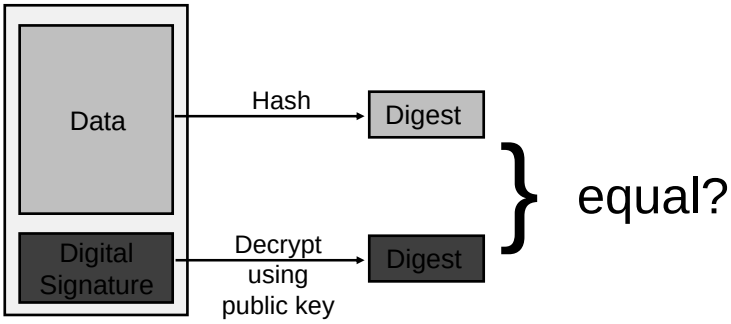


- Main use is for Digital Signatures
  - MD5 (Message Digest 5)
    - 128 bit digest
  - SHA (Secure Hash Algorithm)
    - NIST Standard to complement DSA
    - 160 bit digest

Digital Signatures



Digital Signatures



Signatures

- En général, on signe un hash du message
- Une signature n'est vérifiable que si la clé publique est de confiance
- **Certification :**
  - une clé publique signée par une tierce partie de confiance forme un certificat
    - vérifier la signature du certificat
      ⇒
    - faire confiance au certificat (clé publique) reçu
      ⇒
    - vérifier les signatures correspondant à cette clé publique
  - certification = transmission de la confiance

PKI

- PKI
  - Public Key Infrastructure ou Infrastructure de Gestion de Clés
- une PKI est un ensemble de systèmes, procédures et politiques pour :
  - enregistrer des entités
  - produire des clés privées et des certificats
  - stocker et distribuer les certificats
  - révoquer des clés ou des certificats
- trois entités principales :
  - l'autorité d'enregistrement : AE (doit être en ligne)
  - l'autorité de certification : AC (doit être hors ligne)
  - le service d'annuaire (doit être en ligne)
- tous clients d'une AC doivent obtenir sa clé publique par un chemin de confiance au préalable

X 509 Certificate

Version
Serial number
Algorithm of signature
Name of certification authority
Validity
- Begin
- End

Subject (holder of certificate)
- Name
- Public key

Extensions (optional)
- Key identifier
- Key usage
- Alternative names
- Attributes
- Limitations
- CRL distribution points
- Private extensions

Signature of CA

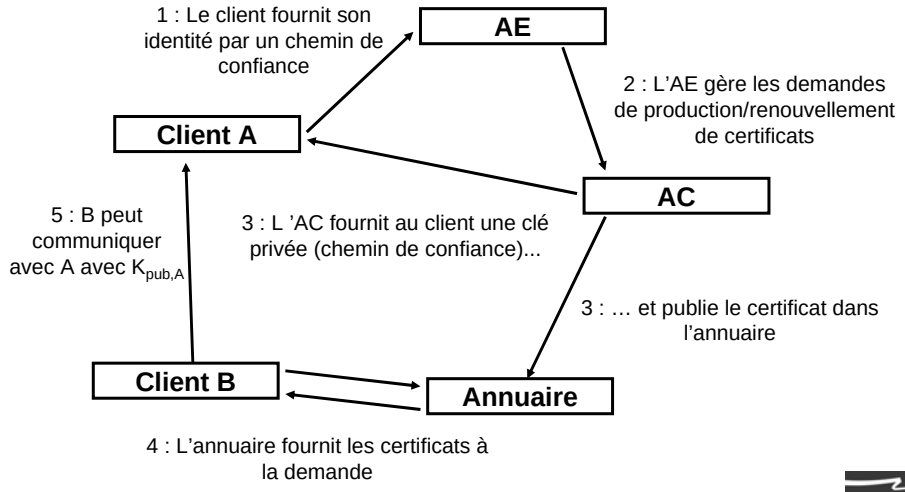
ToBeSigned

PKI Components for Digital Signatures

Infrastructure System
- Registration
- Certification
- Directory
- Time Stamping

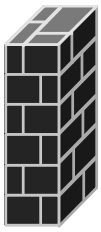
End User System
- Signature Component
- Verification Component
- Visualisation Component

PKI



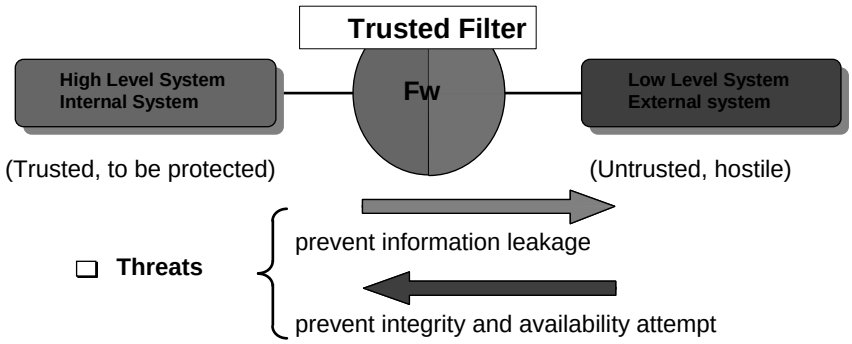
Pare-Feu & Filtre de Confiance

implémentation d'une fonction de sécurité: le contrôle d'accès



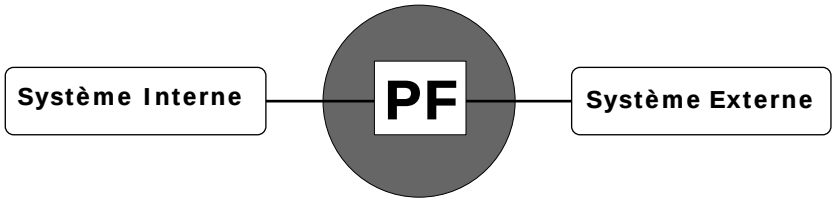
Un exemple d'application des Critères Communs

Firewall requirement



- To interconnect two networks with different sensitivity level
- To counter threats
  - Information compromising (information leakage) from HLS to LLS
  - Availability and integrity from HLS

Pare-feu et Filtre de Confiance

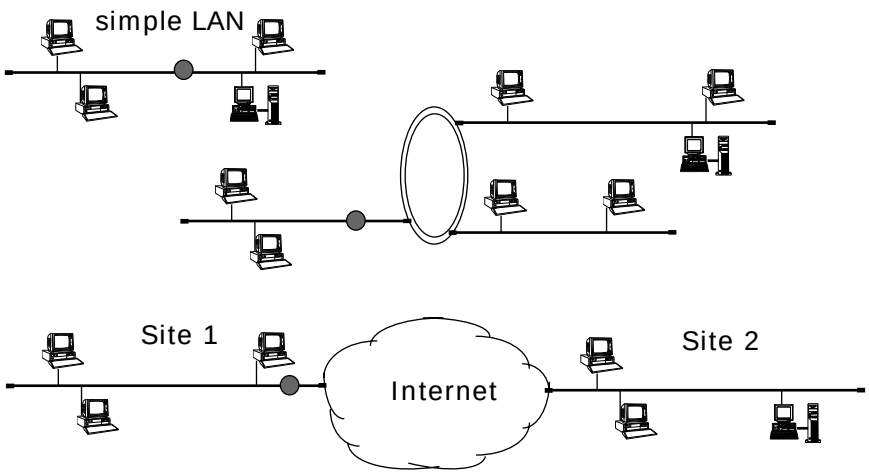


- En Général :
  - Interconnecter deux réseaux de niveaux de sensibilité différents
  - Contrer les menaces
    - Compromission de l'information (fuite d'information) de Système Interne vers Système Externe
    - Atteinte à la disponibilité (bourrage, déni de service) et à l'intégrité (altération des données) de Système Interne

Pare-feu

- Évolution et complexification des entités réseau
- Les produits standards intègrent une certaine sécurité
- Routeur classique
  - Analyse de la source et de la destination (adresse IP et port TCP)
  - Règles simples (acceptation et/ou refus)
- "Firewall"
  - Terminologie floue
  - Focalisé sur Internet
  - Souvent lié aux applicatifs de navigation sur Internet

Network configuration for a Trusted Filter



Information System Security

- Strict legislation/regulation compliance
  - Organizational, geographical and structural compartment of information depending upon sensitivity and Need To Know
- Network evolution and communication development :
  - Data and process are distributed
  - Data volume ("multimedia") increasing drastically with high speed networks
  - Cost reduction (Commercial technology and need factorization)
  - Interoperability requirement
  - Affordable security : need for multi-level system solutions
  - Complexity emergence : size of applications
    - Mobile software, (intelligent) Agents, Java applications
- Ability to counter increasing threats
  - Necessity to provide pragmatical solutions through :
    - Multiple applications : database exploitation, file transfer, e-mail, etc.
    - Configurable security policy : sites, periods, contexts, ...

Trusted Filter

- TF
  - Between 2 LANs operating at 2 different levels
    - Sensitivity X and Y and/or
    - Security Policy {X => Y} and {Y => X} are different
  - Protecting LAN X from LAN Y
  - Full OSI layer filtering (protocol and user data)
- Interoperable
  - Transparent vis-à-vis all OSI layers (applications and protocols)

Threats in the OSI layers

7 : application => identification & authentication

6 : presentation => end-to-end encryption

5 : session => authentication of nodes

4 : transport => encryption

3 : network => encryption

2 : data link => encryption, authentication

1: computer hardware, bus, wire, "ether" (radio, microwaves)

Mediatic Warfare :
integrity

image & voice manipulations

Information Warfare :
availability & integrity & confidentiality

computer (virus, Trojan horse,..)
network (intrusion,saturation)
covert channels (leakage)

Electronic Warfare :
confidentiality & availability

Information Filtering

Application Data

7
6
5

Protocol Data

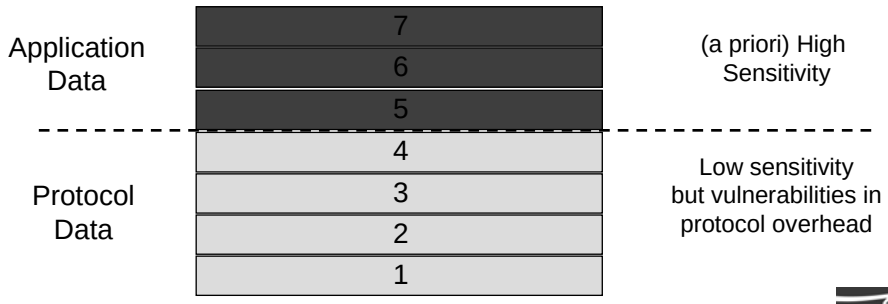
4
3
2
1

Complex syntax and semantically rich layers : but more and more "service layer" with small flexibility in verbose protocols

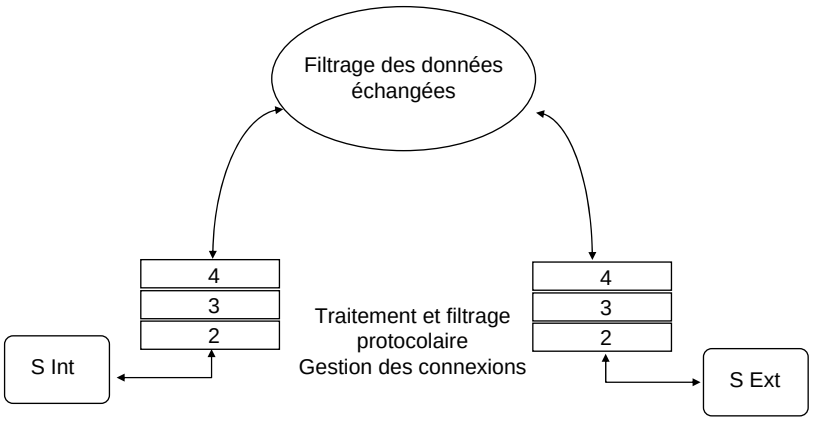
Well known & rigid syntax : but degree of freedom for covert channels

Information Sensitivity

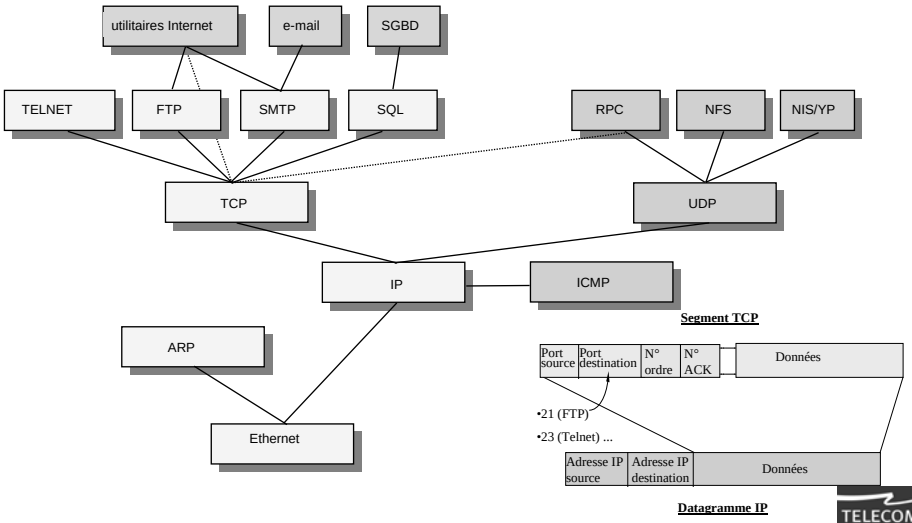
- Nowadays, Systems are "open" : interfaces have no privacy
- Protocols (layers 1 - 7) may be controlled
  - by high sophisticated "format & sequence analyzing" filters
- User & specific application data flows may be controlled
  - by human operator or proprietary automatical filters



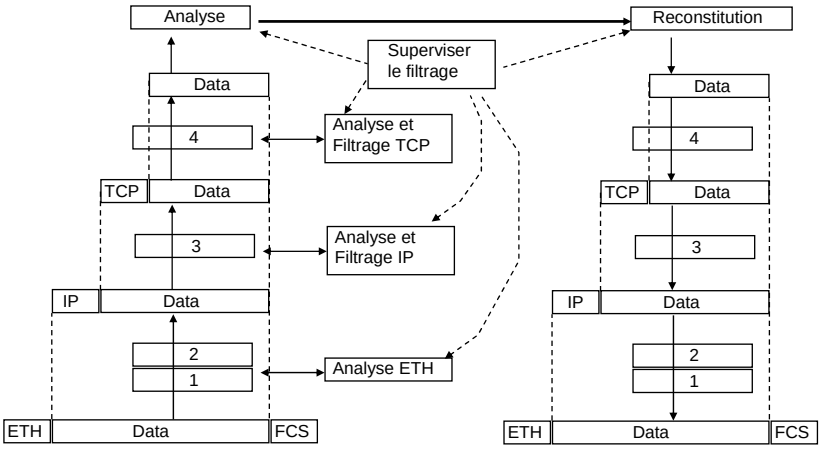
Fonctions de filtrage



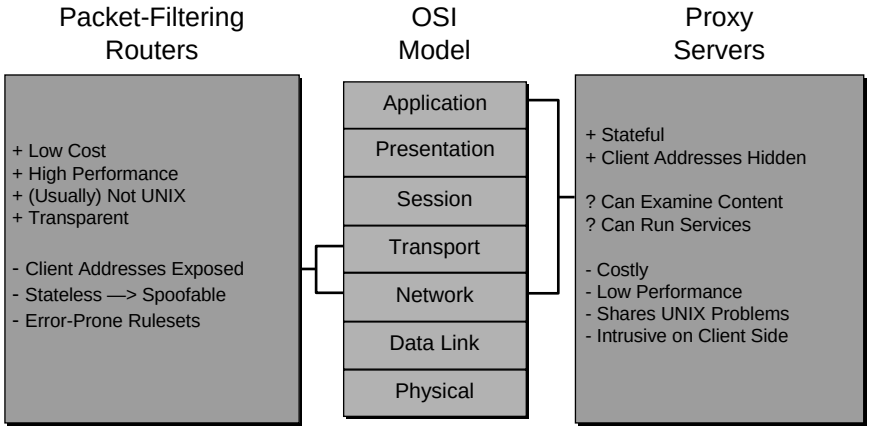
La suite TCP/IP et les applications



Décomposition et recomposition des trames

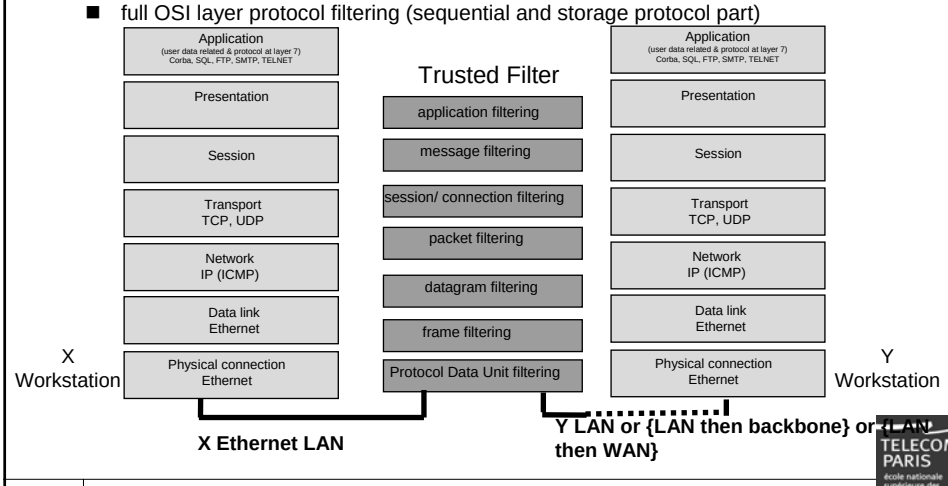


Traditional Firewall Approaches

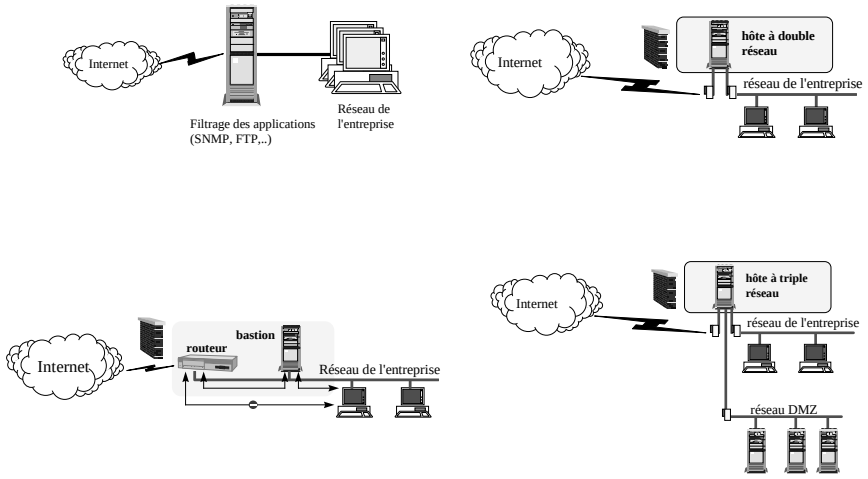


OSI Layer filtering

- user type filtering (identification, authentication, group,...)
- user data filtering (syntactical, semantical for voice, text, image data)
- application class / command / protocol filtering
- full OSI layer protocol filtering (sequential and storage protocol part)



Configurations



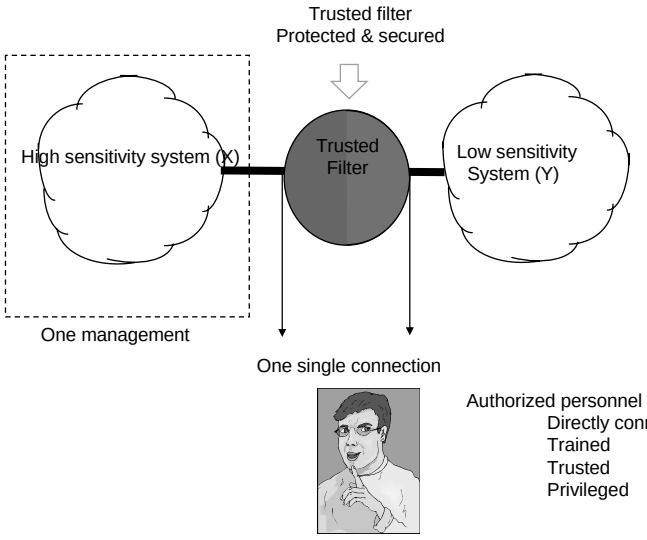
Protection Profile Overview

- Guard
  - Between 2 LANs operating at 2 different levels
    - Sensitivity X and Y and/or
    - Security Policy {X => Y} and {Y => X} are different
  - Protecting LAN X from LAN Y
  - Full OSI layer filtering (protocol and user data)
  - COTS
- Security
  - Protection profile providing a CC high level of assurance EAL 5 and affordable security
- Configurable
  - Protection in Confidentiality, Integrity and Availability which may be configured according to contexts in terms of :
    - Network, time, security severity
- Interoperable
  - Transparent vis-à-vis all OSI layers (applications and protocols)

Subjects & Objects

- Objects
  - Information objects
    - From X or Y networks
      - User data
      - Protocol data
  - Configuration objects
    - Hardware
    - Software (executables)
    - Security relevant data (parameters, ...)
  - Logged objects
    - Security relevant data (security events,...)
- Subjects
  - Authorized Personnel
    - in direct contact with Trusted Filter
      - Security Officer
      - Local Operator
      - Administrator
  - Legitimate X & Y network users
    - in logical contact with Trusted Filter
    - through binding
  - Machine & Network Subjects
    - representing legitimate users

Secure Usage Assumptions



Authorized personnel
Directly connected
Trained
Trusted
Privileged

Organizational security policy

- relating to Objects
  - Traditional => Licit Access Control
    - SU(X) transfers O to SU(Y) at time t (or vice-versa)
  - Covert Channels => Illicit Access Control
    - No other information conveyed while transporting O
- relating to Subjects
  - SA : authorized Personnel
    - Role-based Security Policy
    - Separation of duty
      - SSO (Security Officer) manages
      - SOP (Local Operator) operates
      - SAD (Administrator) administrates System ("system engineer")
    - Accountable of their actions
  - SU : legitimate Users
    - Group-based Security Policy
    - Accountable of their actions

Security policy model

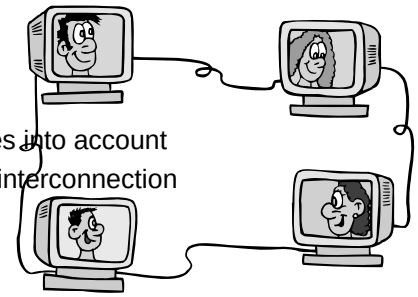
- SA operate the Trusted Filter
  - Security Officer defines & manages Security Policy
  - Operator operates the Trusted Filter
    - visualization of information (OI) in human understandable format
  - Administrator installs & maintains the Trusted Filter
- Users (sometimes authenticated) transfer Object information through the Trusted Filter
  - using the OSI protocol
  - according the security policy
    - licit access control :
      - user(X) is authorized to transfer the authorized object Object
      - belonging to the authorized application A at the moment of exchange t
      - to the authorized user(Y)
    - illicit access control
      - during licit transfer, user(X) is not authorized to convey extra parasitical information to Y
- Trusted Filter generates Logged information
  - security events recorded for audit

Security policy

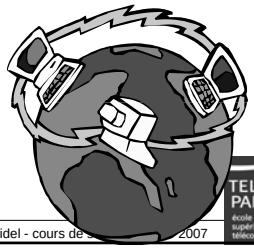
- Policy (actors)
  - Security Officer
    - security configuration and audit, maintenance

  - Operator
    - filter activation and filtering audit

- **Policy of LAN X**
  - takes into account
  - the interconnection



- **Policy of LAN Y**



Threats

- accidental : human errors
  - on FW parameters: not correct filtering parameter entry, ...
  - on transiting information : wrong communication parameter, wrong file, ...
- intentional (1) : a subject (user, outsider, ...) may gain the ability to observe and/or modify
  - on Fw device : hw/sw configuration, security parameter modification, audit trail corruption, ...
  - information from X LAN while in transit :
    - layer 1 - 2 - 3 : network address spoofing attacks, active taps, ...
    - layer 4 - 5 - 6 : covert channel exploitation, ...
    - application layer
      - "de facto standard " protocols (FTP, XML, Corba, ...) : malicious use, ...
      - user data : malicious direct channel exploitation, ...
- intentional (2) : a subject (user, outsider, ...) may gain the ability to consume resources
  - message flooding from LAN Y towards LAN X via Fw, ...
  - browsing LAN X information from LAN Y, ...

Threats

- Threats addressed by Fw
  - relating to Information Objects
    - User Data (human understandable format)
    - Protocol Data: (in)-direct exchange (sequential or storage channels)
  - relating to Configuration Objects
    - from Subjects
      - Administrator, Operator, Users
    - from Trusted Filter Design
      - security functions not existing
      - flaws, resources not sufficient
  - relating to Logged Objects
    - audit data not existing, lost, destroyed, not exploitable
    - events not traced
- Threats addressed by the environment
  - relating to Trusted Filter
    - Direct threats on Trusted Filter: physical attack, crash (or failed)
    - Trusted Filter not running correctly
      - not properly installed, configured or maintained by SA (SAD)
      - not properly managed and operated by SA (SSO and SOP)
  - relating to Information Objects
    - Transfer of direct (bad or malicious) information
      - accidental or intentional
      - at the initiative of X or Y users

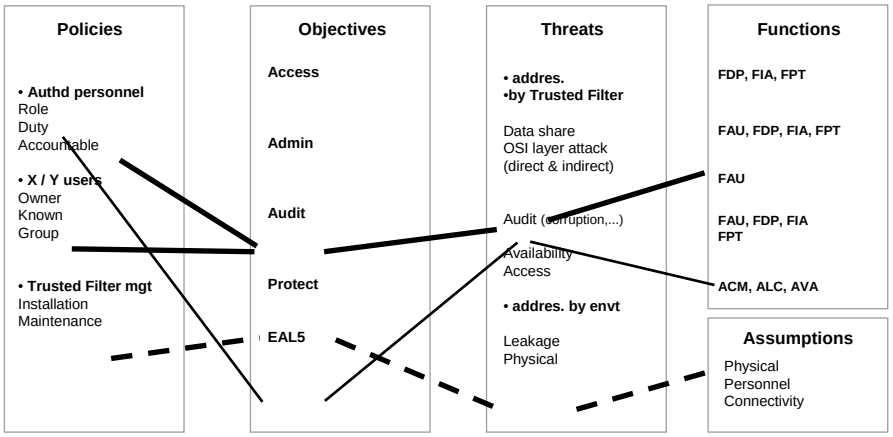
Security objectives

- IT security objectives
  - Security policy is configurable
    - decided by Security Officer
  - Attributes of configurability
    - {X =>Y} and {Y => X}
    - time, context, ...,
    - legitimate users SU (identified through binding SN)
    - application class (file transfer, data base exploitation, ...)
    - flow control (frequency of connections,...)
  - Trusted Filter is correctly
    - designed, protected & operated
- Non IT security objectives
  - Fw
    - physically protected
    - installed properly
    - no other connection
  - Authorized Personnel
    - trained
    - trusted

CC or ITSEC Validation

- CC EAL 5 Validation
  - Target of Evaluation
  - Security formal Model
  - Interpretation informal of the model in the target context
  - Structured description of the architecture
  - Detailed design is structured
  - Test documentation
  - Test tools and scenarios
  - Source code
- ITSEC E4 Validation
  - Target of Evaluation
  - Security formal Model
  - Functional Specifications are semi-formal
  - Interpretation informal of the model in the target context
  - Structured description of the architecture
  - Detailed design is structured
  - Test documentation
  - Test tools and scenarios
  - Source code
  - Informal tracability between design <=> code and graphics

PP Completeness of the Objectives



Examples of Tracability

Les Cyber-attaques

La Guerre de l'information
Les 7 formes de guerres de Martin Libicky
Les vulnérabilité selon les ITSEC
L'attaque d'un système par le renseignement
Le modèle d'attaque

La Guerre de l'information (1) de M Libicky

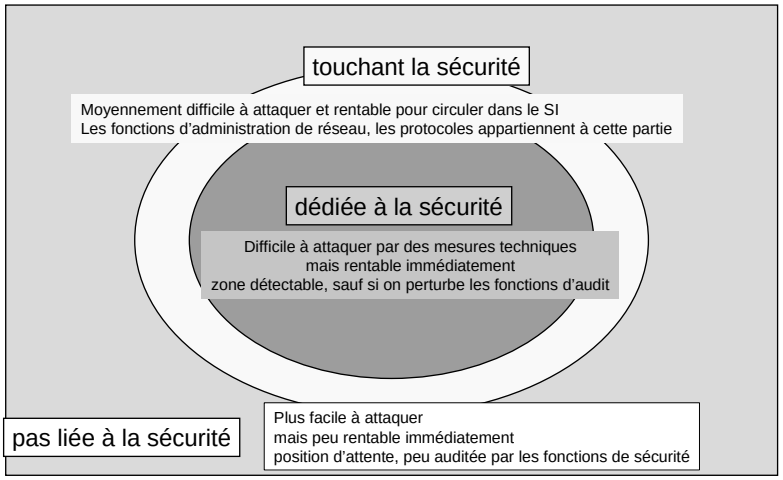
- La guerre électronique (Electronic Warfare, EW)
  - ensemble des formes d'action dans le domaine des ondes électromagnétiques
  - Les trois volets classiques sont
    - les Mesures de Recherche Électromagnétique (MRE) dont les actions consistent à rechercher, intercepter, localiser, identifier et analyser les émissions adversaires et à émettre les synthèses de résultats nécessaires,
    - les Contre-Mesures Électroniques (CME) qui consistent à des actions de brouillage et de déception et
    - les Mesures de Protection Électronique (MPE).
- La guerre de l'informatique (Hacker War, HW)
  - attaques dirigées contre l'outil informatique : les modes opératoires sont basés sur l'exploitation des propriétés du système attaqué
  - multitude d'actions souvent reproductibles comme le détournement de services, le vol ou la consultation d'informations sensibles, le sabotage momentané ou définitif, le contrôle illégal de système géré par informatique (virus, cheval de Troie ou autres vers)

La Guerre de l'information (2) de M Libicky

- La guerre par l'information (Information-based Warfare, I-bW)
  - concerne l'utilisation massive, systématique et organisée d'informations provenant de capteurs divers dans la mise en œuvre de systèmes d'armes. Ceux-ci seront d'autant plus précis et redoutable que la capacité d'exploitation et de synthèse de l'information reçue sera grande.
- Le blocus de l'information (Information Blockade, IBW)
  - vision qui repose sur la constatation que l'économie d'un pays dépend continuellement d'informations extérieures. Un blocus systématique affaiblirait l'économie à moyen et long terme. Pour l'instant cette composante relève de la prospective dans la mesure où les nations ayant un besoin permanent d'informations extérieures sont également souvent celles qui les produisent. Toutefois, la guerre par le blocus de l'information pourrait prendre en compte certains aspects de la guerre médiatique décrite ci dessous.
- La guerre médiatique (Psychological Warfare, PSYW)
  - un ensemble de techniques qui visent à utiliser l'information comme instrument de confusion, de dissuasion et de persuasion ou plus exactement de gestion de l'opinion publique.
- Le conflit cybernétique (Cyber War, CW)
  - vision extrême et futuriste de la guerre de l'information incluant la guerre des systèmes ou guerre de Gibson et la guerre par simulation
    - La guerre des systèmes désigne un monde où des systèmes cybernétiques définis comme des mélanges d'informatique, de communications, d'intelligence artificielle et de robotique seraient conçus pour diriger tout ce qui pourraient tomber sous leur contrôle dans le but de détruire les forces adverses
    - La guerre par simulation est une vision plus réaliste qui tient compte de l'essor de la simulation dans le domaine militaire (outils d'aide à la décision, d'évaluations opérationnelles, jeux de guerre,...) et de l'amélioration permanente des modèles utilisés

La segmentation d'un SI du point de vue de la sécurité :

3 parties découpées selon les ITSEC
pas liée à , touchant, dédiée à la sécurité

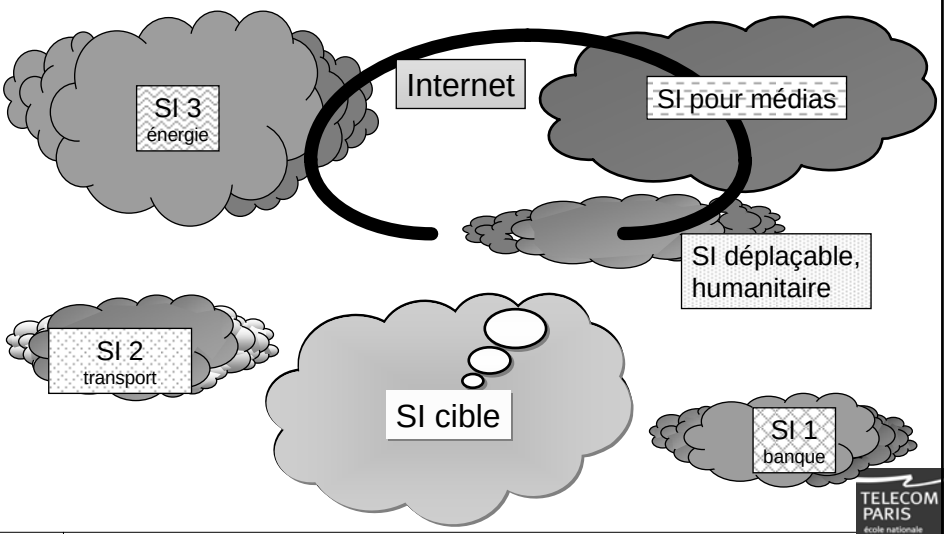


La segmentation «sécurité/zone fonctionnelle» des Attaques

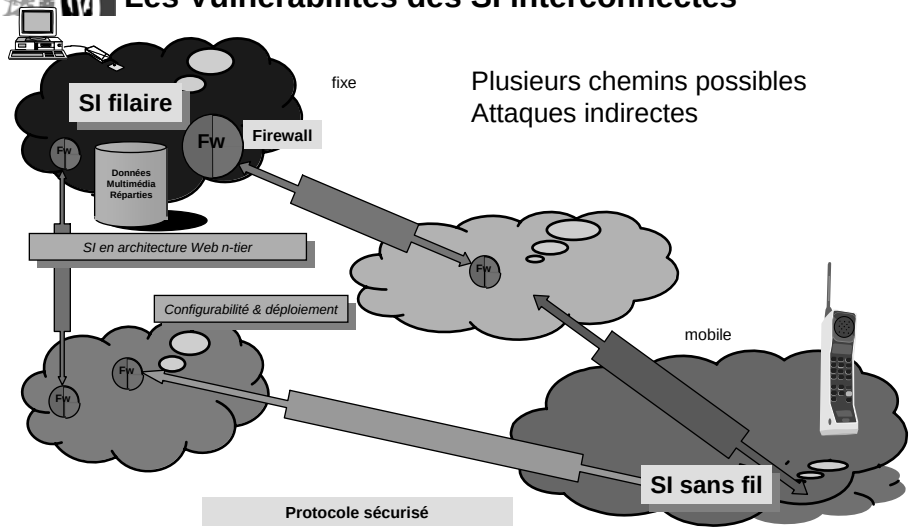
Segmentation des attaques	1 application	2 poste de travail	3 réseau privé	4 réseau distant
A partie liée à la sécurité	gestion des éléments secrets, autorisation, chiffrement de fichiers, messagerie sécurisée,...	fonctions de sécurité du poste (authentification de la station,..), système d'exploitation sécurisé,..	protocole sécurisé, serveur de sécurité, niveaux 1, 2, 3, 4, routeur sécurisé,..	"firewall", serveur de communication, gestion de la sécurité des filtres, chiffrement d'artères,...
B partie touchant la sécurité	services et logiciels intermédiaires, BD, interface client-serveur, M2M,...	système d'exploitation, gestion des entrées-sorties, gestion des tâches et de la mémoire, ergonomie,..	protocoles, réseau local ou privé, niveaux 1, 2, 3, 4, gestion du réseau	certaines caractéristiques des piles protocolaires, gestions de réseaux,...
C partie non liée à la sécurité	fonctions classiques de l'utilisateur, traitements, algorithmes, gestion de données, ergonomie,..	processeur, mémoire, bus, système d'exploitation, gestion des fenètres, performances,..	choix des protocoles, fonctions internes des piles protocolaires, niveaux 2, 5, 6,...	choix des protocoles, fonctions internes des piles protocolaires et de passerelles,..

- **Un scénario d'attaque va consister à circuler dans ces pavés**
  - **pour aller progressivement de C4 à C1**
  - **en passant successivement par les pavés A4, …B3, … C2, B2, A2,**
  - **pour atteindre finalement C1 (si on veut paralyser une application)ou A4 (si l'on veut prendre en main le SI et sa sécurité)**
- **Cette sorte de «jeu de l'oie» est**
  - **très difficile à franchir par la ligne A (mais efficace)**
  - **plus facile à atteindre par la ligne C (mais plus lent et avec un résultat moins certain)**

Le SI et ses banlieues : l'extension géographique d'une cible d'attaque



Les Vulnérabilités des SI interconnectés



Plusieurs chemins possibles
Attaques indirectes

Les SI : les invariants / les permanents

Les "incontournables"
Microsoft
- Windows
- Bureautique

SUN, IBM, HP
- UNIX

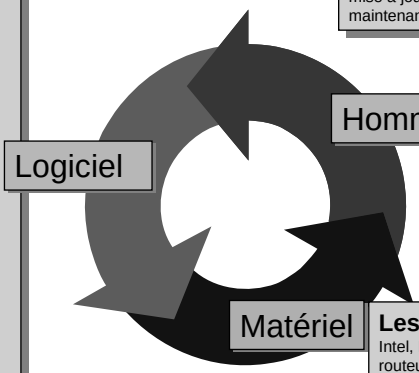
Messagerie
- Microsoft
- Lotus

Souches protocolaires
SGBD
- Oracle

Supervision
- CA
- HPOpenview

Butineurs
- IExplorer

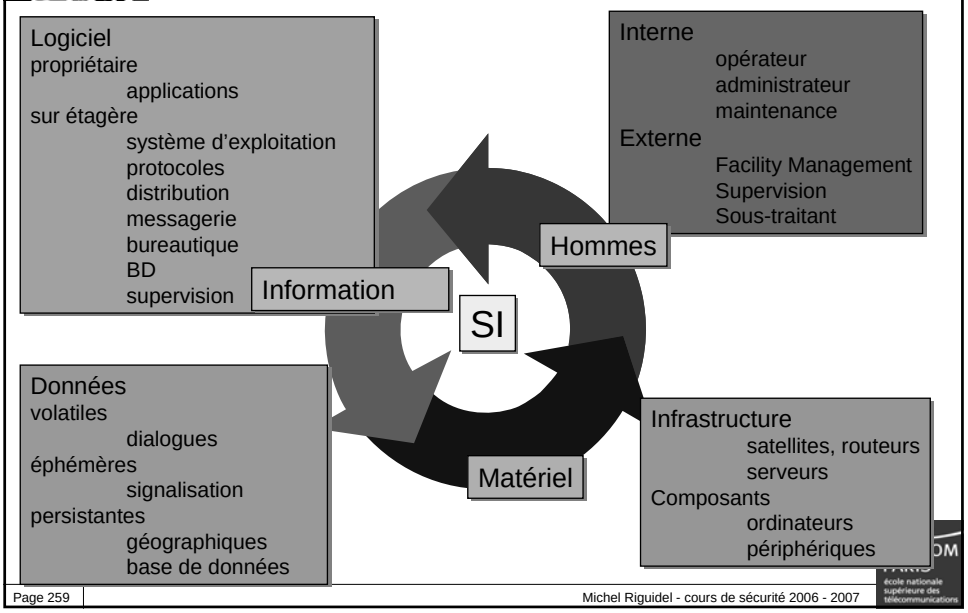
Annuaire X500
Technologie Web
- Browser sur serveur
- avec moteur Java



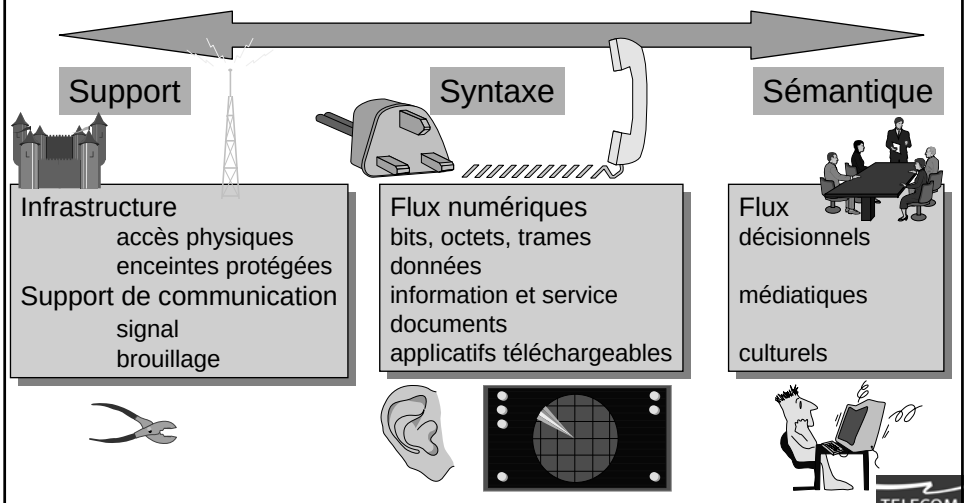
Les "insoupçonnables"
mise à jour logicielle
maintenance préventive et corrective

Les "incontournables"
Intel, Motorola, …
routeurs Cisco, PABX, Commutateurs
imprimantes
Photocopieurs en réseau

Les Flux



Axe de communication avec le SI



Axe de communication

Axe de communication	n°	support de l'attaque	angle d'attaque	forme d'attaque	métrique	nature de la défense	nature de l'attaque
sémantique	G	individu	culture	psychologique - médiatique	sondage d'opinion, simulation de modèle de crise et de modèle de sociétés	campagne de sensibilisation, pression médiatique	gestion de l'opinion publique (manipulation et propagande)
	F	ensemble d'individus	flux organisationnels	économique	nombre de personnes immobilisées, sans travail	se couper de l'information extérieure	coupure d'approvisionnement, Embargo
syntaxe	E	organisation	organisation				infiltration, perturbations
	D	distribution de services et de documents	information	informatique, espionnage classique	valeur du secret	sécurité de systèmes d'information	vol, falsification
	C	communication	réseaux et systèmes	informatique	taille de la brèche	chiffrement, cryptologie	pénétration, écoute
médium	B	support de la transmission	vecteur de transmission	électronique	réduction du flux d'informations	Tempest	brouillage
	A	infrastructure	urbanisation,...	physique	en m2 et jours d'indisponibilité	bâtiment protégé	destruction

Axe de l'interface entre l'attaquant & le SI

À découvert | À la merci | À l'abri

Usurper l'identité du sujet
- vol de l'identité
- vol de la signature
- vol du mot de passe

Attaque directe
- destruction
- atteinte à l 'intégrité
- saturation du réseau
- atteinte à la disponibilité

Complicité interne
- synchrone ou asynchrone

Entremise, Intervention
- d'un sujet ou d'un objet
- écoute passive
- « man in the middle »

Attaque semi-directe
- atteinte à l 'intégrité
- saturation du réseau
- atteinte à la disponibilité

Attaque semi-indirecte
- atteinte à la confidentialité
- saturation
- rejeu

Encapsuler dans un objet
- cheval de Troie
- virus
- écoute passive

Attaque indirecte
- mine logicielle

Axe Structure du SI

1 à 1	n à p	Tout à Tout
Structure fermée cloisonnement structure maître esclave multi-niveaux politique de sécurité avec rôles bac à sable Java	Structure hybride informatique communicante structure arborescente, en grappes, hiérarchisées architecture client-serveur	Structure ouverte interopérabilité informatique partagée informatique distribuée réseaux bus serveur

Les priorités de l'attaque

- **utilisation du défaut de sécurité**
  - Mettre en doute la confiance de l'utilisateur
  - Mise en défaut de l'exigence d'assurance de sécurité du SI
- **utilisation du défaut de protection**
  - Mise en défaut de l'exigence de fonctionnalités de sécurité du SI
- amplifiée par
  - banalisation et accès de plus en plus facile à la technologie (coût faible)
  - interconnexion des réseaux
  - conscience et sensibilisation insuffisante
  - Envie du "vrai" (authentique) => 1e priorité (intégrité des données du SI)
  - Protection des secrets => 2ème priorité (confidentialité du SI)
  - Protection des fonctions de sécurité => 3ème priorité
    - authentification, contrôle d'accès
    - confidentialité, intégrité de l'information
    - non répudiation
    - disponibilité des ressources
  - ➔ démocratisation des outils et du savoir-faire de piratage
  - ➔ nouvelle délinquance & idéologie

Les dimensions essentielles de succès d'une attaque

- La connaissance du Système Cible
  - la fonctionnalité du Système et son exploitation
  - la mise en application de la politique de sécurité
    - technique (sécurité et partie cryptologique), organisationnelle, physique
  - l'administration du réseau à l'intérieur et à l'extérieur du SI
- La discrétion de l'Attaquant
  - détectabilité peu nécessaire en cas de destruction du SI ou d'impact fort (terrorisme)
  - dans tous les autres cas, la détectabilité est conditionnée par :
    - célérité de l'attaque : tellement rapide que l'application de la politique de sécurité ne peut pas réagir en temps réel
    - les actions d'attaque ont une durée certaine mais sont furtives (actions sur des zones peu auditées par les utilisateurs ou les administrateurs)
- La compromission de l'Attaquant vis à vis de l'environnement et du système
  - Lorsque la connaissance du SI est a priori faible et lorsque la date de l'attaque est proche, la compromission est inéluctable
  - D'où la nécessité de périodes de renseignement longues, pour éviter ce scénario
- L'impact de l'Attaque
  - L'impact est maîtrisé si le scénario d'attaque est constitué en «modules» d'attaques bien identifiés, séparés et progressifs
  - Non mesurable: Attaques aveugles, d'un seul tenant («attaque en bloc dans l'obscurité»)

Le modèle en étapes d'une attaque

- Au niveau du piratage informatique, un modèle en étape peut être appliqué.
- Il comprend 4 étapes:
  - ➔ L'établissement d'une liaison physique
  - ➔ L'identification d'un protocole de communication
  - ➔ La reconnaissance des services disponibles
  - ➔ L'accès au système d'information

Applications accessibles.
Services accessibles.
Protocole(s) de communication.
Lien physique

étape A
L'établissement d'une liaison physique

- La première étape consiste à trouver un moyen d'accès au système cible
  - Celui-ci peut être un des postes du système
  - Il peut aussi résulter des ressources de communication que le système cible utilise.
- Si le système utilise des liaisons téléphoniques commutées (ou d'autres liaisons à établissement de connexion à la demande)
  - la connaissance du numéro d'appel est un élément précieux
    - Ce numéro peut être trouvé par des moyens classiques de renseignement ou par essais successifs.
    - La recherche au sein d'une tranche de numéros se fait par programmation d'un automate pour essayer tous les numéros et identifier ceux qui correspondent à une liaison informatique.
- Si le système cible utilise exclusivement des liaisons permanentes,
  - il est alors nécessaire de s'introduire sur le réseau qui supporte ces liaisons permanentes. Ceci peut être fait,
    - soit par l'accès normal aux services de ce réseau et la connaissance de l'adresse du système cible sur le réseau (cas des réseaux privés utilisant le réseau Internet),
    - soit par réussite d'une première attaque donnant accès aux organes de routage du réseau considéré.

étape B
L'identification du protocole de communication

- Les systèmes informatiques utilisent pour dialoguer entre eux des protocoles de communication
  - c'est à dire des ensembles de règles qui leur permettent de se connecter puis de communiquer.
  - Pour dialoguer avec un ordinateur, il est nécessaire de connaître le (ou les) protocole(s) de communication que celui-ci sait traiter.
- Les protocoles de communication sont assez peu nombreux pour que par essais successifs, il soit possible de trouver celui qui est reconnu.
  - En réalité, par le contenu des réponses à certaines sollicitations, il est possible en un nombre réduit d'essais de savoir quels sont les protocoles reconnus.
  - Lorsque le type des équipements distants est connu la combinatoire des protocoles se réduit considérablement.
- Les générateurs et les analyseurs de protocoles apportent une aide efficace pour cette phase des travaux.
  - Ces fonctions, de génération et d'analyse, peuvent être émulées par logiciel.

étape C
La reconnaissance des services disponibles

- La reconnaissance des services réseau disponibles n'est pas si difficile
  - Les services s'identifient lorsqu'ils reçoivent une demande distante.
  - Ces dispositifs pratiques pour assurer l'interopérabilité sont aussi utilisables dans le cadre du piratage informatique.
  - La connaissance du système permet de connaître les fonctionnalités potentielles.
- Le connaissance des services optionnels peut nécessiter des tests individuels.
  - Ceux-ci peuvent être réalisés rapidement et sont facilement automatisables. L'usage d'un générateur de protocole peut, pour cette étape aussi, être d'une bonne efficacité .
    - Remarques : Lorsque l'action est menée directement sur un poste du système, la méthode d'approche reste identique : identification des protocoles, puis des services accessibles depuis ce poste.
- Tous les postes et tous les liens d'accès à un système n'utilisent pas nécessairement les mêmes protocoles et n'ouvrent pas les mêmes services

étape D
L'accès au SI (1)

- L'attaquant du système cible dispose d'un moyen d'accès et d'un ensemble de services de communication qui lui sont accessibles.
  - Si le système cible a été sécurisé,
    - ces services sont réduits au strict nécessaire pour les applications supportées par le système cible et sont dans un état technique réputé sûr.
    - L'attaquant doit savoir continuer son attaque avec ces moyens réduits, ce qui peut être très difficile.
  - Dans le cas contraire,
    - la grande majorité des cas, beaucoup de services sont ouverts, ils ne font l'objet d'aucune surveillance rigoureuse, et leurs caractéristiques fonctionnelles précises n'ont fait l'objet d'aucune analyse particulière
- L'attaquant va alors
  - Par farfouillage (ou butinage) prendre connaissance de l'environnement et glaner des informations lui permettant d'approfondir ses actions sur le système.
    - Il pourra ensuite par altération modifier des environnements d'exécution et ainsi agrandir son domaine d'investigation.
  - Par essais successifs essayer de se connecter aux applications du système.
    - Dans certains cas, ceci peut ne présenter aucune difficulté particulière.
  - Par exploitation des bugs contenus dans les services disponibles, il est possible de sortir du domaine dans lequel ces services sont normalement cantonnés et ainsi d'atteindre d'autres environnements d'exécution, donc d'autres données.

L'accès au SI (2)

- A ce niveau, 3 cas sont à envisager
  - Le système est protégé et l'attaquant ne réussit pas à détourner les services disponibles à son profit.
  - L'attaquant réussit à se connecter à certaines applications ou services disponibles et à les utiliser. Il accède aux données gérées par ces sous ensembles. Ceci représente la majorité des cas.
  - Par itération, l'attaquant prend la maîtrise de l'administration du serveur. Il peut alors se déclarer comme utilisateur, s'allouer des droits et faire toutes les investigations qu'il désire.
  - L'attaquant peut essayer de rebondir vers un autre serveur connecté au précédent.
    - Cet autre serveur le reconnaîtra comme un usager du premier serveur et lui donnera accès à certains services. Sur cette nouvelle liaison, il pourra appliquer à nouveau ces outils d'attaque et chercher à forcer ce nouveau serveur.
  - Depuis ce nouveau serveur, il peut attaquer d'autres serveurs, y compris le premier qui, le reconnaissant comme un intervenant d'un serveur du système peut lui ouvrir des droits plus étendus que lors de la première connexion.
    - Le processus est itératif, ce qui nécessite des approches d'autant plus structurées que la cible visée est précise.
    - C'est un travail long et fastidieux, la progression se fait par à coup

Conclusions

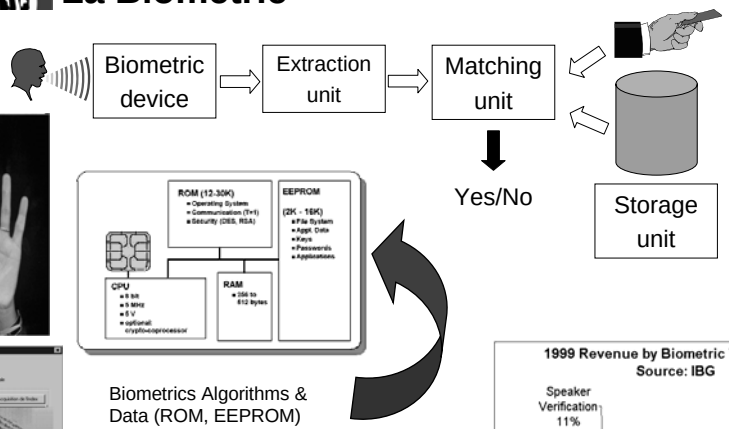
- Comme toute forme de lutte, le piratage informatique exploite les faiblesses du système cible pour parvenir aux finalités qui lui sont assignées.
  - La complexité des systèmes informatiques fait qu'il existe toujours des failles. Selon le contexte celles-ci peuvent être exploitées ou non.
  - Il y a des systèmes faciles à attaquer et d'autres qui le sont beaucoup moins.
- Il n'existe pas de méthodes permettant de réussir une attaque logique.
  - Il existe des "recettes" permettant dans tel ou tel contexte de connaître, altérer, gêner, arrêter, un système d'information.
  - Une application de ces recettes nécessite des spécialistes maîtrisant bien leurs outils car les contextes rencontrés demandent des ajustements permanents. Une approche méthodique est aussi nécessaire pour comprendre le système et ajuster les actions.
  - Le modèle en étapes est le principe de base du piratage informatique
- Il n'existe pas de méthodes permettant, dans tous les cas, de sécuriser un SI et de contrer de façon certaine une attaque logique.

La Biométrie

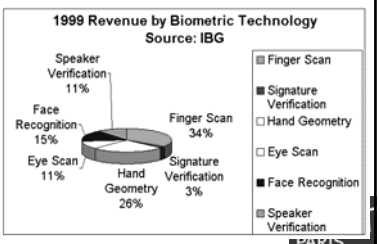
Monde Biométrique & Univers numérique

- Biométrie
  - L'individu est **unique** (et tangible), dure toute une vie et … vieillit
    - Pas (encore) de clones
  - Des marques caractéristiques l'identifient plus ou moins
    - Impossible de modifier ces marques
      - ➔ empreintes digitales, ADN (preuve pour la justice)
      - ➔ iris, morphométrie du visage?, de la main, voix ?, signature manuelle, geste
- Numérique
  - Le document numérique est
    - **volatile** : intangible, indépendant de son support
    - **vulnérable** : pas d'original et de copies, mais des clones
- Relier les Individus physiques aux Réseaux & Systèmes d'Information (SI)
    - injecter, à un moment donné, un «représentant» numérique dans le SI qui identifie une personne physique (et une seule)
      - enregistrer au préalable (au moins une fois) un étalon et stocker ce spécimen, et ce, de manière sécurisée
    - utiliser cette représentation pour garantir ou assurer la sécurité de certaines opérations
      - retrait bancaire, accès à un édifice ou véhicule, ouverture de session informatique, …
- Si le biométrique est numérique, il devient vulnérable
    - sécuriser ce représentant
      - intimité numérique pour la réalité virtuelle, jeton pour authentification, …
    - en évitant les copies
      - usurpation de l'identité par vol de ce jeton sous forme de rejeu
    - et les méprises
      - utilisation abusive ou frauduleuse

La Biométrie



Biometrics Algorithms & Data (ROM, EEPROM)



Le code biométrique

- Ce code sert déjà à identifier l'individu
  - code ADN (crimes, …)
  - empreintes digitales (intrusions, vols, …)
  - voix au téléphone (écoute téléphonique)
  - visage (caméra de surveillance)
- Ce «code» est unique ; il n'est pas secret
  - de plus en plus l'homme laisse des traces numériques souvent à son insu
  - ce code n'est en aucune façon une «clé cryptographique»
- La saisie de ce code est complexe et n'est pas immédiate
  - dans la pratique, le masque numérique enregistré n'est pas **unique**
    - différentes façons de photographier un visage
  - et possède une part de **flou**
    - expérience non répétitive (voix, etc.)
  - exploitation et robustesse : un traitement mathématique et/ou statistique intervient pour valider le masque de manière plus fiable
  - le résultat biométrique fournit une **chaîne de bits**
    - cette chaîne de bits n'est pas engendrée par un moteur qui fabrique du hasard
  - il doit être comparé à un patron originel

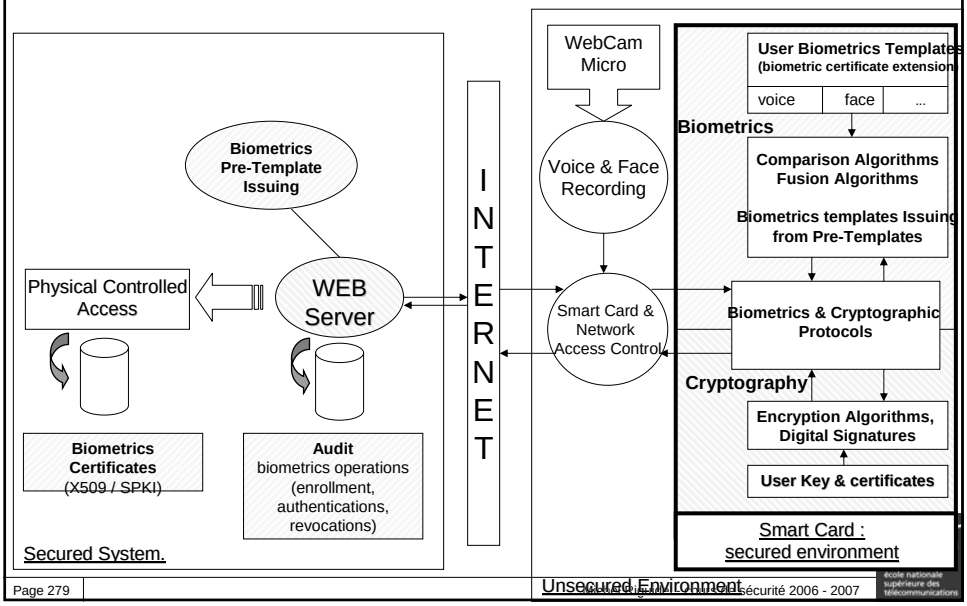
Biométrie et sécurité

- Système de sécurité
  - objectif de sécurité en fonction d'une opération sensible
    - rentrer dans un bâtiment, effectuer une opération bancaire, identification pour un vote tout en restant anonyme pour ce vote
  - menaces (usurper l'identité de la personne physique)
  - politique de sécurité et fonction de sécurité
    - identification (pas anonyme), authentification, non répudiation, imputabilité, contrôle d'accès à partir d'une liste d'individus (ACL : access control list)
  - mécanisme de sécurité
    - cryptographie : chiffrement (confidentialité) ou signature électronique (intégrité)
    - stéganographie : contrôle de l'origine ou du contenu (tatouage des images, des sons)
- Périmètre et Limites de la biométrie
  - individu physique dans la boucle
    - individu présent (protocole synchrone) et absent (protocole asynchrone)
    - délégation à un sujet numérique (agent logiciel travaillant pour le compte de)
    - «certificat biométrique»
  - groupes d'individus (entité morale) : somme de n individus
- Biométrie dans la chaîne de confiance : déploiement difficile et infrastructure lourde
  - il faut sécuriser la biométrie
    - attaque simple du rejeu à un moment de la chaîne
    - assurer une présence vivante pour éviter un fantôme (photo, doigt synthétique)
    - sécuriser le représentant de référence dans une base de données protégées, dans une carte à puce
  - en utilisant un protocole cryptographique
  - et (éventuellement) une entité de confiance personnelle
    - carte à puce, mots de passe

La Biométrie dans le numérique

- Utilisation potentielle de la biométrie
  - supprimer (?) les clés : mots de passe (digicode, ordinateur, carte bleue), clés de voiture, …
  - remplacées par une saisie facile d'un échantillon numérique
    - d'une partie du corps (empreinte digitale : effleurer un capteur) ou
    - du comportement (prononcer des mots, frapper des touches sur un clavier)
  - **conforter la sécurité d'un dispositif en accompagnant un secret par de la biométrie**
    - Le téléphone portable est un capteur biométrique merveilleux pour la voix. On peut s'en servir pour des authentifications de confort (en plus du mot de passe) pour vérifier le locuteur, avec une option de débrayage quand le propriétaire est enroué …
- Les SI enregistrent déjà beaucoup la biométrie
  - Présence numérique: on parle au téléphone, on frappe au clavier, ...
  - Traces numériques
    - on laisse déjà beaucoup de traces de sa présence dans les réseaux
    - trace directe (voix, visage, frappe au clavier) ou indirecte de sa présence (position géographique dans une cellule GSM, achat avec carte bancaire)
- Le code biométrique : profil(s) biométrique(s)
  - Chaque individu a un «code» spécifique
  - Chaque application (bancaire, télétravail, …) a un contexte déterminé
    - Quelles sont les sources utilisables ?
      - Capteurs (électronique et sécurité)
      - Traitements (mathématique, statistique et sécurité)
    - Quel est le bon profil ?
      - Pour l'utilisateur : en termes éthiques, ergonomiques
      - Pour le fournisseur : en termes économiques, juridiques, technologiques, …
    - Choix du profil en fonction de l'application
      - Le téléphone (GSM, UMTS) numérise par essence déjà la voix
      - Le distributeur de billets nécessite une frappe au clavier (et une présence physique debout ou assis), en présence de bruits ambiants (la voix n'est pas adaptée)
    - Question
      - hasard : les caractéristiques biométriques ne sont pas aléatoires
        → le code ne se comporte pas comme une clé cryptographique
      - unicité du code : jumeaux monozygotes ? futurs clones ?

Architecture pour la biométrie: bioPKI



Les Virus informatiques

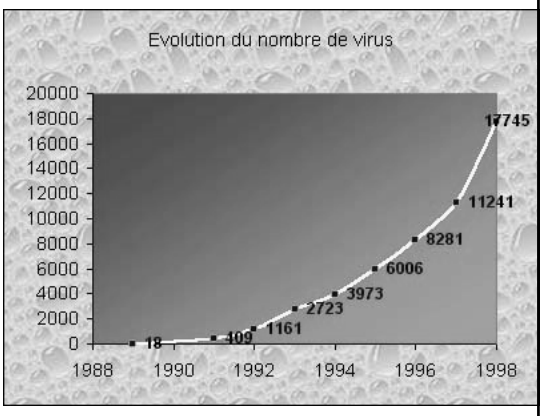
Qu’est ce qu’un virus ?

- Virus biologique
  - Le mode de reproduction des virus biologiques est unique en son genre et les place à la frontière de l'animé et de l'inanimé.
  - Incapables de se débrouiller seuls, les virus vampirisent une cellule en larguant dans celle-ci leur message génétique, ADN ou ARN.
  - Une fois introduit dans l'organisme hôte, le brin viral est transporté jusqu'à l'usine à protéines de la cellule qui le lit et exécute ses instructions.
  - C'est ainsi que naissent de nouveaux virus qui, une fois libérés, contaminent à leur tour d'autres organismes
- Virus logique
  - Tout programme d’ordinateur capable d’infecter un autre programme en le modifiant de façon à ce qu’il puisse à son tour se reproduire.
  - Est appelé **VIRUS** un programme qui a la propriété de se reproduire et de passer d’un système à un autre

Code pénal -Article 462-3. - Quiconque aura, intentionnellement et au mépris des droits d'autrui, entravé ou faussé le fonctionnement d'un système de traitement automatisé de données sera puni d'un emprisonnement de trois mois à trois ans et d'une amende de 10.000 F à 100.000 F ou de l'une de ces deux peines.

Chronologie

- 1960 : Core War : jeu de programme de combat dans la mémoire vive
- 1982 : 1er Virus : programme parasite sans but négatif, par Fred Cohen.
- 1986 : virus « pakistanais »
- 1988 : Robert Morris arrêté pour fraude informatique
- 1989 : 18 virus recensés
- 1992 : virus MichelAngelo
  - 200000 machines touchées
- 1998 : 17745 virus recensés
- 2000 : virus I love you
- 2002 : > 58 000 virus
- Aspects économique
  - Protection par Antivirus
    - 1998 en France 260 MF
  - Dégâts à cause des virus
    - nettement supérieur



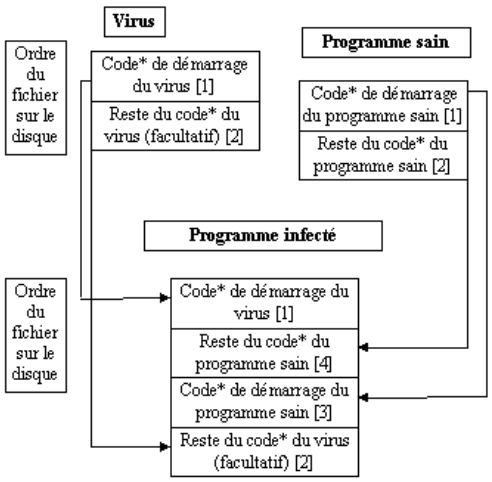
Typologie des virus

- Les virus classiques
  - Virus infectant le secteur d'amorçage
    au démarrage, support infecté, plus très courant (cf MS-DOS)
- Les virus d'Internet
  Utilisation de langage de programmation adapté à Internet
    - Java, utilisé aussi pour les applets Java ou Active X
  Propagation : téléchargement, email...
- Les virus Macro
  - infection de fichiers cibles, de Normal.dot dans Word, de macros particulières
- Programme destructeurs
  - Les vers (Worms)
  - Les chevaux de Troie
  - Les bombes logiques
  Ils peuvent être combinés avec des virus.

Petit exemple

5000 shell "dir *.bas /b >TOTO"	Cherche les fichiers cibles, et inscrit les noms dans "TOTO"
5001 open " toto" for input as 1	Ouverture du fichier "TOTO"
5002 B$= " 5000 merge virus.bas "	B$ contient le code du virus à ajouter au programme sain.
5003 While not eof(1)	Boucle qui s'exécute tant que " TOTO " n'est pas lu complètement.
5004 input# 1,a$	La variable a$ contient les noms des cibles
5005 open a$ for append as 2	Ouvre le fichier a$
5006 print# 2,b$	Ajoute le code du virus au programme sain
5007 close 2	Ferme le fichier contaminé
5008 wend	Fin de la boucle
5009 close 1	Ferme le fichier " TOTO "

Infection du virus classique



« I Love You »

- 4 mai 2000, virus de type worm, VBScript
- transmission par email (fichier joint : LOVE-LETTER-FOR-YOU.TXT.vbs)
- Séquences
  - Préparation de l'exécution
  - Recopie locale du virus
  - Modification de la base de registre
  - Préparation d'autres infections virale
  - Création d'un fichier HTML destiné aux correspondants IRC
  - Examen de la messagerie (outlook)
  - Infection de fichier
  - modification de la BdRegistre
  - modification de la page d'accueil d'IE
  - envoi automatique de messages
  - infection de fichiers

Les virus logiques

problème bénin ou véritable cancer informatique

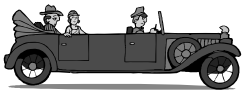
- Les virus biologiques
  - Virus dangereux pour l'homme : grippe, poliomyélite, sida, hépatite, …
  - Virus « utile » : Évolution de l'espèce ?
- Les virus logiques
  - Contrôle du périmètre
    - Difficile de manager leur cycle de vie : temps, espace
  - Détectabilité - discrétion
    - On peut remonter à la source ?!?
- Quelles sont les parades ?
  - Antivirus, …
  - La gestion correcte des ressources informatiques
    - Disk Operating System
      - On gère par la fenêtre le disque mais pas la mémoire
      - La communication, on la gère avec le BIOS
    - Virus
      - avant tout Windows, incapable de gérer correctement les ressources d'une machine
  - La sécurité et la protection des réseaux et systèmes d'information
  - La sensibilisation

Les virus informatiques :

une arme de la cyberGuerre (machines pour engendrer des milliards de virus polymorphes et tous différents)

- Qui sont les attaquants ? Quelles sont les motivations ? Quelle est la menace ?
  - « Hackers » (pirates)
    - hackito ergo sum
    - défi ludique

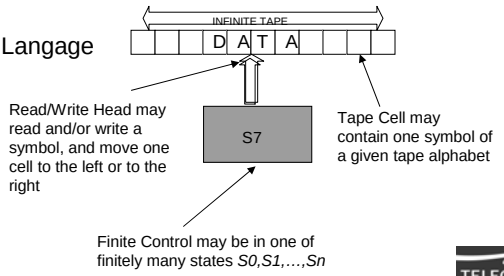
  - Groupes organisés
    - Déstabilisation, compétition déloyale



- Quelles sont les vulnérabilités ?
  - Dégâts
    - Ordinateurs : patrimoine intellectuel, données perdues
      - Intégrité
    - Dysfonctionnements
      - Disponibilité

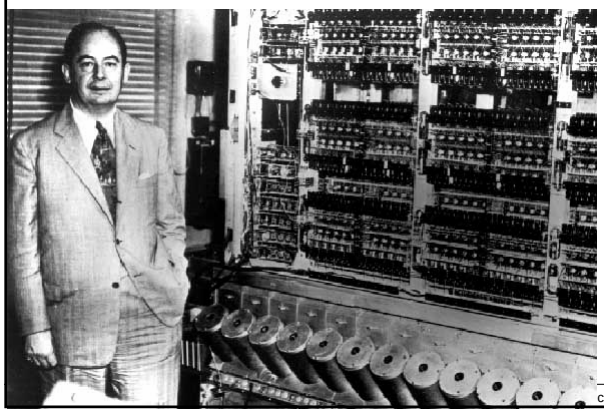
(Church –) A Turing (1912- 1954)

- 1936 : Entscheidung Problem (D Hilbert)
  - 23e problème : indécidable
  - Cadre rigoureux pour définir décidable et calculable
    - La Machine de Turing
      - Notion de procédure
      - Ordinateur en papier-crayon
- 1948
  - Manchester
  - 1er ordinateur et 1er Langage



John von Neumann (1903-1957)

- Bombe H
- Théorie des Jeux
- Sur la Théorie des Ensembles
- Précurseur de l'IA
- Ordinateur
  - Logiciel + Données dans la mémoire
  - Architecture des ordinateurs séquentiels



Les virus : une analogie (ou une métaphore)

- Les analogies au XIXème siècle
  - L'« intelligence » de S Laplace
  - Le roman de Marie Shelley (1818) : Frankenstein
  - Les démons de JC Maxwell (« on governors »)
- Les analogies au XXème siècle
  - robots, cerveaux, neurones, bugs (insectes) et virus
    - Le mouvement brownien / la mécanique newtonienne
    - La théorie de l'information de Shannon (1950)
      - information/entropie
    - Norbert Wiener : La Cybernétique
      - Cybernetics, or the Control and Communication in the Animal and the Machine (1948) : Kubernêtikê (art de gouverner un navire)
    - Von Neumann : les automates reproductibles
  - Les virus : Fred Cohen (86)
    - bout de programme, en général petit, qu'on insère dans un autre programme, parasite autonome qui exploite les mécanismes du programme contaminé
    - **Il n'existe pas de détecteur universel de virus**
  - Années 80 : Sociologie => virus informatique, virus HIV, …

Les autres Analogies

- Les Réseaux de Neurones
- Les Algorithmes génétiques

- Et le Bug ?
  - vermine ou bogue : toute erreur de programmation
    - les virus : c'est du code et ça se détecte
    - les bugs : c'est souvent de l'absence de code ou du code erroné
  - Bug de l'an 2000
    - les réseaux hétérogènes comportent intrinsèquement des dispositifs de protection qui interdisent la circulation et maintiennent stérile le terreau des réseaux informatiques
- Les métaphores
  - Puces, souris, démons d'Unix
- Les paradigmes informatiques
  - Les Objets
  - Les Agents intelligents Mobiles

Évolution des Systèmes d'Information et des Réseaux

- Darwin
  - Architecture Cisc et Risc des puces informatiques
  - Les souris à 1, 2 ou 3 boutons
  - Les langages informatiques
    - Fortran, Pascal, Ada
    - C, C++
    - Java
- Élection et/ou sélection
  - Allées et retours pour généraliser et simplifier, complexifier et restreindre
- La situation informatique (la loi de Moore)
  - « Alliance » conservatrice : Intel, Cisco, Microsoft
  - Mouvement de convergence
    - Informatique , Multimédia, Télécommunication
      - Numérisation & shannonisation
  - Virtualisation du logiciel & Trivialisation du matériel
  - « Le réseau est un ordinateur » (Internet du futur, métacomputing)
  - Impasse en productivité logicielle
    - Difficile de construire des logiciels > 1 000 000 lignes de codes

Les solutions à venir

- L'informatique depuis 50 ans
  - On broie tout Contenu en Zéros et Uns
  - Mise en boite, mise en forme, mise en transmission
    - Codage : compression, …
    - Format : MP3, MPEG2, MPEG4, …
- Échapper à la farine numérique
  - Le Quantique
    - En deçà des électrons : les photons
    - Créer des gerbes de photons
    - Plus de lignes d'écran de télévision, de pixels d'images, …
  - La Sémantique
    - Revenir à des langages de haut niveau d'abstraction qui appréhende la signification du contenu

XXIème siècle : l'Informatique Quantique

- Plus d'électrons, mais des photons
  - La communication et la cryptographie quantiques
    - Distribution de secrets par voie optique
    - Confidentialité (principe d'Heisenberg)
  - Les algorithmes quantiques (Shor, 94)
    - Logique quantique : factoriser des nombres en une durée exponentiellement plus rapide qu'avec un ordinateur séquentiel
    - Les ordinateurs quantiques
      - Du bit au qubit
- Plus de maladies virales, plus de codage génétique
  - Mais des ouragans quantiques ?

Des virus positifs: Tatouage sémantique de logiciel

- Insertion d'un code léger, protégeant l'objet, assurant l'extérieur de son immunité et ne gênant en rien sa bonne exécution
  - Techniques, fondées sur
    - la stéganographie
      - Art de cacher une information dans un document en clair
    - l'interprétation abstraite
      - pour
    - le marquage électronique (par étiquetage et tatouage) et
    - l'analyse sémantique statique de code objet mobile
      - pour en assurer
    - l'authenticité, la sécurité et la sûreté de fonctionnement
  - Travail réalisé avec l'école normale supérieure
    - M Riguidel, P & R Cousot

Tatouage de logiciels

- **Le tatouage**
  - cacher une information dans un programme
  - donner au programme des comportements dont l'analyse statique permet de retrouver l'information cachée
- **Analyse du code**
  - basée sur l'analyse sémantique statique permettant de déterminer ce que le code fera à l'exécution dans tous les comportements possibles du programme
  - cette sémantique n'est pas calculable
  - pour certaines propriétés du programme (ex: les types) une sémantique approchée peut être trouvée: la sémantique abstraite
  - l'analyse étant indécidable, elle est incomplète. Cette incomplétude permet de cacher de l'information stéganographique.
- Tatouage sémantique de code Java
  - dans leur version publique, permet à l'utilisateur de s'assurer
    - de l'origine du code,
    - de son intégrité,
    - de son immunité
      - prouver son bon comportement (pour éviter par exemple les virus et les falsifications) après ses exécutions et éventuelles transformations successives sur les divers hôtes qui ont tour à tour abrité le programme mobile.
  - dans leur version privée, permet au propriétaire
    - d'incruster dans le code de manière indécelable et indélébile une greffe logicielle identifiant ce composant logiciel
      - étiquette pour ses attributs - désignation, auteur, propriétaire, destinataire, etc.
    - évitant son piratage en le rendant inactif dans un contexte illicite : tatouage invisible actif camouflé dans le corps de l'objet

Les Aspects légaux contre le piratage informatique

Criminalité & Délinquance informatique

La situation juridique internationale

Première approche du problème

- Facteurs criminogènes de la délinquance informatique
  - questions complexes de la sécurité informatique
  - multiplicité des matériels et des logiciels
  - inexpérience et inconscience des utilisateurs
  - anonymat et caractère «virtuel» de certaines opérations
  - mobilité internationale des personnes, des services et des biens
  - chiffrement de certaines communications (crime de groupes organisés)
- Analyse empirique des problèmes
  - violation du secret, de l'intimité numérique
  - infractions économiques
    - fraude informatique, «hacker»
    - espionnage
    - violation de la propriété intellectuelle
  - dissémination des contenus illégaux

La criminalité informatique

- Histoire de la délinquance et de la criminalité informatique
  - Années 60
    - manipulation, sabotage, espionnage, utilisation illégale des ordinateurs
  - Années milieu de 70
    - début des études légales et des statistiques
  - Années 80
    - hacking, virus, vers
    - piratage de logiciels
    - manipulation de distributeurs d'argent
    - détournement des télécommunications (téléphones, cartes de téléphones, …)
  - Années 90
    - Internet : distribution de contenus illégaux
    - utilisation de l'ordinateur et des communications par des groupes organisés
- Définition
  - 1983 (OCDE) : infraction informatique
    - tout comportement illégal, immoral ou non autorisé qui implique la transmission et/ou le traitement automatique de données

La criminalité informatique

- Nature des statistiques
  - piratage de logiciels (15 %)
  - manipulation de distributeurs d'argent
  - hacking et obtention illégale de données (10 %)
  - fraude informatique
  - falsification, altération ou effacement de données
  - sabotage informatique
  - virus (30 %)
- Manque de statistiques exactes, difficulté d'avoir des statistiques valides
  - confiance, réputation et images de marque à conserver (banque, …)
  - espionnage difficile à comptabiliser
- Montée de l'obtention illégale de données
- Vulnérabilité des systèmes d'information
  - commerce électronique
  - transaction bancaires

Les lois informatiques

- Changements des paradigmes de la loi
  - avant le milieu du 20ème siècle
    - les codes criminels de tous les pays ont protégé d'une manière prédominante les objets tangibles
  - vers la fin du 20ème siècle
    - l'émergence de la société de l'information a accordé une importance croissante aux valeurs incorporelles, immatérielles et à l'information
    - Ces nouvelles valeurs ne pouvaient pas être protégées par analogie avec des biens corporels, mais a exigé de nouveaux textes légaux
    - Le champ de la loi criminelle informatique est devenu un champ complexe avec beaucoup de nouvelles questions légales, assez différentes

Les principales vagues de législation

- Protection du secret, des données privées
  - Années 70 et 80
    - protection des données (78 en France)
- Répression des infractions économiques
  - Années 80
    - évolution de la protection des objet tangibles vers des objets intangibles
    - accès illégaux sur des ordinateurs (88 en France)
- Protection de la propriété intellectuelle
  - Années 80
    - les programmes ordinateurs ne sont pas protégés par brevets mais par «copyrights» (85 en France)
    - protection des plans de semi-conducteurs (86 en France)
    - protection des bases de données (85 en France)

Les principales vagues de législation

- Contenus illégaux et malfaisants
  - Année 90
    - montée d'Internet
    - pornographie, haine, violence, racisme
    - clarification du fournisseur d'accès et du fournisseur de service
- Lois spécifiques pour les ordinateurs et réseaux
- Lois sur la sécurité minimale
  - création d'exigences pour des mesures minimum de sécurité
    - obligation minimum pour l'intérêt des droits privés et de l'intérêt public
  - limitations de mesures de protection
    - interdiction de mesures spécifiques de sécurité dans l'intérêt des droits du secret ou de la poursuite efficace des infractions (limitation en cryptographie)

La situation actuelle

- Sur le plan national
  - des réponses complètes et internationales aux défis de l'infraction informatique manquent dans la plupart des pays
  - les réponses (sanctions) sont en général nationales
  - incertitudes et échappatoires sur la protection du secret, le hacking, la protection commerciale et les contenus illégaux
- Sur le plan international ou supranational
  - Conseil de l'Europe, G8, OCDE, Interpol, Nations Unies
    - manque de coordination entre les organismes (programmes redondants)
    - les réponses internationales et supranationales sont vagues
    - elles se concentrent trop sur les questions légales

Les solutions futures

- Les mesures contre la criminalité informatique doivent être internationales
  - des stratégies nationales différentes pourraient créer des refuges informatiques ou des sanctuaires du crime informatique
  - on veut éviter les barrières internationales des flux d'information et des services
  - le contrôle des données et des flux d'information n'est pas souhaité
  - la masse de ces flux rend le contrôle difficile voire impossible
- Ne pas enfreindre les libertés civiles
  - les futures mesures contre l'infraction doivent être complètes
  - Actions: éducation, technologie, auto-contrôle de l'industrie et loi
- Différences entre la propriété tangible et la propriété intangible
  - l'information n'est pas un bien physique
  - protection de l'auteur et du détenteur de l'information
  - protection de la personne intéressée par l'information
  - protection de la société contre l'information illégale et malveillante
  - droit à l'accès à l'information (lire ses données personnelles dans les fichiers)

Orientations de la Communauté européenne

- Harmonisation sur la protection des données et la protection de la propriété intellectuelle
- Mesures non légales
  - renseignement et analyse sur les liens entre infraction haute technologie et crime organisé
  - éducation et éveil des consciences sur la sécurité
  - projet de R&D en sécurité des technologies de l'information et des transactions d'argent
  - création de structures adéquates pour lutter contre les contenus illégaux (protection de mineurs, contre pornographie, racisme, appel à la haine, violence)
  - code de conduite de l'industrie et coopération policière
  - développements de procédures de traçabilité

Orientations de la Communauté européenne

- Mesures légales (Article 100a du traité de l'Union)
  - Élaboration d'une directive pour la responsabilité des fournisseurs de service et des fournisseurs d'accès à Internet
  - Considération sur une directive pour
    - définir les contenus légaux, illégaux et malfaisants et
    - définir des sanctions et
    - pour restreindre les flux internationaux non inscrits dans la directive
  - Inclusion d'une liste d'actes illégaux, couvert par des sanctions adéquates (commerce électronique), pour garantir la sécurité et protection des consommateurs dans les réseaux européens
  - Amélioration de l'information
    - base de données sur les statuts de l'infraction informatique

Orientations de la Communauté européenne

- Mesures légales en coopération avec le conseil de l'Europe et le G8
  - définir les règles minimum pour lutter contre l'infraction informatique internationale par la loi
  - recommander des pouvoirs contraignants adéquats pour pouvoir enquêter sur les infractions des réseaux internationaux
    - exigences d'une poursuite efficace en respectant les droits des suspects et des témoins
  - prendre en charge les enquêtes internationales (enquête en ligne)
  - définir la portée des juridictions nationales
  - résoudre les conflits de juridiction qui surviennent dans les réseaux internationaux
  - créer un ensemble de règles communes pour disposer d'un dossier d'enregistrement de police et de statistiques judiciaires

Travaux internationaux et supranationaux

- Les organisations internationales
  - OTAN
  - Union Européenne
  - OCDE
  - Le Groupe des 7 (ou 8) : G8
    - États Unis, Canada, Italie, France , Allemagne, Japon, Royaume Uni, Russie
  - ITU, ISO
  - WTO (OMC) ancien GATT
  - Nations Unies
- Difficulté à converger vers des solution concrètes
  - plus l'organisation est éloignée de l'état, plus les décisions sont génériques
- Initiative pour conférence et travaux de coordination
  - Union européenne, Conseil de l'Europe, G8, OCDE, Interpol, Nations Unies, OMC
    - créer des base de données sur la criminalité informatique
    - associer les pays en voie de développement pour éviter de créer des refuges de délinquance

La sécurité des documents électroniques

Le tatouage, les restrictions et le blocage d'accès pour leur protection

Le document analogique

- Il possède un **contenu** original profondément **attaché** à son **support physique**
  - Encre sur papier, peinture sur toile, gravure magnétique sur ruban plastique, pellicule d'argent sur film
  - **Marquage intrusif** et irréversible du contenu sur le contenant
- Il a une durée de vie limitée
  - tout support physique est **périssable**; il vieillit, s'étiole
  - le contenu **s'altère**, s'efface
- On peut faire des copies de **copies** de moins en **moins fidèles** à l'original
  - éventuellement certifiées conformes
- Il est limité dans le temps (vieillissement) et dans l'espace
  - Un document (une œuvre) est **compact**
    - Peut être confiné dans un volume fini
  - Si l'objet est **brisé** ou déchiré, l'opération est définitive
- On peut imiter l'original
  - La contrefaçon : quasi identique
  - Le faux : on calque la trame et on personnalise
    - Papier d'identité (photo, nom, adresse, etc)
    - Billets de banque (numéro, série, etc)

Le document numérique

- Il est **indépendant** de son **support physique**
- Il est **immarcescible**
  - Cependant, les supports physiques disparaissent vite
    - Cartes perforées, bandes magnétiques, disquettes 19 pouces, disquettes, clés USB, CDRom, DVD, …
  - Et les standards évoluent rapidement
    - Grandes archives (musée du cinéma, etc) : La durée de vie de réécriture d'un patrimoine numérique peut excéder la durée de vie du nouveau standard ou du nouveau support
    - Les documents Word d'aujourd'hui seront illisibles dans 10 ans …
  - Finalement, le document numérique est aussi frappé par **l'obsolescence** et sans réelle pérennité
- Il est **friable**
  - Il peut être fragmenté et recomposé
    - Déchiqueté dans les secteurs de disque dur (stockage), dans des paquets IP (communication)
- Il n'est pas borné dans l'espace
  - dans des serveurs d'architecture d'égal à égal (P2P)
    - « napstérisation » de contenus illicites : saupoudrer des contenus « innocents » sur plusieurs serveurs que l'utilisateur final intègre et consolide seul, le rendant seul responsable (?)
- Il est précis, fiable et parfaitement **reproductible**
  - On peut dupliquer une œuvre à l'infini
- Il n'existe que des **clones**, tous identiques

Le document numérique est opaque

- Fichier
  - Un fichier est une suite de caractères ASCII
  - Il est transparent à l'utilisateur final qui maîtrise tout
- Document
  - Une structure complexe d'entités logiques et physiques disparates, visibles et invisibles, non transparente pour le récepteur du document
    - Page, paragraphe, style d'écriture, police de caractères, …
  - Possède un format structuré
    - Page HTML, « fichier » MP3, document Word, images multimédia (JPEG, MPEG2, …)
    - Les formats « compliqués » sont interprétés
      - Les codeurs et décodeurs MPEG2 Sony, Philips, Thomson, … sont compatibles mais pas identiques
      - Le film audio vidéo original, écrit et formaté par le codeur X, puis décodé et lu par le décodeur Y, ne produira pas en sortie, la même séquence de bits que le film original
      - La signature électronique ne peut pas être appliquée pour authentifier le contenu original d'un fichier multimédia
  - Point de vue sur un fichier
    - Le point de vue de la représentation sur papier ou sur écran
    - La totalité du fichier est rarement lisible par l'utilisateur final
  - Document propriétaire (Microsoft, Adobe) avec méta-données
    - Peu de gens savent tout ce qui est vraiment écrit dans un document
      - Version du logiciel, historique des corrections du document, etc
- Les fichiers ou documents peuvent être compressés
  - Texte : Zip
  - Multimédia : MPEG2 avec la transformée en cosinus discret (DCT) avec fenêtre glissante, le mouvement est « squelettisé »
- Les fichiers ou documents ont un cycle de vie
  - Création, mise à jour, archivage, obsolescence, destruction

La signature électronique de document

- La signature électronique est théoriquement fiable et insoupçonnable
- Pourtant, on ne sait pas ce que l'on signe
  - Exemple caricatural

Je soussigné Albin, autorise Blanche
À exécuter ceci
Et à faire cela
En échange, elle me versera 1000 €
À Lausanne, le 26 Novembre 2003
Signé Albin

Ici, texte écrit en police blanche

Je soussigné Albin, autorise Blanche
À exécuter ceci
Et à faire cela
En échange, elle me versera 1000 €
À Lausanne, le 26 Novembre 2003
Signé Albin

En fait, Albin a écrit une partie du texte avec une police de la même couleur que le fond du document

Texte avec une police de caractère uniforme

L'enregistrement numérique de la vie, prise en otage

- Le coût du stockage est divisé par 2 tous les ans
  - Le patrimoine intellectuel, culturel, industriel, personnel croit dans les mêmes proportions
  - Le stockage irrigue tous les secteurs d'activité
- L'observation numérique de l'activité humaine
  - Capteurs numériques, quasi permanents, à mon insu
    - Opérateur de télécoms
      - connaît ma position géographique dans la cellule des relais GSM
    - Banquier
      - connaît les montants de mes dépenses, leurs dates et les références des vendeurs, donc mes déplacements et pérégrinations
    - Fournisseur Internet
      - connaît mes heures de connexion sur les serveurs, et plus encore
- « Ma » production numérique
  - À mon insu : ma voix, mes textes
  - De mon plein gré : 1 Giga-octets par an

Le monde numérique est en clair

- Le monde numérique en clair
  - Internet
    - peu de données chiffrées
  - La téléphonie mobile
    - sur GSM, seule la partie radio est chiffrée
  - Aux deux extrémités de la communication
    - au début à la création et à la fin à la réception
      - On voit des images, On écoute des sons, On lit des textes … en clair
      - On exécute des programmes en clair
        - ➔ Les ordinateurs totalement chiffrés ne marchent pas (encore)
  - Entre ces extrêmes, le transport / le stockage peut être chiffré de bout en bout
- Cryptographie
  - Finalement peu utilisée
  - Les éditeurs de logiciels ne font rien pour la rendre conviviale

La sécurité des contenus

- **Transport ou stockage stricts** : plus aucun problème en 2007
  - La cryptographie est un outil puissant, universel qui marche parfaitement
    - Algorithme de chiffrement : AES
  - Audrey envoie un message à Bertrand
    - Audrey et Bertrand se rencontrent (virtuellement) et partagent un secret
    - Audrey chiffre son message, Bertrand le déchiffre
      - La communication est sécurisée : eux deux seuls peuvent déchiffrer le message
      - Le transport du message est sécurisé : Protection sémantique, syntaxique
  - La disponibilité n'est pas garantie : on peut empêcher la communication
- **Distribution** : **rien n'est** encore vraiment **réglé** en 2007
  - En ligne (sur Internet, GPRS) ou hors ligne (CDROM, DVD)
  - Bertrand est libre
    - Il peut disposer du document et l'utiliser comme bon lui semble …
    - Échec cinglant du commerce en ligne pendant la bulle Internet
  - Audrey est propriétaire du document
    - Pour tenir en « laisse » son document
    - Audrey doit ajouter sa griffe, son style, une marque, un témoignage
  - Message parasite scotché au document
    - En plus : Signature à côté ou dedans
    - Sans rien en plus : Signature dedans intrinsèquement
  - Menace
    - pastiche, plagiat, imitation et exploitation des documents

Le monde numérique est sale …

- Les **marques**
  - Stigmate, écriture, signe, symbole, icône ajoutés sur un document préexistant
    - En général intentionnel
      - Repère de classification appliqué à l'objet instancié pour le distinguer des homologues
      - Identification, indice dans des bases de données
  - Écriture dans un livre de bord comme témoignage
    - En général, à l'insu du document et du possesseur du document
      - Audit (.log par un pare-feu, par un système d'exploitation, par une application, …)
      - Inscription dans un registre public (page Web par un moteur de recherche)
  - La marque se délimite dans une zone petite (code-barre, logo, champ d'une base de données)
- Les **empreintes**
  - Matrice dans le contenu, désertée par un corps saillant qui s'est éloigné
  - Périmètre où le contenu est un contenant
  - Ma griffe
    - Interface Homme – Machine, Site Web
  - Ma biométrie sur le réseau
    - Voix, photo, … mais numérique donc falsifiable et/ou reproductible
    - Le téléphone numérique capte ma voix (authentification de confort)
- Les **traces**
  - Succession d'empreintes à ordonner (ou mieux, à dater) pour reconstituer une histoire
  - Ensemble ou Suite de marques : traçabilité, enquête policière, le prédateur suit les traces de la proie
  - Ensemble d'empreintes qui peuvent s'altérer, s'effacer
    - Des pas dans la neige …
    - Le dernier marquage qui se superpose sur l'autre peut l'altérer (tatouage, correction, etc)

Marquage ad hoc

- Méthodes empiriques, heuristiques
  - Imprimante ad hoc
    - L'écart entre les lignes, les mots sont variables selon un code
  - Photocopieuse ad hoc
    - La photocopieuse scanne le document original et produit une copie légèrement modifiée, ce qui permet d'identifier la photocopieuse
  - Copie numérotée d'un rapport
    - Chaque rapport contient une marque particulière (une faute d'orthographe différente)
      - Toute photocopie du rapport permettra de savoir quelle copie du rapport en est à l'origine
- Le Contexte juridique a changé
  - Préservation du **droit de propriété**
    - Droit d'exploitation : contrôle des copies et diffusion illicites
    - Droit moral : contrôle de l'intégrité et de la sémantique d'une œuvre
  - Internationalisation des échanges, diversité des juridictions
  - **Difficulté du contrôle**
- Nécessité de définir de faire appel à la sécurité
  - Avec sa théorie, sa méthodologie (Critères Communs)

Cryptographie, Stéganographie, Tatouage

- Aucun secret n'est partagé
  - Étiquetage, tagguage
    - Présence visible : Tout le monde peut lire le document original et le message supplémentaire
      - Code-barre, logo
    - L'étiquette contient parfois une signature électronique du contenu pour éviter l'usurpation d'étiquette et lier l'étiquette à son contenu; dans ce cas, l'étiquette dépend d'un secret.
- Un secret est partagé par les personnes autorisées
  - Cryptographie
    - Stockage et transport sécurisé
    - Puissant moyen de protéger de l'information : le message est chiffré, puis déchiffré
    - Confidentialité d'un message : Chiffrement de contenu
    - Technique unique, indépendant de la nature du document : Image, son, texte
    - Rien n'est plus détectable qu'un message chiffré sur un réseau, sur un disque
  - Stéganographie, tatouage
    - Le message subliminal est extrait par les personnes qui ont droit d'en connaître (celles qui partagent le secret)
      - Canal caché (subliminal)
      - Imperceptible (invisible, inaudible, illisible par un humain et/ou une machine)
      - Heuristique
    - Stéganographie, canaux cachés
      - Stockage et transport caché
      - Message clandestin, transporté par le message originel
        - ➔ « bande passante » faible : par exemple, derniers bits significatifs d'une image
        - ➔ Facile à effacer : On peut « facilement » lessiver, éroder le message subliminal
    - Tatouage
      - Respect de la sémantique et de l'esthétique du message originel
      - Utilisation pour sécurité, indexation
      - Message clandestin, **parasite**, transporté par le message originel
        - ➔ On peut difficilement lessiver, éroder, effacer le message subliminal

Idée initiale du tatouage de document

- Le Petit Poucet (Charles Perrault)
  - Un petit garçon (qui a un nom pour faire des empreintes) et qui pose des marques pour tracer son chemin
  - Laisser des traces pour retrouver son chemin dans la forêt
    - La première fois
      - Des petits cailloux blancs, invisibles pour les autres, reconnaissable par lui seul
      - Le tatouage doit être **discret** pour éviter que l'ogre ne se doute de quoi que ce soit
    - La seconde fois
      - Des morceaux de pain, trace effaçable par des oiseaux (innocents)
      - Le tatouage doit être **indélébile** pour éviter cette mésaventure
- Montrer (de manière invisible) patte blanche, insérer de manière intrusive, un signe anodin, une marque personnelle (par exemple, mon nom) dans le contenu d'un document, cela prouve quoi ?
  - À moi, je serai sûr que c'est mon document
  - Aux autres, cela peut les déconcerter, et cela ne prouve pas grand chose
  - Comment prouver aux autres ? Et surtout devant la justice ou face à l'attaquant
- Il faut répartir ce tatouage sur tout le document
  - Pour éviter que le pirate ne saisisse qu'une partie non marquée
- Il faut que ce tatouage soit automatique
  - rapide, reproductible, précis, standard
- Il faut que ce tatouage soit irréversible
  - pour être utilisé en tant que preuve
- Il faut définir les objectifs de sécurité
  - pour savoir exactement ce que l'on protège, ce que l'on sécurise, qui on dissuade
  - pour savoir comment on va relire les documents tatoués parmi d'autres documents pour détecter les tatouages que l'on a insérés

Trouver du jeu, du mou dans la « forêt » du document

- Excepté dans un monde déterministe, mathématique, il existe toujours
  - Une marge étroite de liberté pour glisser un court message clandestin, à l'intérieur d'un document, qui soit indécelable par le récepteur
  - Une faible tolérance dans la représentation binaire des œuvres pour incruster une marque, ineffaçable par une entité (ou une procédure) innocente ou malveillante
  - Le tatouage dans un monde déterministe est difficile, la stéganographie y est cependant possible (marquage de textes)
- Image fixe (couleur ou noir & blanc) ou son audio
  - Image naturelle ou son naturel
    - L'œil et /ou l'oreille humaine est faillible (couleur bleu foncé, son grave, etc)
    - Les algorithmes classiques de traitement de signal (fondée sur l'analyse spectrale) sont naïfs (et connus)
    - Le format est figé, connu (.gif, .wav, .jpeg, etc)
    - La manière de la visualiser ou l'écouter est systématique (ligne à ligne ou linéairement)
    - On peut incruster un message subliminal presque partout sur toute la surface de l'image ou dans tout le spectre du son, sans que cela se perçoive
  - Image de synthèse, mathématique
    - Dont le format n'est pas ligne à ligne mais en vecteur
      - On peut cacher de l'information dans la manière de tracer les vecteurs
      - En revanche une impression papier fait oublier le déroulement de l'écriture
    - Dont le contenu est « informationnellement » faible
      - Des dessins et des lignes qui répondent à des équations
      - Le caractère d'originalité et d'individualité du document est faible
      - Pour le copier, il est préférable de reconstituer l'œuvre à partir des équations

Trouver un procédé pour solidariser le tatouage au contenu

- Les ressources du chiffrement sont inépuisables …
  - On peut chiffrer n fois un message, éventuellement avec des algorithmes distincts et des clés différentes
  - Le 3DES, même algorithme (DES) avec 2 clés
- Le tatouage : un marquage sur une peau de chagrin
  - Le nombre possible de tatouages sur un document est faible
    - On peut tatouer un document 2 ou 3 fois
      - Tatouage fort, présent partout, indélébile de l'image originale
      - Tatouage faible, pour le distributeur
      - Tatouage pour indiquer la destination (fingerprinting)
    - En fait, c'est la quantité d'information que l'on peut dissimuler, compte tenu des contraintes, qui est limitée
  - Le tatouage comble un creux, un « trou »
    - Un tintamarre + un tohu-bohu dans du vacarme
    - Du grésillement et du bourdonnement dans une friture de ligne
  - On ne peut pas tatouer comme on veut un document
    - Image en noir et blanc avec un dessin, en couleur avec des pixels, avec des vecteurs
    - Logiciel avec peu d'instructions
- Le tatouage n'est pas un groupe !
  - L'opération n'est pas (en général) :
    - Associative : T1 o (T2 o T3) # (T1 o T2) o T3
    - Commutative : T1 o T2 # T2 o T1
    - Symétrique : il n'existe pas toujours T^{-1}
  - Pour la sécurité, ces propriétés sont très intéressantes
    - On a intérêt à utiliser des tatouages non commutatifs, irréversibles

Contraintes & Propriétés du Tatouage

- Contraintes de préservation et de résistance (persistance)
  - Préserver le contenu sémantique
    - Texte, son, image
  - Préserver le contenu esthétique
    - Image, son, texte
  - Préserver le contenu syntaxique
    - Texte, formats multimédia
  - Pour un texte en langage machine, résistance à la compilation
    - Texte source en C++ avec des variables en français : traduire les variables en anglais est lessivé à la compilation
    - Obfuscation, dissimulation
  - Résistance au passage à l 'analogique
    - Sur écran (TV, ordinateur), sur papier
  - Résistance à la compression
    - MPEG2
  - Résistance au reformatage
    - Transformation géométrique
    - Zoom
    - Translation, rotation, homothétie
    - Similitude
    - Changement de grilles (images en pixels)
- Propriétés
  - Le message dissimulé est indélébile
    - Un nettoyage du « bruit » est inopérant
    - La marque peut être altérée mais résiste à un nettoyage
    - Une écriture supplémentaire ne peut enlever le premier message gravé
    - Tous les lessivages (retatouage, filtrage) font que les marques résistent
  - Le message dissimulé est indétectable
    - Il ne gêne pas la lecture de l'image, l'écoute ou l'exécution
    - Imperceptible (invisible, inaudible)
    - Indécelable (aucun procédé ne peut le révéler)
  - L'algorithme est connu de tous
  - La clé est secrète
    - La clé permet de loger, de placer un ou plusieurs messages
    - Le message est en clair: Il ne peut être lu que si on a la clé
    - Ce message est dupliqué n fois dans un document multimédia pour des raisons de redondances, mais surtout pour assurer l'intégrité du document

Histoire du Tatouage

- En anglais : Watermarking
- En français : Tatouage, Aquamarquage
- Domaine jeune (~ une décennie)
- Début 1992 – 1993
  - 1992 : Tatouage de logiciels (marques effaçables)
  - 1993 : Tatouage de contenus audiovisuels
- Recherche effervescente 1995 – 2002
  - Fortement soutenu par la Commission européenne
    - Tatouage de documents multimédia
    - Évolution méthodes empiriques => formalisation et théorisation
- 1997 – 2000 : Tatouage sémantique de logiciels, « obfuscation » de logiciels Java
    - Logiciels en C, Java
    - Tatouage de Puces matérielle (c'est du logiciel)
- Maturité du Filigrane électronique en 2007
  1. Sons audio : industriel depuis 1997
  2. Images animées vidéo : industrialisable depuis 1999
  3. Images fixes : pas encore de standards et pas industrialisé
  4. Texte structurés : encore dans les laboratoires de recherche

Le champ d'application du tatouage

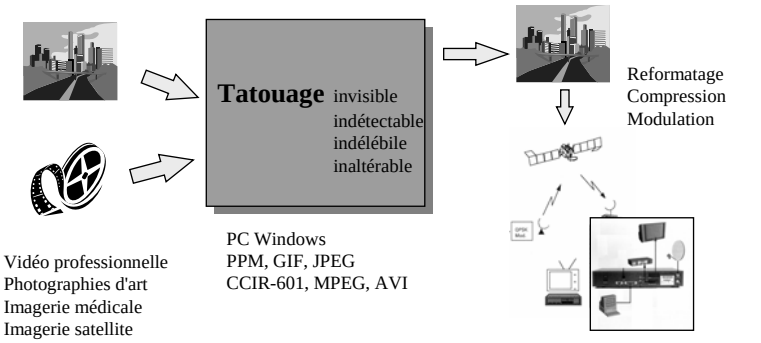
- Les contenus
  - Images
    - Fixes
    - Animées
  - Sons, voix
    - Musique
    - Parole
  - Multimédia
    - Films (MPEG2, MPEG4)
    - Dessins animés
    - Partitions musicales
    - Films en images de synthèse
  - Textes structurés
    - Logiciels source (Java, C)
    - Puces matérielles en langage VHDL, Vérilog
    - Architectures
  - Morphologies
    - Chemins d'un graphe (réseau)

Le champ d'application du tatouage

- Applications
  - **Identification de contenu**
  - **Copyright** : insertion d'une étiquette caractéristique de l'œuvre
  - **Fingerprint** : insertion d'une étiquette caractéristique du diffuseur ou de l'utilisateur
  - Protection des œuvres, des auteurs, des distributeurs, des propriétaires
    - Authentification, intégrité, non-répudiation
    - Protection des droits d'auteurs
    - Traçabilité des documents
    - **Traçage de données** dans des réseaux hétérogènes
  - **Contrôle de contenu** (contrôle parental, indexation…), « super-étiquetage »
  - Indexation qui peut servir à toute autre chose (synchronisation, ajout d'un avatar qui parle le langage des signes)
  - Communication cachée (stéganographie)
- Contraintes générales pour le tatouage d'images
  - Invisibilité
  - Lecture autonome
  - Résistance aux compressions
  - Résistance aux transformations géométriques
  - Résistance aux attaques intentionnelles
- Formats et Protections
  - IPMP (Intellectual Property Management & Protection)
  - Traçage des contenus multimédia et identification des propriétaires
    - Image : JPEG 2000
    - Images animées : MPEG4
    - MPEG7, MPEG21

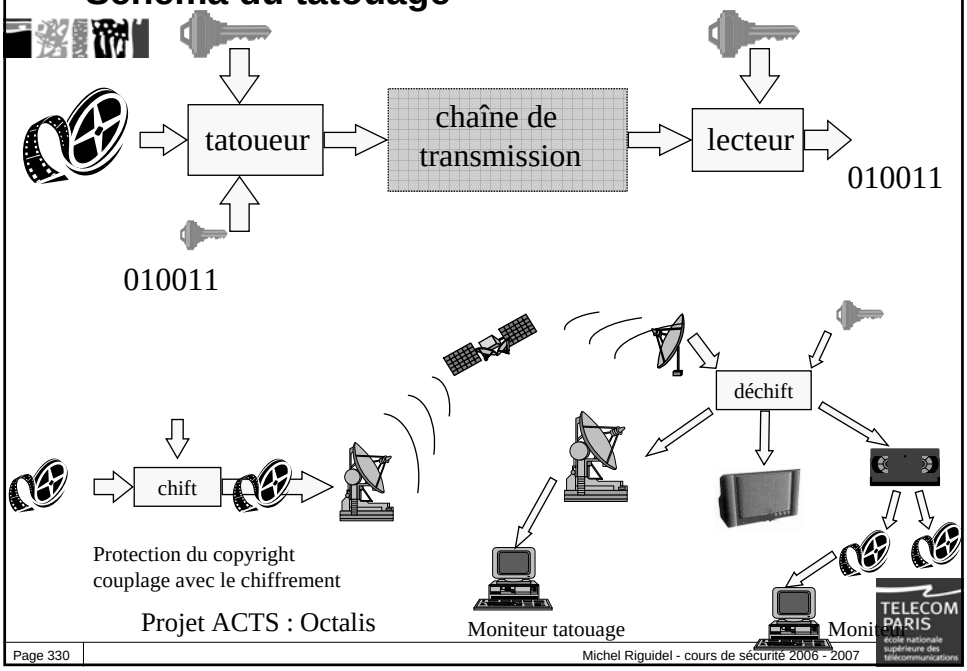
Tatouage d'images et contrôle de la diffusion

- Offrir un mécanisme de protection numérique d'oeuvres audiovisuelles afin de contrer le piratage à grande échelle et les diffusions illicites

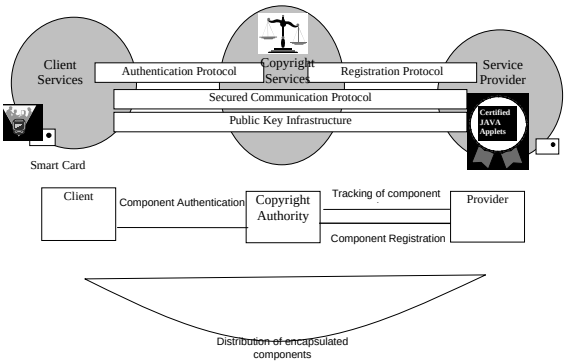


Projet ACTS

Schéma du tatouage



Cadre général de la distribution en ligne



Projet Esprit Filigrane

Objectifs de sécurité pour un document tatoué

- Confidentialité
  - Définition : Protéger contre la consultation abusive de données par des tiers non autorisés
  - Aucune confidentialité du contenu sémantique, syntaxique et esthétique n'est en général exigée
  - Éventuellement, confidentialité du propriétaire et de quelques attributs du document que l'on veut, en outre, cacher
    - Incruster un message chiffré (mais détectable)
    - Incruster un message en clair mais caché
- Intégrité
  - Définition : Vérifier que les données n'ont pas été modifiées accidentellement ou intentionnellement sans autorisation
  - Oui, intégrité de l'œuvre : on ne veut pas que des pirates se saisissent de l'œuvre et la modifient pour une utilisation non autorisée
    - Le tatouage va modifier l'œuvre mais ne provoque pas d'altération du contenu sémantique, ni du contenu esthétique
      - Document Multimédia : Les modifications bit à bits (de l'image, du son) ne sont pas perceptibles
        - ➔ La signature électronique ne convient pas car la signature électronique des formats multimédia (MPG2, par exemple) n'est pas respectée par les « formats » compliqués du multimédia
        - ➔ Les codeurs et décodeurs n'interprètent pas le standards de la même façon
      - Document Logiciel : Les modifications du programme n'affectent pas les résultats
- Disponibilité
  - Pas d'objectif de sécurité en terme strict de disponibilité, mais plutôt en terme d'utilisation (recopie, visualisation, etc)
    - Le tatouage va dissuader le pirate
    - La connaissance de l'existence d'un procédé de dissuasion peut déjà dissuader une partie des attaquants
    - Les attributs de sécurité peuvent recéler une restriction à l'utilisation, une autorisation, une durée de validité pour l'accès à la lecture, etc
    - Éventuellement, brouillage après un certain nombre de lectures, après une certaine durée de validité

Politique de sécurité

- Fonctions de sécurité
  - **Étiqueter (Identifier)**
    - Méta-données accompagnant le document
    - Éventuellement avec la description de la politique de sécurité
      - Écrite en XML
  - **Tatouer (Authentifier)**
    - Marquer le contenu de manière indissociable
  - **Tracer (Audit)**
    - Être capable de surveiller sur les réseaux les copies tatouées
    - En présence de copie illicites, présenter l'affaire à la justice
- Signification du message parasite
  - Un numéro d'identification
    - Qui pointe sur une base de données qui donne le reste des informations (propriétaire, distributeur, etc)
  - Les attributs (en clair ou chiffré)
    - Le propriétaire
    - Le contenu
    - La politique de sécurité de ce contenu
      - Droits de copie (DVD)
      - Durée de validité
- Protection ? : non, dissuasion
  - Contrôle de **l'origine**
    - Protection
      - des droits d'auteurs
      - de la diffusion, de la distribution des œuvres sur un réseau
    - Protection
      - du DVD : Millenium
        - ➔ Philips, Macrovision, Digimarc
      - des œuvres audio musicales
        - ➔ SDMI : Secure Digital Music Initiative
  - Contrôle de la **destination**
    - Protection de la distribution
    - « Fingerprinting »
  - Contrôle du **contenu**
    - signature sémantique de l'oeuvre
  - Contrôle de la **route**

Tatouage de textes : Acrostiche …

- Contrôle de l'origine
- Ballade pour prier Notre-Dame
  - François VILLON
  - **V**ous portâtes, douce Vierge, princesse,
    Iésus régnant qui n'a ni fin ni cesse:
    Le Tout-Puissant prenant notre faiblesse,
    Laissa les cieux et nous vint secourir,
    Offrit à mort sa très chère jeunesse;
    Notre-Seigneur tel est, tel le confesse:
    En cette foi je veux vivre et mourir.
  - Le J était écrit I à cette époque.

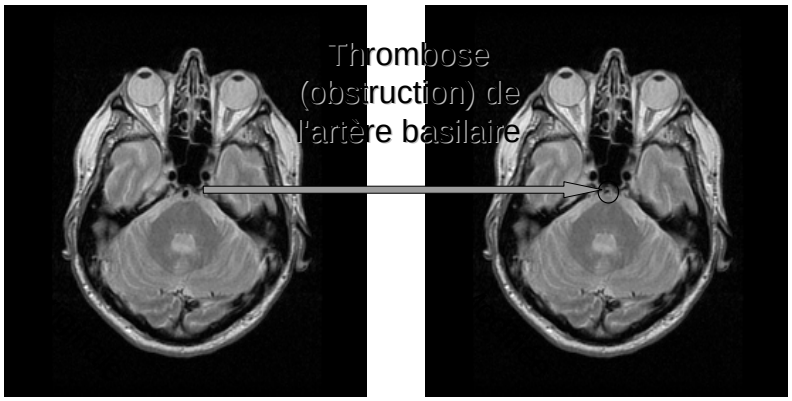
- Contrôle de la destination
- Au destinataire (Louis XIV)
  - **L**ouis est un héros sans peur et sans reproche
  - **O**n désire le voir. Aussitôt qu'on l'approche,
  - **U**n sentiment d'amour enflamme tous les cœurs,
  - **I**l ne trouve pas chez nous que des adorateurs;
  - **S**on image est partout, excepté dans ma poche.

2 types de tatouages

- Indépendant du document
  - On va superposer systématiquement un document epsilon en filigrane
  - D tatoué = D original + epsilon
- Dépendant du document
  - On va substituer systématiquement un pixel, un son, un mot, un style par un synonyme, par un autre presque équivalent
  - D tatoué = D original {– epsilon1 (D) + epsilon2 (D)}
- Propriétés
  - Indépendant du document : tatouages itératifs indépendants
    - Commutatif
      - L'attaquant peut surtatouer un document déjà tatoué et dire qu'il est le premier
    - Réversible
      - Facile d'enlever un des tatouages (pourvu qu'on possède le secret)
      - Tatouage éphémère pour une période définie
  - Dépendant du document : plus approprié en sécurité
    - Non commutatif : T2 o T1 (D) # T1 o T2 (D)
    - Parfois irréversible : T^{-1} n'existe pas
      - Plus difficile de lessiver ce tatouage

La sécurité des images médicales

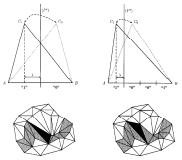
thèse de Gouenou Coatrieux (avec le LTIS Rennes)



ENST, Département Traitement du Signal & Image

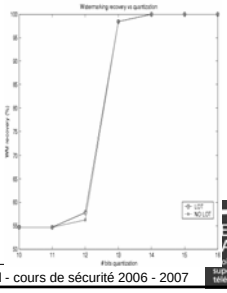
Tatouage d'objets 3D

- Tatouage 3D
  - Fragile : stéganographie
- Tatouage fragile
  - Modifier la structure des maillages
  - Possibilité d'insérer des mill



- Tatouage robuste

  - Robuste à la compression MPEG4



  - thèse de François Cayre
    - (cotutelle UCL/Télécom-Paris)
    - F. Schmitt + H. Maître

ENST, Département Traitement du Signal & Image

Le tatouage : son industrialisation est en peine

- Tatouage Multimédia
  - Faiblesses et failles dans les technologies de tatouage
    - Limites théoriques du tatouage multimédia
      - Voix, son, image fixe ou animée, document audio-visuel, graphiques
    - Difficultés
      - Résistance à la compression, à la transformation géométrique
      - Robustesse du marquage dans la chaîne de distribution
      - Nombreux algorithmes dépendant
        - ➔ de la nature: MPEG2, MPEG4, images JPEG, dessins 2D/3D, ...
        - ➔ du contenu esthétique et de sa perception humaine via les yeux ou oreilles ou
        - ➔ machine via des algorithmes de traitement de signal (lessivage des tatouages,…)
- Intégration et industrialisation dans les DRM
  - Absence de standards et d'infrastructures générales
  - Nécessité de coupler stéganographie, cryptologie et PKI
  - Dialogue nécessaire entre académiques, industriels, pouvoirs publics, opérateurs
    - Verrouillage d'Hollywood et mésentente des industriels du multimédia

Concepts & paradigmes pour sécuriser l'intimité numérique

Michel Riguidel Novembre 2003

Notion d'intimité numérique

- Informations nominales
  - Confidentialité des données personnelles
  - Accès aux données personnelles sur les fichiers institutionnels
- Classe fonctionnelle des Critères Communs (ISO 15408)
  - L'anonymat
    - garantissant qu'un utilisateur peut utiliser une ressource ou un service sans révéler son identité
    - Par exemple: transactions électroniques pour un achat en ligne
  - Le pseudonymat
    - garantissant qu'un utilisateur peut utiliser une ressource ou un service sans révéler son identité, mais peut être tenu **responsable** de ses actes
  - La non-chaînabilité
    - qui représente l'impossibilité pour d'autres utilisateurs d'établir un lien entre différentes opérations réalisées par un même utilisateur
    - pas de **fusion** ou de **croisement** d'informations à partir de différents fichiers ou bases de données
      - dossier médical et assurance, données fiscales, etc
  - La non-observabilité
    - garantissant qu'un utilisateur peut utiliser une ressource ou un service sans que d'autres utilisateurs soient capables de déterminer si une ressource ou un service est en cours d'utilisation
    - pas **d'espionnage** des connexions et actions sur le réseau
    - Pas de traçabilité pour fabriquer un profil d'utilisateur : fidélisation, commerce en ligne, « cookies », clics de souris sur les sites Web

Infosphère personnelle: de plein gré

- Sur soi
  - Carte bancaire
  - Téléphone portable
  - Ardoise, agenda électronique
- Avec soi
  - Ordinateur portable
  - PC : ordinateur personnel ?
- Sous la peau
  - Prothèse électronique
- À domicile
  - Les ordinateurs, domotique programmable
- Au bureau
  - Ma station de travail
- À la banque
  - Mes données bancaires
- Chez le médecin, à l'hôpital
  - Mon dossier médical
  - accès au dossier médical ?

Politiques de sécurité :

Sous mon contrôle, gardé à vue

Protégé par quelqu'un digne de confiance

Infosphère personnelle: à mon insu

- Comptabilité, paiement: anonymat relatif
  - Péage sur autoroute, caisses : payer par carte bancaire peut me mettre en défaut …
  - La banque enregistre mes allées et venues ainsi que mon train de vie
- Opérateur de télécoms: **filature électronique**, pistage et repérage
  - Date, heure, numéros de téléphone des correspondants
  - Positionnement dans les cellules de relais de téléphonie mobile
    - Mon opérateur de téléphonie mobile sait où je suis en temps réel (à 100 mètres près)
    - Traces numériques pour enquête
      - Dernières localisations de personnes disparues
      - élucidation d'assassinat : groupes de personnes se téléphonant à l'endroit et à l'heure du crime
    - Alibi : j'étais ici et je n'étais donc pas là
  - Services géo-dépendants (ma position est transmise à des fournisseurs de services)
    - Des fournisseurs de services m'envoient des publicités quand je passe près d'un magasin, d'un restaurant
- Sur Internet
  - Tout le monde
    - Informations permanentes : Conférence, événements, etc
  - Le Fournisseur d'accès Internet
    - Les transactions, les sites visités, les heures de connexions
  - Les spécialistes (pirates, espions, …)
    - Repérage géographique : mon adresse logique IP
    - Mes activités informatiques
- Dispositif de surveillance vidéo dans la sphère publique
    - Galerie marchande, Hall de gare, dans la rue
    - Distributeurs de banque pour retrait d'argent
- Sur les objets personnels
  - La voiture : Antivol par localisation géographique en général pas déployé
    - respect de la vie privée ou prétexte pour ne pas casser le marché « juteux » (vendre des automobiles et par des assurances)

Infosphère personnelle sur les réseaux

- Sur Internet
  - Googlisme
  - Pages personnelles, Serveurs
- Mes représentants: Avatars, agents, « bots »

- Ma biométrie
  - Photo
  - Voix numérisée
    - Messagerie vocale
  - Le téléphone portable est un excellent capteur biométrique
    - Authentification de confort

Protéger l'individu physique et son attirail électronique

- Protéger la liberté de l'individu, sa vie privée, son intimité numérique
  - Confidentialité des données personnelles, de la localisation (mobilité)
  - Anonymat, pseudonymat
    - Préserver l'anonymat dans les achats, les déplacements, les activités
  - L'intimité numérique
    - Les données nominatives dans les différents fichiers (ses caractéristiques physiques, intellectuelles, morales, intimes, ses convictions politiques, religieuses)
    - Les traces de sa carte bancaire, de son téléphone portable, de ses connexions Internet
    - Messagerie électronique dans les entreprises
- La sécurité de la personne
  - Menaces
    - vis à vis de l'individu
      - L'atteinte à sa liberté, sa vie privée, son intimité
        - ➔ Écoutes et localisations illégales
        - ➔ Observabilité, Chaînabilité, Croisement des bases de données diverses
    - **individu "pirate" vis à vis des autres individus**
      - Profiter de la faiblesse des surveillances personnelles pour attaquer
  - Solutions
    - Sécurité souvent **conflit d'objectif avec la sécurité des organisations** (état, entreprise)
      - Entité de confiance personnelle (dispositif intelligent portable)
    - Biométrie
      - Identification de la personne

Infosphère personnelle

- Volume
  - En 2007 : 1 Giga-octet en moyenne ?
    - Beaucoup de données dupliquées, en coupé-collé ou aspirées à partir du Web
  - En rapport avec le degré d'informatisation de l'environnement
    - Fracture numérique
  - En rapport avec le prix des disques durs (divisé par 2 tous les ans)
    - Double tous les ans
  - Étalonnage (estimation)
    - Œuvre de Jean Sébastien Bach : 200 Méga-octets
    - Encyclopédie générale de la connaissance humaine : 2 Giga-octets
- Centre de gravité
  - Évolution : estimation
    - 1990 : à 95% au bureau, sous mon contrôle
    - 2007 : à 40% à l'extérieur de son domicile / bureau, indépendant de mon contrôle
- Dynamicité (permanente / volatile)
  - Centripète : effet d'accumulation
  - Vieillissement des informations
    - Peu de fonctions d'oubli
  - Glu numérique qui piège les individus « branchés »
- Les objets communicants
  - connexions
    - Intermittente (aux objets personnels et à la famille proche)
    - Permanente (bureau, domicile)

Enregistrement numérique

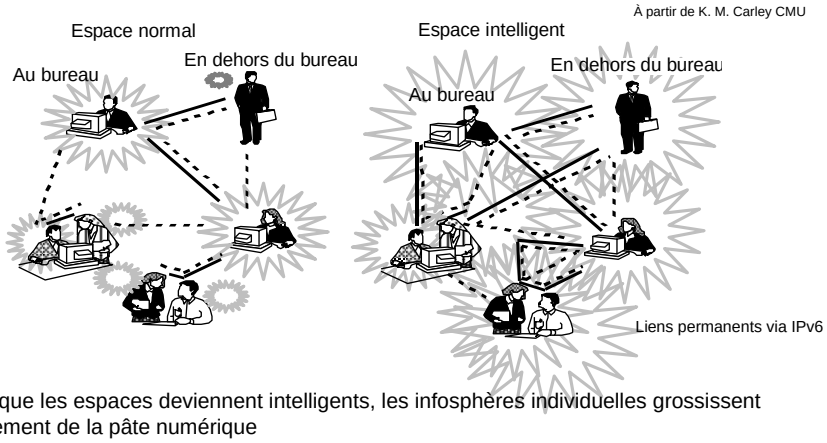
- Protection des données personnelles
  - Encre indélébile mais aisément falsifiable
- Enregistrement numérique de la vie
  - Le coût de l'enregistrement de la vie d'une personne ne coûte presque plus rien
    - Conversations par téléphone, butinage sur les réseaux
    - Devoir de mémoire, mais il faut savoir oublier et sélectionner le passé
  - Le respect de la vie privée et de l'intimité est un droit fondamental
    - Cauchemar : toute la société deviendrait un immense « loft » en télé-réalité interactive
- L'activité du « monde développé » est enregistrée
  - Dans les actualités télévisuelles, il y a toujours une vidéo amateur qui est là pour témoigner d'un accident, d'une catastrophe
  - Observations du monde par des capteurs intelligents
    - Biais de la société: les informations et les sujets brûlants sont là où sont les caméras ou les capteurs

PAN-Bluetooth-WLan-UMTS-Internet

Mobilité & Infosphères

évolution des espaces : normal & intelligent

À partir de K. M. Carley CMU



A mesure que les espaces deviennent intelligents, les infosphères individuelles grossissent
Épaississement de la pâte numérique

Infosphères : cercles
Interaction : lignes en gras
Réseau de connaissance : lignes pointillées

Sphère ?

- Des données dispersées dont certaines ne sont plus sous mon contrôle
  - Cette sphère se prolonge dans tous les recoins de la planète
  - Le contrôle d'accès aux informations est de plus en plus difficile à réaliser
- La partition privée – publique n'est plus adéquate, informatiquement parlant
  - Les sphères sont éclatées en réseau : les mondes virtuels ont une réalité
    - Sphères gigognes, superposées
      - Astrid est à la terrasse d'un cybercafé, en conversation avec ses collègues Bertrand et Charles
      - Elle lit ses mails sur Internet
      - Elle reçoit un coup de fil sur son portable et s'entretient avec son mari Donatien
  - Sphère privée hétérogène
    - Cloisonnement des domaines
      - Partie très privée, à protéger fortement : surtout en confidentialité
        - ➔ Jardin secret
        - ➔ Données servant à sécuriser : mots de passe
      - Partie privée, à protéger fortement : surtout en intégrité
        - ➔ Données officielles
      - Partie privée, à partager avec mes proches : intégrité, disponibilité
        - ➔ PC de la famille
- Le monde numérique est en clair
  - Les données (messages, …) sont rarement chiffrées
    - Suspicion sur un réseau quand transite des données chiffrées
    - Si ces données sont chiffrées, qu'est ce qu'il cache celui-là?
  - Tout Internet est en clair à 95%
  - Toutes les conversations téléphoniques sont en clair
    - Le GSM est chiffré sur la partie radio, du terminal portable au relais radio
  - La télévision est en clair
    - TV cryptée: club fermé d'abonnés

Des sphères gigognes qui se chevauchent
les différentes granularités

- La sphère privée de la personne physique : « privacy »
  - Corps humain : réseau biologique, prothèse numérique (dans le futur)
  - Mes objets personnels : carte bancaire, téléphone portable, assistant numérique, ordinateur personnel
  - Menaces & vulnérabilités
    - Utilisation frauduleuse de carte bancaire, vol de téléphone portable
    - Viol de l'intimité numérique (liberté, confidentialité)
    - Atteinte à l'intégrité: intrusion (virus, …)
  - Mes relations avec mes proches (famille, amis, collègues)
- La sphère privée de la personne morale : imputabilité, responsabilité
  - Intrusion dans les locaux d'une entreprise, dans le système d'information, …
  - Saturation malveillante de ressources
    - réseaux engorgés, serveurs à bout de souffle, imprimante avec gaspillage de papiers, télécopieur saturé, pare-feu ou détecteur d'intrusion enregistrant des événements anormaux truffant le disque
- La sphère ouverte des anonymes : renseignement, audit
  - Confiance a priori dans les citoyens, les contribuables, les usagers
    - Problème de la gestion des crises : perturbations sociales, terrorisme, …
  - Protection des infrastructures critiques
    - Interdépendances de ces structures géantes et fragiles
      - Informatique et électricité, Transport et Entreprises à flux tendus, …

Sphère numérique ouverte et/ou fermée ?
Ruban de Möbius

- Les systèmes sont devenus des rubans de Möbius !
  - Ils sont ouverts et fermés : pas d'intérieur, ni d'extérieur
  - Communauté ouverte et dynamique : des entrants, des sortants
- Le refuge du club fermé dans espace confiné au périmètre minimum
  - Site connexe
    - In vitro (pour éviter les fuites, les conséquences imprévisibles d'une expérience)
    - Coffre-fort à serrure savante : carte à puce avec un cœur de cryptographie
    - Cage de Faraday : silence électromagnétique
    - Bac à sable : Machine virtuelle Java, calcul inoffensif, interdiction de toucher aux fonctions essentielles de l'ordinateur
  - Sites non connexes
    - Tranchées numériques : VPNs pour rétablir la contiguïté du partage de l'information
- L'hospitalité des formes semi-ouvertes : le campus, la gare, le café, l'avion
  - Une communauté virtuelle semi-privée
    - Des permanents, des habitués, des gens de passage, des étrangers
    - Des entrants et des sortants
  - Coopération entre personnes aux politiques de sécurité différentes et avec des confiances mutuelles différentes
- La tolérance de l'agora, espace ouvert au cœur de la cité
  - Des anonymes, des "étrangers"
    - Serveurs Web
  - Situation différente suivant l'environnement
    - temps de paix, « vigipirate », « rue des snipers », …
    - objectifs de sécurité d'une entreprise (valeur, image de marque, …)

Cookies

- Pièces d'informations générées par un serveur web et mémorisées dans l'ordinateur pour un futur accès
  - introduits par Netscape
  - Avant leur apparition, Internet était un protocole « stateless » : rien ne liait la demande d'une page sur un site aux demandes ultérieures
  - Netscape a décidé d'étendre le protocole pour permettre aux sites de taguer le navigateur d'un utilisateur d'informations qui seront à sa disposition lorsqu'il retourne sur un site
  - Le cookie est mémorisé dans l'ordinateur de l'utilisateur sans que ce dernier le sache ou l'ait consenti
  - Des informations personnelles sont formatées par le serveur web, transmises et sauvegardées par l'ordinateur de l'utilisateur
  - Le cookie est clandestinement et automatiquement transféré de la machine de l'utilisateur vers le serveur web
    - Les cookies constituent un outil idéal pour maintenir des profils d'utilisateurs
    - Ils peuvent renfermer n'importe quel type d'information
    - Ils sont principalement utilisés à l'établissement d'une session lors de services électroniques ou pour la mémorisation des préférences d'un utilisateur
- On peut gérer les cookies
  - Les éditeurs de logiciels ne nous aident pas beaucoup …

Les Privacy Enhancing Technology (PET)

- Outils
  - pour gérer ses profils personnels
  - pour gérer son intimité numérique
- Les PETs se fondent sur le principe du « besoin d'en connaître »
  - ne transmettre une donnée personnelle qu'à ceux qui en ont réellement besoin pour réaliser la tâche qu'on leur confie
  - Plutôt que d'anonymat, on peut plus parler de pseudonymat
    - ces outils respectent des limites, c'est-à-dire que certaines informations personnelles peuvent être divulguées aux autorités judiciaires en cas de litige ou d'enquête
    - l'utilisateur peut être tenu responsable des ses actes
- Différentes sortes de PETs sont disponibles
  - permettent de gérer les cookies
  - offrent aux utilisateurs la possibilité de surfer sur Internet anonymement pour éviter que les publicitaires puissent suivre leurs habitudes (shopping) et donc éviter le spamming
- Les PETs fournissent ou aident à fournir les propriétés de l'intimité numérique
  - l'anonymat, le pseudonymat, la non-observabilité et la non-chaînabilité
  - pour les adresses IP, la situation géographique, l'accès anonyme à des services et pour une autorisation respectant la vie privée
  - pour parvenir à un bon compromis entre authentification et anonymat
- Ces outils sont à la discrétion de l'utilisateur
  - c'est lui qui prend l'initiative de les installer, de les configurer pour obtenir le niveau de pseudonymat qui lui semble nécessaire
  - Il y a dans cette démarche une notion nouvelle qui est celle de la gestion de son identité par l'utilisateur lui-même

La signature électronique et ses aléas…

- Quand on signe un document informatique,
  par construction non transparent,
  qu'est ce que l'on signe vraiment ?
- Exemple (caricatural)

Je soussigné Antoine, autorise Béatrice
À exécuter ceci
Et puis faire cela
En échange, elle devra me verser 1000 €
À Genève, le 21 Novembre 2003
Signé : Antoine

En fait, Antoine a écrit ici,
en police de caractère blanc

Envoyé, signé électroniquement
avec toutes les bonnes mesures
cryptographiques qui vont bien

En échange, elle devra me verser 1000 €

Les données d'autrui sous mon contrôle

- Gestion des droits numériques
  - Logiciels, fichier musicaux, base de données (encyclopédies, …)
    - Tatouage : la griffe de l'auteur et/ou du propriétaire incrustée intimement de manière subliminale dans le corps de l'oeuvre
  - Copyrights, propriété intellectuelle, rétribution des auteurs
    - Un fil à la patte pour les œuvres numériques : protocole cryptographique
- Des appareils et des systèmes sous mon contrôle ?
  - Téléphone portable
    - Carte SIM gérée par l'opérateur de télécoms
  - Ordinateur personnel
    - Mauvaise réputation des systèmes d'exploitation fermés et propriétaires
    - Une solution: Le logiciel libre, le logiciel « open source »
  - Le réseau Internet
    - Le chemin des données n'est pas sous le contrôle de l'utilisateur
    - Hégémonie dans les fournisseurs de routeurs, de systèmes exploitation, de puces informatiques
      - Publicité récente : « dans le monde, une seule entreprise transporte vos données »
- Maîtrise des technologies de l'information
  - Enjeu géostratégique
  - Qui maîtrise un logiciel de plus d'1 million de lignes de codes ?

Politique de sécurité des infrastructures critiques

Les infrastructures critiques et leurs interdépendances

- vulnérabilité des organisations et de la fragilité des constructions humaines
  - société de l'information, interconnectée, complexe et fragile
  - nombreuses interdépendances entre les SI et les divers domaines d'activités
    - banque, énergie, transport, santé, défense et administration
  - ces interdépendances engendrent des vulnérabilités nouvelles
- approche systémique de sécurité
  - pour protéger les infrastructures critiques
  - pour atténuer les effets de cascades entre infrastructures, en cas d'accident grave ou de cyber-attaque
- immunisation
  - pour protéger les systèmes numériques
  - stériliser les systèmes d'information

Une dérive inéluctable

- L'uniformisation du monde numérique
  - 1ère Vulnérabilité
    - Un monde complexe mais monolithique
- La flexibilité et l'optimisation
  - 2ème Vulnérabilité
    - Un monde optimal en tension par la flexibilité des organisations et les flux tendus
    - Le repliement des infrastructures sur elle-même
      - Le partage des ressources par des infrastructures de même espèce
- La mondialisation
  - 3ème Vulnérabilité
    - La Morphologie prégnante des infrastructures capillaires
    - Le rôle incontournable et critique d'Internet
      - Un joug dangereux
      - Une scène pseudo-œcuménique pour tous les acteurs

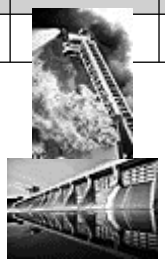
Les interdépendances des infrastructures

- La versatilité des menaces
  - La catastrophe
    - Accident fatal, la Nature
  - La tragédie
    - Déroulement et dénouement par des hommes
      - Démonstration idéologique
- La modélisation d'une infrastructure et de sa politique de sécurité
  - La protection d'une infrastructure
  - La sécurité des interdépendances
- Un Monde en réseau
  - Les réseaux (acception la plus générale du terme)
    - Typologie
    - Les risques

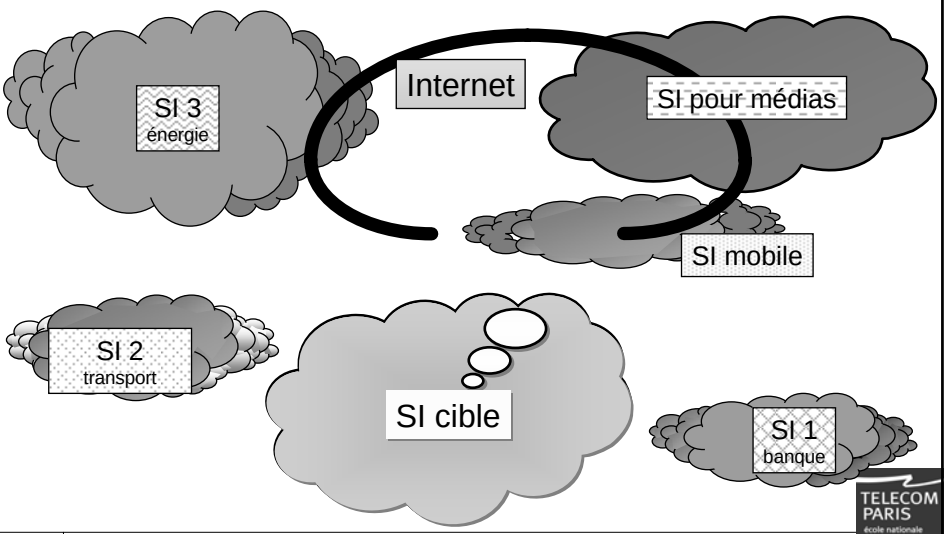
ACIP : évaluation de la protection des infrastructures critiques (Projet IST du 5ème PCRD)

- Feuille de Route pour la protection des infrastructures critiques

Domaines	Information & Communication	Banque & Finance	Énergie	Transportation	Vital HS	Gouvernement

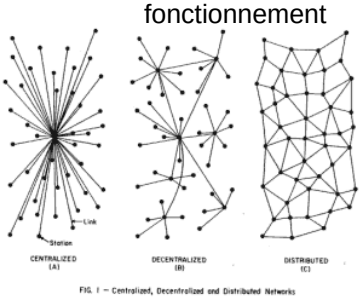


Le Système et ses banlieues
l'extension géographique d'une cible d'attaque



Rôle incontournable et critique d'Internet

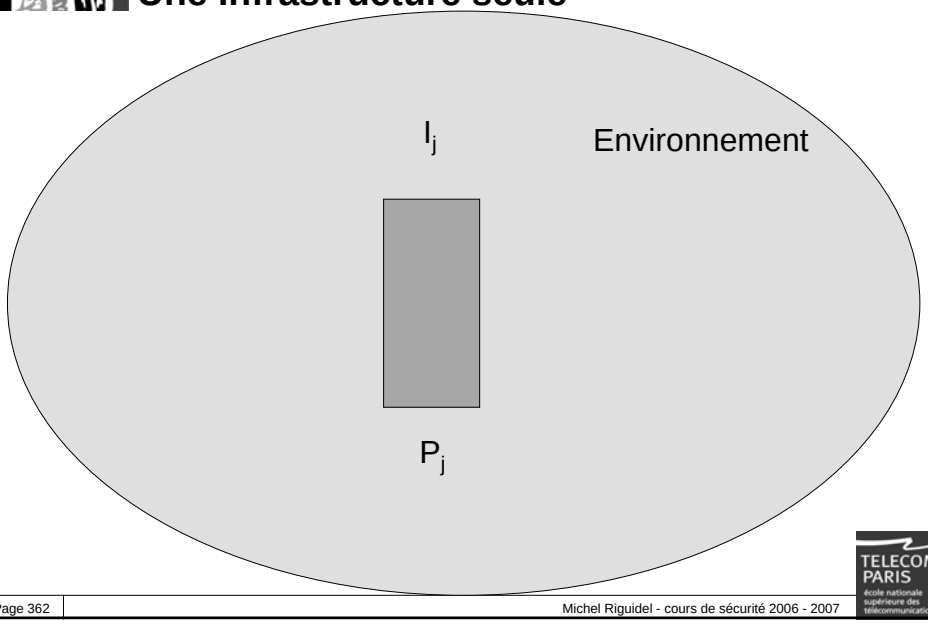
- Internet était dans sa conception et à ses débuts, en pleine Guerre Froide, un maillage redondant qui offrait une sûreté de fonctionnement



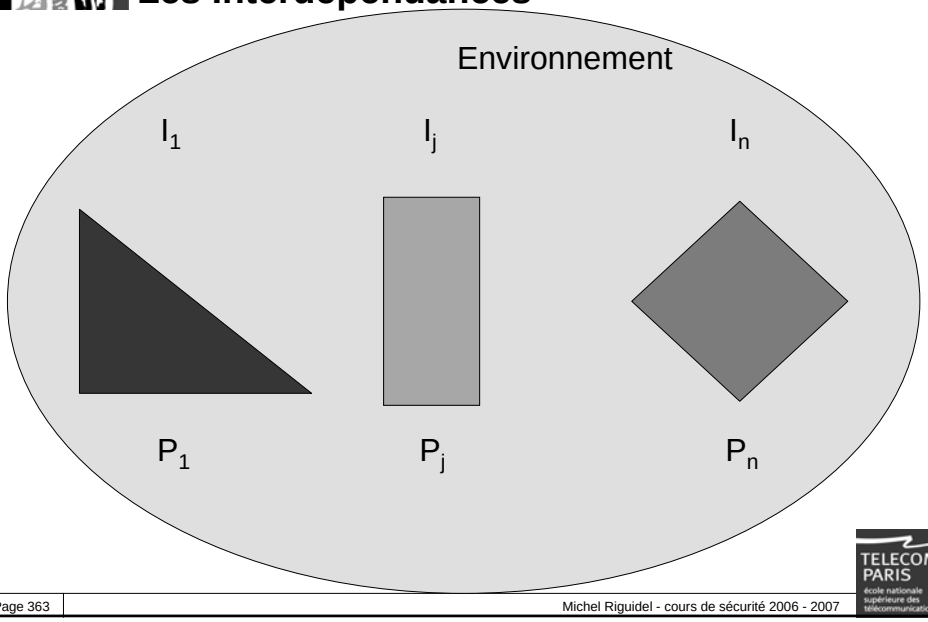
Les recherches pionnières de Paul Baran dans les années 1960, qui envisageait un réseau de communication capable de survivre à une attaque ennemi.
Le croquis montre trois différentes topologies de réseaux décrites dans son mémoire pour la RAND, On Distributed Communications: 1. Introduction to Distributed Communications Network (Août 1964). Une structure de réseau distribué offre la meilleure « survivance ».

- Internet s'est ouvert au secteur économique et à l'ensemble du monde, en optimisant le coût de son infrastructure
- Internet a ainsi suivi la même destinée que toutes les infrastructures contemporaines, et n'a plus rien à voir avec une toile démultipliée de routes informatiques

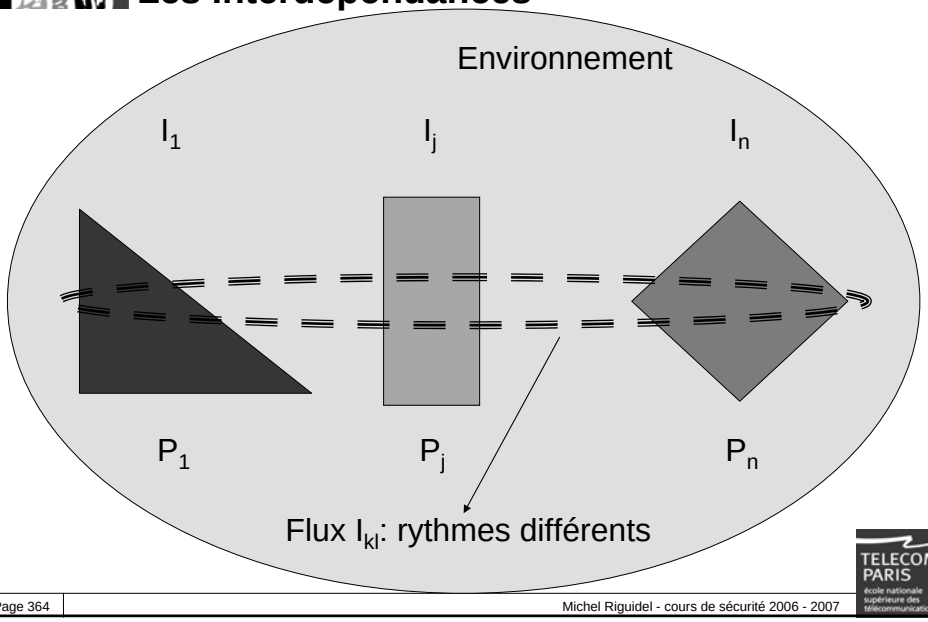
Une Infrastructure seule



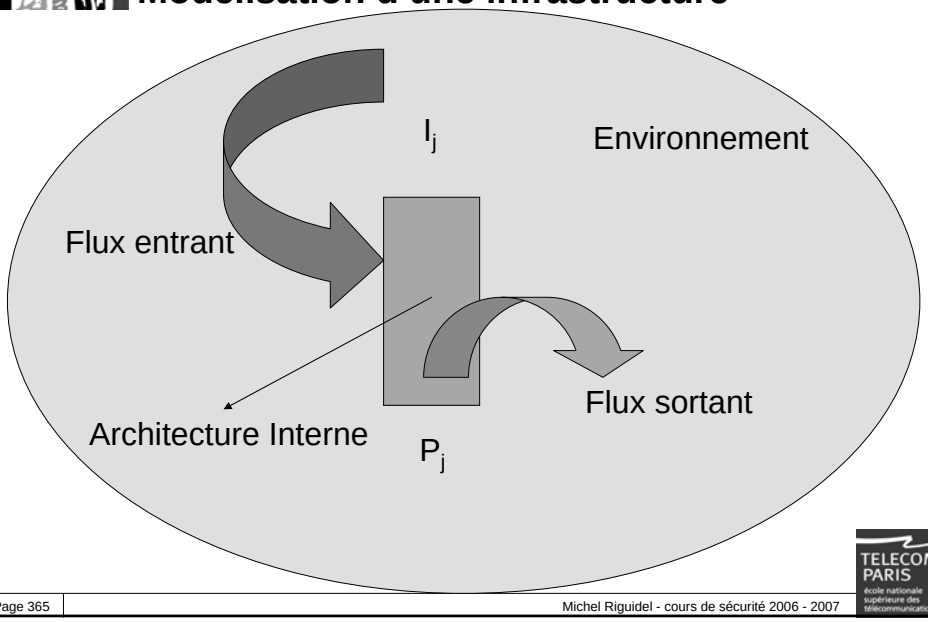
Les Interdépendances



Les Interdépendances

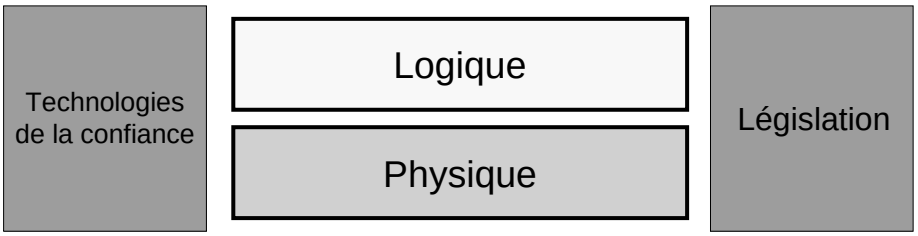


Modélisation d'une infrastructure



Les 2 plans physique et logique

Protection, Dissuasion, …



- Infrastructure critique
  - Physique : le point de vue technique
    - les réseaux des hommes, des moyens mis en œuvre, des ressources matérielles et logicielles
  - Logique : le point de vue super-structurel
    - les aspects business, financiers, relationnels, organisationnels

Infrastructure critique
de type Informatique & Communication

- Les 2 plans physique et logique
  - Physique
    - Tous les aspects techniques et matériels
  - Logique
    - Tous les aspects informatiques logicielles qui concernent l'administration, la gestion de la configuration, de la sécurité, etc

Infrastructure, architecture, structure, ontologie
Marchandise intangible : logiciel et contenu

PKIs, DNS, DRM, TCPA, …
IPR, Contenu illicite

Logique

Physique

Biométrie
Matériel, capteurs
Infrastructure

Acceptabilité par les utilisateurs
et par les fournisseurs
Déploiement, Vérification

Un Nouveau Plan

Virtuel

Logique

Physique

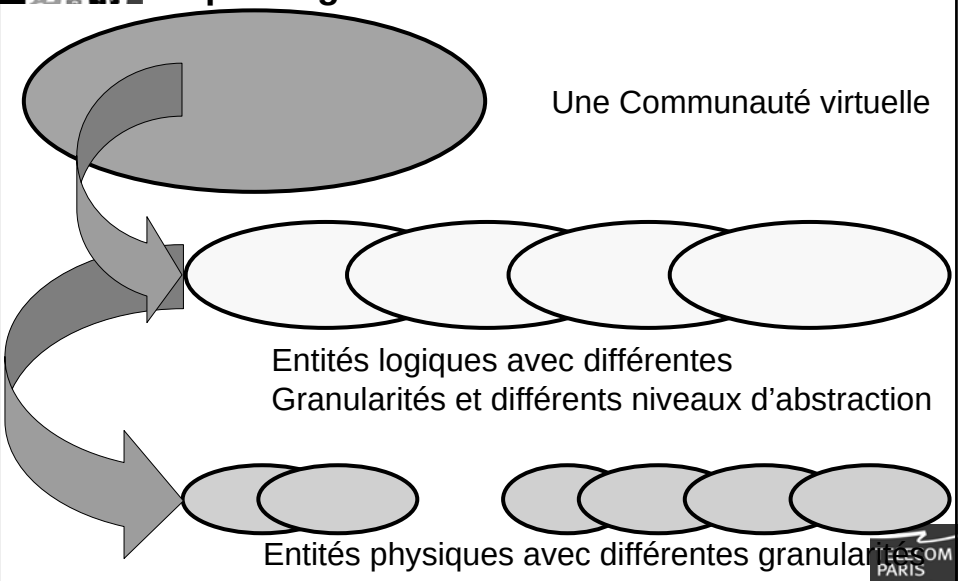
Introduction d'une nouvelle **complexité**

Comment sécuriser ces entités virtuelles?
Comment se protéger des entités virtuelles?
Comment définir des lois et des règles pour des mondes virtuels

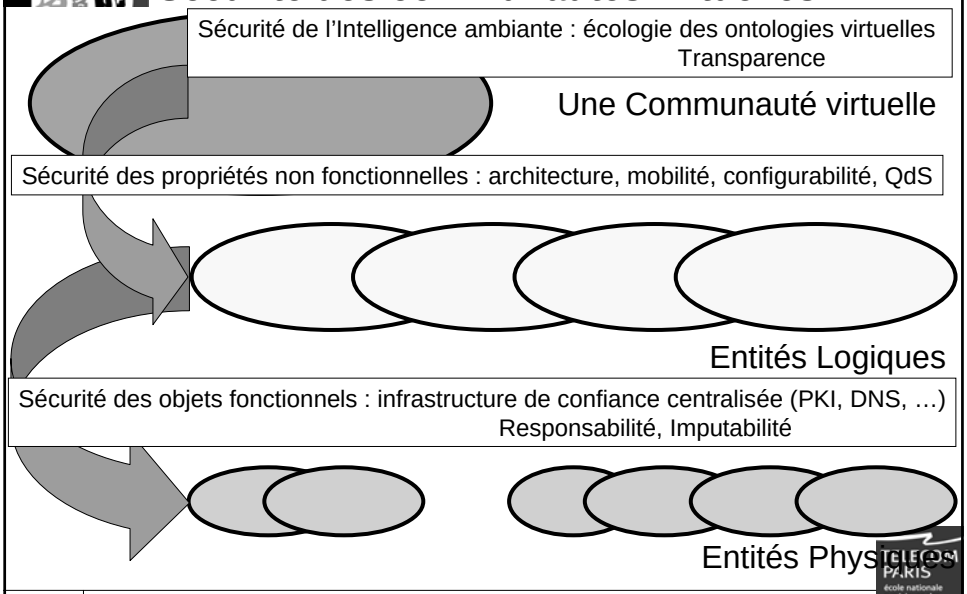
Le paradigme virtuel

- Jongler à différents niveaux d'abstraction logique
  - Valeur ajoutée par la fertilisation croisée
  - Artifice pour réduire la complexité visible
  - Plus de bijection entre entité logique et objet physique
    - Gestion et manipulation d'ensemble d'objets
      - Ensemble de sujets anonymes
      - Architecture intentionnelle (le nom est une fonction, etc)
- Exemple de paradigmes virtuels
  - Mémoire
    - Pages, swap, caches, etc
  - Machine
    - Bytecode
  - Réseau Privé
    - Tunnel cryptographique
  - MPLS
    - Circuits virtuels avec paquets
  - Réseaux de recouvrement
  - Grilles
    - Organisation dynamique répartie, temps réel pour opérer un calcul

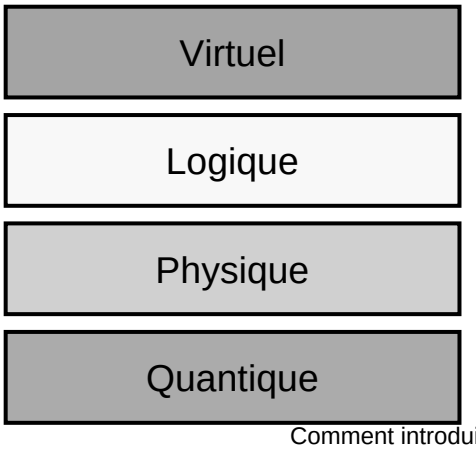
Le paradigme virtuel: arbre d'abstractions



Sécurité des communautés virtuelles



Un Plan futur



Emergence de l'**aléatoire**: l'âge **Quantique**

Comment introduire la confiance avec l'incertitude d'Heisenberg et des architectures aléatoires?

La sécurité des systèmes

- La complexité et ses lois
  - Il est de plus en plus difficile d'écrire le catalogue des situations
    - L'informatique devient un monde toujours nouveau et irréversible
  - Le nombre de lois et de règles croît : il y a une asymptote
- Intégrer de plus en plus la sécurité comme une propriété intrinsèque du système, de l'équipement, du service
- Avantage à l'attaquant
  - « La planète est un village » …
    - Pour l'environnement (pollution), l'économie
    - Pour l'interconnectivité : échanges et communications rapides
  - L'univers numérique est un monde où des étrangers anonymes se côtoient
    - Climat de défiance, voire d'hostilité
      - compétition, espionnage, guerre économique
    - La confiance ex nihilo n'existe pas
      - ne soyons pas naïfs envers nos « amis » sur le « Net »
    - Il faut se recréer ses propres villages de confiance : « exception » culturelle, défense nationale, infrastructure critique (nucléaire, électricité, eau, distribution alimentaire, …)
- L'espoir change de camp …
  - Reprendre la main avec
    - des paradigmes virtuels
    - Le quantique : initialisation et distribution de secrets
  - Ordre numérique
    - Éthique des calculs

Pour une gouvernance numérique

- Vulnérabilité de la société de l'information et de la connaissance
  - La société de l'information interconnectée est de plus en plus complexe et fragile
    - Interdépendances
      - énergie (centrale nucléaire, centrale électrique, ...)
      - transport (trafic aérien, port, trains, routes, …)
      - information (TV, radio, presse) et communication (téléphone, informatique)
      - santé (hôpitaux), éducation et loisirs
      - défense, administration
      - système bancaire, commerce électronique futur
  - La civilisation de la rentabilité, du contact et de la spontanéité
    - Vies trépidantes et entreprises agiles à "flux tendus"
      - Réactions en chaînes et/ou décisions automatiques hasardeuses
      - Discontinuité dans le comportement des systèmes et organisations (rupture de stock, déficit de temps, phénomène de disette) aux conséquences inattendues
- Pour un ordre numérique sur la planète ?
  - La sécurité est difficilement compatible avec un monde libertaire, fluide et non contrôlé
    - Intérêts contradictoires à divers niveaux
  - Donner des grands principes (d'éthique, de responsabilité, de transparence, d'ouverture, d'autonomie, de subsidiarité, …) pour mettre en vigueur des règles du jeu réalistes
    - applicables par l'ensemble de la communauté internationale et
    - acceptées
      - localement par les utilisateurs et
      - globalement par des reconnaissances mutuelles

Références

- M. RIGUIDEL, La sécurité des réseaux et des systèmes, Vuibert, encyclopédie informatique, 2006
- M. RIGUIDEL, Le Téléphone de demain, Le Pommier, 2004
- M. RIGUIDEL, La sécurité à l'ère numérique, Hermès-Lavoisier, 2004
- M. RIGUIDEL, Creating a new security for tomorrow's communication networks and information systems, Annales des Télécommunications, 55, n° 7-8, 18 pages, 2000
- M. RIGUIDEL, Pour l'émergence d'une nouvelle sécurité dans les réseaux de communications et les systèmes d'information futurs, OFTA, Arago Vol. 23, Paris, 2000.
- M. RIGUIDEL, Réflexions sur l'évolution de la sécurité des systèmes d'information, Systèmes et sécurité (Vol 4 n°1), 37 pages, 1995.