Introduction à la sécurité des systèmes d ’information

G. Florin, S. Natkin

11/03

1- Introduction

Les trois lois de la robotique (I. Asimov)

- Un robot ne peut porter atteinte à un être humain ni en restant passif, laisser cet être humain exposé au danger
- Un robot doit obéir aux ordres donnés par des êtres humains sauf quand de tels ordres sont en contradiction avec la première loi,
- Un robot doit protéger sa propre existence dans la mesure ou une telle protection ne s ‘oppose pas à la première et seconde loi.

La peur des ordinateurs

Importance croissante du rôle de la diffusion de l ’information via des systèmes techniques de plus en plus complexes, dans des domaines de plus en plus variés.

- Longtemps concentré sur les effets possibles d’une erreur de programmation dans le contrôle de processus critique (transport, énergie…) [Laprie 95]
- Se porte sur le détournement possible des nouvelles technologies de l’information et la communication par soit des pirates, soit par un état aspirant au meilleur des mondes [IHESI 98].

Souffrons-nous du complexe de Frankenstein ou faut-il craindre avec raison les effets pervers d’une informatisation trop rapide de la société?

Sécurité des systèmes informatiques

Couvre en français deux domaines:

Les méthodes et moyens mis en oeuvre pour éviter les défaillances "naturelles" dont les effets ont un caractère catastrophique (safety)

Les méthodes et moyens mis en oeuvre pour se protéger contre les défaillances résultant d'une action intentionnelle (security)

La folie des ordinateurs

- Dépression électronique la plus courante : un refus clair et définitif de faire quoi que ce soit
- Défaillance plus complexe:
  - faire trop tôt ou trop tard ce qu'il devait faire
  - accomplir des actions différentes de celles attendues (cas de folie grave)
- Caractère influençable:
  - se laisser pervertir par un pirate et détruire votre courrier, transformer votre écran en une œuvre d'art minimaliste ou inonder la planète de messages pornographiques.
  - se soumettre à un marchand pour guetter à votre insu vos comportements de consommateurs.
  - devenir un agent d'un état policier et surveiller vos communications

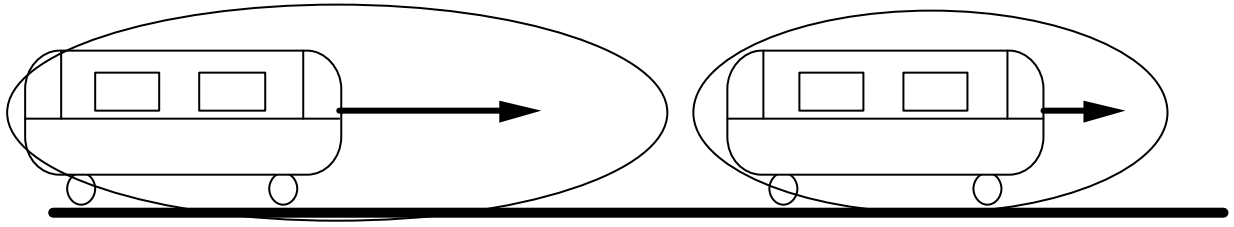
Conséquences aujourd’hui

- Dans la majorité des cas assez bénignes
  - "retaper" deux ou trois fois la même chose, suite à la "perte d'un fichier".
- Domaines d'utilisation de l'informatique où les états d'âme de nos collaborateurs électroniques peuvent avoir des conséquences considérables.
  - la paralysie des serveurs Web,
  - le vol de sommes considérables,
  - la faillite d'une entreprise qui ne peut plus facturer, la création d'embouteillages monstrueux,
  - l'échec du tir d'Ariane V
  - une panne de courant paralysant une métropole.

Et demain ?

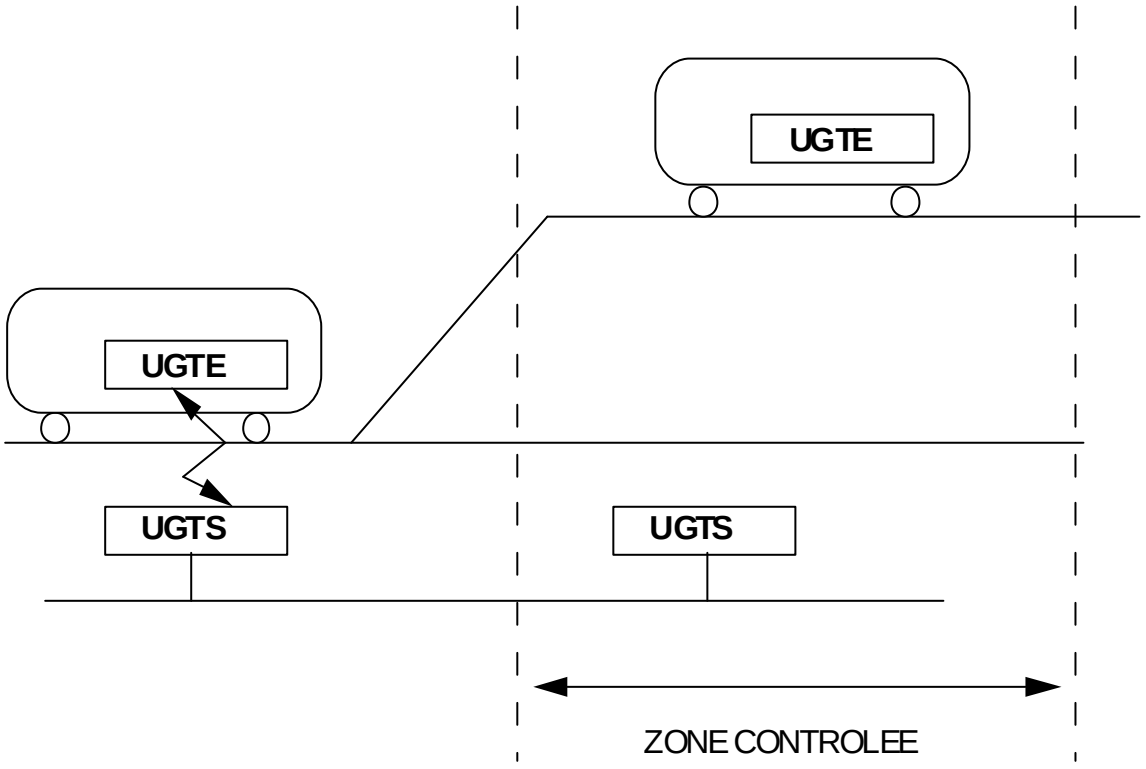
- Le développement d'applications qui reposent sur l'authentification numérique (comme la signature électronique) crée une dépendance dont les effets individuels ou collectifs peuvent être désastreux. Le jour ou les systèmes électroniques ne sauront plus reconnaître votre carte d'identité à puce, existerez vous encore ?
- Constatons à nouveau que ces évènements peuvent aussi bien résulter d'une défaillance ou d'un sabotage.

Exemple 1: pilotage automatique de Maggaly

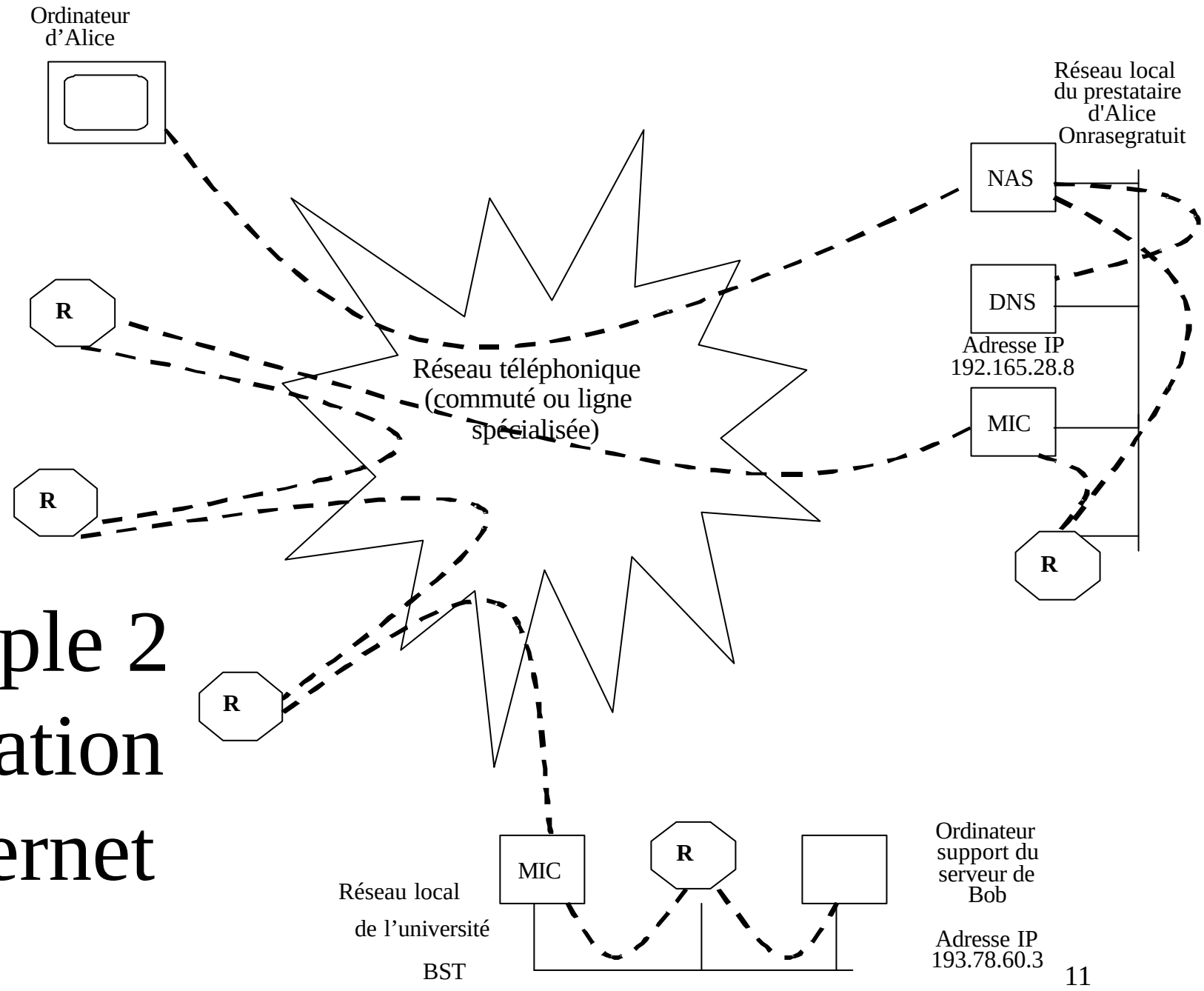


LE CANTON MOBILE DEFORMABLE

Architecture répartie



Exemple 2 Utilisation d'Internet



Internet n'est pas : un réseau sécuritaire

L'accès indus aux informations transmises, la modification de ces informations, le déguisement, sont relativement aisés

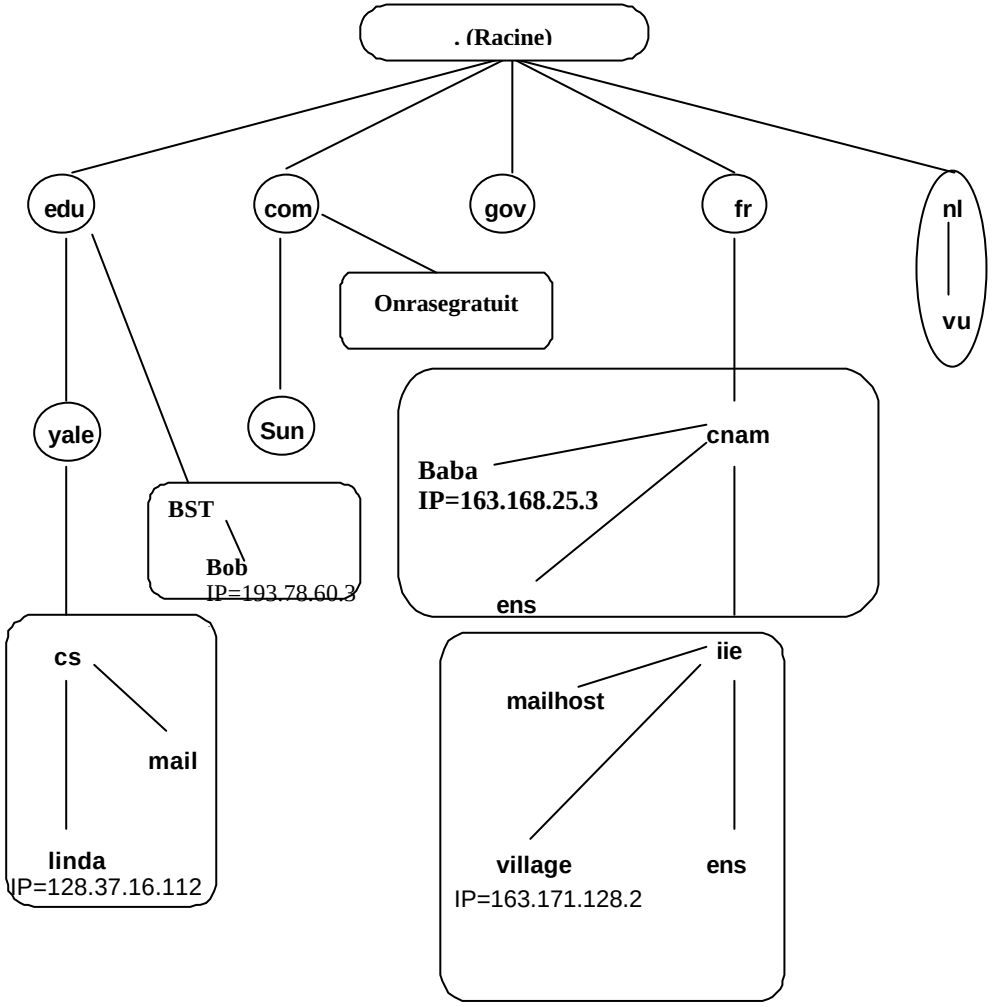
Pourquoi?

- Internet n'est pas contrôle par un prestataire central

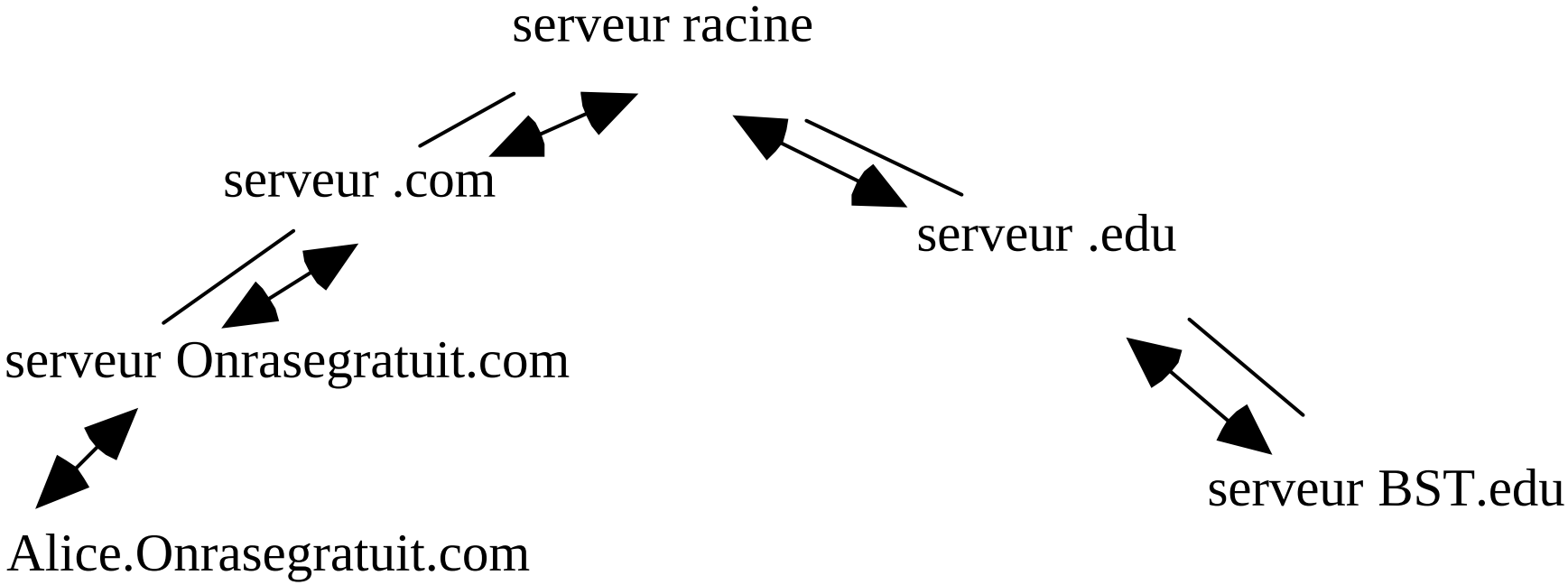
(Pas de contrôle formel des utilisateurs, ni de la nature du trafic)

- Les choix de conception des protocoles utilises (tcp/ip) ne sont pas orientés vers la sécurité

Domain Name Server



Résolution des noms



Scénario d’une attaque

Estelle veut tromper Alice sur l’adresse de Bob.BST.edu.

- elle trouve l’adresse IP du serveur de DNS de Onrasegratuit.com .
- elle lance elle-même (avant la première requête d’Alice) une interrogation sur ce nom sur le serveur de Onrasegratuit.com.
- elle attende que celui ci propage sa demande et l’intercepte
- elle répond avec une fausse adresse en se faisant passer pour le serveur de .com.
- la réponse, considérée comme bonne, est stockée dans la base du serveur de Onrasegratuit.com.
- lorsque Alice fait sa demande le serveur lui donnera la fausse réponse.

L ’origine des risques est souvent humaine

- Défaillances des systèmes techniques (usure des équipements, panne catalectique, catastrophes naturelles)
- Erreur de conception
- Erreur de réalisation
- Erreur d ’exploitation
  - La négligence , l ’inattention…
  - Les fautes réelles (violation d ’une procédure formalisée)
- Malveillance à caractère ludique
- Fraude, Vol
- Sabotage

Quelques statistiques : coût des sinistres en MFF en 1996 (Clusif)

Accidents		
Physiques (incendie, explosion, dégât des eaux…)	1630	12,81
Pannes	1110	8,73
Force majeure	35	0,28
Perte services essentiels (Télécoms, électricité…)	280	2,20
Total	**3055**	**24,02**
Erreurs humaines		
Utilisation	800	6,29
Conception, Réalisation	1020	8,02
Total	**1820**	**14,31**
Malveillances		
Vol, vandalisme physique	240	1,89
Fraude non physique	2300	18,08
Sabotage	5	0,04
Attaque logique	1090	8,57
Divulgation	1100	8,65
Autres (copies de logiciels)	3110	24,45
Total	**7845**	**61,67**
TOTAL	**12720**	**100**

La complexité : qu'est ce qu'un système informatique normal ?

Impossibilité d'une spécification : nous ne savons pas définir exactement ce que nos machines doivent faire ou ne pas faire

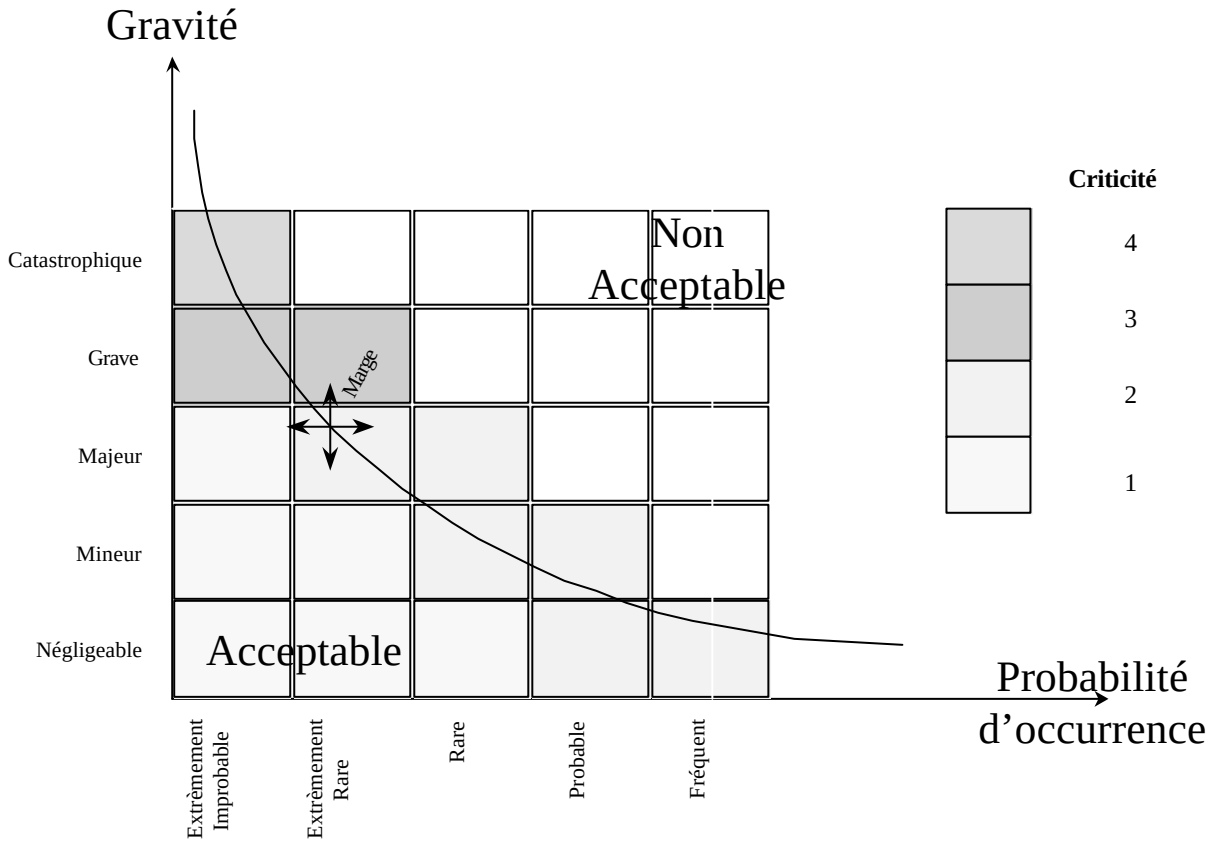
- Complexité de l'environnement (le monde qui interagit avec le système)
- Les utilisateurs
- Les pannes
- Les attaques
- Complexité des fonctions: les demandes des utilisateurs qui ne maîtrisent pas la viabilité et la fragilité intrinsèque de cette expression de besoins.

Comment concevoir et développer qu'un système informatique normal ?

- Les limites des possibilités de validation de ces systèmes par rapport à ce qu'ils doivent faire et surtout ce qu 'ils ne doivent pas faire.
- L 'incapacité d 'évaluer correctement les conséquences des éventuelles défaillances et donc, a fortiori, des agressions.
- L 'incapacité de vérifier à posteriori ce que fait un système automatisé de traitement de l 'information.

Nous n'avons pas encore inventé les trois lois de la robotique qui limiteraient drastiquement leurs comportements dangereux et nous confions chaque jour des opérations de plus en plus complexes à nos systèmes informatiques.

Niveaux de gravité et niveaux de probabilité



De la pratique sociale des ordinateurs

- Un exemple : l'usage du courrier électronique.
- Il n'y a pas de pratique sociale définie pour les nouveaux usages de l'Internet.
- La peur du pilote automatique de métro est en grande partie liée à un usage professionnel non maîtrisé

LE CADRE JURIDIQUE (1)

Validité juridique d'opérations informatiques

Certaines transactions informatiques entraînent des obligations légales de responsabilité => Elles sont considérées comme valides juridiquement par la loi ou la jurisprudence.

Exemples

Ordres de virement informatique (par exemple deux fois le même ordre de paiement doit-être honoré) ou ordre de commande dans le cas d ’un contrat de droit privé

Factures électroniques et comptabilité reconnues par l ’administration fiscale

Principe et conditions d ’utilisation de la signature électronique comme élément de preuve (position commune arrêtée par le conseil de l ’union européenne le 28 juin 1999)

CADRE JURIDIQUE (2)

Loi informatique et liberté

La Loi 78_17 du 6/1/1978 Définit la constitution et le rôle de la CNIL (Commission Nationale Informatique et Liberté)

Une entreprise ou une administration qui traite des fichiers administratifs nominatifs est responsable relativement à la non divulgation des informations qu'elle gère.

- Nécessité de formalités préalables à la mise en oeuvre des traitements automatisés pour la collecte, l'enregistrement et la conservation des informations nominatives
- Exercice du droit d'accès
- Dispositions pénales de non respect

CADRE JURIDIQUE (3)

Loi no 85-660 du 3/7/1985

Décrit les règles relatives aux contrefaçons et au droit d'auteur

Par exemple la copie (autre que pour sauvegarde) est punissable de trois mois à deux ans de prison , d'une amende de 6000 à 12000 Francs.

Loi no 88-19 du 5/1/1988

Loi relative à la fraude informatique

Sont passibles de sanctions pénales pouvant atteindre 5 ans de prison, une amende de 2 millions les faits suivants:

. accès frauduleux aux données.

. l'introduction de données

. l'entrave au fonctionnement du système.

CADRE JURIDIQUE (4)

Loi relatives à l'usage de la cryptographie (loi du 19/03/99)

En France l 'usage de moyens de chiffrement est limité:

Utilisation libre concernant l'authentification et l'intégrité et des moyens de chiffrement à clefs de moins de 128 bits (ceux ayant des clefs de plus de 40 bits doivent être déclarés)

Déclaration de commercialisation et d'importation pour les produits de chiffrement ayant des clefs comprises entre 40 et 128 bits

Demande d'autorisation de distribution et d 'utilisation pour les produits de chiffrement ayant des clefs de longueur supérieure à 128 bits

Demande d 'autorisation pour l 'exportation de produit de chiffrement

Auprès du Service Central de Sécurité des systèmes informatiques (SCSSI)

Conclusion

Il existe donc une probabilité raisonnable de pouvoir cohabiter et même collaborer avec les ordinateurs. Il suffit de prendre le temps de savoir ce que nous voulons en faire et comment. Lorsque le problème est bien posé, les solutions techniques existent déjà souvent et, dans le cas contraire, seront inventées.

2-Politique de sécurité

NOTION DE POLITIQUE DE SÉCURITÉ D ’UN SYSTÈME D ’INFORMATION

Assurer la sécurité ne peut être défini et mis en œuvre
que relativement à des objectifs clairement définis:

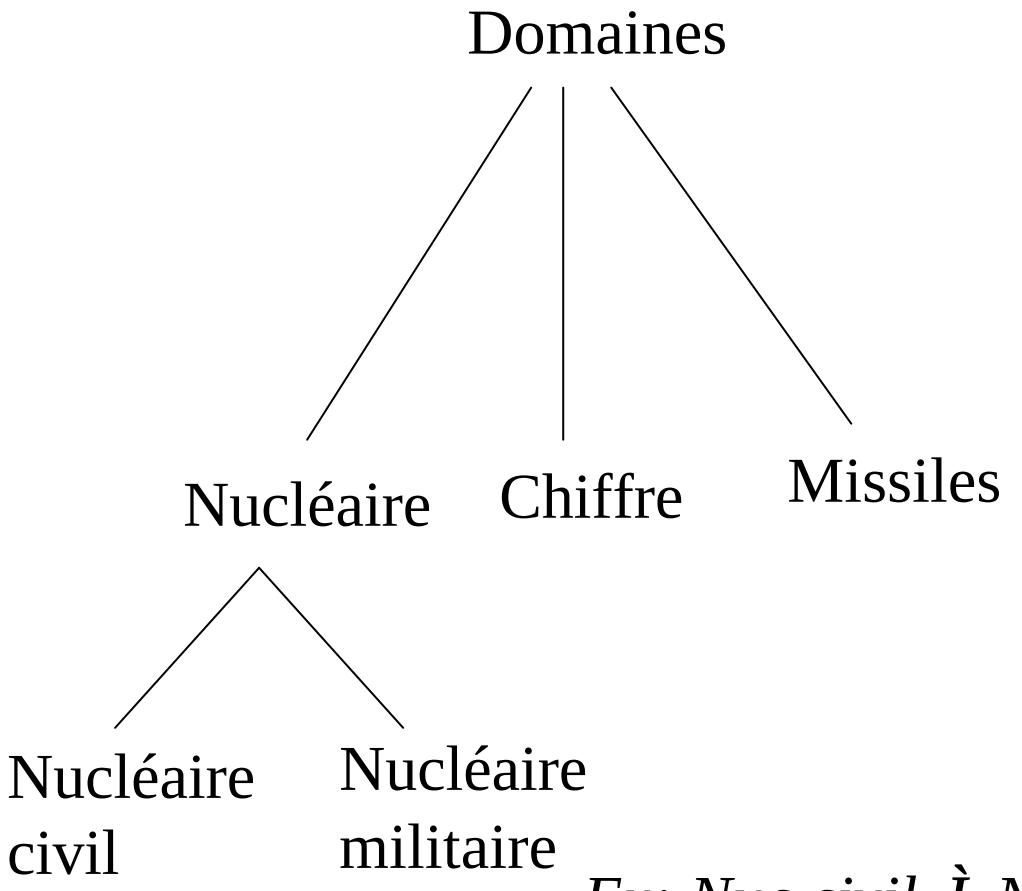
1) Un périmètre d’application
(qui est concerné ou et quand, avec quels moyens…)
qui détermine le système d'information sur lequel porte la politique.
2) Des règles définissant les actions autorisées (**les droits**)
ou interdites réalisées par des hommes sur des hommes ou
des biens matériels ou immatériels.
3) La nature et la force des attaquants éventuels
4) La nature des défaillances auquel doit être
capable de résister une politique

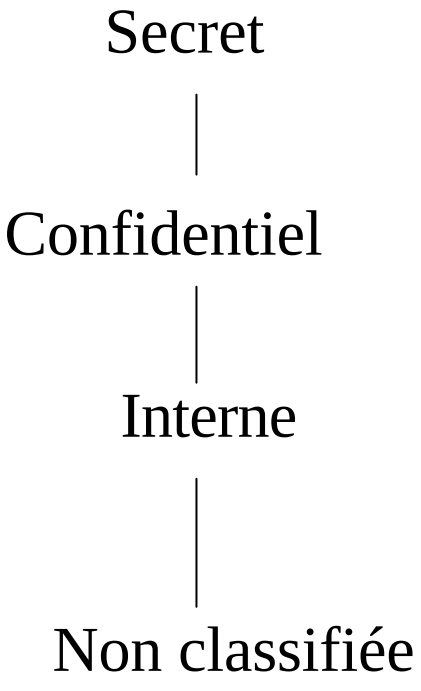
POLITIQUES DE ROLES ET NOMINATIVES DISCRETIONNAIRES ET OBLIGATOIRES

Une politique telle que tous les droits d'une politique sont attribués aux personnes uniquement en fonction du rôle qu'elles jouent dans le système d'information (administrateur système, responsable de sécurité, chef comptable…) est appelée **politique de rôle**. Une telle politique doit préciser les procédures appliquées pour attribuer un rôle à une personne.
Une politique telle qu'au moins un droit est attribué à une personne intutae personnae est dite **politique nominative**.

Une politique de sécurité est **discrétionnaire** si l'entité qui possède un objet à tous les droits pour propager les droits sur cet objet.
Si ce processus de propagation est limité par des règles générales, alors la politique est dite **obligatoire**

EXEMPLE: PROTECTION DE L ’ACCÈS AU DOCUMENTS (1): HIÉRARCHIES





Ex: Nuc.civil Ì Nucléaire, Non classifié < Interne

EXEMPLE: PROTECTION DE L ’ACCÈS AU DOCUMENTS (2): RÈGLES

Toute personne est habilitée à certains niveaux dans certains domaines:
Général X:((secret, nucléaire), (confidentiel, chiffre))

Tout document est classé par un couple:
Doc A (confidentiel, nucléaire civil)
Doc B (interne,missile)

Pour avoir lire ou écrire à un document D(a,b)
il faut avoir une habilitation (x, y) avec $a \leq x$ et $b \subset y$.
Le Général X peut lire A car nucléaire civil $\subset$ nucléaire et secret<confidentiel
Il ne peut lire B car il n ’a aucune habilitation dans un domaine inclus dans les missiles

EXEMPLE: PROTECTION DE L ’ACCÈS AU DOCUMENTS (3): NIVEAU D ’ATTAQUE

Le niveau d ’attaque considéré est maximal:
Agresseurs spécialistes en espionnage militaire, disposant de moyens matériels et financiers illimités

La politique doit rester opérationnelle quelle que soit la nature des défaillances et erreurs pouvant affecter les systèmes physiques considérés.

EXEMPLE: POLITIQUE D ’ACCÈS À UN SERVEUR WEB DE DOSSIERS MÉDICAUX (1)

Identification de tous les acteurs (humain, physique) pouvant agir sur le système.

Le personnel d'un hôpital classés par unités de soin (US),
les médecins en relation avec l'hôpital (M),
l'administrateur du système (A),
les patients qui ont ou sont soignés à l'hôpital (P)
le reste de l'humanité.

EXEMPLE: POLITIQUE D ’ACCÈS À UN SERVEUR WEB DE DOSSIERS MÉDICAUX (2)

Identification de toutes les ressources sur lequel une action peut porte
les pièces des dossiers médicaux

- Des dossiers D,
- Une table d'accréditation des médecins TM
- Une table des patients TP
- Une table patient/médecin TPM
- Des courriers électroniques ME

EXEMPLE: POLITIQUE D ’ACCÈS À UN SERVEUR WEB DE DOSSIERS MÉDICAUX (3)

les actions possibles sont créer, détruire, lire, modifier un document, accréditer un médecin externe, autoriser l'accès à un dossier à un médecin externe. Les droits donnés sont, par exemple:

•Un droit illimité d'accès des dossiers par les membres du CHU
•Un droit d'accréditation d'un médecin ayant signé la convention accordée par A (procédure papier)
•Un droit de lecture de M à D, dossier d'un patient P,
accordé par par P et uniquement si M est accrédité (procédure papier)
•Un droit de modification sur le serveur de la table l'accréditation d'un médecin
TM accordé à un administrateur A ou des membres désignés d'une unités de soins US, tous membres du CHU….

EXEMPLE: POLITIQUE D ’ACCÈS À UN SERVEUR WEB DE DOSSIERS MÉDICAUX (4): NIVEAU D ’ATTAQUE

Le niveau d ’attaque considéré est intermédiaire:
Agresseurs utilisant des techniques espionnage civil, disposant
de moyens matériels et financiers importants mais limité

La politique doit rester opérationnelle en présence de pannes catalectiques
(interruption de services) des systèmes physiques impliqués

3 Formalisation des politiques de sécurité

MATRICE DES DROITS

définit à chaque instant les droits de chaque utilisateur sur chaque objet.
créer (cr), lire (lec), modifier (mod), détruire (dt)

	Dossier P 1	Dossier P 2	TM	TP	TPM	ME
US	cr, lec,mod,dt	cr, lec,mod,dt				cr, em,lec
MED 1	lec					cr, em,lec
MED 2	lec					cr, em,lec
A			cr, mod	cr, mod	cr,dt	
PAT 1	lec					
PAT 2		lec				

EOLUTION DE LA MATRICE DES DROITS

La matrice des droits évolue en fonction des évènements suivants:

- évolution de la population des utilisateurs
- création et destruction des objets
- création et destruction des droits
- propagation des droits

MODELE DE BELL LAPDULA (1)

H={non classifié, privé, confidentiel, secret} niveaux de classification
non classifié <privé< confidentiel< secret
DOM={domaine, nucléaire, nucléaire civil,
nucléaire militaire, cryptographie, missile...}

Relation d'ordre partiel sur R=HxDOM notée ≤ de la façon suivante:

$$\forall h_1 \in H, \forall h_2 \in H, \forall d_1 \in DOM, \forall d_2 \in DOM \quad (h_1, d_1) \leq (h_2, d_2) \Leftrightarrow h_1 \leq h_2 \text{ et } d_1 \subset d_2$$

Par exemple (confidentiel, nucléaire civil) ≤ (secret, nucléaire)
car nucléaire civil ⊂ nucléaire et confidentiel < secret
Cette relation dote R d'une structure de treillis:

MODELE DE BELL LAPDULA (2)

A chaque personne p est associé un niveau d'habilitation N(p).
N(p) est ensemble d'éléments de R deux a deux non comparables selon la relation ≤ et couvrant tous les domaines.
Le général X est habilité {(secret, nucléaire),
(confidentiel, chiffre) (missile, non classifié)}.
On note P ={ (p, N(p))}. P constitue les sujets de la politique.

A chaque document d est associé un niveau de classification c(d)∈ R
D ={ (d, c(d))}.D constitue les objets de la politique.

L'état courant du système est constitué par (P, D)

MODELE DE BELL LAPDULA (3)

Les actions possibles (post conditions) sur un document d sont:

- Créer(d, cl): Ajoute à D un document d de niveau de classification cl.
- Lire(d): lire un document d. Lire ne modifie ni D ni P
- Lire+Modifier(d,cl'): Lire et modifier d et lui attribuer
un nouveau niveau de classification cl'.

Ceci revient à ôter à D le couple (d,cl) et ajouter le couple (d,cl').

MODELE DE BELL LAPDULA (4)

A tout instant pré conditions qui déterminent les actions possibles
sont données par les règles suivantes:

- $p \in P$ peut Créer(d,cl) si $\exists n \in N(p)$ tel que $cl \leq n$:

Une personne ne peut créer que des documents d'un niveau
de classification inférieur ou égal à un des éléments
de son niveau d'habilitation.

- $p \in P$ peut Lire(d) si $\exists n \in N(p)$ tel que $c(d) \leq n$:

Une personne ne peut lire que des documents d'un niveau
de classification inférieur ou égal à un des éléments
de son niveau d'habilitation.

- $p \in P$ peut Lire+Modifier(d,cl') si elle peut Lire(d) et Créer(d,cl').

Par exemple le général X peut créer un document classifié
(secret, nucléaire civil), lire un document classé (confidentiels, chiffre)
et lire et modifier un document (secret, nucléaire).
Il ne peut faire aucune de ces opérations surun document classé (confidentiel, missile).

MODELE DE BELL LAPDULA: LA REGLE * (5)

Un général T ayant une habilitation comprenant
(nucléaire civil, secret) et (missile, confidentiel)
ouvre en lecture un document d classé (missile, confidentiel)
et crée un document d' classé (nucléaire civil, secret).
Il recopie tout ou partie de d dans d'.
Le général X peut alors lire d' et a donc accès
a des informations qui ne lui étaient pas destinées.

Il faut donc rajouter la règle suivante:

- Si p∈ P peut Créer(d,cl') ou Lire+Modifier(d,cl') et Lire(d)

alors on doit avoir c(d) ≤cl'. Autrement dit a partir d'un document
que p peut lire il ne peut que créer ou modifier
des documents de classification supérieure.

MODELE DE BELL LAPDULA (6)

Cette spécification comporte une lacune:
la procédure d'habilitation n'est pas décrite (P est invariant).

Elle possède un défaut qui est liée à la granularité de la notion de document:Elle conduit à sur classifier tous les documents.

Numéro de paragraphe	Titre	Classification
P0	Sommaire	(confidentiel, domaine)
P1	Autant en emporte le vent	(secret, missile)
P2	Quelle est verte ma vallée	(secret, nucléaire civil)
P3	Hiroshima mon amour	(confidentiel, nucléaire militaire)
P4	Remerciements	(non classifié, domaine)

Le document total est classé (secret, domaine). Un document composé de P2,P3 est classé (secret, nucléaire).

4- Propriétés de sécurité

TERMINOLOGIE: AUTHENTIFICATION

C'est la propriété qui assure la reconnaissance sûre de l ’identité d ’une entité

L'authentification protège de l'usurpation d'identité.

Signature (au sens classique) = Authentification:
La première idée contenue dans la notion habituelle de signature est que
le signataire est le seul à pouvoir réaliser le graphisme (caractérisation psychomotrice)

Entités à authentifier:
- une personne
- un programme qui s ’exécute (processus)
- une machine dans un réseau

TERMINOLOGIE: NON REPUDIATION

C'est la propriété qui assure que l'auteur d'un acte ne peut ensuite dénier l'avoir effectué.

Signature (au sens habituel) = Authentification+Non répudiation :

La seconde idée contenue dans la notion habituelle de signature
est que le signataire s'engage à honorer sa signature:
engagement contractuel, juridique, il ne peut plus revenir en arrière.

Deux aspects spécifiques de la non répudiation dans les transactions électroniques:

a) La preuve d'origine

Un message (une transaction) ne peut être nié par son émetteur.

b) La preuve de réception

Un récepteur ne peut ultérieurement nier avoir reçu un ordre
s'il ne lui a pas plu de l'exécuter alors qu'il le devait juridiquement.

Exécution d'ordre boursier, de commande, ..

TERMINOLOGIE: INTEGRITE

C'est la propriété qui assure qu'une information n'est modifiée que par des entités habilitées (selon des contraintes précises)

Une modification intempestive (même très temporaire)
est à interdite sur une écriture comptable validée

Le code binaires des programmes ne doit pas pouvoir être altéré

Les messages de l ’ingénieur système doivent pouvoir être lus et non modifiés

TERMINOLOGIE: CONFIDENTIALITE

C'est la propriété qui assure qu'une information ne peut être lue que par des entités habilitées (selon des contraintes précises)

Un mot de passe ne doit jamais pouvoir être lu par un autre que son possesseur

Un dossier médical ne doit pouvoir être consulté que par les malades et le personnel médical habilité

TERMINOLOGIE: AUDITABILITE

C'est la propriété qui assure la capacité à détecter et à enregistrer de façon infalsifiable les tentatives de violation de la politique de sécurité.

TERMINOLOGIE: DISPONIBILITE ET FIABILITE

Disponibilité :capacité de rendre un service
correct à un instant donné,
Fiabilité :capacité à rendre continûment un service correct

Relèvent de la terminologie de la **sûreté de fonctionnement**
On retiendra toutefois que les actions de sabotage
d'un système visent justement à diminuer sa disponibilité ou sa fiabilité

5-Menaces et attaques

LES MENACES AYANT POUR OBJECTIF LE VOL DE DONNEES

Détournement des données

Exemples: espionnage industriel , espionnage commercial, violations déontologiques

Détournement des logiciels

Exemple:copies illicites

LES MENACES AYANT POUR OBJECTIF LA FRAUDE OU LE SABOTAGE

Par modification des informations ou des dispositifs techniques et humains

Exemple : La fraude financière informatique, la destruction des informations (logique), le sabotage destiné à rendre inefficaces certaines fonctions (déni de service)

CLASSIFICATION DES ATTAQUES
ATTAQUES VISANT L ’AUTHENTIFICATION

Déguisement (Mascarade)

Pour rentrer dans un système on essaye de piéger des usagers et de se faire passer pour quelqu'un d'autre:

Exemple: simulation d'interface système sur écran,
simulation de terminal à carte bancaire

CLASSIFICATION DES ATTAQUES
ATTAQUES VISANT L ’INTEGRITE DES DONNEES

Modification de messages, de données

Une personne non autorisée, un usager ou même un agent autorisé s'attribuent des avantages illicites en modifiant un fichier, un message (le plus souvent cette modification est réalisée par programme et entre dans la catégorie suivante)
Ex modification des données sur un serveur Web

CLASSIFICATION DES ATTAQUES
ATTAQUES VISANT L ’INTEGRITE DU FLUX DE DONNEES

Répétition ("replay")

Espionnage d'une interface, d'une voie de communication (téléphonique, réseau local) pour capter des opérations (même cryptées elles peuvent être utilisables)

Répétition de l'opération pour obtenir une fraude.

Exemple: Plusieurs fois la même opération de crédit d'un compte bancaire.

CLASSIFICATION DES ATTAQUES
ATTAQUES VISANT L ’INTEGRITE DES PROGRAMMES

Modification des programmes

Les modifications à caractère frauduleux

Pour s'attribuer par programme des avantages.
Exemple: virement des centimes sur un compte

Les modifications à caractère de sabotage

Pour détruire avec plus ou moins de motivations des systèmes ou des données

CLASSIFICATION DES ATTAQUES
ATTAQUES VISANT L ’INTEGRITE DES PROGRAMMES (2)

Deux types de modifications

a) Infections informatiques à caractère unique

Bombe logique ou cheval de Troie

- Dans un programme normal on introduit un comportement illicite mis en action par une condition de déclenchement ou trappe
(la condition, le moment ou l'on bascule d'un comportement normal à anormal)

Exemples:licenciement de l'auteur du programme

b) Infections auto reproductrices

Il s'agit d'une infection informatique simple (du type précédent)
qui contient de plus une partie de recopie d'elle même afin d'en assurer la propagation

***Virus* :** à action brutale

Ver : à action lente (détruisant progressivement les ressources d'un systèmes)

QUELQUES CLASSES DE VIRUS (implantation)

- Les virus à secteur d ’amorçage
- Les virus à infection de fichiers
- Les macro virus
- Les virus furtifs
- Les virus polymorphes (mutants)
- Les virus réseaux

CLASSIFICATION DES ATTAQUES
ATTAQUES VISANT LA CONFIDENTIALITE

Les attaques ayant pour but le vol d'information via un réseau par **espionnage des transmissions de données** (espion de ligne, accès aux données dans des routeurs et des serveurs Internet)

Canaux cachés

CLASSIFICATION DES ATTAQUES
ATTAQUES VISANT LA CONFIDENTIALITE (2)

Analyse de trafic

On observe le trafic de messages échangés pour en déduire des informations sur les décisions de quelqu'un.

Exemples:
Bourse : augmentation des transactions sur une place financière.
Militaire : le début de concentration entraîne un accroissement de trafic important.

Inférence

On obtient des informations confidentielles à partir d'un faisceau de questions autorisées
(et d'un raisonnement visant à faire ressortir l'information).

CLASSIFICATION DES ATTAQUES
ATTAQUES VISANT LA DISPONIBILITE
(DENI DE SERVICE)

Attaque par violation de protocole

Erreur très rare en fonctionnement normal et non supportées par le protocole

Attaque par saturation

Envoi de messages trop nombreux provoquant un écroulement des systèmes et réseaux

6- Mise en œuvre d ’une politique de sécurité

ÉTAPES TYPES DANS L'ÉTABLISSEMENT D'UNE POLITIQUE DE SÉCURITÉ

Définition de la politique

Identification des vulnérabilités

. En mode fonctionnement normal (définir tous les points faibles)
. En cas d'apparition de défaillances un système fragilisé
est en général vulnérable : c'est dans un de ces moments intermédiaires qu'une intrusion peut le plus facilement réussir

Évaluation des probabilités associées à chacune des menaces

Évaluation du coût d'une intrusion réussie

Choix des contre mesures

Évaluation des coûts des contre mesure

Décision

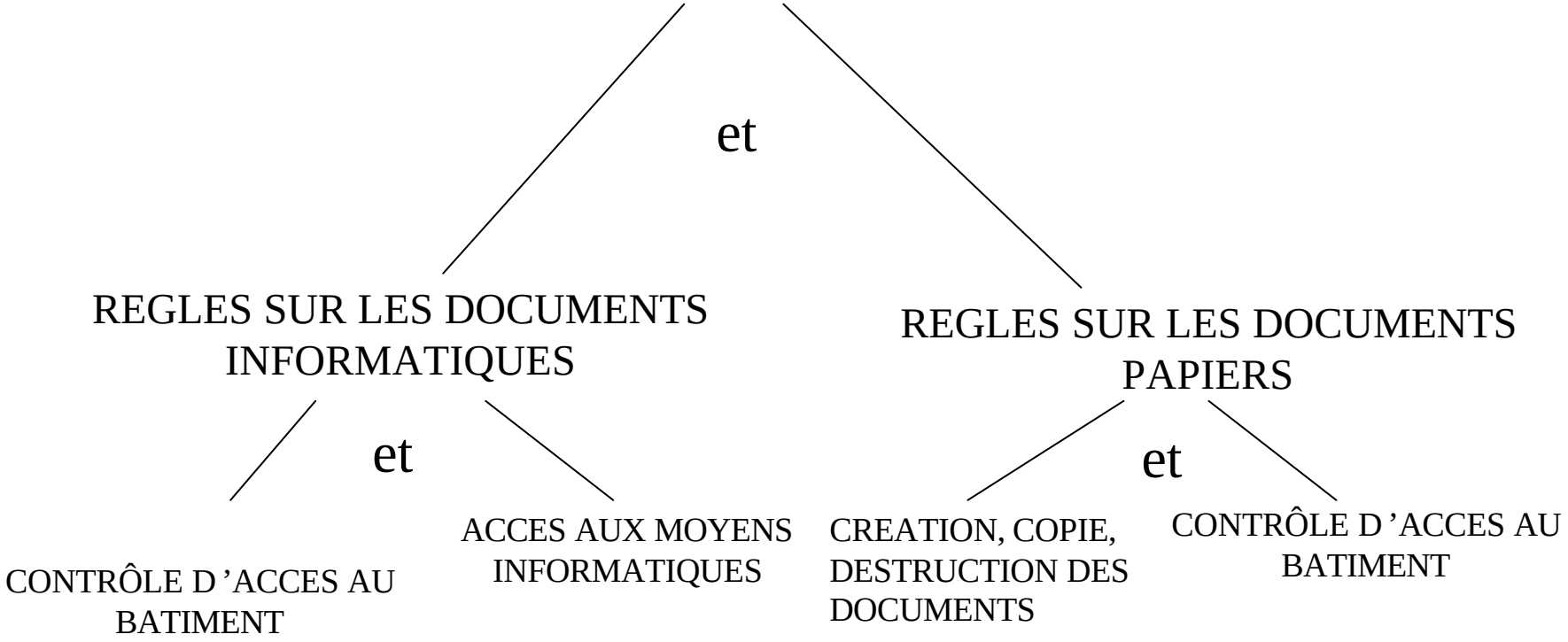
MOYENS

La réalisation d ’une politique de sécurité résulte de la mise en œuvre cohérente de:

- Moyens physiques (architecture des bâtiments, systèmes de contrôle d ’accès, destructeurs de documents…)
- Moyens informatiques
- Règles d ’organisation et moyens procéduraux: règles de fonctionnement qui doivent être respectées

CONTRUCTION DEDUCTIVE DES MOYENS MIS EN OEUVRE

CONFIDENTIALITE DES DOCUMENTS



COHÉRENCE DES MOYENS

Les moyens doivent être « complets »: dans le cadre des hypothèses considérées, quoi qu'il arrive la politique est respectée

Les moyens doivent être non contradictoires et raisonnablement contraignants: Ils ne doivent pas constituer un obstacle à la réalisation des fonctions opérationnelles de l 'organisation considérée (Par exemple les procédures trop complexes sont souvent contournées)

Les moyens doivent être homogènes par rapport aux risques et aux attaques considérés: (Par exemple il est inutile de chiffrer tout les documents informatiques si ils partent en clair dans les poubelles)

Le respect des procédures est un des points essentiels de l 'efficacité: Elles doivent donc être comprises et acceptées par toutes les personnes concernées.

PRINCIPE GENERAUX DE MISE EN ŒUVRE (1)

Assurer la mise en oeuvre d ’une politique de sécurité consiste à garantir que, à chaque instant, toutes les opérations sur les objets (ressources) ne sont réalisables et réalisées que par les entités (physique ou informatique) habilitées.

La base de la réalisation de la sécurité sont

le confinement: L’ensemble des objets sont maintenus dans des domaines étanches, l ’accès ce fait via un guichet protégé

le principe du moindre privilège: Pour qu'un système fonctionne en sécurité il faut donner à ses utilisateurs exactement les droits dont il ont besoin pour s'exécuter : **ni plus ni moins**.

PRINCIPE GENERAUX DE MISE EN ŒUVRE (2)

Tout accès à un objet se fait via
“un guichet”

Pour réaliser une opération une
entité se présente au guichet.

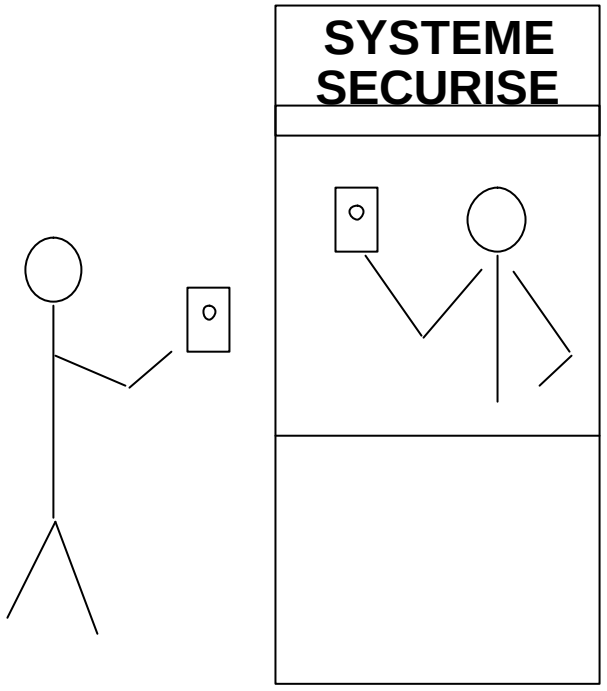
Elle s’authentifie,

Elle authentifie le guichet
(risque de mascarade)

Elle présente une autorisation
montrant qu’elle à les droits
qu ’elle a pour réaliser
l’opération,

Le guichetier contrôle que
l ’autorisation est valide

L’opération est réalisée**.**



PRINCIPES GENERAUX (3)

Pour construire des guichets de contrôle informatique il faut:

Pouvoir protéger des données secrètes qui constituent par exemple la base de l'authentification ou qui doivent être étanches en lecture (Confidentialité)

Protéger contre des modifications interdites certaines données accessibles uniquement en lecture ou en exécution (code des opérations) (Intégrité)

Pouvoir authentifier clients et guichets,

Pouvoir garantir que l'exécution de l'opération ne peut être faite que par le guichetier fait selon sa spécification (Protection)

Pouvoir garantir que les transferts de données entre le client sont protégés en écriture ou lecture et écriture (intégrité ou confidentialité à

Pouvoir enregistrer de façon non falsifiable toutes les opérations (non répudiation)

Pouvoir noter toutes tentatives de fraude (auditabilité)

PRINCIPES GENERAUX (4)

Pour pouvoir administrer le système il faut:

- Gérer (création, destruction, nommage) les entités et les données d'authentification de ces entités
- Gérer (création, destruction, nommage) des guichets incontournables et les données d'authentification de ces guichets associés à chaque opération.
- Gérer (création, destruction, nommage, propagation) des droits)

EXEMPLE PHYSIQUE

- Règle 1: Seules les personnes membres du personnel ou invitées par un membre du personnel habilité à inviter peuvent circuler dans le bâtiment.
- Moyens pour assurer la règle:
  - Guichet à toutes les entrées
  - Distribution de badges selon une procédure
  - Contrôle par tous du port des badges

EXEMPLE INFORMATIQUE

- Règle 2: Seule les personnes habilitées par un administrateur système ont accès au système informatique
- Moyens pour assurer la règle:
  - Système d ’authentification (Login +mot de passe) géré par l ’administrateur: (création et destruction des comptes)
  - Modification périodique des mots de passe par les utilisateurs
  - Protection informatique du contrôle d ’accès aux comptes
  - Audit des tentatives de fraude
  - ….
- Contre exemple à la règle du moindre privilège
  - Un administrateur système ne devrait pas avoir accès au sens des fichiers utilisateurs, c’est rarement le cas

EXEMPLES D ’ATTAQUES VISANT AU VOL D'INFORMATIONS CLASSÉES (1)

Type d'attaque	Description	Contre mesure
Récupération du contenu des poubelles		Destruction de tous les documents jetés
Subornation de personnel	1. Se faire embaucher comme employé d'entretien (travail hors heures ouvrables). 2. Photocopier ou photographier tous les documents accessibles ayant un niveau de classification secret.	1. Contrôler (?) les embauches et développer une prise de conscience des problèmes de sécurité. 2. Tous les documents classés doivent être systématiquement rangés dans des armoires ou des coffres. 3. Contrôler périodiquement l'application de cette procédure.

EXEMPLES D ’ATTAQUES VISANT AU VOL D'INFORMATIONS CLASSÉES (2)

Type d'attaque	Description	Contre mesure
Mascarade par accès à un compte privilégié (1)	1. Récupérer un mot de passe utilisé en accès distant par espionnage de ligne. 2. Entrer sur un compte invité en réseau 3. Copier le fichier des mots de passe chiffrés au login 4. Attaque par dictionnaire du fichier connaissant des login privilégiés 5. Se connecter sur le compte privilégié	1. Pas de connexion Internet dial up ou connexion via des lignes protégées 2. Utilisation d'un protocole d'authentification forte avec authentification par carte. 3. Limitation des services accessibles à distance par garde barrière 4. Stratégie de gestion des mots de passe

EXEMPLES D ’ATTAQUES VISANT AU VOL D'INFORMATIONS CLASSÉES (3)

Type d'attaque	Description	Contre mesure
Mascarade par accès à un compte privilégié (2)	1. Réaliser un logiciel pour PC qui est extérieurement un jeu sur PC avec accès Web et qui par ailleurs trappe et copie les identifiants et mots de passe. Variante, transformer un jeu existant en virus. 2. Offrir ce jeu à un collaborateur un Attendre que le logiciel précédent envoie le mot de passe. 3. Procéder comme précédemment en 2.	1. Recommander la plus grande vigilance aux collaborateurs quant à l'installation de logiciels sur leur PC. Ceci concerne également les Plug In et les Applets 2. Utiliser un Anti Virus systématiquement

EXEMPLES D ’ATTAQUES VISANT AU VOL D'INFORMATIONS CLASSÉES (4)

Type d'attaque	Description	Contre mesure
Mascarade par accès à un compte privilégié (3)	1. Se faire embaucher comme employé d'entretien (travail hors heures ouvrables). 2. Un soir se logger sur un terminal 3. Copie du fichier des mots de passe chiffré au login 4. Attaque par dictionnaire du fichier connaissant des login privilégiés 5. Connexion sur le compte privilégié	1. Contrôler (?) les embauches et développer une prise de conscience des problèmes de sécurité. 2. Authentification par carte ou disquette… 3. Mise en place d'une protection empêchant la copie du fichier des mots de passe au login 4. Stratégie de gestion des mots de passe

EXEMPLES D ’ATTAQUES VISANT AU VOL D'INFORMATIONS CLASSÉES (5)

Type d'attaque	Description	Contre mesure
Espionnage des écrans par rayonnement électromagnétique	1. Développer ou acheter discrètement une machine à capter et analyser le rayonnement magnétique des écrans. 2. L'installer à proximité de l'établissement (attention les antennes sont voyantes) 3. Installer en permanence du personnel pour scruter les écrans jusqu'à ce que quelqu'un se décide à éditer un document intéressant. 4. Ou développer un logiciel de reconnaissance des formes et d'analyse de texte.	1. Utiliser des écrans à faible rayonnement. 2. Interdire l'édition de documents secrets en dehors de salle protégée par une cage de Faraday.

Bibliographie

http://deptinfo.cnam.fr/Enseignement/DESS/surete/

- *Les protocoles de sécurité de l'Internet*, S. Natkin, Dunod 2002
- *La science du secret*, J. Stern, Odile Jacob Ed, Paris 1998
- *Risque et information*,Cahiers de la sécurité intérieure, IHESI, Paris 1998.
- *Secrets and Lies, Digital Security in a Networked World*, Bruce Schneier,John Wiley and sons ed, 2000
- *Guide de la Sûreté de fonctionnement*, J.C Laprie et als : Laboratoire d'Ingénierie de la Sûreté de Fonctionnement, CEPADUES Editions,1995
- *Sûreté de Fonctionnement des systèmes informatiques*, J.C. Geffroy et Gilles Motet, Intereditions, Dunod, Paris, 1998
- *Les robots*, I. Asimov, Ed J'ai lu, Paris 2001