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

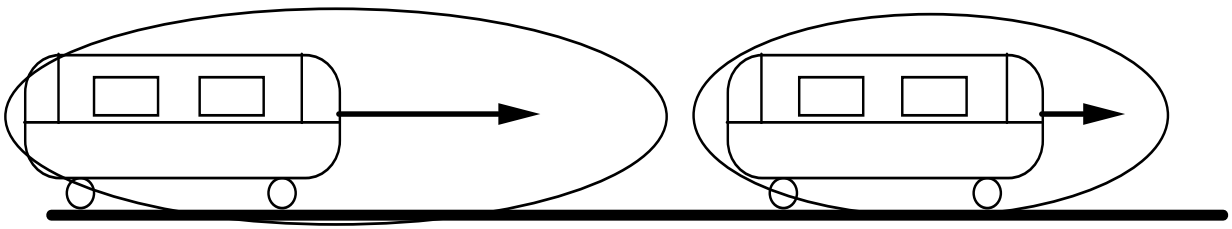
Conséquences aujourd’hui

- 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 ?

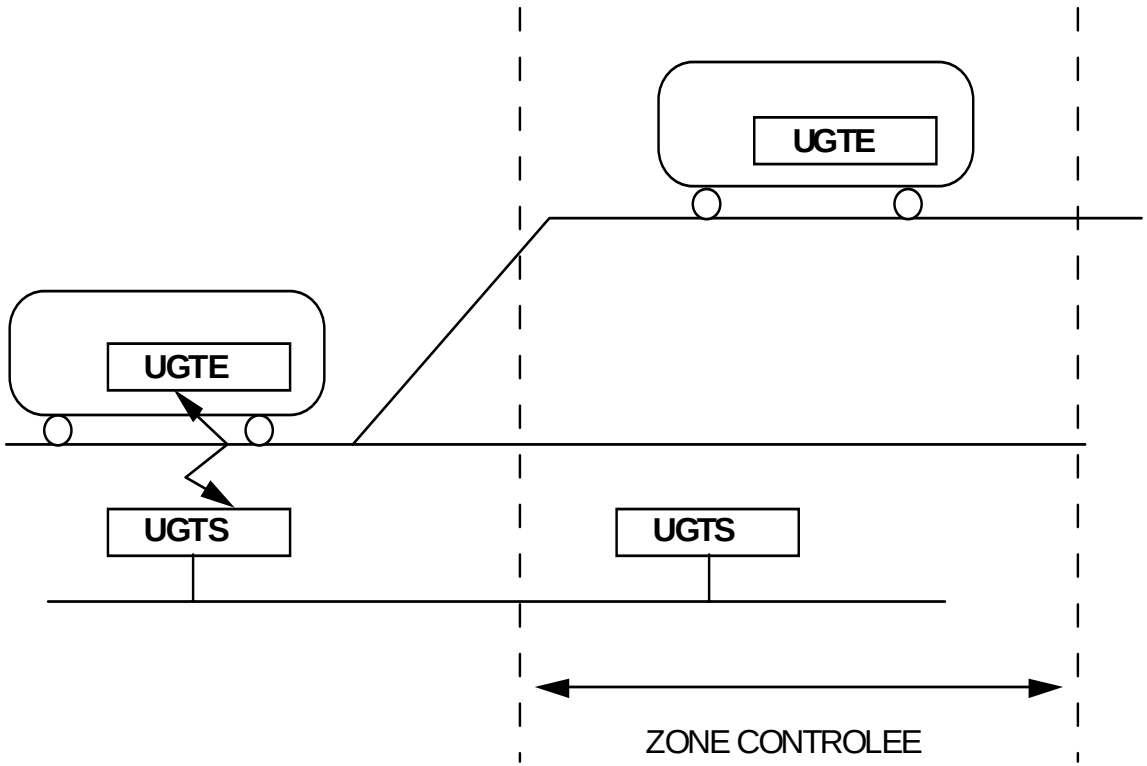
- Le développement d'applications qui reposent sur l'authentification numérique (comme la signature électronique) crée une dépendance dont les effets individuels ou collectifs peuvent être désastreux. Le jour ou les systèmes électroniques ne sauront plus reconnaître votre carte d'identité à puce, existerez 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

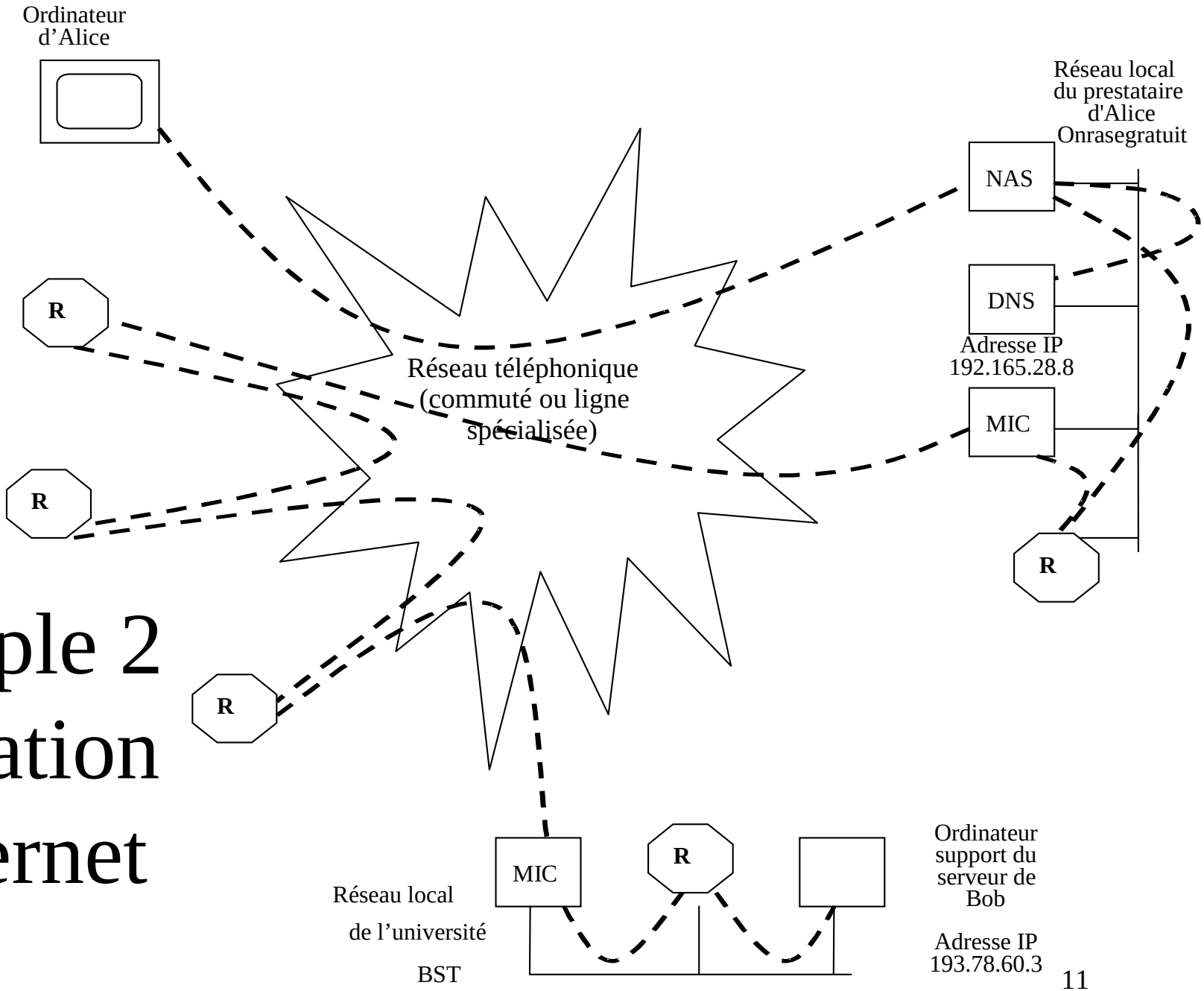


LE CANTON MOBILE DEFORMABLE

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

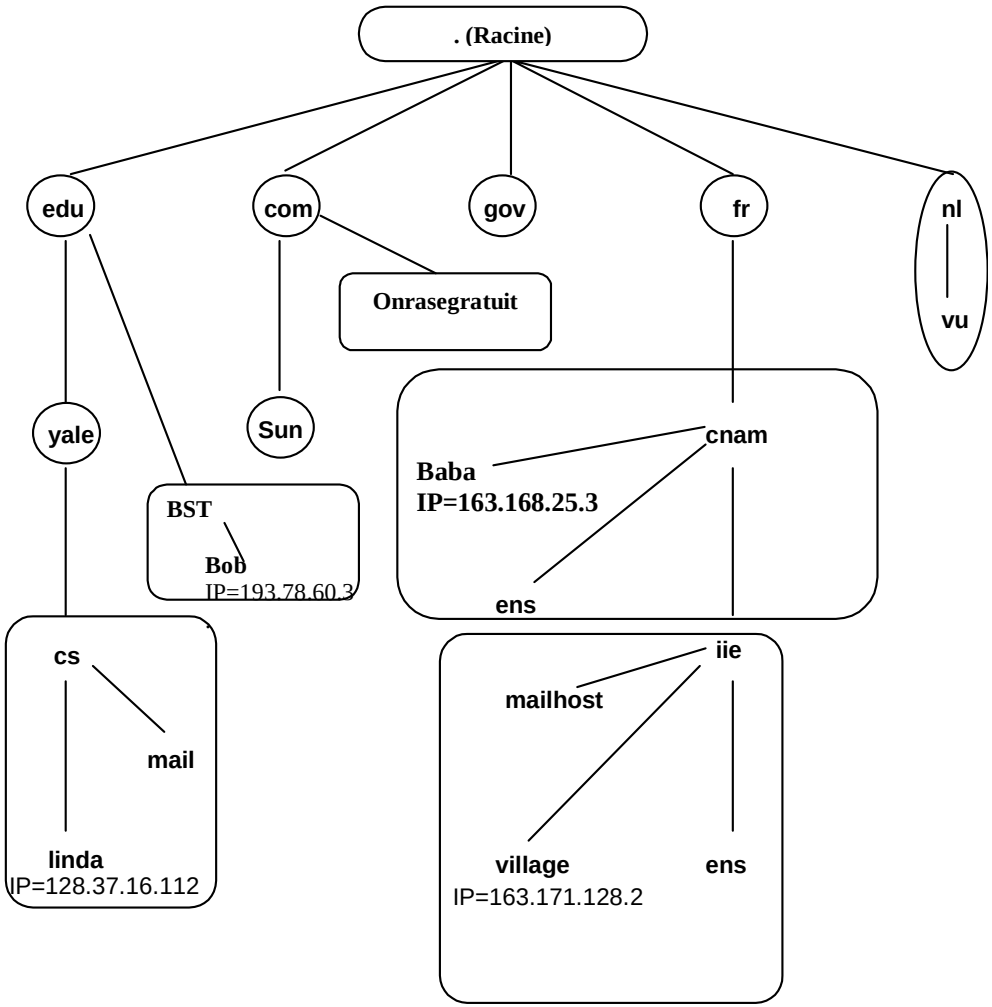
Pourquoi?

- Internet n'est pas contrôle par un prestataire central

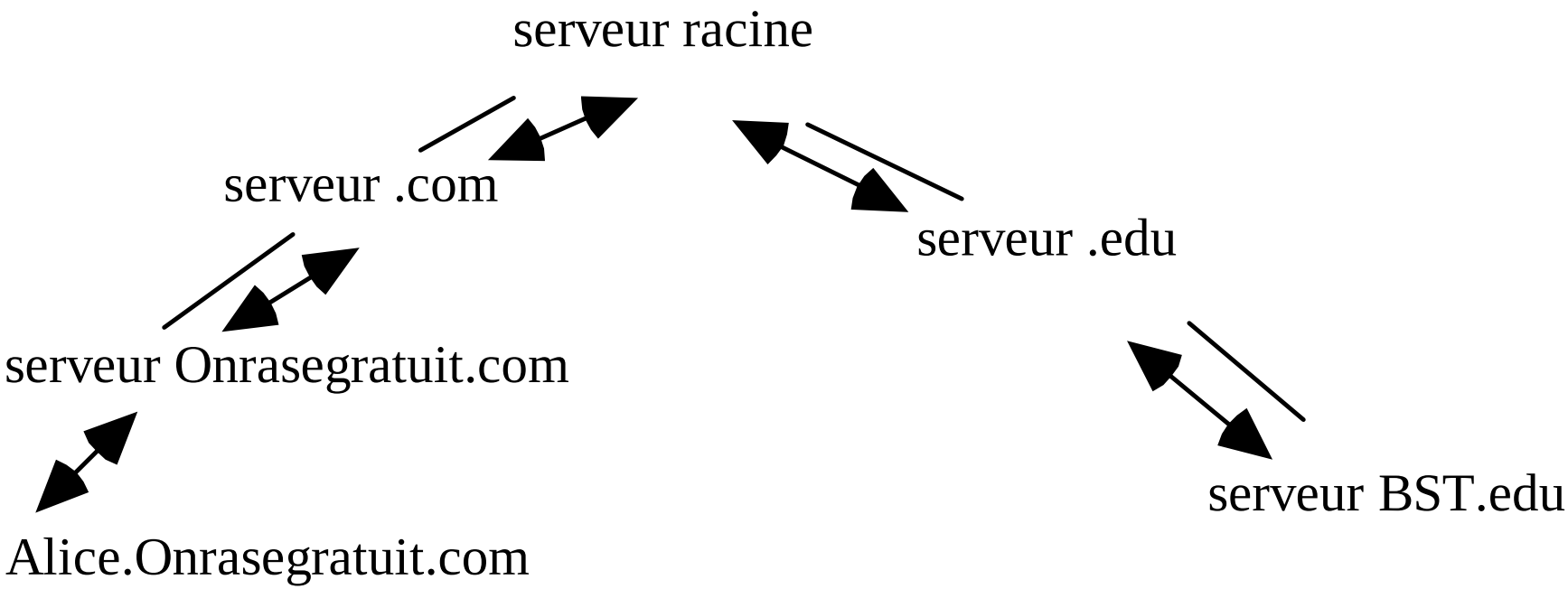
(Pas de contrôle formel des utilisateurs, ni de la nature du trafic)

- 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

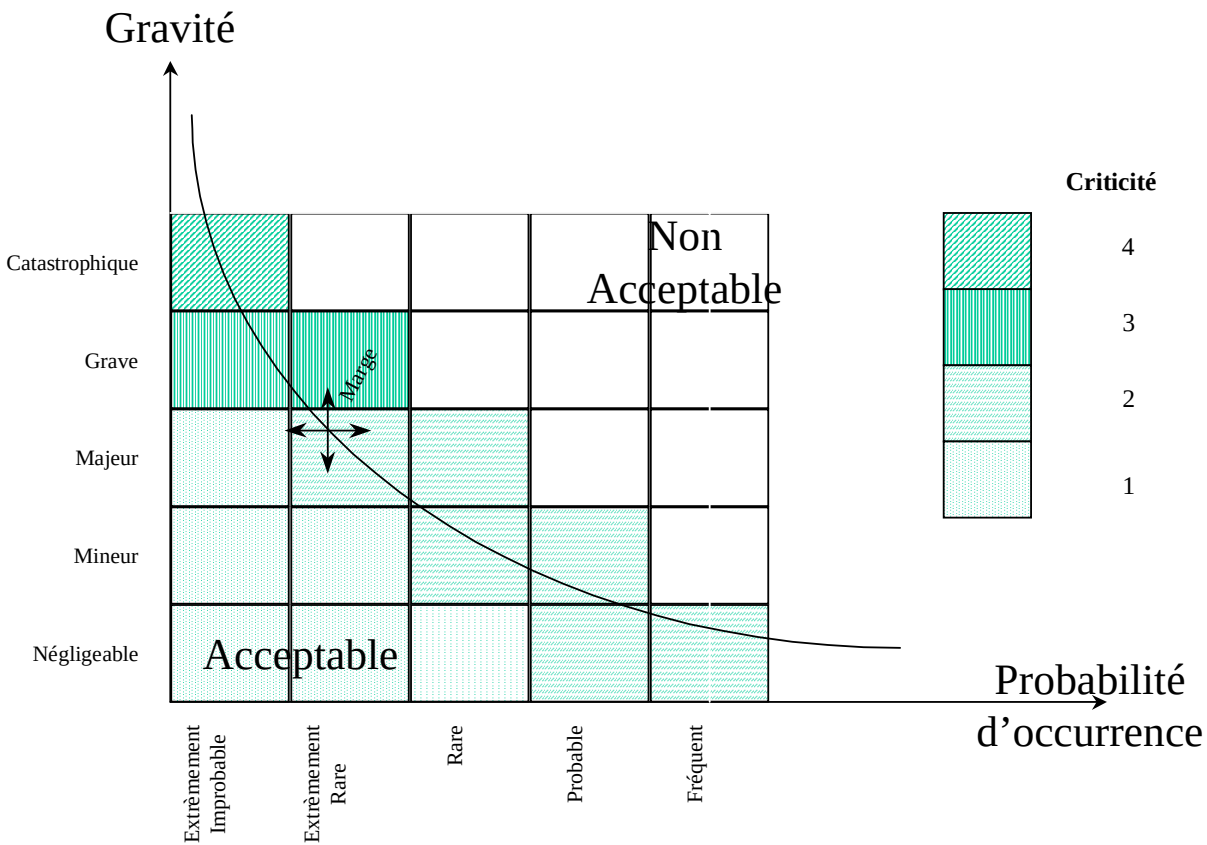
- Complexité de l'environnement (le monde qui interagit avec le système)
- Les utilisateurs
- Les pannes
- Les attaques
- Complexité des fonctions: les demandes des utilisateurs qui ne maîtrisent pas la viabilité et la fragilité intrinsèque de cette expression de besoins.

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:

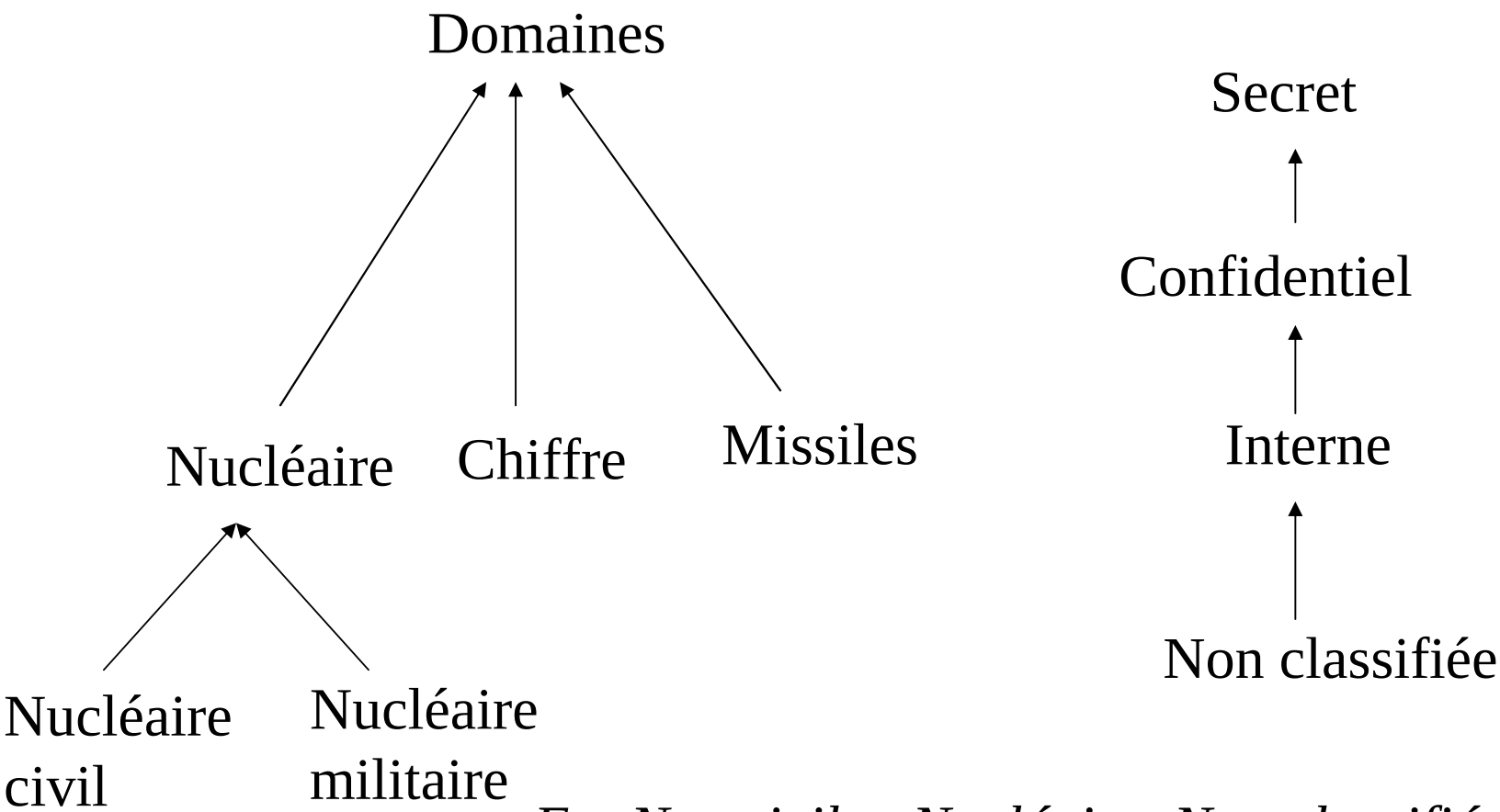
1) Un périmètre d’application
(qui est concerné ou et quand, avec quels moyens…)
qui détermine le système d'information sur lequel porte la politique.
2) Des règles définissant les actions autorisées (**les droits**)
ou interdites réalisées par des hommes sur des hommes ou
des biens matériels ou immatériels.
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 ⊂ 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

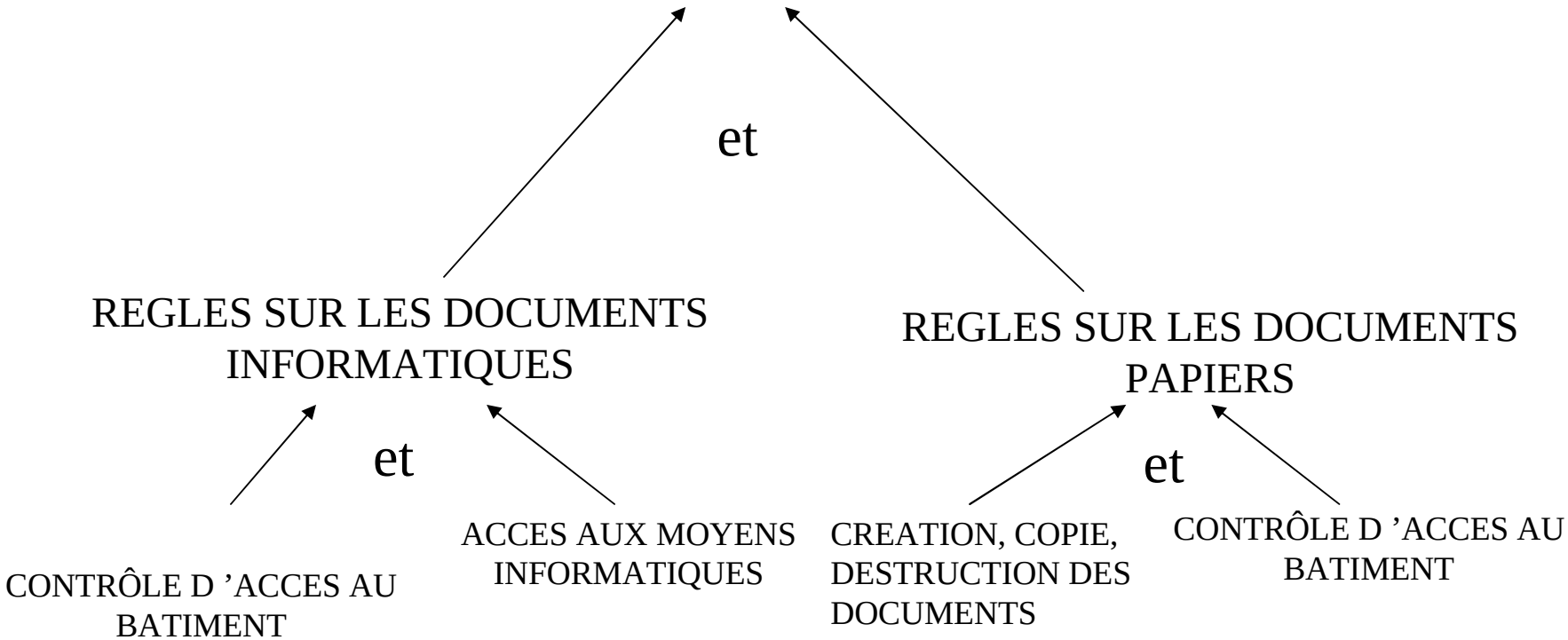
MOYENS

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.

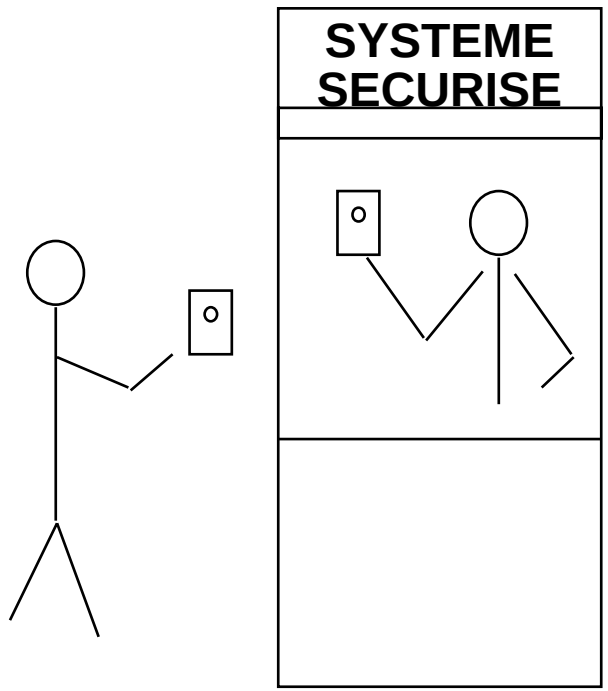
Elle s’authentifie,

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

LES TECHNIQUES DE CRYPTOGRAPHIE

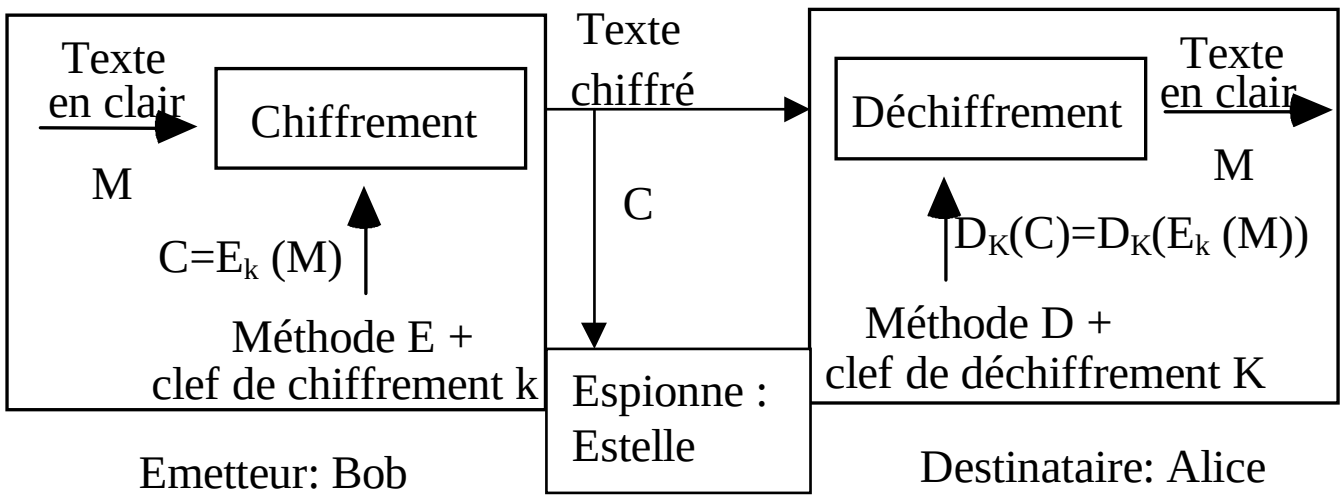
G. Florin

S. Natkin

Mars 2003

Généralités

Définition


Texte
en clair
M
Chiffrement
C=Ek (M)
Méthode E +
clef de chiffrement k
Emetteur: Bob
Texte
chiffré
C
Espionne :
Estelle
Déchiffrement
Texte
en clair
M
DK(C)=DK(Ek (M))
Méthode D +
clef de déchiffrement K
Destinataire: Alice

Chiffrement

Bob, doit transmettre à Alice, un message M $\in$ MESSAGES_A_ENVOYER.
M est dit “en clair“.

Estelle, une espionne, d’écouter la voie de communication pour connaître M.

Bob, construit un texte chiffré C$\in$ MESSAGES_CHIFFRES.

$$C = E_k(M). \quad \text{ou} \quad C = \{M\}_k^E$$

La fonction E_k dépend d’un paramètre k appelé clef de chiffrement.

Le **chiffrement** est donc une transformation d'un texte pour en cacher le sens

La possibilité de chiffrer repose donc sur la connaissance de l’algorithme de chiffrement E et de la clef k de chiffrement.

Déchiffrement

Le **déchiffrement** est l'opération inverse permettant de récupérer le texte en clair à partir du texte C chiffré.
Il repose sur la fonction D_K de MESSAGES_CHIFFRES dans MESSAGES_A_ENVOYER telle que

$$M= D_{K'}(C) \text{ ou } C = \{M\}_K^D$$

On doit avoir

$$D_K (E_k(M))=M$$

D_K est donc une fonction inverse à gauche de E_k.

Pour un couple cr = (E,D) donné de famille de fonction de chiffrement et de déchiffrement, l'ensemble des couples (k, K) vérifiant cette propriété est noté CLE(cr).

Crypto-systèmes

Pour que ces opérations assurent la confidentialité du transfert entre Alice et Bob, il est nécessaire qu'au moins une partie des informations E, D, k, K soit ignorée du reste du monde.

Décrypter ou casser un code c'est parvenir au texte en clair sans posséder au départ ces informations secrètes. C'est l'opération que doit réaliser Estelle pour retrouver M.

L'art de définir des codes est la cryptographie. Un spécialiste en cryptographie est appelé cryptographe.

L'art de casser des codes est appelé cryptanalyse ou cryptologie. Un spécialiste en cryptanalyse est appelé cryptanalyste.

Un crypto-système est l'ensemble des deux méthodes de chiffrement et de déchiffrement utilisable en sécurité.

Crypto-systèmes symétriques

Tels que soit k=K, soit la connaissance d'une des deux clefs permet d'en déduire facilement l'autre.

Conséquences :
Dichotomie du monde : les bons et les mauvais

Multiplication des clefs (un secret n'est partagé que par 2 interlocuteurs), donc pour N interlocuteurs N.(N-1)/2 couples

La qualité d'un crypto système symétrique s'analyse par rapport à des propriétés statistiques des textes chiffrés et la résistance aux classes d'attaques connues.

En pratique tant qu'un crypto système symétrique n'a pas été cassé, il est bon, après il est mauvais.

Crypto-systèmes asymétriques (a clefs publiques)

Tels que la connaissance de k (la clef de chiffrement) ne permet pas d'en déduire celle de K(la clef de déchiffrement).

Un tel crypto-système est dit asymétrique, la clef k est appelée la **clef publique**, la clef K est appelée la **clef privée**.

Fondement théorique : montrer que la recherche de K à partir de k revient à résoudre un problème mathématique notoirement très compliqué, c'est à dire demandant un grand nombre d'opérations et beaucoup de mémoire pour effectuer les calculs.

RSA (l'algorithme le plus utilisé à l'heure actuel) la déduction de K à partir de k revient à résoudre le problème de factorisation d'un grand nombre un problème sur lequel travaille les mathématiciens depuis plus de 2000 ans,

On estime que le plus rapide ordinateur que l'on puisse construire utilisant la meilleure méthode connue met plus de 1000 ans pour retrouver la clef privée d'un système RSA utilisant un modulo de 1024 bits (ordre de grandeur de la taille des clefs).

Asymétrie de l ’usage des clefs

BANQUE_MODERNE, désire autoriser ses clients à envoyer des ordres de virement chiffrés
Elle publie dans un annuaire infalsifiable

Nom = BANQUE_MODERNE, Algorithme de Chiffrement = E, Clef Publique = k

La banque conserve secrète la clef privée K.

Tout client peut calculer $C = E_k(M)$.

Seul la banque peut déchiffrer le message $M = D_K(C)$.

L ’algorithme d ’Estelle (Cryptanalyste)
Etape 1) Recherche des crypto -systèmes possibles

Hypothèses
Estelle veut décrypter C= E_k(M).
Estelle ne connaît ni D, ni E ni k, ni K.
Elle peut connaître des informations sur sa syntaxe et la sémantique de M.

Etape 1) Recherche des crypto systèmes possibles
CR={cr=(D,E)}

L ’algorithme d ’Estelle
Etape 2) Réduction de l ’espace des clefs

Pour tout cr déterminer le plus petit ensemble CLE_REDUIT⊂CLE(cr)
contenant la clef utilisée.
Si card (CLE_REDUIT={(k,K)})=1, M= $D_K(C)$. Fin

A priori, tous les couples (k,K) sont équiprobable sur CLE(cr)
Estelle doit acquérir une connaissance soit déterministe (clefs impossibles) ou probabiliste (clefs improbables)qui facilite ses essais (réduit l ’entropie)

Exemples
Estelle possède M’ et C’ chiffrée avec le même cryptosystème et les mêmes clefs déduction de propriétés des clefs: **attaque à texte en clair**.
Estelle peut chiffrer des messages M avec E_k (sans connaître k) **attaque à texte en clair chois**

Estelle connaît des propriétés de l ’algorithme de génération de (k,K).

L ’algorithme d ’Estelle
Etape 3) Analyse syntaxique

Déterminer le plus petit ensemble MESSAGES_SYNTAXIQUEMENT_CORRECTS ⊃ MESSAGES_A_ENVOYER qui vérifie des propriétés de syntaxe connues d’Estelle

Objectif : Construire un test d’arrêt simple pour le calcul mené à l’étape 4
Une règle syntaxique est sous une forme ou une autre un invariant d’un langage. Elle implique donc une certaine redondance de l’information.
Exemples
Le plus grand mot de la langue française a 25 lettres (anticonstitutionnellement). Possibilité d’écrire 10^{34} mots de 25 lettres ou moins 80000 mots dans le dictionnaire Hachette
"le" est nécessairement suivi d’un nom masculin

- Règles logique classique (toutes les suites de huit bits à partir du début du texte appartiennent à l’alphabet ASCII)
- Règles résultant de l’application d’un test statistique permettant d’accepter ou de rejeter une hypothèse (la répartition des caractères ASCII dans le texte en clair suit la même loi que la répartition des lettres dans la langue française). Fréquences d'apparition (en anglais)

Lettres	Digrammes	Trigrammes
E 13,05	TH 3,16	THE 4,72
T9,02	IN 1,54	ING 1,42

L ’algorithme d ’Estelle
Etape 3) Analyse syntaxique 2

Deux cas possibles

Etape 3.1 Construction de l’espace des messages

Informations très précise sur la syntaxe de M (M est un mot de passe sur 8 caractères qui est très probablement composé d’un mot ou de deux mots français concatènes).

Etape 3.2 Construction d’une règle syntaxique

$\exists$SYN tel que alors $\forall$ M

$\in$ MESSAGES_SYNTAXIQUEMENT_CORRECTS SYN(M)=vrai.

L ’algorithme d ’Estelle
Etape 4) Recherche Exhaustive

Construire MESSAGES_POSSIBLES$\subset$ MESSAGES_SYNTAXIQUEMENT_CORRECTS tel que mes $\in$ MESSAGES_POSSIBLES

Soit Etape 4.1 : Recherche sur l’espace des clefs de chiffrement
mes $\in$ MESSAGES_SYNTAXIQUEMENT_CORRECTS et $\exists$ (k, K) $\in$ CLE_REDUIT(cr) et E_k(mes)=C

Soit Etape 4.2 : Recherche sur l’espace des clefs de déchiffrement
$\exists$(k, K) $\in$ CLE_REDUIT(cr)et D_K(C)=mes et SYN(mes).

Si card(MESSAGES_POSSIBLES)=1, M=mes, Fin

Attaque à texte chiffré en parcourant itérativement soit l’espace des clefs de chiffrement soit celui des clefs de déchiffrement.

L ’algorithme d ’Estelle
Etape 5) Analyse sémantique

Trouver une règle sémantique SEM
(le message porte sur la cocaïne ou les fausses factures)
telle que :
card ({X MESSAGES_POSSIBLES tel que SEM(X)})=1
Si une telle règle existe M=X, Fin

Sinon Estelle a échouée

Point de vue du cryptographe
Etape 1

Opération autrefois difficile,
devenue simple: standard de cryptographie, systèmes commercialisés.
la sécurité d ’un crypto-système ne repose plus que sur le secret des clefs
(sauf dans le domaine militaire).

Point de vue du cryptographe
Etape 2

Choisir un crypto système cr dont l'espace des clefs est très grand.

Choix des clefs est le plus imprédictible possible
(éviter les mots d'un dictionnaire , nombres pseudo aléatoires à grain de génération difficile à devi

Limiter l 'usage des clefs

Choisir un bon crypto asymétrique tel que le calcul de K à partir de k,
ou même de la réduction des K possibles connaissant k est un problème reconnu scientifiquement
comme très difficile.
Si par un hasard extraordinaire, Estelle arrive à résoudre ce problème,
elle devient célèbre, riche et par conséquent heureuse en amour.
Elle n'a donc plus aucune raison d'embêter Bob et Alice.

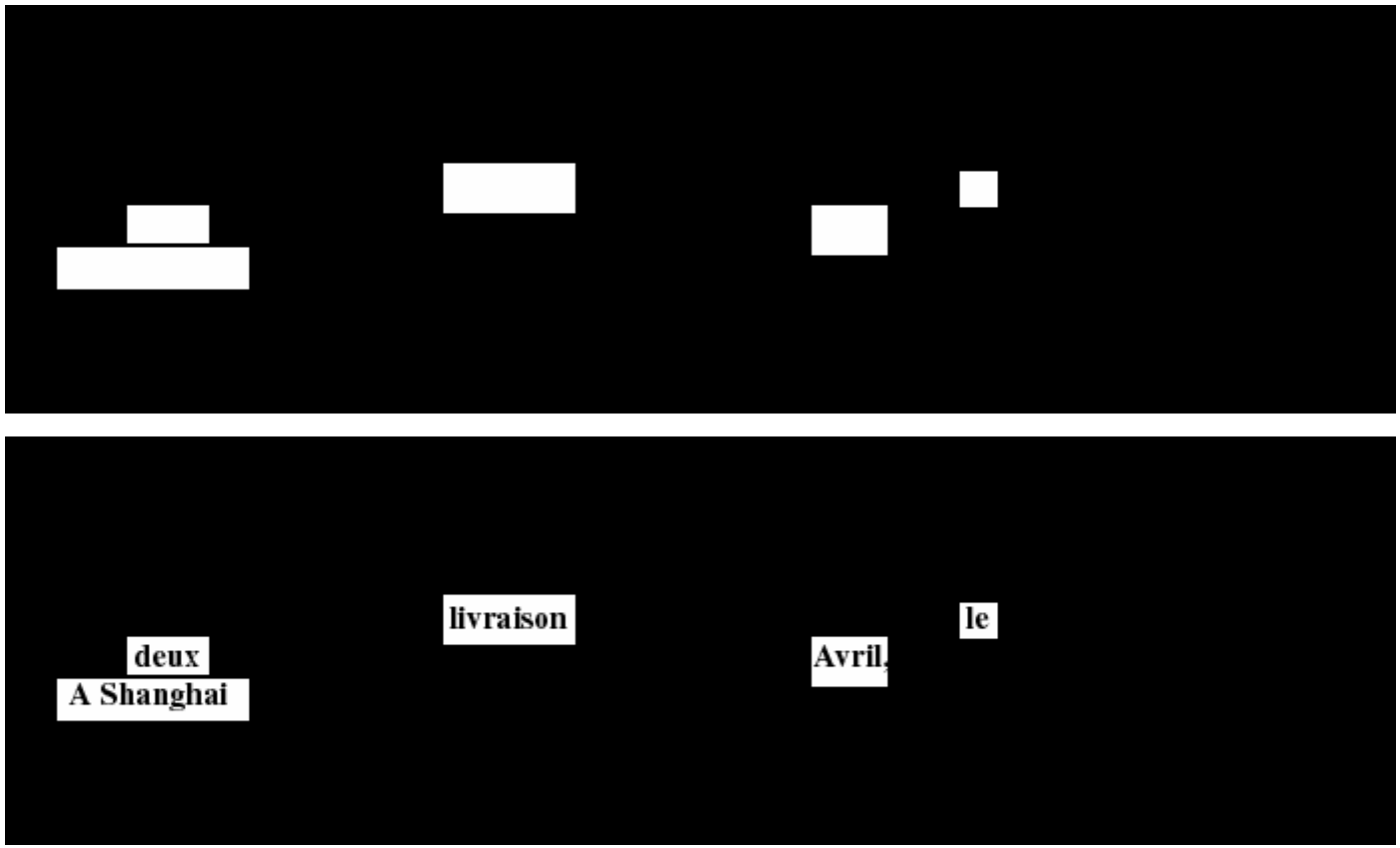
Point de vue du cryptographe
Etape 3

Deux stratégies :

Limiter la redondance (compression à un niveau syntaxique bas)

Augmenter la redondance en donnant plusieurs syntaxes possibles pour un même message (texte caché dans une image)

Masque classique



Cher ami
Je pense pouvoir assurer la livraison des 3O tonnes de blé prévue le 10 mars.
Mes deux assistants ne pourront venir vous voir avant Avril, mais je vous attends au Lotus Bleu
A Shanghai
Rastapopoulos

Point de vue du cryptographe
Etape 4
le masque jetable

Méthode imparable : le **chiffre parfait** ou masque jetable.

M sous forme d'une suite de n bits. Clef k_M de n bits, parfaitement aléatoire (suite uniforme de bits) utilisée qu'une seule fois (l'étape de réduction de l'espace des clefs n'a apportée aucune information)
$\Rightarrow$ Essai de toutes les clefs de CLE(cr) qui est l'ensemble des suites de n bits.

Chiffrement: $C=E_{k_M}(M)=M \oplus k_M$
Ou $\oplus$ représente le ou exclusif

Déchiffrement: $M=D_{k_M}(C)=C \oplus k_M$

très rapide et sans faille.

Point de vue du cryptographe
Etape 4
le masque jetable 2

$\forall$Mess $\in$ MESSAGES_SYNTAXIQUEMENT_CORRECTS $\exists$X $\in$ CLE(cr) tel que

$$C=E_X(Mess)$$

$X=C \oplus Mess \Rightarrow$

$$C= X \oplus Mess = C \oplus Mess \oplus Mess = C$$

En balayant tout l'espace des clefs on trouvera tous les messages de MESSAGES_SYNTAXIQUEMENT_CORRECTS.
Le fait d'avoir espionné pour connaître C n' a apporté aucune information.

Point de vue du cryptographe
Etape 4
le masque jetable 3

Notons :
A l'événement : C a été reçu par Estelle
B l' événement : M a été émis par Bob

Information apportée par la réception de :

$$I=-\log_2(\text{Probabilité(B sachant A)}/\text{Probabilité(B)})$$

Or comme toutes les clefs sont équiprobables, C a pu être construit avec à partir de n'importe quel message possible M'.Donc A et B sont indépendants.

$$\text{Probabilité(B sachant A)}=\text{Probabilité(A).Probabilité(B)}/\text{Probabilité(A)}=\text{Probabilité(B)}$$

$$I=-\log_2(\text{Probabilité(B)}/\text{Probabilité(B)})=-\log_2(1)=0$$

Crypto-systèmes symétriques

Chiffrement par substitution

Principe général

A chaque lettre ou groupe de lettres on substitue une autre lettre ou un autre groupe de lettres.

substitution mono alphabétique

Pour chaque lettre de l'alphabet de base on se donne une autre lettre utilisée dans le texte chiffré.

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
Q	W	E	R	T	U	Y	I	O	P	A	S	F	G	H	J	K	V	M	D	N	C	Z	B	L	X

Exemple historique: Le chiffre de César On décale les lettres de 3 positions

A B C D E F G H I J K L M N O P Q R S T U V W X Y Z
D E F G H I J K L M N O P Q R S T U V W X Y Z A B C

Forme générale des chiffre par décalage sur l'alphabet à 26 letres :

$$E_k(x)=x+k \bmod 26$$

$$D_k(y)=y-k \bmod 26$$

Chiffre de Vigenère

	0	1	2	3
	c	l	e	f
CL	2	11	4	5

$$E_{CL}(x_n)=(x_n+CL\ (n \bmod 4)) \bmod 26$$

t	e	x	t	e	s	e	c	r	e	t
19	4	23	19	4	18	4	2	17	4	19
2	11	4	5	2	11	4	5	2	11	4
21	15	1	24	6	3	8	7	19	15	23
v	p	b	y	g	d	i	h	t	p	x

Autres chiffres par substitution

Les substitutions homophoniques

Au lieu d'associer un seul caractère crypté à un caractère en clair on dispose d'un ensemble de possibilités de substitution de caractères dans laquelle on choisit aléatoirement.

Les substitutions de polygrammes

Au lieu de substituer des caractères on substitue par exemple des digrammes (groupes de deux caractères)

- Au moyen d'une table (système de Playfair)
- Au moyen d'une transformation mathématique (système de Hill).

Le masque pseudo aléatoire

Principe du masque jetable mais en utilisant un masque pseudo aléatoire. Le grain est la clef

Les chiffres par transposition

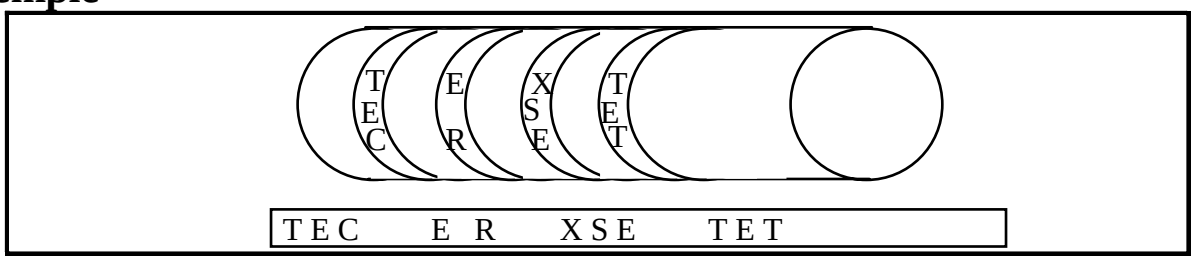
Principe général

On procède à un réarrangement de l'ensemble des caractères (une transposition) qui cache le sens initial.

La technique est très peu résistante aux attaques statistiques.

Le plus souvent on utilise deux visions géométriquement différentes du texte.

Exemple



- On enroule une fine langue de papyrus ou de peau sur un tambour d'un diamètre donné (technique assyrienne 400 av JC).

- On écrit horizontalement un texte sur la lamelle enroulée.

- Quand la lamelle est déroulée les lettres sont incompréhensibles.

- Pour décrypter le message il faut un cylindre du bon diamètre.

Transposition matricielle

- Le message en clair est écrit dans une matrice.

- La clé une permutation de [1..n] ou n est le nombre de colonne

- La technique de transposition consiste à lire la matrice en colonne selon un ordre donné par la clef.

Exemple

1	6	4	3	2	5
M	E	S	S	A	G
E	S	E	C	R	E
T	A	C	H	I	F
F	R	E	R	P	A
R	T	R	A	N	S
P	O	S	I	T	I
O	N				

Le message crypté est donc:
METFRPO ARIPNT SCHRAI SECERS GEFASI ESARTON

Chiffre symétrique moderne

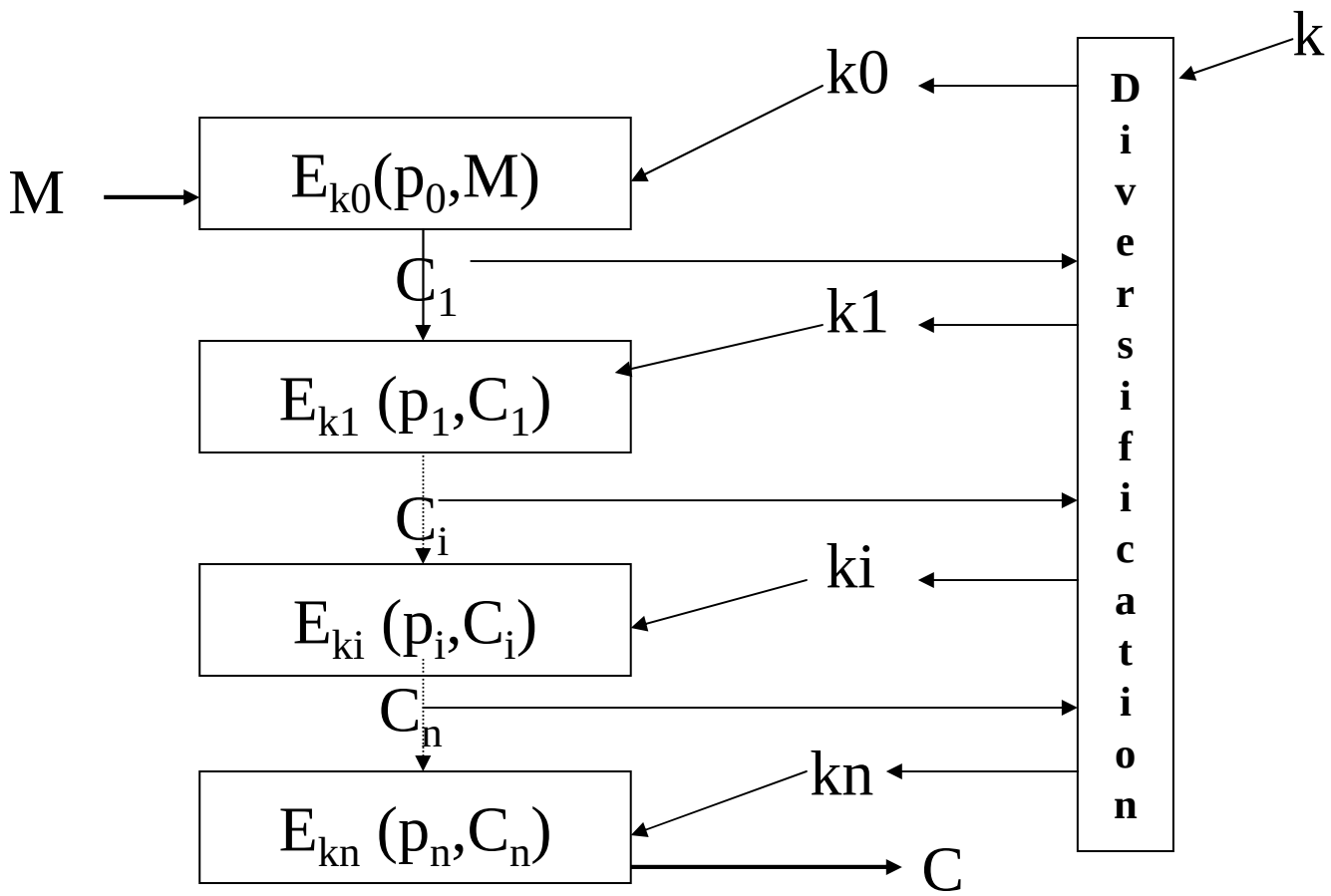
Prrincipes de confusion et de diffusion

Combinaison complexe d ’opérations de transposition et de substitution portant sur des chaînes de bits longues

Opérateurs booléens ou arithmétiques selon l ’implantation visée

Suite itérative d ’une fonction dépendant du calcul à l ’étage précédent, d ’une clef dérivée calculée en fonction de l ’itération et de la clef initiale (principe des système cryptographiques produits de Shannon et du chiffrement en chaîne)

Systèmes cryptographiques produits et chiffrement en chaîne



Réseaux de Feistel

Soit F(i ,B) une fonction de chiffrement qui utilise les mêmes clefs et paramètres que E mais porte sur des blocs B de longueur égale à la moitié de M.

E est donné par :

- On permute les deux blocs ce qui donne (R,L),
- C=E(M)=(LC, RC)

avec LC=R et RC=L⊕ F_{ki}(i,R).

E est son propre inverse.

- la première permutation donne (RC,LC)=(RC,R),
- l'ajout de la fonction donne (RC⊕ F_{ki}(i,R),R)= (L⊕F_{ki}(i,R) ⊕ F_{ki}(i,R),R)=(L,R)

Modes de chiffrement

$M=O_0,O_1,..., O_n,O_{n+1},..., O_{2n},\ldots$

Par blocs (ECB: Electronic CodeBook)
$C=E(O_0,O_1,..., O_n),E(O_{n+1},..., O_{2n})\ldots$

En chaîne (CBC: Cipher Block Chaining)
$C=E(S_0=(I_0,I_1,..., I_n)\oplus(O_0,O_1,..., O_n))$,
$E(S_1 = S_0 \oplus (O_{n+1},..., O_{2n})),\ldots$
Fournit un meilleur brouillage et un contrôle d ’intégrité

Cryptanalyse différentielle

Nouvelles techniques d ’attaque à texte chiffré choisi:

$$A \longrightarrow A \oplus K \longrightarrow E(A \oplus K)$$

$$B \longrightarrow B \oplus K \longrightarrow E(B \oplus K)$$

$$A \oplus B \longrightarrow A \oplus B \oplus K \longrightarrow E(A \oplus B \oplus K)$$

Analyse pour tout A des sorties

$\Delta(A)=\{E(B \oplus K) \oplus E(A \oplus B \oplus K)\}$

Le DES: historique

-Dès le début des années 1960 la technologie des circuits intégrés permet de travailler à des circuits combinatoires complexes permettant d'automatiser:

la méthode de substitution.

la méthode de transposition.

=> Idée d'appliquer ces techniques en cascade dans un produit de chiffres.

- Mise au point à partir de 1968 d'une méthode de chiffrement basée sur 16 étages de substitutions et transpositions basés sur des clés (IBM)

- Appel d'offre NBS (1973) pour la mise au point d'un système de cryptographie

- Proposition IBM (1975)

- Adoption définitive et normalisation du DES d'IBM (1978) par le NBS ("National Bureau of Standards").

-Normalisation ANSI X3.92 connue sous le nom de DEA ("Data Encryption Algorithm").

Le DES: Principes (1)

Choix possibles pour la sécurité

- Méthodes simples de chiffrement et des clés très longues .

Le DES

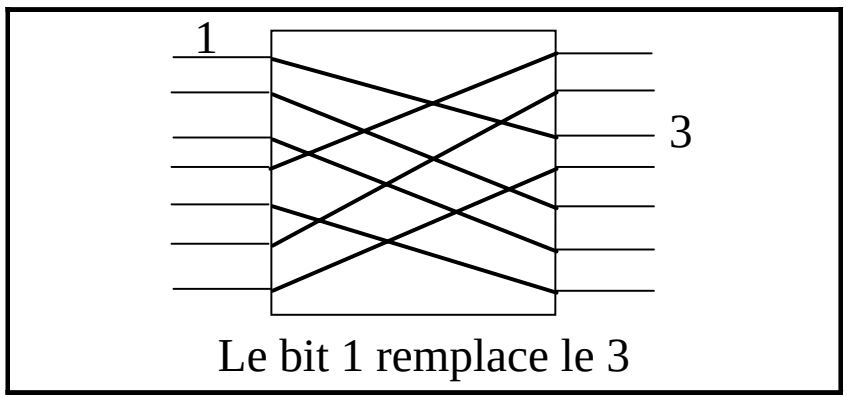
- Produit de transpositions et substitutions nombreuses et compliquées pour une clé relativement courte
  => facilité de transport.

- Les chiffres à substitution et à transposition sont faciles à réaliser en matériel.

Les boîtes de transposition "P-Box"
Les boites de substitution "S-Box"

Le DES: P-box

Exemple pour 8 bits (solution matérielle)



Facile à réaliser par simple câblage

Autre solution (logicielle) par des tables

Exemple de transposition sur 64 bits : permutation initiale du DES

58 50 42 34 26 18 10 2 60 52 44 36 28 20 12 4
62 54 46 38 30 22 14 6 64 56 48 40 32 24 16 8
57 49 41 33 25 17 9 1 59 51 43 35 27 19 11 3
61 53 45 37 29 21 13 5 63 55 47 39 31 23 15 7

Le bit 1 remplace le 58

Le DES: S_Box

Fonction d'expansion E

32	1	2	3	4	5	4	5	6	7	8	9	8	9	10	11	12	13	12	13	14	15	16	17
16	17	18	19	20	21	20	21	22	23	24	25	24	25	26	27	28	29	28	29	30	31	32	1

S-Box

2	12	4	1	7	10	11	6	8	5	3	15	13	0	14	9
14	11	2	12	4	7	13	1	5	0	15	10	3	9	8	6
4	2	1	11	10	13	7	8	15	9	12	5	6	3	0	14
11	8	12	7	1	14	2	13	6	15	0	9	10	4	5	3

Le codage de 100101, conduit à choisir l'élément (2,5) de valeur 13, soit en binaire 1101.

Le DES architecture générale (1)

Deux modes

- Mode cryptage par bloc de 64 bits
- Mode cryptage à la volée ("stream")
(octets par octets avec des registres à décalage)

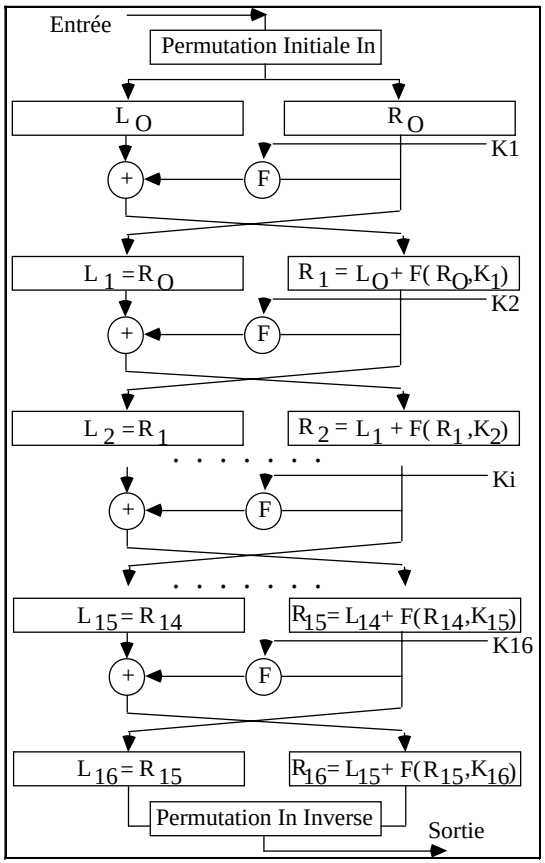
Utilisation d'une clé sur 56 bits

En fait 8 fois 7 bits avec une parité
(initialement 128 bits)

19 étages de logique combinatoire

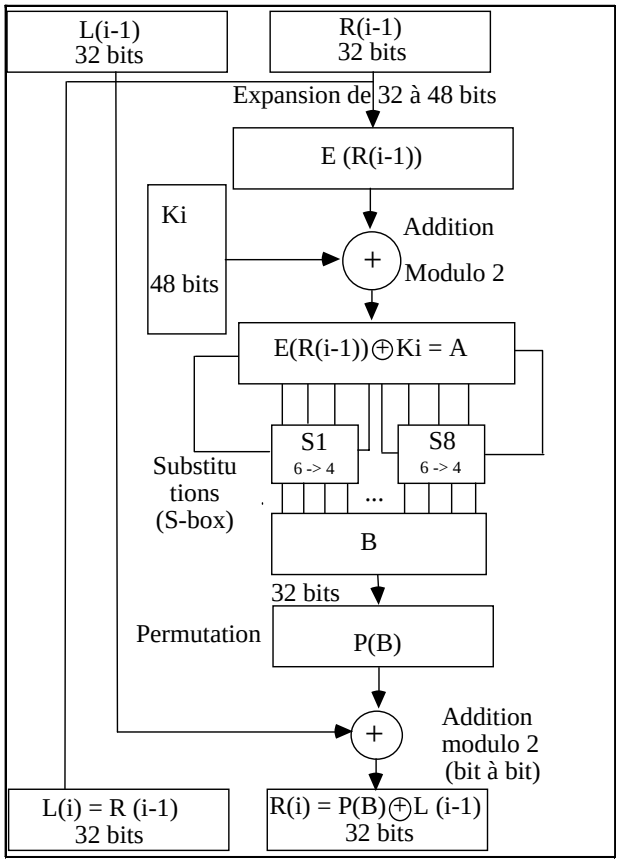
Appliquent des transpositions substitutions sur des blocs de 2 x 32 bits
- 1 étage amont, 2 en aval sont des transpositions simples fixes
- 16 étages intermédiaires dépendent de la clé de façon complexe.

Le DES architecture générale (2)

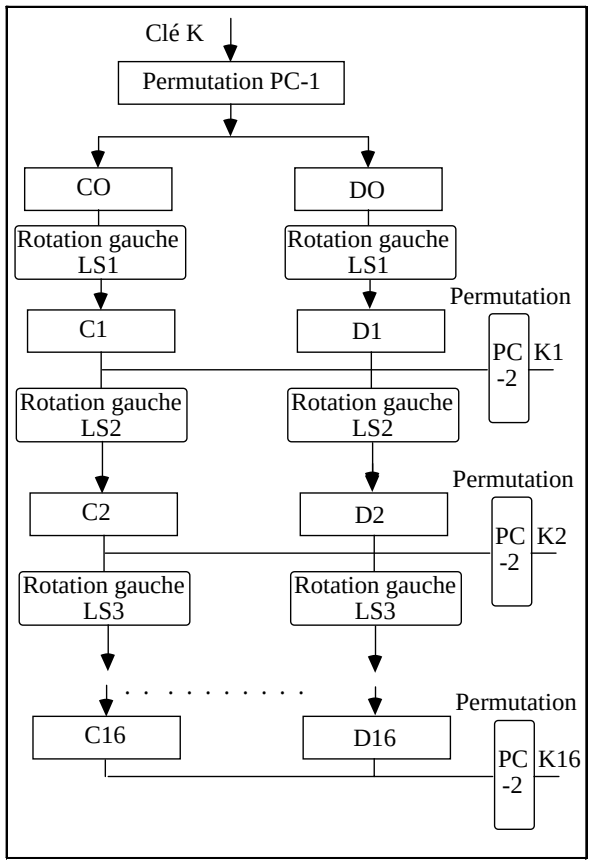


Réseau de Feistel: Chaque ronde est son propre inverse

Le DES architecture générale (3)



DES: Diversification des clefs



DES: Controverse

- Performances Excellentes - cryptage à la volée à débits potentiellement très élevés (dizaine/ centaine de Mégabits/seconde).

- Utilisation multiples : Transmission de données informatiques, Cryptage de chaînes de télévision à péage.

Controverse sur la sécurité du DES
Problème de longueur des clés

Des puces spéciales permettant l'essai de 10^6 clés par seconde ont été construites Elles peuvent être organisées en processeurs spéciaux massivement Le DES 56 est attaquable par des moyens informatiques plus ou moins lourds à la portée des états.

Problème du choix des substitutions

Les principes de choix des S-box n'ont complètement été rendus publique:

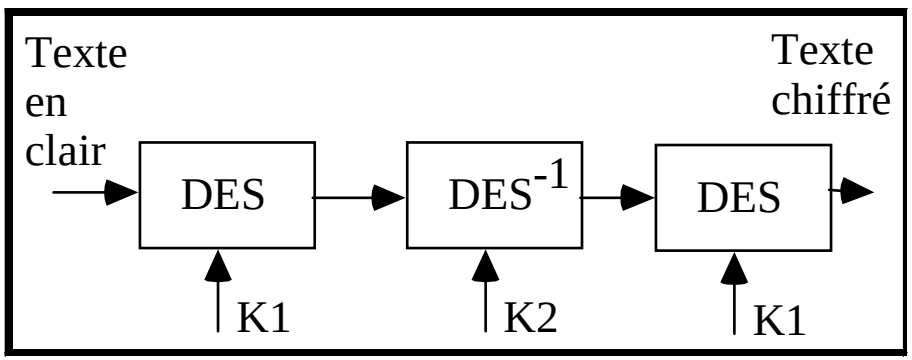
- Aucune S-Box n'est une fonction linéaire ou affine des entrées.
- Une différence d'un bit sur deux entrées d'une S-Box produit au moins deux bits différents sur les sorties
- Si un bit d'une entrée est donné et que l'on fait varier les autres bits, pour un bit de sortie donné, le nombre de cas ou il prend la valeur 0 est voisin du nombre de cas ou il prend la valeur1.

Elles sont conçues pour résister à la cryptanalyse différentielle.
Personne n'a jamais rien trouvé concernant d'éventuelles propriétés cachées des boites de substitution.

Triple DES

Utilisation de DES en cascade

Avec deux clés K1, K2 (128 bits).



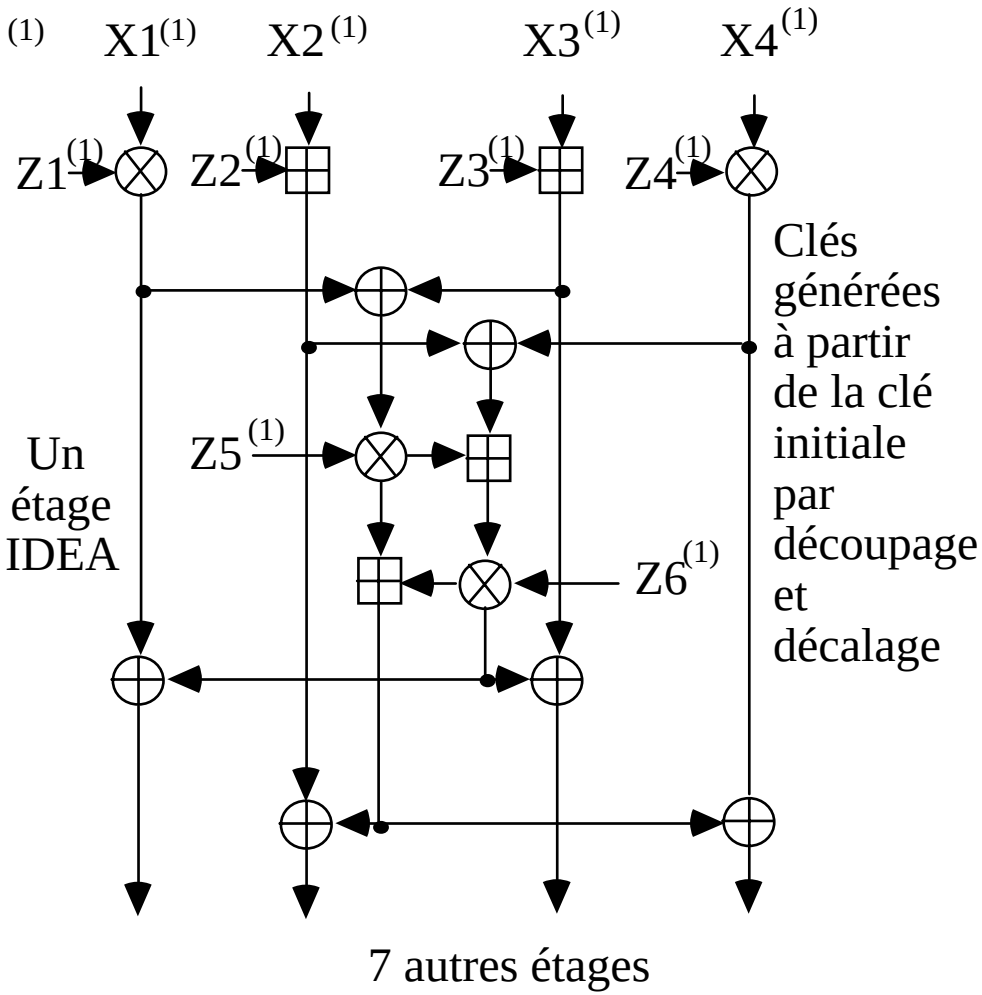
IDEA: Principes (1)

Autre solution de chiffrement par blocs de 64 bits basé sur huit étages facilement réalisable en matériel ou en logiciel.

Les opérations utilisées sont des opérations arithmétiques:

- ou exclusif $\oplus$
- addition modulo 2^{16} $\boxplus$
- multiplication modulo $2^{16}+1$ $\otimes$

IDEA: Schéma


(1)
X1(1)
X2(1)
X3(1)
X4(1)
Z1(1)
Z2(1)
Z3(1)
Z4(1)
Clés générées à partir de la clé initiale par découpage et décalage
Un étage IDEA
Z5(1)
Z6(1)
7 autres étages

IDEA:Conclusions

- IDEA est considéré par les spécialistes comme l'un des meilleurs cryptosystème à clé privée.

- La longueur de clé est élevée (128 bits).

- La vitesse de chiffrement et de déchiffrement peut-être élevée au moyen de circuits spéciaux.
  Circuits à 55 Mb/s et 177 Mb/s
  En logiciel sur 386 33Mhz: 880 Kb/s

- Les attaques semblent difficile mais le système est assez récent

Les chiffres asymétriques

RSA: Chiffrement et déchiffrement

Chiffrement (publique)

- La clé publique est un couple d'entiers:

$$\mathbf{K = (e, n)}$$

- Le chiffrement se fait au moyen de l'élévation à la puissance e modulo n:

$$\mathbf{E_K\ (M) = M^e\ mod\ n}$$

Déchiffrement (secrète)

- La clé secrète est un couple d'entiers:

$$\mathbf{k = (d, n)}$$

- Le déchiffrement se fait au moyen de l'élévation à la puissance d modulo n:

$$\mathbf{D_k\ (M) = M^d\ mod\ n}$$

RSA :Détermination des clefs

1. **Détermination de n**
   Trouver **deux entiers premiers** p et q très grands: **Calculer n = p q**
   p et q doivent rester secrets:La sécurité du système repose sur la difficulté de factoriser
   un grand entier n en deux entiers premiers p et q.
   n doit avoir un longueur supérieure à 512 bits. p et q doivent vérifier diverses autres conditions.

2. **Détermination de e**
   Calculer **z = (p-1) (q-1)**
   Choisir un entier **e premier avec z.**
   La clé publique est (e , n)

3. **Détermination de d**
   Choisir un entier d tel que : **e d =1 mod z** (d inverse de e dans l'arithmétique mod z)
   La clé privée est (d , n)

RSA: Inversibilité

Fonction d'Euler

Pour n entier $z = \phi(n)$ est le nombre d'entiers premiers avec n.

- si n est premier $\phi(n) = n-1$
- si n = p.q avec p et q premiers

$$\phi(n) = (p-1)(q-1)$$

Théorème d'Euler

Si a et n sont premiers entre eux

$$a^{\phi(n)} \bmod n = 1$$

Pourquoi RSA marche

$$D_K(E_k(M)) = ((M)^e \bmod n)^d \bmod n$$
$$= (M^e)^d \bmod n = M^{e.d} \bmod n$$

Mais on a choisi $e.d = 1 \bmod z$

Donc il existe un entier j tel que $e.d = j\,z + 1$

$M^{e.d} = M^{j.z}\, M \bmod n = M \bmod n$

En effet d'après le théorème d'Euler:

$M^{j.z} \bmod n = (M^z)^j \bmod n = (1)^j = 1$

Exemple (B. Schneier)

1) Soit deux entiers premiers p =47,q =71

$n = p.q = 3337$

2) $z= (p-1)(q-1)= 46 . 70 = 3220$

Choisissons e = 79 (premier avec n)

3) Calcul de l'inverse de e modulo z

Une solution possible: le théorème d'Euler

$e^{\phi(n)} = e\, e^{\phi(n)-1} \bmod z = 1 \bmod z$

Donc $d = e^{-1} = e^{\phi(n)-1} \bmod z$

Numériquement $79^{78} \pmod{3220} = 1019$

4) Pour chiffrer M = 6882326879666683

Décomposons M en blocs dont la valeur est inférieure à n= 3337

=> Des blocs de 3 chiffres

M= 688 232 687 966 668 3

Chiffrer 688: $688^{79} \bmod 3337 = 1570$

E(M) = 1570 2756 2091 2276 2423 158

Déchiffrer 1570:$1570^{1019} \bmod 3337 = 688$

RSA: Calcul des nombres premiers: Algorithmes probabilistes de Miller Rabin

Tirer aléatoirement un nombre p impair; Soit m impair tel que $p=2^k m+1$,
Soit a un nombre aléatoire tel que $1 \leq a \leq p-1$; $b:=a^m \bmod m$;
Si $b \equiv 1 \bmod p$ alors test:=faux fsi
Sinon
    i:=1;test:=vrai;
    tant que $i \leq k-1$ et test:=faux
        Si $b \equiv -1 \bmod p$ alors test:=faux fsi
        Sinon
        $b:=b^2 \bmod p$
        fsi
    ftq
si test=vrai réponds p est premier sinon réponds p est décomposable fsi

Prob (p décomposable et réponds premier) $\leq 1/4$

RSA calcul des puissances modulo n

Calcul de $z = M^e \bmod n$

On note e(i) le ième bit dans la décomposition binaire de e

$$e = \sum_{i=0}^{t-1} e(i).2^i$$

z:=1;
Pour i=t-1 à 0 faire
    z:=z^2 mod n;
    si e(i)=1 alors z:=z.M mod n fsi
fpour

Exemple

calcul de 1570^{1019} mod 3220

La représentation binaire de 1019 est 1111111011 d'ou t=10

i	e(i)	z	z^2 mod n	$z^2.M^{e(i)}$ mod n
9	1	1	1	1570
8	1	1570	2194	796
7	1	796	2923	735
6	1	735	2968	1308
5	1	1308	2320	1733
4	1	1733	3326	2752
3	1	2752	1851	2880
2	0	2880	1955	1955
1	1	1955	1160	2535
0	1	2535	2500	688

RSA: performances

L ’algorithme précédent est en O(3t) multiplications.
Multiplications sur 512 Bits= 64 multiplication en moyenne sur 32 bits. 192 multiplication p
l ’élévation à la puissance.

Utiliser des longueurs de clés de plus en plus importantes
Valeurs utilisées 512 bits, 640 bits, 1024 bits (considéré comme assez sûr pour plusieurs
2048 bits
Utiliser des circuits intégrés de cryptage de plus en plus performants
Actuellement une dizaine de circuits disponibles.
Vitesse de cryptage de base pour 512 bits:
de 10 à 100 Kb/s
Évolution en cours de l'ordre de 1 Mb/s

Remarque: Compte tenu de la complexité des traitements le DES est environ toujours 10
à 1000 fois plus rapide que le RSA.

RSA: faiblesses d ’implantation

- Ne jamais utiliser une valeur de n trop petite,
- Ne pas utiliser une clef secrète trop courte
- N'utiliser que des clefs fortes, c'est à dire telles que p-1 et q-1 ont un grand facteur premier
- Ne pas chiffrer des blocs trop courts (les compléter toujours a n-1 bits), de façon à détruire toute structure syntaxique
- Ne pas utiliser un n commun à plusieurs clefs, si ces clefs peuvent être utilisées pour chiffrer un même message.
- Si une clef secrète (d,n) est compromise, ne plus utiliser les autres clefs utilisant n comme modulo
- Ne jamais chiffrer ou authentifier un message provenant d'un tiers sans le modifier (ajouter quelques octets aléatoires par exemple)

La nécessité des clefs fortes est un point discuté.

RSA: Cryptanalyse

On montre que le calcul d ’une des clefs à partir de l ’autre est équivalent au problème de la factorisation de n

On n ’a pas encore montré que la cryptanalyse du RSA est équivalente au problème de la factorisation

Complexité temporelle du meilleur algorithme séquentiel de factorisation (crypte algébrique)

$$O(e^{1,92+o(1)(\log(n)^{1/3}(\log\log(n))^{2/3}})$$

Actuellement un calcul en parallèle utilisant quelques milliers d'ordinateurs pendant quelques mois permet de factoriser des nombres d'une centaine de chiffres (400 bits)

Utiliser des n=1024 ou 2048 bits selon protection cherchée est de moins ou plus de cinq ans.

Prévoir un moyen pour augmenter cette valeur par sur chiffrement ou déchiffrement suivi d'un rechiffrement.

RSA cartes bancaires

Limitation des calculs du fait de la puissance de calcul disponible.

n sur 320 bits (de l'ordre de 95 chiffres)

clé publique 3 pour tout le monde

RSA: Conclusions

Solution assez générale.

Utiliser le RSA brièvement au début d'un échange pour échanger des clés symétriques de session d'un algorithme efficace

Efficacité en sécurité
La méthode est officiellement sûre si l'on respecte certaines contraintes de longueur de clés et d'usage.
Personne depuis 2500 ans n'a trouvé de solution rapide au problème de la factorisation ...

Bases théoriques de la cryptographie asymétriques

La cryptographie asymétrique n ’est jamais inconditionellement sûre (chiffre parfait): Estelle peut toujours faire une attaque exhaustive en utilisant la clef publique.

Théorie de la complexité calulatoire de la cryptanalyse

Complexité algorithmique

Nom du problème	Enoncé	Complexité
Factorisation	Soit n=p.q ou p et q sont deux entiers premiers et très grands, vérifiant quelques propriétés qui sont précisées dans la présentation du RSA. Trouver p et q connaissant n	NP Super polynomial
Extraction des racines dans un anneau non intègre	Soit n=p.q ou p et q sont deux entiers premiers et très grands, vérifiant quelques propriétés qui sont précisées dans la présentation du RSA. Soit $b \in (0..n-1)$, Trouver $x \in (0..n-1)$ tel que $b=x^t \bmod n$	NP Super polynomial
Logarithme discret	Soit p un nombre premier très grand tel que p-1 a un grand facteur premier soit $g \in (0..p-1)$ tel que $\forall y \in (1,..p-2)\ g^y \neq 1 \bmod p$, soit $b \in (0..p-1)$ Trouver $x \in (1,..p-2)$ tel que $g^x=b \bmod p$ n. b. On montre que g est un élément primitif du groupe multiplicatif Z/Zp, c'est à dire que les puissances de g modulo p engendrent (1,..p-1). Donc le problème précédent a une solution.	NP Super polynomial
Isomorphie de deux graphes	Soit G(X,U) et G'(X,U') deux graphes isomorphes. Trouver la permutation permettant de passer de G à G'. n. b. X est un ensemble d'entier (sommets du graphe). Un élément de U ou de U' (arc du graphe) est un couple (a,b) d'éléments de X. Le problème consiste à trouver une permutation π de X tel que la fonction qui a $(a,b) \in U$ fait correspondre $(\pi(a),\pi(b))$ soit une bijection de U dans U'.	NP-complet Exponentiel
Problème du sac à dos	Soit x un nombre et $X=\{x_1, x_2,..x_n\}$ un ensemble de nombres. Trouver un sous-ensemble S de X tel que $x = \sum_S x_i$	NP-complet Exponentiel

Fonctions à sens unique

C'est une fonction f(M) facile à calculer
mais telle qu'il est extrêmement difficile de déduire M de f(M).

Exemple:

Calcul modulo n (dans un anneau fini)

M^2 est facile à calculer modulo n (M^e).

$\sqrt{M}$ est difficile à calculer (log M).

Fonction à sens unique avec brèche secrète

C'est une fonction f(M) facile à calculer telle qu'il est extrêmement difficile de déduire M sauf si l'on connaît un secret K.
Deux exemples utilisés en pratique:
• Problème de la factorisation (RSA),
n=pxq, p et q sont premier, e est défini comme dans le RSA et public
$f(M)= M^e \bmod n$,
brèche connaissance de p ou q
• Problème du logarithme discret (El Gammal)
p est premier, a est un élément primitif de Z^p, $b= a^x \bmod p$, k est quelconque, p, a, b sont publics, $a^k \bmod p$ est connu
$f(M)= M. b^k \bmod p$,
brèche connaissance de x
En effet $1/b^k = 1/(a^k)^x$

Fonctions basées sur la théorie de la complexité

Algorithme basé sur le sac à dos
Cassé car la brèche montrait que le problème de
l ’inversion de f était un cas polynomial d ’un problème
NP complet.

Echec sauf sur les algorithmes probabilistes (A apport nul de connaissances)

Fonction de hachage

Une fonction de hachage h est une fonction qui à un message M de longueur quelconque fait correspondre un message H(M) (notée aussi $\{M\}^H$) de longueur constante.
L'intérêt d'une fonction de hachage est que M peut être arbitrairement grand alors que $\{M\}^H$ a une longueur donnée.
Terminologie: Résumé, fonction de contraction, digest, empreinte digitale, …

Exemple: Hasch codes des systèmes de fichiers, codes détecteur d 'erreurs

Fonction de hachage sécuritaire

f(M) telle que f est une fonction de hachage par rapport à M

f est à collision faible difficile: il est calculatoirement difficile de trouver M significatif tel que f(M)=K

f est à collision forte difficile:il est calculatoirement difficile de trouver M et M’ tel que f(M)=f(M ’)

Elle est avec clef si son calcul dépend d ’une information secrète la clef K

MD5: Principes (1)

Une fonction de hachage à sens unique.qui génère une signature sur 128 bits.

Le message est décomposé en blocs de 512 bits soient 16 sous-blocs Mj de 32 bits.
Pour chaque bloc de 512 bits on réalise 4 séries de 16 applications successives des fonctions de base FF, GG , HH, II qui dépendent des sous-blocs Mj et de constantes a, b, c, d,

$$FF(a,b,c,d,Mj,s,ti) \longrightarrow a = b + ((a = F(b,c,d) + Mj + ti) \lhd s)$$

$$GG(a,b,c,d,Mj,s,ti) \longrightarrow a = b + ((a = G(b,c,d) + Mj + ti) \lhd s)$$

$$HH(a,b,c,d,Mj,s,ti) \longrightarrow a = b + ((a = H(b,c,d) + Mj + ti) \lhd s)$$

$$II(a,b,c,d,Mj,s,ti) \longrightarrow a = b + ((a = I(b,c,d) + Mj + ti) \lhd s)$$

Dans les formules précédentes $\angle$s désigne un décalage à gauche de s positions

MD5 Principes (2)

Les fonctions F,G,H,I sont données par:

$$F(X,Y,Z)=(X \wedge Y) \vee (\neg X \wedge Z)$$
$$G(X,Y,Z)=(X \wedge Z) \vee (Y \wedge \neg Z)$$
$$H(X,Y,Z)=(X \oplus Y \oplus Z)$$
$$I(X,Y,Z)=Y \oplus (X \vee \neg Z)$$

$\{k\}_a^{asy}$

Usage de la cryptographie asymétrique: confidentialité

Algorithme de Bob

Récupérer la clef publique d'Alice a

$$CS = \{k\}_a^{asy}$$

$$MCHIF = \{M\}_k^{sym}$$

Début

De Bob à Alice,

Ceci est un message secret,

crypto-système symétrique: sym,

clef de session:CS,

Message:MCHIF,

Fin

Algorithme d'Alice

$$k = \{CS\}_A^{asy}$$

$$M = \{MCHIF\}_K^{sym}$$

$\{k\}_a^{asy}$

Usage de la cryptographie asymétrique: authentification et signature

Algorithme de Bob

$$SIG = \{\{M\}^H\}_B^{asy}$$

Début

De Bob à Alice,

Ceci est un message signé,

Message:M,

Signature Sig

Fin

Algorithme d'Alice

Récupérer la clef publique de Bob b

$$H' = \{SIG\}_b^{asy}$$

$$H = \{M\}^H$$

Si H=H' signature OK
Sinon erreur

Signature

Une signature manuscrite idéale est réputée posséder les propriétés suivantes:

- La signature **ne peut-être imitée.**
Elle prouve que le signataire a délibérément signé le document.

- La signature **authentifie** le signataire.
Seul le signataire peut avoir signé.

- La signature appartient à un seul document (elle **n'est pas réutilisable**).

- Le document signé ne peut être partiellement ou totalement **modifié**

-La signature peut être **contrôlée**.

- La signature ne peut-être **reniée**.

Signature Numérique

Base de la signature numérique:une fonctions de hachage
H sécuritaire et d ’une fonction à sens unique f avec brèche.

La signature est composée de $f^{-1}(\{M\}^H)$

Seul le signataire sait calculer f^{-1}
Tout le monde peut calculer H et f et donc pour M donné vérifier la signature

Si H est a collision faible, on ne pourra pas coller une signature sur un document à créer

Si h est à collision forte difficile Estelle ne pourra pas fabriquer 2 documents, un que Bob peut signer ,l ’autre pas, ayant le même hache donc la même signature

Signature El Gamal

Clef publique d ’Alice:
p premier, $g<p$, $y=g^x \bmod p$

Clef privée d ’Alice
$x<p$

Signature de M par Alice
choisir k tel que k et p-1 soient premiers entre eux
calculez $a=g^k \bmod p$ et b tel que $M=(xa+kb) \bmod p-1$
a,b sont la signature de M par Alice

Vérification par Bob
$y^a a^b \bmod p=g^M \bmod p$

Exemple (Schneier)

Clef publique, p=11, g=2
Clef privée x=8<11
Publique $y=2^8 \bmod 11=3$

Signature de M=5
Choix de k=9 aléatoire et premier avec 10=11-1
$a=2^9 \bmod 11=6$
Recherche de b tel que M=5=(8 x 6+9 x b) mod 10
soit b=3 (48+27=75≡ 5 mod 10)
contrôle $3^6 6^3 \bmod 11=2^5 \bmod 11=10$

Validité de la signature

Pour signer à la place d ’Alice il faut trouver x tel que
$y=g^x \bmod p$ donc résoudre le problème du logarithme discret

Pour signer M ’ de tel façon que signature(M)=signature (M ’)
On doit avoir:
$y^a a^b \bmod p = g^{M'} \bmod p$
donc résoudre le problème du logarithme discret

Validité du contrôle

$y^a \bmod p = (g^x)^a \bmod p = g^{xa} \bmod p$

$a^b \bmod p = g^{kb} \bmod p$

$y^a . a^b \bmod p = g^{(xa+kb)} \bmod p$

Or

$g^M \bmod p = g^{(s(p-1)+xa+kb)} \bmod p = g^{(s(p-1)+xa+kb)} \bmod p$

$= g^{(s(p-1))} \bmod p \cdot g^{(xa+kb)} \bmod p = g^{(xa+kb)} \bmod p$

(théorème d ’Euler)

Génération de nombres pseudo aléatoires sécuritaires

Problème important:
Pour créer des nonces
Pour générer des clefs

Propriété attendue

Quelque soit l ’observation du pirate il ne peut
acquérir de l ’information sur le nombre qui va être généré

Formalisation

Suite Pseudo aléatoire:
Il s ’agit d ’une suite de nombres X_0,X_1,...
X_0 , S_0 grain
$0<X_i<N$
$X_n=f(X_{n-1},S_{n-1})$
$S_n=g(X_{n-1}, S_{n-1})$

Tout test statistique fait accepter l ’hypothèse
« X est une suite de nombres uniformément répartis dans 0,N »
ou
« $Prob(X_n/X_0, X_1, \ldots X_{n-1})=Prob(X_n) =1/N$ »

Suite Pseudo aléatoire sécuritaire

Propriété pas suffisante pour la sécurité:
Les X sont transmis, éventuellement en clair, les S restent cachés
il faut qu ’un pirate qui a observé $X_0,….,X_{n-1}$ ne puisse en déduire X_n
Deux solutions:
1) La suite est aléatoire (bruit thermique d ’une résistance)
2) Le grain est le plus aléatoire possible (fonction de la vitesse de frappe au clavier, d ’un nombre d ’interruption…) et
la fonction de s donnée par a=f(b,s) doit être à sens unique

Exemple ANSI X9.17

Choisir une clef K pour le DES et X_0 imprévisibles et secrets,
T_n est la date courante
$S_n=E_k(E_k(T_n)+X_{n-1})$
$X_n=E_k(E_k(T_n)+S_n)$

Bibliographie

S.Natkin Les protocoles de sécurité de l'Internet, Dunod 2002

J. Stern- La science du secret Ed Odile Jacob 1998

A.S. Tannenbaum - Computer Networks Prentice Hall

D. Stinson - Cryptographie, Théorie et pratique, Thomson Publishing International France

B. Schneier - Cryptographie appliquée Thomson Publishing International France

D.E. Denning - Cryptography and data security Addison Wesley 1982

LES PROTOCOLES DE SECURITE

G. Florin

S. Natkin

Mai 2003

Notations

A: clef d ’Alice (déchiffrement symétrique)
a : clef d ’Alice (chiffrement symétrique)
A: clef privée de Alice (déchiffrement asymétrique)
a: clef publique de Alice (chiffrement asymétrique)

$\{X\}_{Clef}^{CRY}$ Chiffrement /Déchiffrement selon le crypto sytème CRY avec la clef Clef

Crypto systèmes symétriques

$\{X\}_{a}^{SYM}$ Chiffrement $\{X\}_{A}^{SYM}$ Déchiffrement

Crypto systèmes asymétriques

$\{X\}_{a}^{ASY}$ Chiffrement (clef publique) $\{X\}_{A}^{ASY}$ Déchiffrement (clef privée)

$\{X\}^{H}$ Résumé de sécurité $\{X\}_{A}^{SIG} = \{\{X\}^{H}\}_{A}^{ASY}$ Signature de X par Alice

Notations protocolaire

Format des messages :Type, Emetteur, Destinataire, Contenu

Alice

Bob

M

Dans le protocole Alice envoie M à Bob

Les partenaires fiables

Système à clef privée: Le gardien des clefs

Alice	A	Date début/ Date fin a
Bob	B	Date début/ Date fin b
Charles	C	Date début/ Date fin c

Ce tableau est protégé en intégrité et confidentialité
Chaque participant connaît sa clef et celle du gardien G

Systèmes à clefs publiques: Annuaire de certificats

Alice	a	Date début/ Date fin a	
Bob	b	Date début/ Date fin b	
Charles	c	Date début/ Date fin c	

Ce tableau est protégé en intégrité (voir plus loin)
Chaque participant connaît sa clef privée et la clef publique de l ’annuaire

Authentification

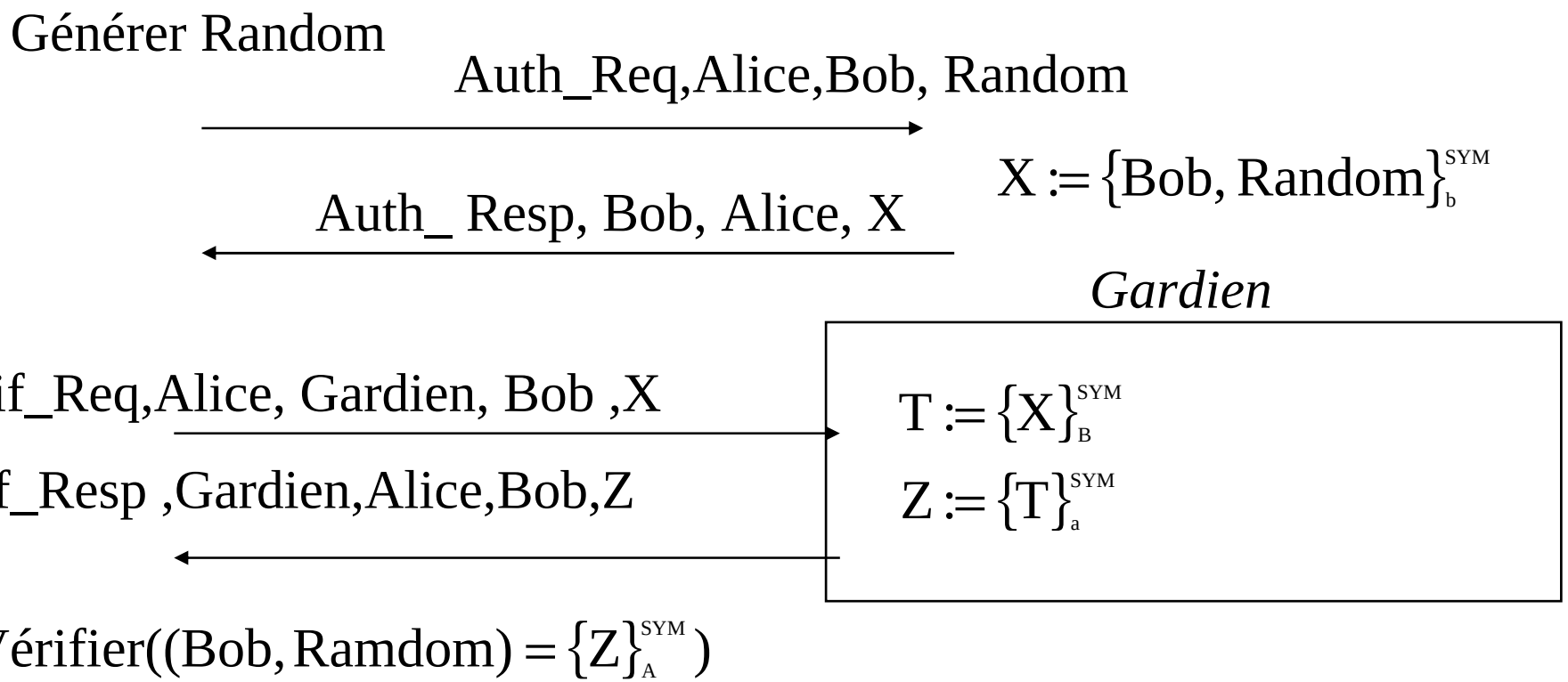
Protocole permettant à Bob de prouver à Alice qu'il est Bob

Bob détient un secret sur lequel repose l'authentification
Bob ne doit pas révéler le secret à Alice

Il existe un tiers fiable qui a authentifié Bob
(gardien des clefs ou annuaire de certificats)

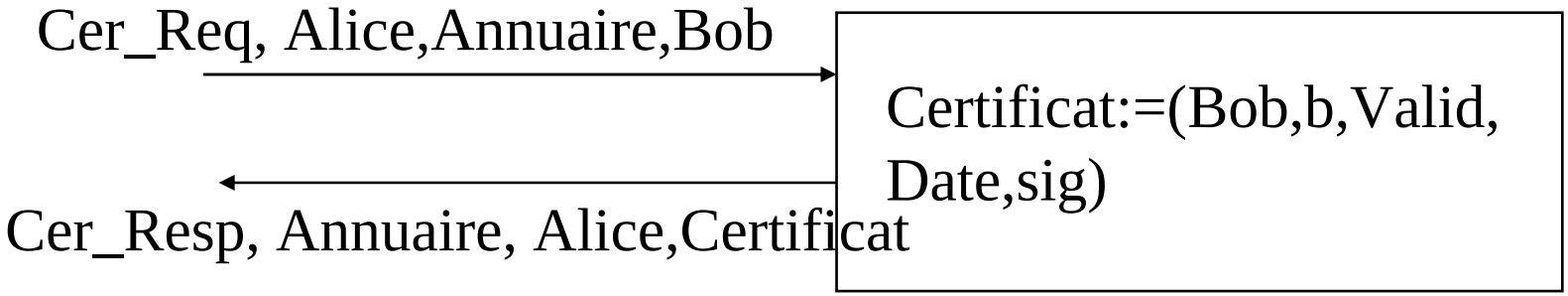
Authentification avec un crypto système symétrique

Alice *Bob*



Authentification à clef publique

Alice *Annuaire* *Bob*



Contrôler les certificats

Générer Random

Auth_Req, Alice, Bob,Random

$$X := \{\text{Bob, Random}\}_{B}^{ASY}$$

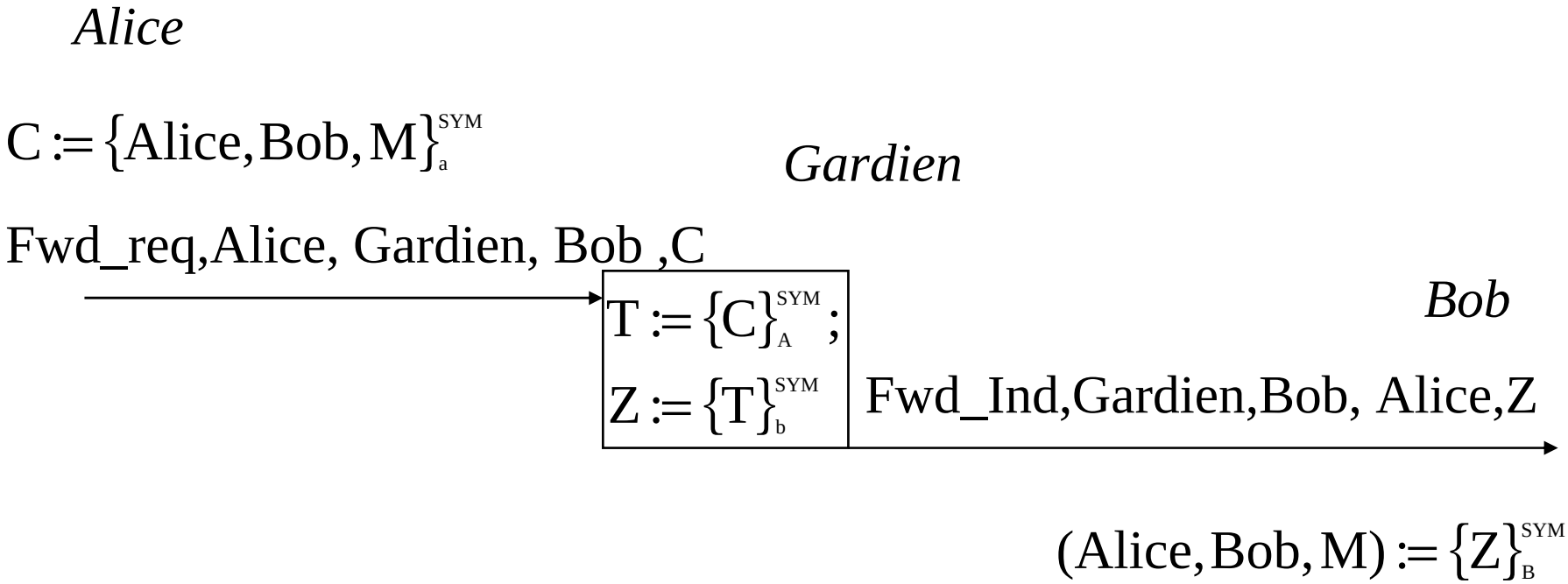
Auth_Resp, Bob,Alice,C

$$\text{Vérifier}((\text{Bob, Ramdom}) = \{Z\}_{b}^{SYM})$$

Confidentialité

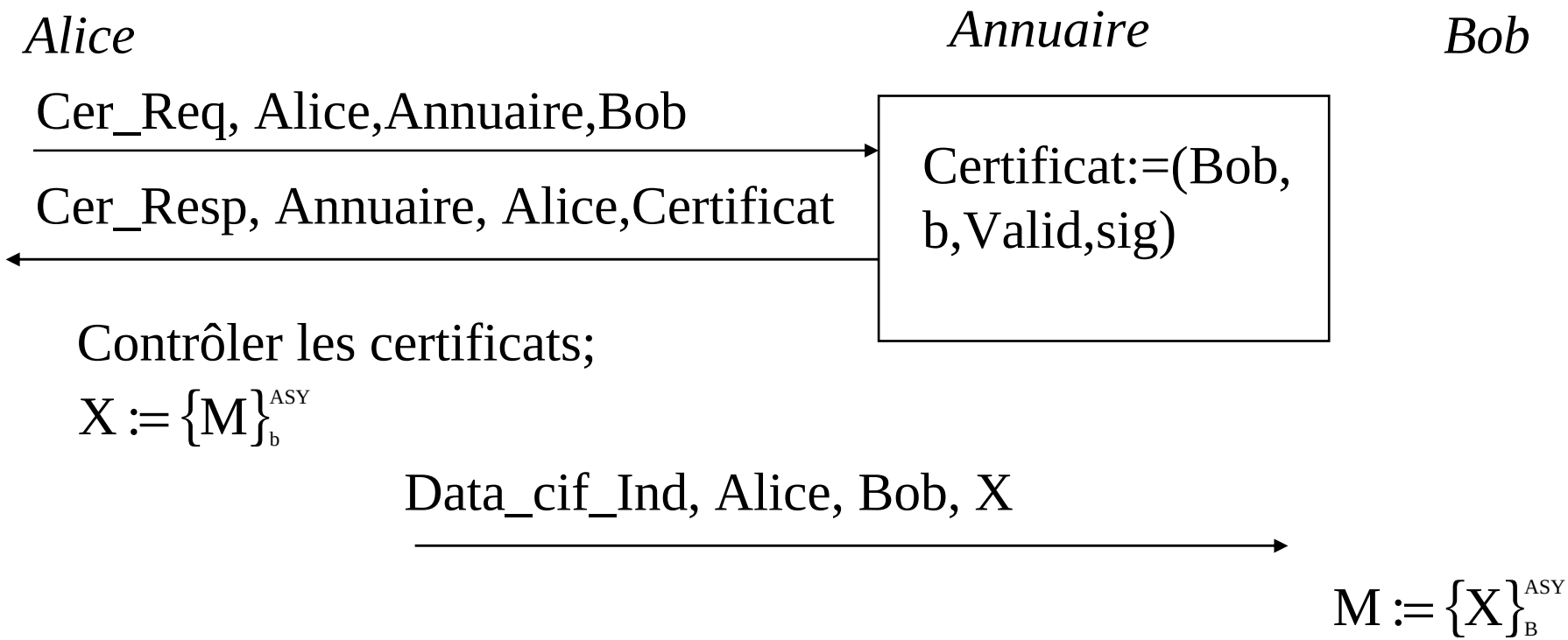
Alice doit transmettre à Bob un message que eux seuls doivent connaître

Confidentialité avec chiffre symétrique



M peut être une clef de session, qui est ensuite utilisée pour chiffrer les autres messages entre Alice et Bob

Confidentialité avec chiffre asymétrique



Très peu utilisé car très lent, sert à échanger des clefs d ’algorithmes symétriques beaucoup plus rapides
On échange ainsi une clef de session pour chiffre symétrique

Signature et intégrité

Alice doit envoyer à Bob un message, tel que Bob puisse contrôler que le message n'a pas été modifié et a bien été créé par Alice

Signature avec chiffre symétrique

Alice

$$Sig := \{\{M\}^{H}\}^{SYM}_{A}$$

Bob

Sig_Ind,Alice, Bob ,M,Sig →

Gardien

$$T := \{Sig\}^{SYM}_{a}$$

$$Z := \{Sig\}^{SYM}_{\mathbf{B}}$$

← Cif_Req,Bob,Gardien, Alice,Sig

Cif_Resp, Gardien,Bob,Alice,Z →

$$V := \{M\}^{H}$$

$$\text{Vérifier } V = \{Z\}^{SYM}_{b}$$

Signature à chiffrement asymétrique

Bob *Alice*

$Sig := \{Bob, Alice, M\}_B^{SIG}$ Bob,Alice,M,Sig

Annuaire

Cert_Req,Alice,Annuaire,Bob

Certificat:=(Bob,b,
Cert_Req, Valid,sig)

Cert_Resp, Annuaire, Alice,Certificat

Contrôle des certificats;

$V = \{Bob, Alice, M\}^H$;

Vérifier($V = \{Sig\}_b^{ASY}$

Intégrité des messages et flots de messages

Intégrité d ’un message: problème voisin de la signature
Utilisation de fonction de Hachage sécuritaire ou de MAC basé sur un chiffre symétrique en mode chaîné

Intégrité du flot de message: Possibilité de rejeu
Utilisation d ’un **Nonce** (Used Only Once), qui distingue chaque message:
Numéro de séquence sur un modulo grand
Heure
Nombre aléatoire

Gestion des clefs

Annuaire des certificats

NOM	Clef	Validité	Extensions	Signature
Alice	a	Valida	Para	$\{Alice, a, Valida, Para\}_{AC}^{SIG}$
Bob	b	Validb	Parb	$\{Bob, b, Validb, Parb\}_{AC}^{SIG}$
Charles	c	Validc	Parc	$\{Charles, c, Validc, Parc\}_{AC}^{SIG}$

AC: autorité de certification

Norme de représentation des certificats X509

Norme de protocole d'accès: LDAP

Contrôle des certificats

Toutes entités impliquées dans un schéma à clef publique doit détenir la clef publique de l ’autorité de certification.

Tout accès à un certificat doit être contrôlé:
Vérifier que la signature est valide
Vérifier que la date courante est dans la période de validité

Pour éviter les rejeux de certificats invalidés le serveur d ’annuaire doit :
Soit s’authentifier
Soit dater et signer sa réponse
Soit transmettre périodiquement des listes de révocation datée et signées

Stockage des clefs asymétriques

Clef publique de l'autorité, ne doit pas pouvoir être modifiée: Dans le code en dur , sur un support fiable (carte à puce)

Clef privée de l 'utilisateur, ne doit pas pouvoir être lue: sur un support confidentiel (carte à puce) ou un fichier chiffré avec un mot de passe (local au poste ou sur disquette)

Certificat de l 'utilisateur: Annuaire+support local ou carte ou disquette

Annuaire: Annuaire central+version locales (cache, annuaire privé

Protocole de création des certificats version répartie

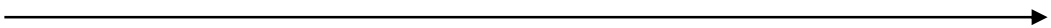
Client Alice *Autorité de certification*

génération de A, a, MP

Stockage $ESYM_{MP}$(Alice, A, Date)

X:= E_{RS} (Alice, a, Date)

Alice, Autorité, X



D_{RS} (X)

Contrôle de

l ’identité d ’Alice

Mise à jour de l ’annuaire

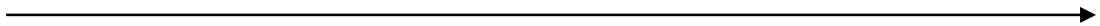
Y=Alice,a,Date, D_{RS} (Alice, a, Date)

Autorité, Alice, Y

Protocole de création des certificats version centralisée

Autorité de certification

Alice, Autorité



Contrôle de
l'identité d 'Alice
génération de A, a, MP

$ESYM_{MP}$(Alice, A, Date)
fichier, disquette, carte à puces

MP (voie confidentielle)

Mise à jour de l 'annuaire
Y=Alice,a,Date, D_{RS} (Alice, a, Date)

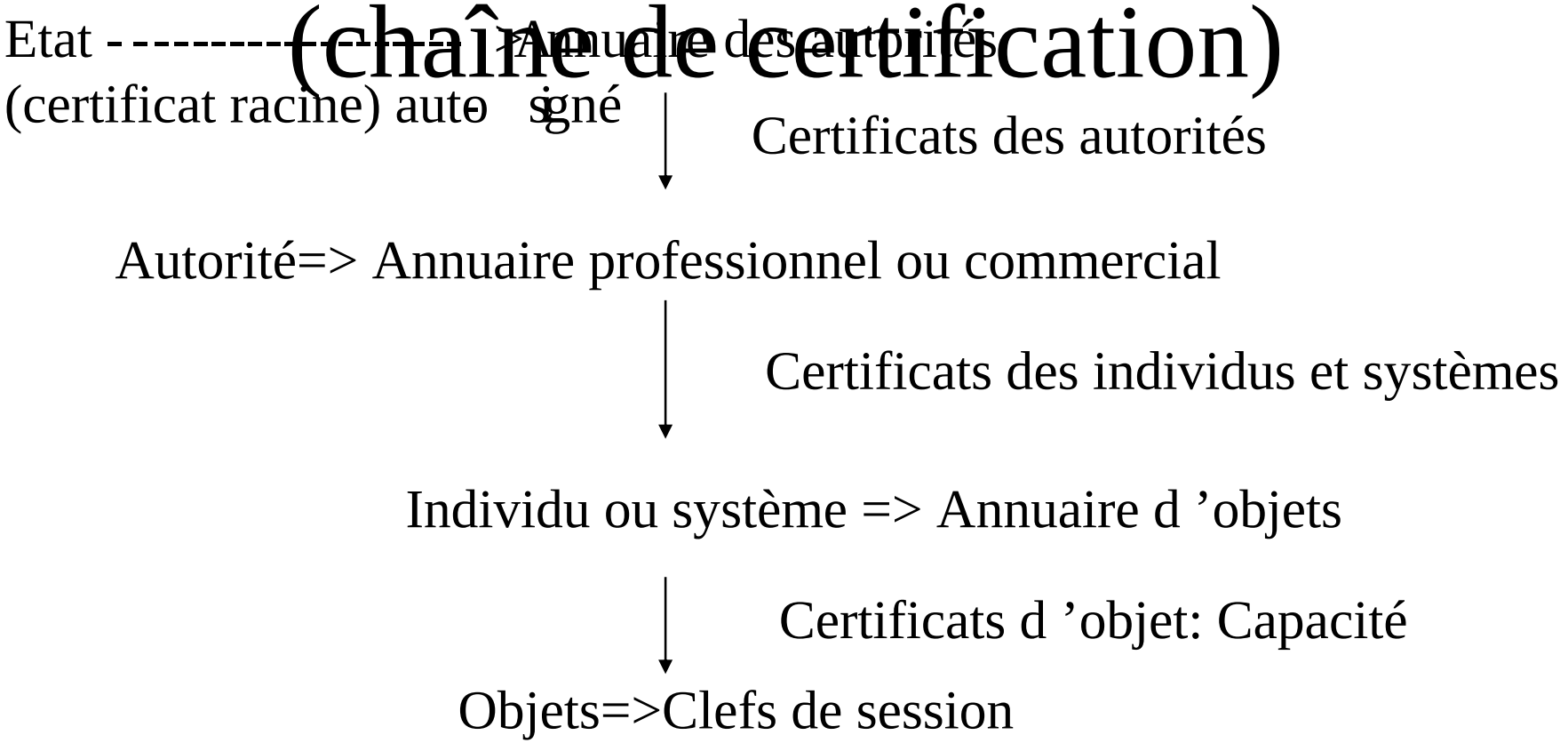
Hiérarchie des clefs

Plus on utilise une clef plus elle est vulnérable
Clef utilisée pour chiffrer une suite de transfert de fichier
vs clef utilisée pour chiffrer un numéro de carte bleue

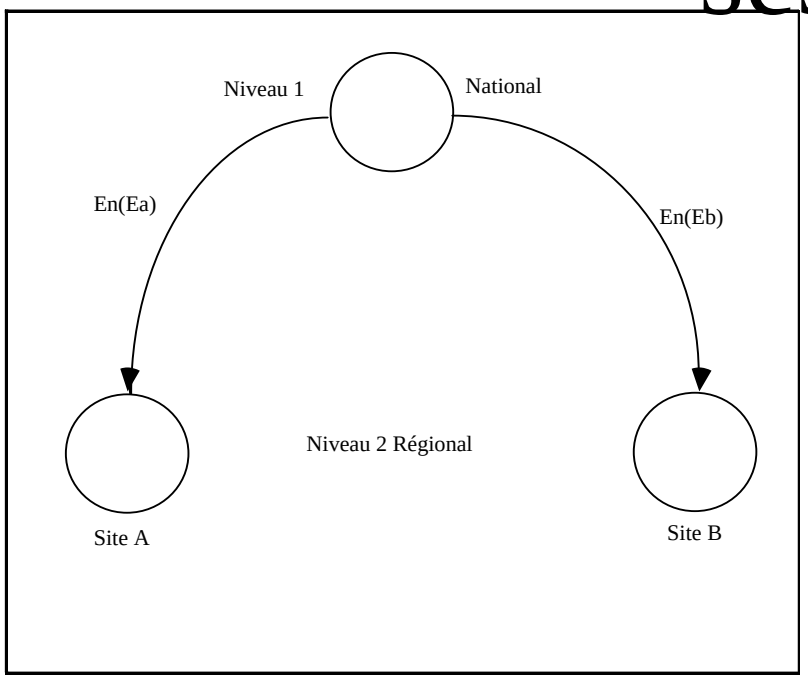
Plus elle sert a protéger des données péreines, plus elle doit être fiable
Signature électronique d ’un article de presse vs Signature électronique d ’un testament

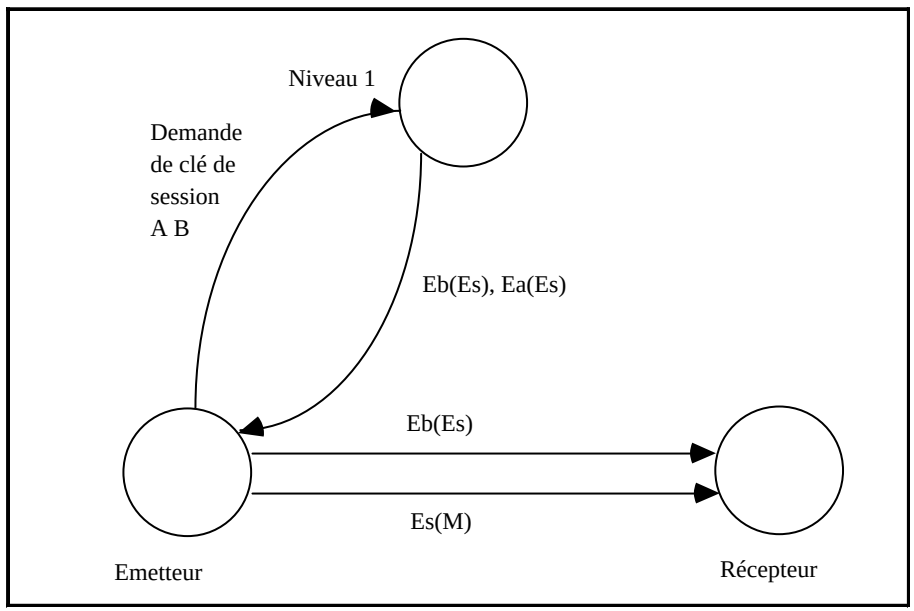
On peut utiliser des canaux très lents mais très fiables pour véhiculer des clefs qui seront utilisées sur des voies plus rapides
et moins fiables (téléphone rouge)

Système asymétrique: Hiérarchie des autorités de certification (chaîne de certification)



Système symétrique hiérarchie des clefs de session





apport nul de connaissance (zero knowledge protocols)

Principes généraux

En utilisant les algorithmes à clefs publiques
S,D(s)----------->? E(D(S)) = S
La base est que seul celui qui doit s'authentifier sait faire D

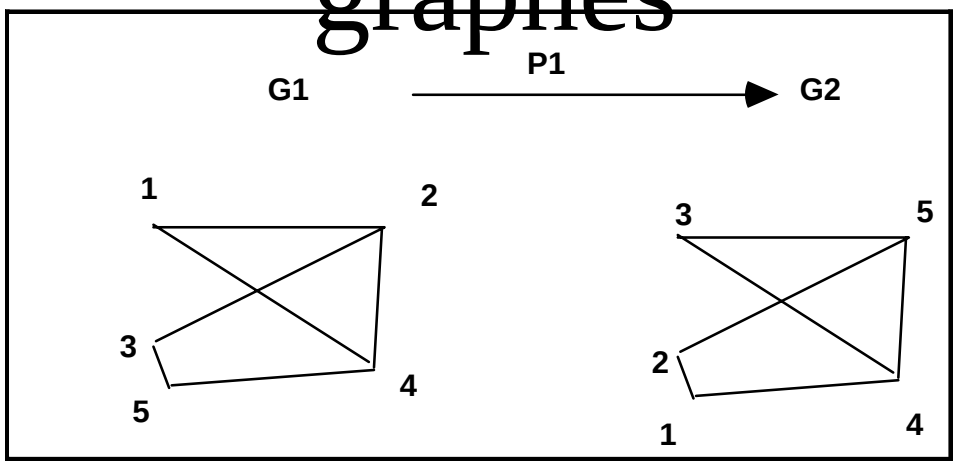
Dans les algorithmes a absence de connaissance:
Protocoles d'authentification probabilistes

Le veritable emetteur est seul a savoir répondre
à une question à coup sûr

Le pirate sait répondre avec une probabilité p
et échoue avec une probabilité 1-p

Un échec prouve une tentative d'usurpation
Après k succès la probabilité d'une tentative d'usurpation est p^k

Exemple d ’école: isomorphie de graphes

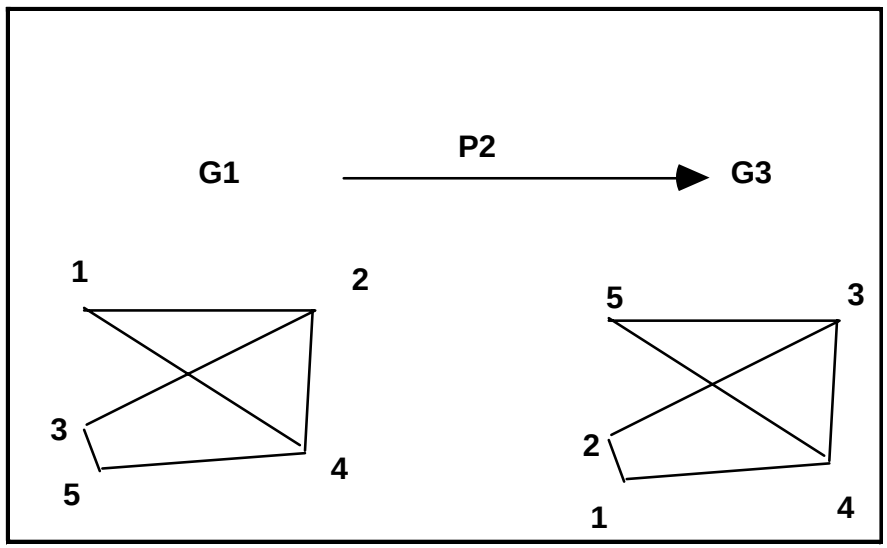


G1 et G2 Sont publics

P1 (1->3, 2->5, 3->2, 5->1, 4->4) est secrète

Isomorphie de graphes (2)

Au moment de l'authentification celui qui doit s'authentifier (le prouveur) publie un troisième graphe g3 soit déduit de g1 soit déduit de g2 (il ne dit pas quel est Le graphe de départ)



P2 (1->5, 2->3, 3->2, 5->1, 4->4) est secrète

Isomorphie de graphes (3)

Celui qui cherche a vérifier l'authentification (le vérifieur) connaît les trois graphes,mais pas le processus de génération.
Il demande:

A) avec une probabilité 1/2 comment passe t'on de g1 a g3?
B) avec une probabilité 1/2 comment passe t'on de g2 a g3?

Le prouveur peut toujours répondre:

Dans l'exemple cas a il répond p2
Cas b il répond $p1^{-1}$op2
(Il connaît p1 et sait donc calculer son inverse)

Le pirate a génère un graphe soit a partir de g1 soit a partir de g2 (publics).
Supposons g1

Dans le cas a il sait répondre
Dans le cas b il ne sait pas (pb np complet)

Le protocole de Fiat-Shamir (1)

Basé sur la complexité de calcul d'une racine carrée dans une algèbre modulo N ou N est le produit de deux grands nombres premiers p et q

0) Données publiques
Le prouveur choisit un nombre S et calcule $V=S^2$ mod (N). Il publie V

1) Authentification
Le vérifieur demande au prouveur de s'authentifier
Le prouveur a choisit un nombre aléatoire R

2) Phase d'enchère:
Le prouveur calcule $X=R^2$ mod (N). Il envoie X au vérifieur

3) Phase de défi:Le vérifieur met le prouveur au défi:
Il choisit un nombre aléatoire binaire D et l'envoie au prouveur

4) Phase de preuve
Le prouveur répond en envoyant Y au vérifieur
Si D=0 Y=R
Si D=1 Y=R*S mod (N)

Le protocole de Fiat-Shamir (2)

5) Phase de vérification

Le vérifieur calcule Y^2

Il doit trouver:

Si D=0 $Y^2 = X$

Si D=1 $Y^2 = X*V \bmod (N)$

ANALYSE

Si le fraudeur connaissait des la phase 1, la question posée en 3, il pourrait toujours tromper le valideur:

Si D=0 il choisit R quelconque et calcule $X=R^2$

Si D =1 il choisit un nombre K arbitraire et pose

$X = K^2*V \bmod(N)$

$Y = K*V \bmod (N)$

Ceci vérifie donc $Y^2 = X*V \bmod(N)$

(mais il ne connaît pas R, la racine de X)

Il est donc indispensable de procéder dans cet ordre

Donc ne connaissant pas la question le fraudeur doit a priori choisir entre les deux stratégies et a donc une chance sur deux de d'être capable de répondre

Partage d’un secret: protocoles à seuil

Certaines opérations sont suffisamment sensibles pour devoir **engager la responsabilité de plusieurs** personnes.

On peut faire **vérifier l'identité** de plusieurs usagers simultanément possesseurs d'un **mot de passe** pour engager une action.

Mais cette approche peut ensuite être encore raffinée en souhaitant **donner une part de responsabilité plus importante** selon un grade:
Ex : Il suffit de la présence du responsable financier pour ouvrir le coffre ou de trois chefs de service ou ...

-Le problème du partage d'un secret:

Comment diviser une clé d'accès représentée par **une valeur numérique V en parts** (t+1 par exemple)
De telle façon qu'un groupe de porteurs de t+1 parts peuvent reconstituer la clé alors qu'un **groupe de porteurs de t parts ne le peuvent pas**.
Les porteurs de parts **doivent pouvoir reconstituer V** dans un système informatique d'autorisation sans jamais connaître V.

Protocole de Shamir (1)

V **valeur numérique** entière

. On **génère aléatoirement t valeurs entières**

$a_1 , a_2 , ... , a_t$

. **On leur associe un polynôme** dont le terme constant est **V** :

$$P(x) = a_t x^t + a_{t-1} x^{t-1} + ... + a_1 x + V$$

Une part du **secret est un couple (x_i,P(x_i)**) x_i non nul
les parts sont générées par des xi différents

Pour éviter une possible **attaque force brute** par un groupe de por
agissant par essais et erreurs pour compléter leur connaissance:
on choisit **un entier premier** N grand,
les calculs sont faits en arithmétique modulo N

Protocole de Shamir (2)

V **valeur numérique** entière

. On **génère aléatoirement t valeurs entières**

$a_1 , a_2 , ... , a_t$

. **On leur associe un polynôme** dont le terme constant est **V** :

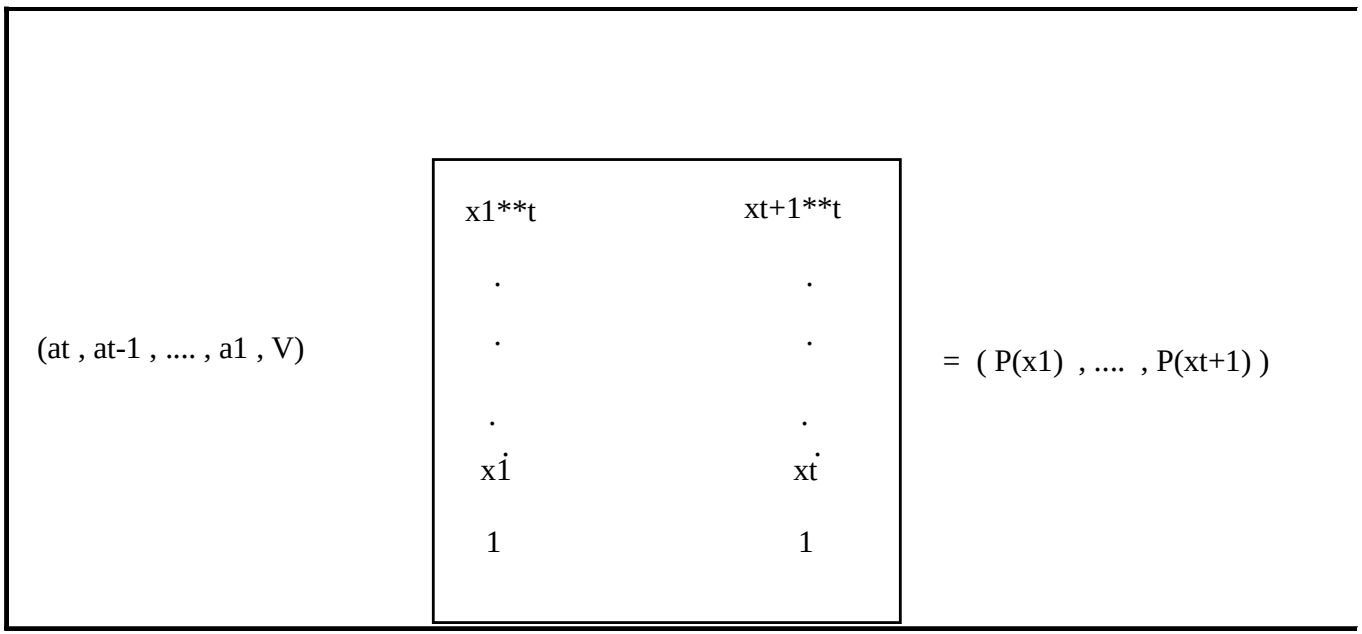
$$P(x) = a_t x^t + a_{t-1} x^{t-1} + ... + a_1 x + V$$

Une part du **secret est un couple (x_i,P(x_i)**) x_i non nul
les parts sont générées par des xi différents

Pour éviter une possible **attaque force brute** par un groupe de por
agissant par essais et erreurs pour compléter leur connaissance:
on choisit **un entier premier** N grand,
les calculs sont faits en arithmétique modulo N

Protocole de Shamir (3)

Tout groupe d'au moins t+1 possesseurs de parts peut résoudre le système linéaire de détermination des coefficients du polynôme et ainsi trouver V:



Comme les xi sont différents et non nuls la matrice est régulière

Tout sous groupe de porteurs dont la somme des parts est inférieure ou égale à t ne peut déterminer V.

La protection

G. Florin, S. Natkin
Novembre 2001

SCHÉMA D ’ACQUISITION ET D ’ÉVOLUTION DES DROITS

Quand un utilisateur se connecte sur son compte

- Il est authentifié
- il dispose alors de droits sur certains objets:
  - Les droits sur les objets systèmes que l ’administrateur lui donne.
  - Tous les droits sur les objets qu ’il crée.
  - Les droits sur d ’autres objets que les autres utilisateurs lui ont accordés.
  - Les droits de propagation des droits que l ’administrateur lui autorise
- Il peut créer de nouveaux objets et les droits correspondants
- Il peut propager des droits et donc donner des droits

C ’est la définition et le contrôle de ce schéma qui en théorie devrait garantir le respect des règles de sécurité.

LES TECHNIQUES DE LA SECURITE INFORMATIQUE

- Authentification des personnes
- Gestion des droits et contrôle d'accès (protection)
- Protocoles de sécurité
- Validation des systèmes

1- Spécification des politiques de contrôle d ’accès

GENERALITES

Le contrôle d ’accès est la base des mécanismes informatiques:
Il permet de spécifier la politique dans le domaine de l ’informatique.

Il définit la façon dont le système contrôle ces droits.

Il devrait, en théorie, encapsuler toutes les autres techniques informatiques
Pour l’instant ce n’est pas le cas.

CONCEPTS DE BASE

- Un ensemble de ressources physiques interconnectées et d'utilisateurs pour lequel est défini une politique de sécurité et est administré l'ensemble des règles et mécanismes de protection est appelé **cellule d'administration** (ce qui correspond dans l'environnement NT à la notion de domaine).
- A chaque utilisateur est associé un **compte**. Celui ci détermine les moyens qui doivent être utilisés pour authentifier cet utilisateur, les limite apportée au droit de connexion (les machines sur lesquelles il peut se connecter, le nombre maximal de connexions simultanées, les heures qui lui sont autorisées ou interdites…), et les droits initiaux qui lui sont accordés lors d'une connexion.
- Un **groupe** est un ensemble de droits communs à plusieurs utilisateurs. Par exemple sous NT à l'initialisation d'un domaine, le groupe administrateur à en particulier le droit de créer des groupes et des comptes ou de modifier la configuration physique du domaine de sécurité. Le groupe des invités a très peu de droits mais ses membres ne sont pas authentifiés.

EXEMPLES DE SPECIFICATION DE LA POLITIQUE

Un utilisateur a les droits de son compte (accès aux fichiers, programmes utilisables, ressources partagées accessibles) Déterminée par une politique de compte.

Sous NT, les droits d ’un utilisateur sont définis
les droits des groupes auquel il appartient (utilisateur de base + groupe des comptables).La gestion des comptes peut être très fine (par exemple on peut interdire au groupe des utilisateurs de base de se connecter la nuit)
Sous Unix (BSD), il y a trois groupes prédéterminés (moi, mon groupe, l ’univers). Par contre on peut spécialiser individuellement les droits sur les ressources.

Sous 95,98 et Mac OS il n ’y a rien de sérieux**.**

PRINCIPES A RESPECTER

Principe du **moindre privilège** : Un objet ne doit disposer que des droits qui lui sont strictement nécessaires pour réaliser les tâches
qui lui sont dévolues.

Utilisation de politique obligatoire : La politique doit le moins possible dépendre des utilisateurs en tant que personne,
mais reposer sur les rôles de la politique de sécurité du
système d'information.

Séparation des rôles de création des comptes et d 'attribution des droits

Les rôles d 'attribution des droits doivent être attribués par domaines de responsabilité

MATRICE DE CONTRÔLE D ’ACCES

Définit à chaque instant
les droits de chaque sujet sur chaque objet

	M1	M2	F1	F2	P1	P2
P1	**R,W,E**		**Own,R, W**	**R**		
P2		**R,W,E**		**Own,R, W**		
S1	**R,W,E, Create, Destroy**	**R,W,E, Create, Destroy**	**R,W,E, Create, Destroy**	**R,W,E, Create, Destroy**	**Create, Destroy**	**Create, Destroy**

MATRICE DE CONTRÔLE D ’ACCES (2)

A l'origine les types de sujet et d'objets sont prédéfinis (système)
sujets: utilisateurs, processus, groupes d'utilisateurs ou de processus
objets: segments ou pages mémoires, fichiers, processus, programmes

Ceci rend difficile la mise en oeuvre du principe du moindre privilège

Evolution vers une notion orientée objet
sujets: utilisateurs, objets
objets: métodes d'accès aux objets

	M1				
	R	**W**	**E**	**Create**	**Destroy**
P1	**1**	**1**	**1**		
P2					
S1	**1**	**1**	**1**	**1**	**1**

EVOLUTION DE LA MATRICE DE CONTRÔLE D ’ACCES

La matrice des droits évolue en fonction des évènements suivants:

- **création et destruction des sujets et des objets**
- **création et destruction des droits**
- **propagation des droits**

Exemple
Dans UNIX les droits d'un processus sont hérités de son père et donc originellement de l'utilisateur (fork du login)
Lorqu'un processus exécute un programme il hérite (SUID=vrai) en général des droits du possesseur du programme.

2-Authentification des personnes

AUTHENTIFICATION DES PERSONNES

L'**authentification** = **vérification de l'identité** d'une entité.

L'une des mesures les plus importantes de la sécurité:
- Impossible d'assurer la confidentialité, l'intégrité, la non répudiation sans la garantie de l'identité de l'entité soumettant une requête.
- L'authentification devrait être assurée en continu.
(pas une fois pour toutes à l'ouverture d'un objet (en début de session)
Personne **:**elle peut quitter son poste en le laissant ouvert
=> procédure de déconnexion automatique, procédure d ’authentification périodique.
Entité informatique**:**une substitution peut avoir lieu
(surtout en réseau, nécessité de protocoles de sécurité)

L'authentification des personnes peut se faire par trois méthodes:
Ce que connaît l ’utilisateur (Mot de passe),
ce que détient l ’utilisateur (carte…),
ce qu ’est l ’utilisateur (Méthode biométrique)

CE QUE CONNAÎT L ’UTILISATEUR

Le mot de passe, le code confidentiel.Technique la plus simple et la plus répandue

Problèmes bien connus:

- Si le mot de passe est simple il peut être trouvé par une attaque par dictionnaire
- Si le mot de passe est compliqué l’utilisateur le note pour s’en souvenir !

Quelques parades:

- **Ne jamais utiliser** son login, son nom, le nom de son chien, son n°de tél., un mot d’un dictionnaire…Utiliser chiffres et lettres avec des caractères spéciaux au moins 6 à 7 caractères, mais trouver un mémotechnique
- **Obliger l'usager à changer** régulièrement de mot de passe.
- **Surveiller les tentatives d'accès** illicite par comptage (les afficher).
- **Prévenir l'usager des connexions** précédentes sur son compte en affichant la date et l'heure (par exemple du dernier accès).

CE QUE DETIENT L ’UTILISATEUR

Un secret matérialisé physiquement

La clé traditionnelle, la carte (magnétique, à code barre, à puce)

Technique simple, répandue.

Les problèmes :

- la perte, le vol du support
- la duplication (plus ou moins facile mais toujours possible)

CE QU ’EST L ’UTILISATEUR

les méthodes bio métriques

Une solution en rapide développement, peut-être très efficace,souvent onéreuse, peut-être difficile à accepter dans certains cas par l'utilisateur

Nécessité d'études approfondies (analyse de la variabilité) du caractère utilisé

- à l'intérieur du groupe humain des usagers autorisés.
- ou dans une population quelconque

Incertitudes des techniques bio métriques

- La variabilité intra-individuelle.
- La variabilité inter-individuelle.

conduisant à deux types d'erreurs possibles:

- Le rejet à tort d'un individu autorisé
- L'acceptation à tort d'une personne non autorisée.

QUELQUES TECHNIQUES BIOMÉTRIQUES À L'ÉTUDE

- L'empreinte digitale
- La vascularisation de la rétine
- La voix
- La géométrie de la main
- Dynamique de la signature
- Dynamique de la frappe clavier
- Empreinte génétique

3 Architecture des systèmes de protection

IMPLANTATION DE LA MATRICE DE CONTRÔLE D'ACCÈS: SYSTÈMES À CAPACITÉS

On appelle liste de **capacités (Capability)** une structure décrivant pour chaque objet O’ la liste des méthodes M_O de O que O’ peut exécuter.

Ceci revient à stocker les droits dans l’environnement de l’objet O qui demande l’opération et donc à stoker la matrice de protection en ligne.

IMPLANTATION DE LA MATRICE DE CONTRÔLE D'ACCÈS: LISTES DE CONTRÔLE D ’ACCÈS

On appelle **liste de contrôle d’accès** (**ACL : Access Control List**) associées à un objet O, une structure décrivant pour chaque objet O’ la liste des méthodes M_O de O que O’ peut exécuter.

Ceci revient à stocker les droits dans l’environnement de l’objet O qui exécute l’opération demandée et donc à stoker la matrice de protection en colonne.

COMPARAISON DES STRATEGIES (1)

Les listes de contrôle vision "centralisée" : ce sont les objets considérés comme serveurs de méthodes qui connaissent les objets client habilités à demander l'exécution d'une méthode.

- Pour créer, modifier ou révoquer un droit il suffit de s'adresser à ce serveur.
- Le serveur doit connaître tous les clients potentiels et tout processus de propagation d'un droit passe par le serveur .

COMPARAISON DES STRATEGIES (2)

Les capacités stockent les droits dans l'environnement des objets appelant une méthode (clients). Un tel objet montre au serveur, lors d'une demande de service, qu'il possède une capacité à faire cette demande.

- Version facilitant la répartition: laisse à chaque objet une capacité de créer et gérer ses droits.
- La révocation d'un droit est une opération complexe, puisqu'il faut à priori invalider le droit dans l'environnement de tous les objets qui le détiennent.

NOTION DE TICKET (PRIVILEGE, CLEF D'ACCES)

Un ticket est une structure qui représente à chaque instant les rôles que joue un objet dans le système.

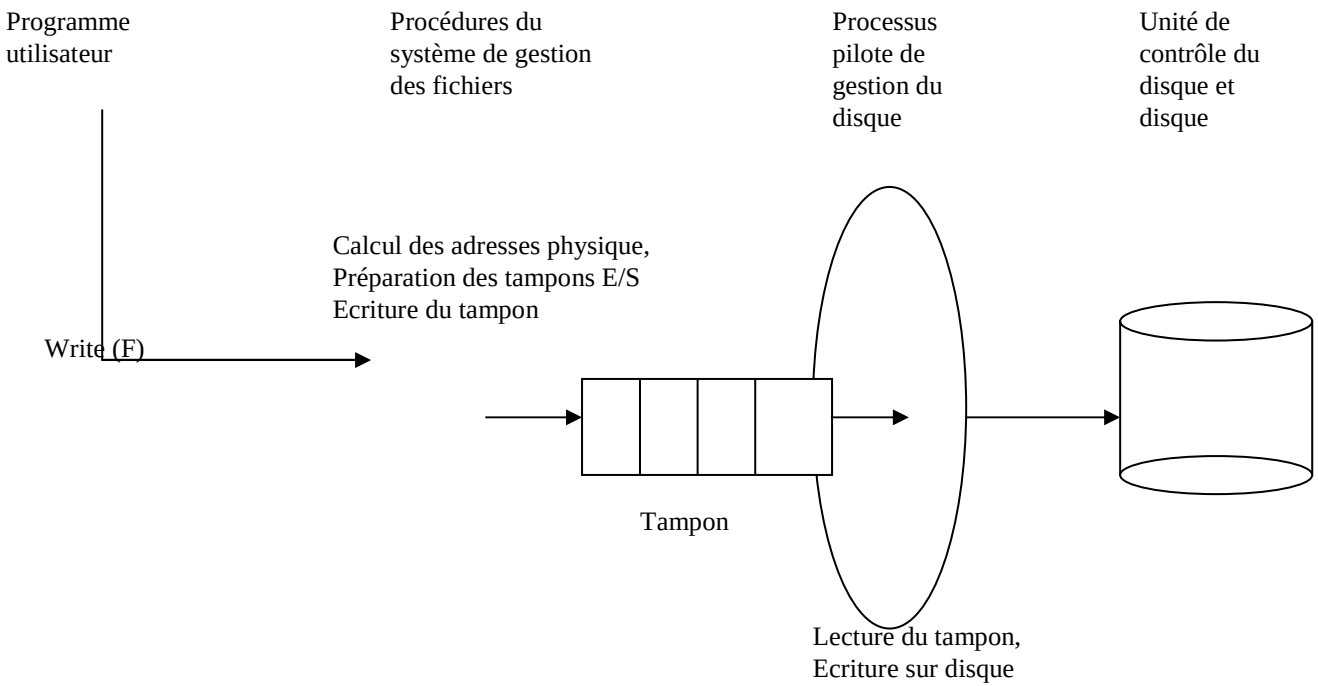
- Comme une capacité, un ticket est intègre et a une durée de vie limité. Il est stocké dans l'environnement de l'appelant.
- Ce n'est pas un droit.
- L'appelé qui, recevant un ticket, consulte une ACL liant les rôles et les droits d'accès. Ceci détermine si l'appelant à ou n'a pas un droit d'exécution.

HIERARCHIE DES MECANISMES DE PROTECTION UN EXEMPLE (1)

Un utilisateur ouvre un fichier de texte sous un éditeur, procède à diverses modifications et écrit (opération enregistrer) une nouvelle version du fichier.

- L'utilisateur doit pouvoir éditer son fichier et donc lire et écrire sur le disque lorsque cela est nécessaire
- Il ne doit pas pouvoir lire ou écrire sur des fichiers qui ne lui sont pas accessibles et de façon plus générale accéder à toute zone du disque sans contrôle d'accès.
- Les mécanismes mis en place ne doivent pas pouvoir être contournés pour donner à un autre utilisateur non autorisé un accès un fichier F

HIERARCHIE DES MECANISMES DE PROTECTION UN EXEMPLE (2)



CONTRÔLES À RÉALISER (1)

- Vérifier lors de l’appel au système de fichiers, que l’utilisateur a le droit d’écriture sur le fichier.

Un pirate peut essayer de déposer directement une requête dans le tampon ou exécuter directement une entrée sortie sur le disque.

- Vérifier que seul une procédure système E/S peut écrire sur le tampon et que seul le gestionnaire de périphérique peut faire des E/S physiques

CONTRÔLES À RÉALISER (2)

Un pirate peut tenter de modifier la structure de donnée qui définissent les différents droits. Soit en appelant la procédure qui est normalement utilisée pour modifier les droits, soit en essayant d'accéder directement à cette structure en mémoire.

- Contrôler le droit d'exécuter les procédures système et contrôler que seules les procédures systèmes ayant des droits adéquats peuvent accéder en lecture ou en modification aux descripteurs des droits.

Le pirate peut essayer de modifier le code exécutable qui assure l'un des contrôles pour le rendre plus permissif.

- Contrôler que tous les éléments de code critique ne peuvent être modifiés en mémoire.

NECESSITE DE LA HIERARCHIE DES MECANISMES

Si (Condition) Alors autoriser action

Un virus pourrait modifier un tel programme de contrôle d ’accès:

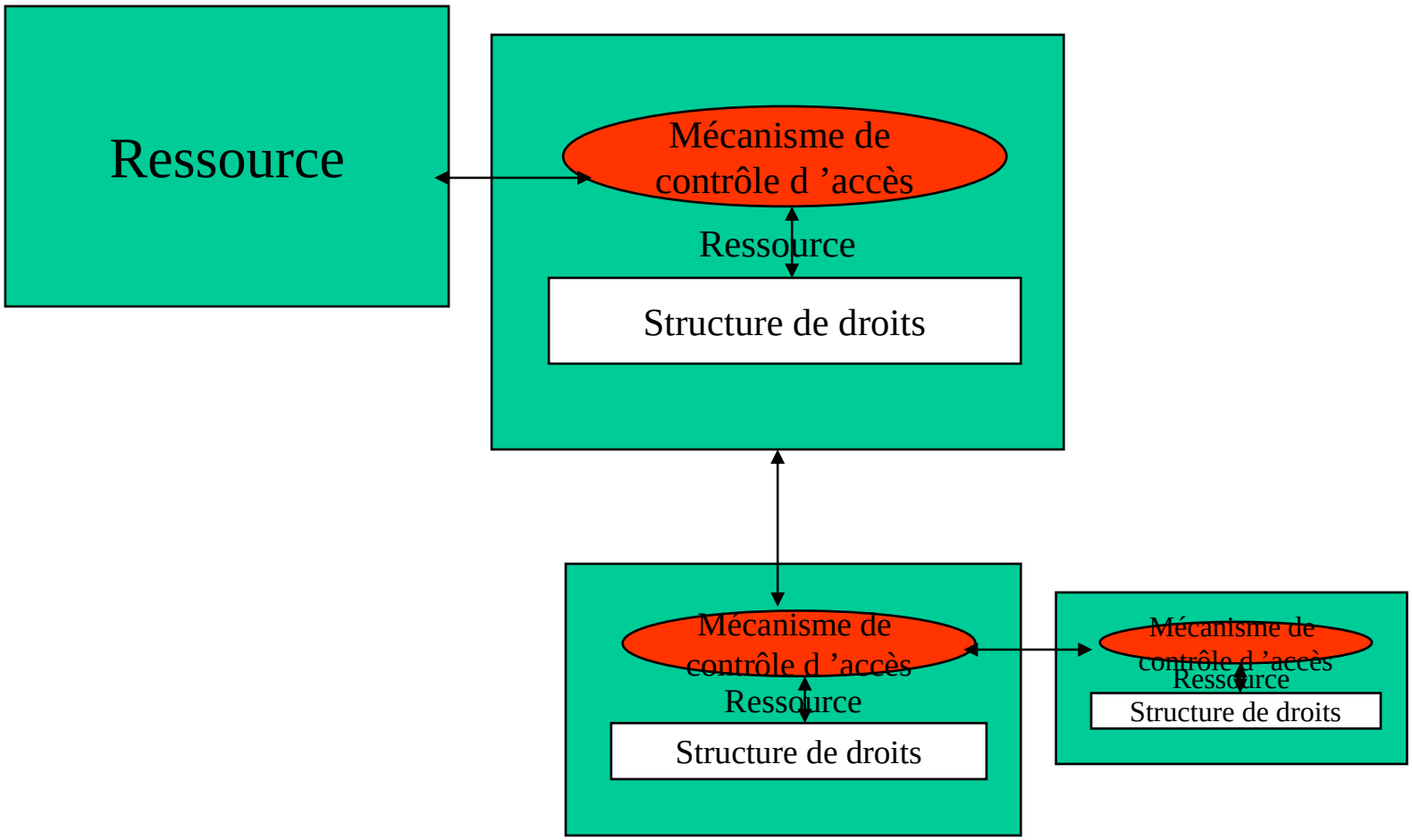
Si c ’est moi Alors autoriser l ’action

Le maillon faible est l’élément le plus bas : celui qui peut modifier les mécanismes qui servent à contrôler tous les contrôles peut tout modifier.

Ces mécanismes ne doivent pas pouvoir être modifiés par une opération logicielle : *seule une intervention physique sur le matériel doit permettre d’altérer ces mécanismes*.

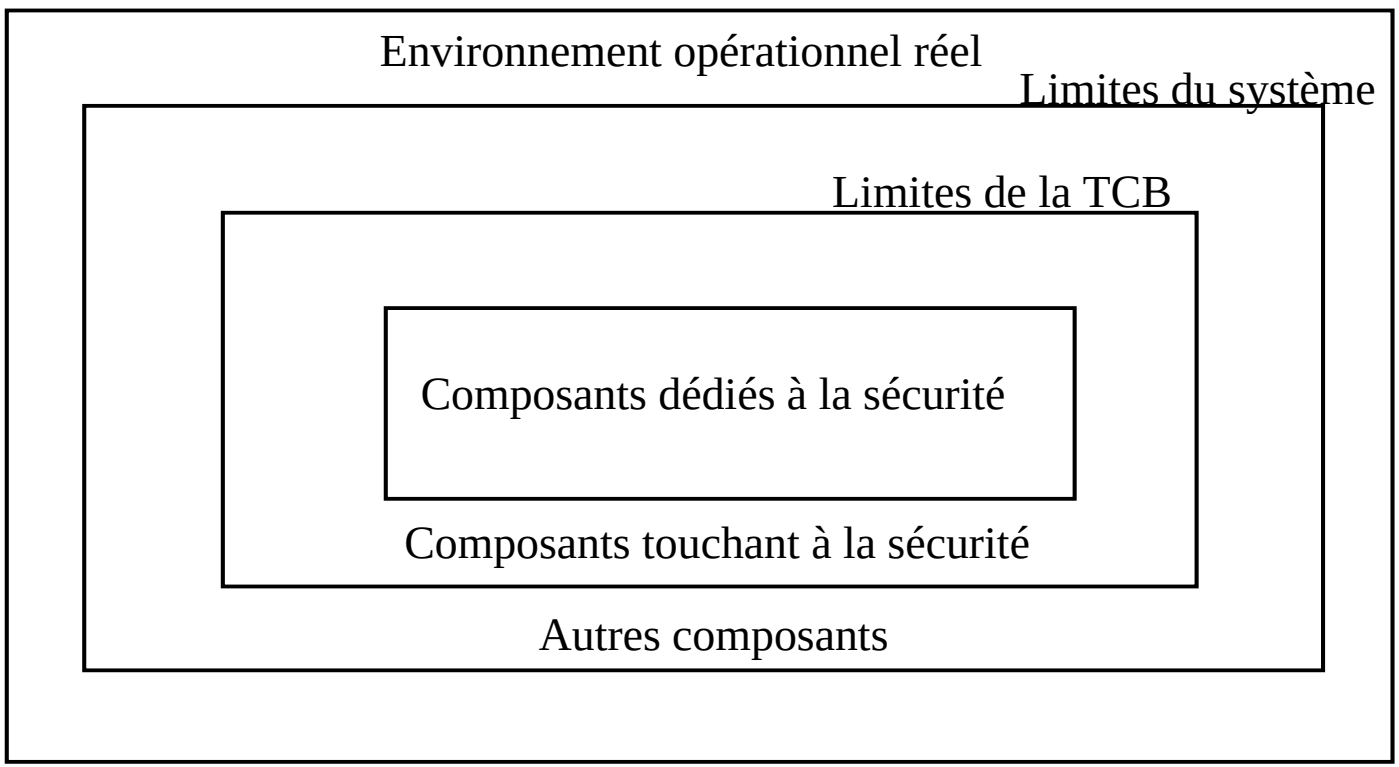
On est ramené à des problèmes de sécurité physique et organisationnelle : qui a accès aux ordinateurs.

HIERARCHIE DES MECANISMES



NOYAU DE SECURITE
ET
MONITEUR DE REFERENCE (1)

L'implantation des mécanismes de sécurité est basé sur une hiérarchie des fonctions (ITSEC)



NOYAU DE SECURITE
ET
MONITEUR DE REFERENCE (2)

Les composants dédiés à la sécurité reposent sur un moniteur de sécurité qui va assurer le contrôle d'accès. Celui ci constitue les niveaux de contrôle de la hiérarchie de protection

Le moniteur doit être

- **inviolable,**
- **incontournable,**
- **correct (par rapport à un ensemble de propriété permettant d'implanter des politiques de sécurité)**

Le moniteur de référence est le "méta guichet" qui permet de gérer des guichets et les droits d'accès aux guichets

NOYAU DE SECURITE
ET
MONITEUR DE REFERENCE (3)

Un moniteur de référence est construit selon une hiérarchie de mécanismes dont l'étanchéité dépend du type d'attaque:

Sur chaque machine il s'agit de mécanismes matériels liés à l'adressage et à l'exécution de certaines instructions. Pour contourner ces mécanismes il faut modifier le matériel:

- Gestion de la mémoire
- Mode d'exécution des processus et contrôle d'accès aux instructions privilégiées
- Code en mémoire morte
- Système matériel d'authentification (lecteur de carte à puces par exemple)

En outre ans un système réparti, une partie du moniteur est composé de protocoles de sécurité

MECANISMES MATERIELS POUR LE NIVEAU BAS

• Les instructions de base de la machine et des périphériques ne doivent pas pouvoir être modifiées. Plus cette notion sera étendue plus facile sera la protection. (utiliser des périphériques spéciaux pour réaliser les opérateurs cryptographiques.)

• Le code d'initialisation du système et les structures définissant les droits de base non modifiables implantés en mémoire morte.

• La mémoire centrale doit être segmentée. Lors de l'exécution de chaque instruction le processeur doit vérifier, selon la nature de l'instruction, si le processus appelant a le droit d' exécuter, lire ou écrire sur chaque segment de mémoire référencé.

•Le droit d'exécuter certaines instructions de base de la machine (comme les accès physique au périphériques) peut être également contrôlé lors de chaque appel (peut être remplacé par une utilisation fine de la mémoire et du chargement: n'accorder le droit d'exécution sur un segment de mémoire contenant des instructions privilégiées qu'à des processus privilégiés).

MACHINES A ANNEAUX DE PROTECTION (1)

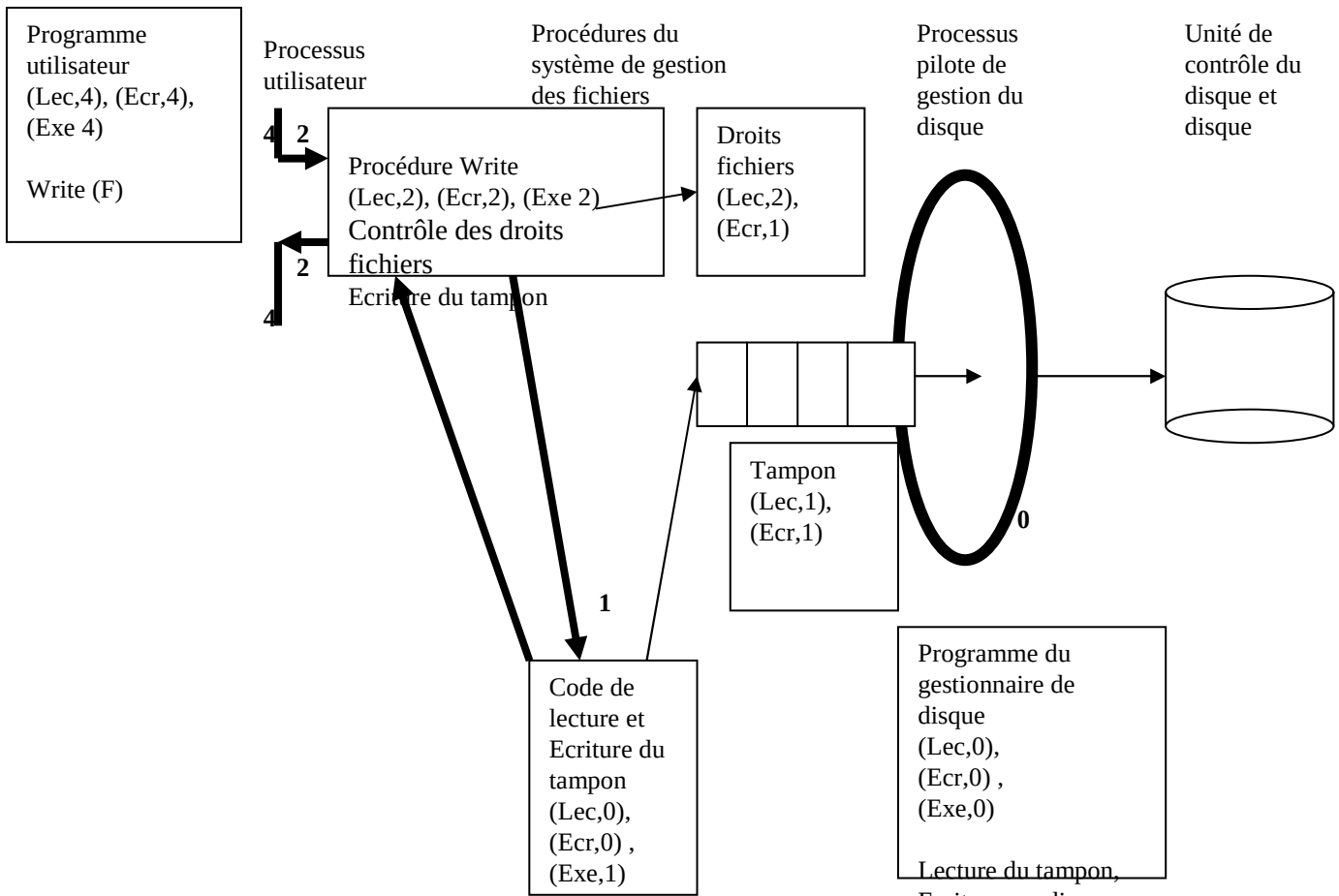
A chaque instant un processus s'exécute dans un contexte donné, les contexte étant hiérachisés (Anneaux de protection)
Un niveau est associé à chaque instruction machine et à chaque référence mémoire (segment ou page)

Certaines instructions ne sont exécutables que dans le domaine le plus privilégié, en particulier celles qui définissent le droit d'accès à une référence mémoire en lecture, écriture ou exécution.

MACHINES A ANNEAUX DE PROTECTION (2)

- L'appel d'une opération (type d'instruction, référence mémoire) implique le contrôle du droit d'accès à l'instruction ou à la référence (le niveau d'appel doit être supérieur ou égal à celui de l'objet référencé). Sinon il y a déroutement.
- Le déroutement provoque un accès à un guichet : Il doit s'agir d'un appel à une instruction privilégiée de changement d'anneau, qui va provoquer l'exécution d'un code de contrôle du droit dans le domaine appelé et une acceptation ou un rejet.

MACHINES A ANNEAUX DE PROTECTION (3)



MACHINES A DOMAINES

A un objet est associé un espace qui lui soit propre : son **domaine** de protection.

- Tant que l'exécution du code de cet objet référence des adresses qui sont situées dans son espace propre, il ne se passe rien de particulier.
- Dès que l'objet référence une adresse à l'extérieur de son espace, il y a déroutement de l'exécution et vérification du fait que la référence externe est une demande d'exécution d'une méthode d'un autre objet. Si ce n'est pas l'instruction n'est pas réalisée.
- Dans le cas contraire, il y a copie des paramètres d'appel du domaine de l'appelant vers le domaine de l'appelé. Et d 'une capacité à exécuter la méthode.
- La première opération que réalise la méthode appelée est de vérifier la validité de la capacité. Si celle si est valide la méthode est exécutée.

PROPRIETES DES CAPACITES

- Elle doit être intègre : seul l'objet qui peut donner un droit doit être capable de la fabriquer ou de la modifier,
- Elle doit avoir une portée limitée soit en terme du nombre d'exécutions de la méthode qu'elle autorise soit en terme de durée.
- Elle doit permettre de déterminer si le détenteur de la capacité a le droit de propager le droit contenu dans la capacité et dans quelle limite.
- En principe elle ne doit pas pouvoir être copiée.

IMPLANTATION DES CAPACITES

- Dans les machines à capacités propriétés sont assurées par un mécanisme partiellement matériel et partiellement logiciel qui gère les capacités dans un domaine propre.
- Dans un système réparti une capacité est un élément du message transmis par l'appelant signé par l'objet qui est habilité à délivrer les droits.

  Peut comporter des indications de limite de validité et de droit de propagation.

  L'appelant peut également signer le message complet permettant son authentification par l'appelé.

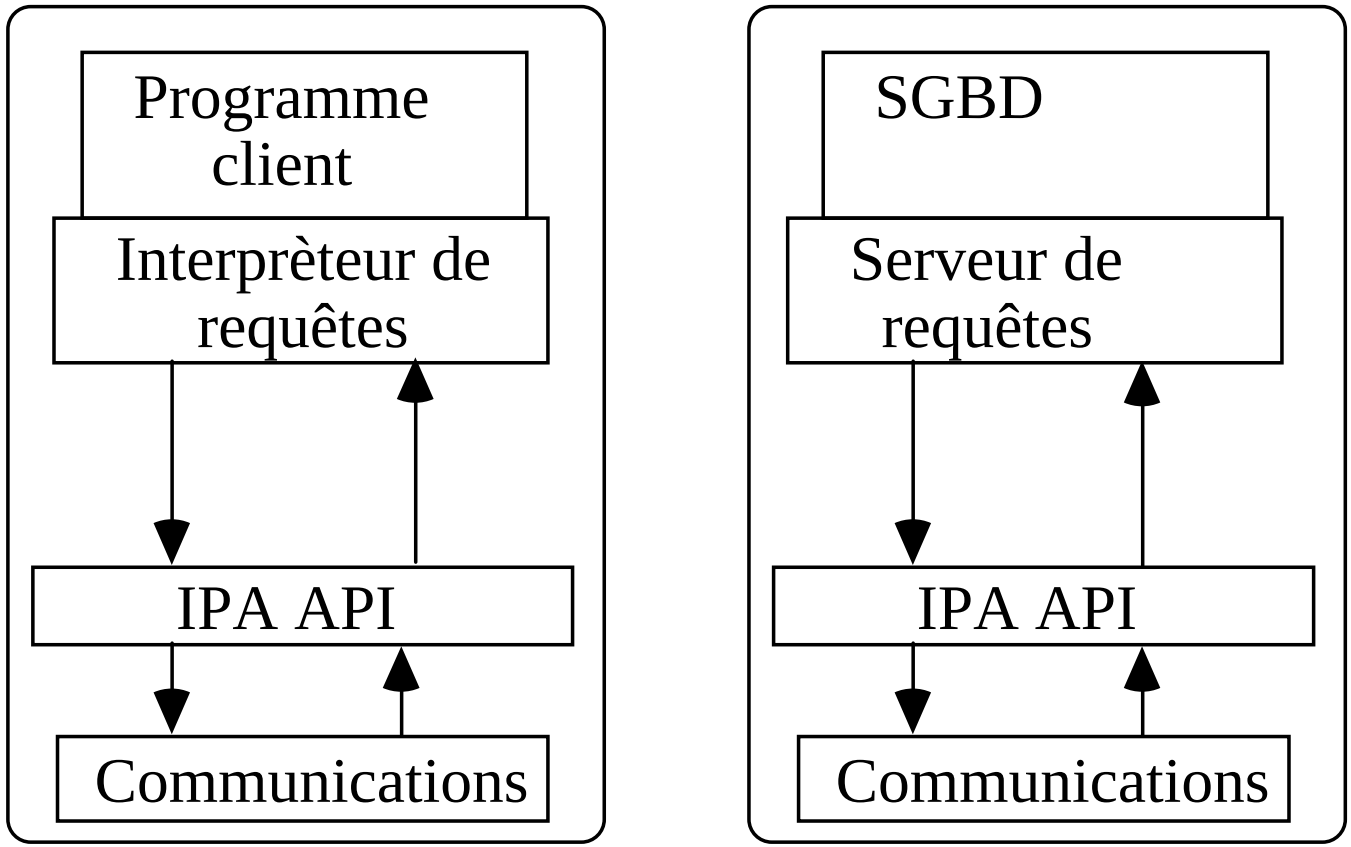
  Cette solution a pratiquement toutes les propriétés requises, mais ne permet pas d'éviter la copie.

L ’APPEL DE PROCEDURE A DISTANCE SECURISE

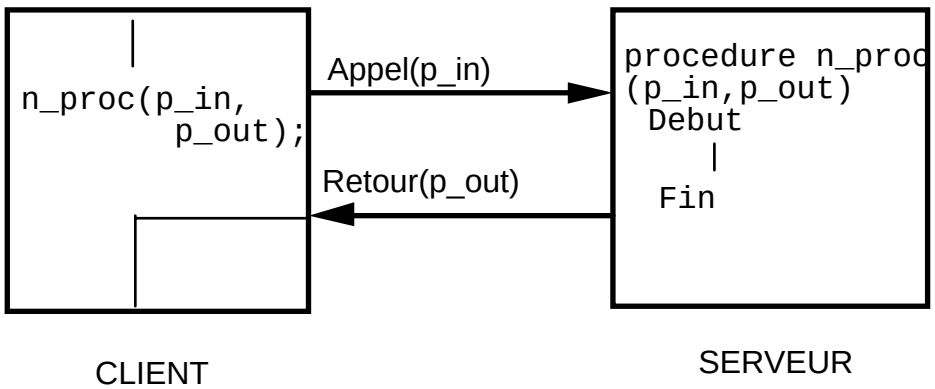
Le service d ’appel de procédure à distance (APD/RPC)

- Présentation **syntaxique et sémantique** du mécanisme précédent **en terme d'appel de procédure distante.**
- A travers un API simulant l ’appel de procédure local:
  - synchrone
  - sans mémoire

Les API client/serveur



Fonctionnement de l ’APD



La souche client

C’est la procédure d’interface du site client:

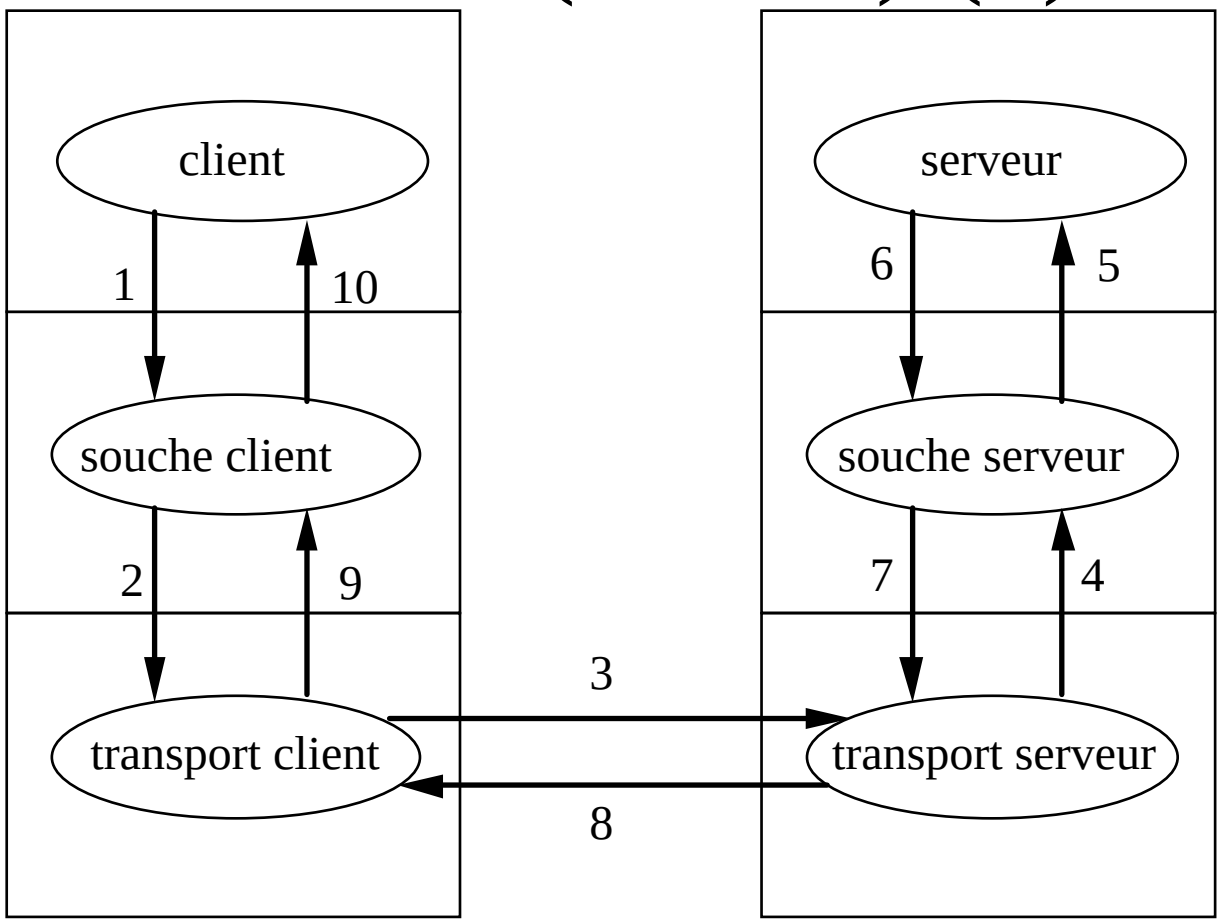
- qui reçoit l’appel en mode local
- le transforme en appel distant
- en envoyant un message.
- reçoit les résultats après l'exécution
- retourne les paramètres résultats comme dans un retour de procédure.

La souche serveur

C’est la procédure sur le site serveur qui:

- reçoit l’appel sous forme de message,
- fait réaliser l’exécution sur le site serveur par la procédure serveur
- retransmet les résultats par message.

Implantation de l ’APD par souches (STUB) (1)



Détails des étapes (1)

Étape 1

- Le client réalise un appel procédural vers la procédure souche client.

- La souche client collecte les paramètres , les assemble dans un message **(“parameter marshalling”).**

Étape 2

- La souche client détermine l’adresse du serveur.

- La souche client demande à une entité de transport locale la transmission du message d'appel.

Étape 3

- Le message est transmis sur un réseau au site serveur.

Détails des étapes (2)

Étape 4

- Le message est délivré à la souche du serveur.

Étape 5

- La souche serveur désassemble les paramètres, et réalise l'appel effectif de la procédure serveur.

Étape 6

- La procédure serveur ayant terminé son exécution transmet à la souche serveur dans son retour de procédure les paramètres résultats.La souche serveur collecte les paramètres retour, les assemble dans un message ("parameter marshalling").

Détails des étapes (3)

Étape 7

- La procédure souche serveur demande à l'entité de transport locale la transmission du message.

Étape 8

- Le message est transmis sur un réseau au site client.

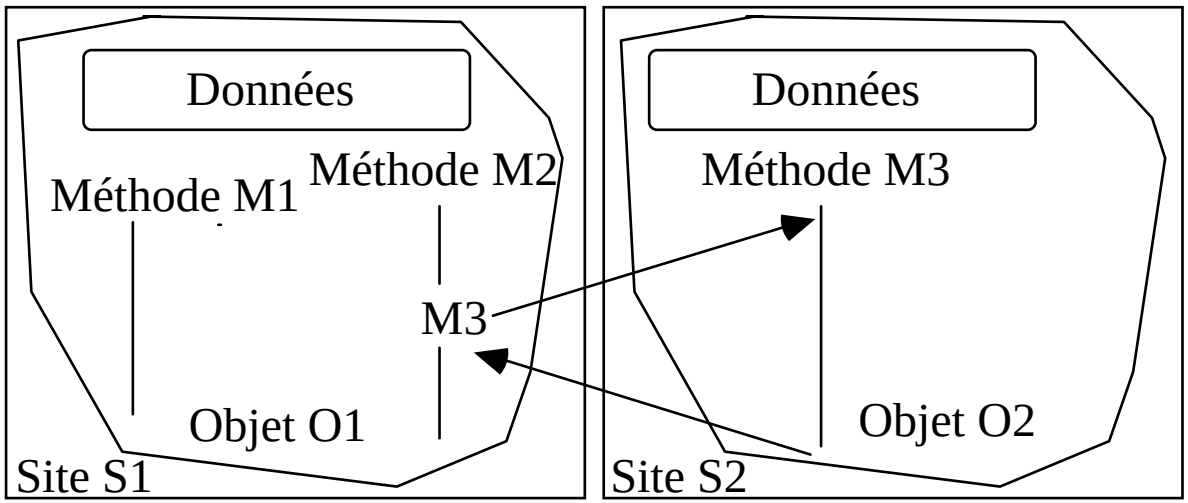
Étape 9

- Le message est délivré à la souche du client. La souche client désassemble les paramètres retour.

Étape 10

- La procédure souche client transmet les résultats au client en effectuant le retour final de procédure.

Objets répartis



Objectifs de l ’APD sécurisée

- Répartir la notion de machine à domaines
- En utilisant des messages de capacités ou de ticket
- Eventuellement dans un contexte d ’objets répartis
- Les étapes de l ’APD incluent des fonctions de sécurité

Etapes 1 de l ’APD Sécurisé

Etape 1: L ’appel provoque un déroutement local car c ’est une référence hors du domaine de l ’appelant.

L ’appelant passe une capacité (ou un ticket) avec les paramètres d ’appel

Etape 2, 3 et 4 de l ’APD Sécurisé

La souche client ouvre une connexion sécurisée avec la souche serveur, avec authentification des deux entités, protection en intégrité et éventuellement en confidentialité (SSL par exemple)

Les paramètres et la capacités sont transmis sur cette connexion

Etapes 5 et 6
de l ’APD Sécurisé

La souche serveur appelle l’objet local en passant la capacité ou le ticket

L ’objet local contrôle les droits et exécute la méthode

Etapes 8, 9 et 10 de l ’APD Sécurisé

La souche serveur ouvre une connexion sécurisée avec la souche client, et retourne les paramètres