Introduction à la sécurité des réseaux et des systèmes d'information

Prof A. Chouarfia

Faculté des Mathématiques et Informatique

USTO-MB Oran

Novembre 2010

Sommaire

Prof A. Chouarfia USTO-MB
Faculté FMI
Novembre 2010

Introduction

- **Le réseau: système support avec ses caractéristiques matérielles (switch, routeurs,…) et logicielles (protocoles)**
- **Le système d'information: systèmes d'exploitation et applications diverses et variées**
- **La sécurité informatique: Ensemble de moyens mis en œuvre pour éviter ou minimiser les défaillances naturelles dues à l'environnement ou au défaut du système d'information et les attaques malveillantes intentionnelles dont les conséquences sont catastrophiques .**

Sûreté Vs Sécurité

- Sûreté de fonctionnement (Safety)

- Sécurité de fonctionnement (Security)

Solutions

- Solutions pour le réseau système support: FireWall, VPN , Solutions sécurisées

- Solutions pour le système d'information: Approches de développement, Modèles de développement, Méthodes de développement, revue de code, analyse statique et dynamique du code, etc.…

Sécurité informatique

1-Recherche du risque sécurité dans la chaîne de développement et/ou de production en utilisant des méthodes appropriées

2-Inspection des différents éléments de sécurité mis en œuvre lors du cycle de développement ou de production (ISO17799)

3-Préparation aux certifications BS7799

Minimisation des risques

- Entreprise classique: Estimer le coût du risque et le coût de sa protection

- Entreprise industrielle sensible(systèmes temps réel):Classifier les risques de pannes en

  * Pannes catastrophiques qui ne devraient pas se produire => prévoir des techniques très sévères de validation/certification.

  Mise en service d'un système si et seulement si une 'confiance' (fiabilité) très élevée lui est accordée

  * Pannes non catastrophiques dont il faut estimer le coût de protection

1.2 Conséquences d'une sécurité non maîtrisée jusqu'à 2010

- Perte de temps (réinstallation de systèmes)
- Perte de données (réécriture ou régénération des données perdues)
- Domaines informatiques

  -Détournement d'argent

  - Faillite d'entreprise

  - Echec de tir d'une navette spatiale

  - Panne de courant électrique paralysant une région

1.2 Conséquences d'une sécurité non maîtrisée à partir de 2010

- Les applications reposeront sur l'authentification numérique (signature électronique ou biométrie)

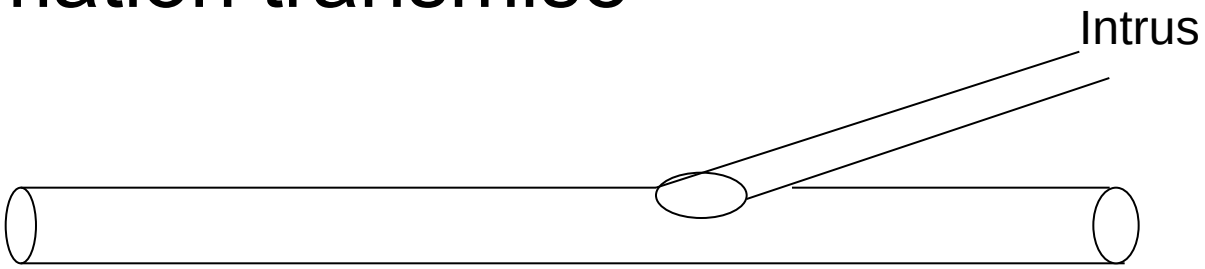
Dépendance des systèmes électroniques, nous n'existons plus si le système électronique ne reconnaît pas notre signature

Répartition des causes

- 26% accidents(incendies, inondations,catastrophes naturelles,pannes,force majeure)
- 17% erreurs humaines et défauts de qualité(conception,utilisation,prévention)
- 57%malveillance à 80% d'origine interne(vol d'équipement, copies illicites, vengeance, intrusion et écoute, etc.…)

Scénario d'une attaque

1-Insertion d'une bretelle par l'intrus lui permettant de lire et/ou modifier l'information transmise

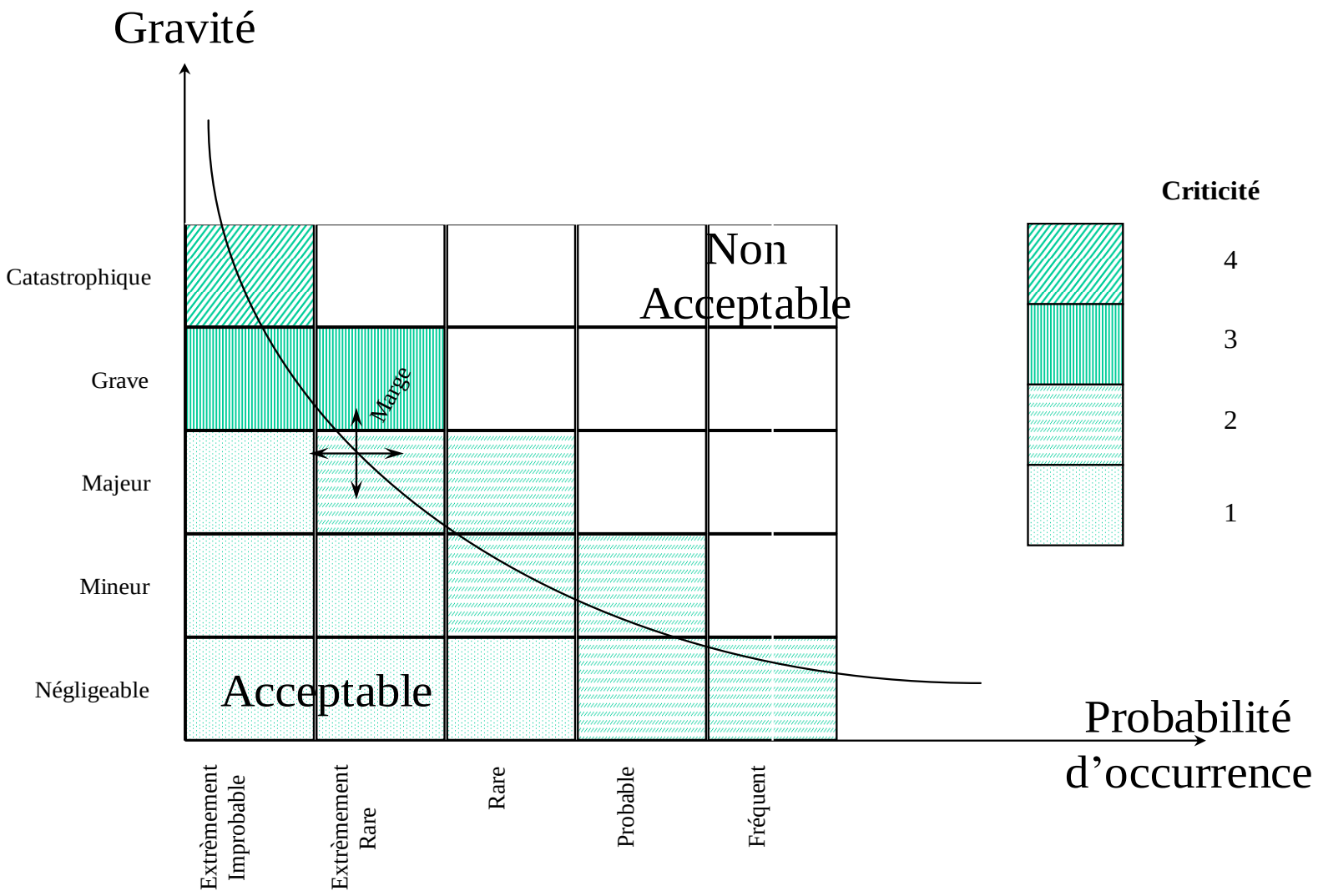


2- Système multi-sessions ou questions/réponses

1.3 Niveaux de gravité et niveaux de probabilité d'occurrence

- Le niveau de gravité est échelonné sur cinq niveaux: négligeable, mineur, majeur, grave et catastrophique

- Le niveau de probabilité est aussi échelonné sur cinq niveaux: extrêmement improbable, extrêmement rare, rare, probable et fréquent


Gravité
Catastrophique
Grave
Majeur
Mineur
Négligeable
Non Acceptable
Acceptable
Marge
Criticité
4
3
2
1
Extrèmement Improbable
Extrèmement Rare
Rare
Probable
Fréquent
Probabilité d'occurrence

1.4 Dispositions juridiques

Cas de jurisprudence

Des actions informatiques entraînent des obligations légales de responsabilité, elles sont considérées comme valides juridiquement

Exemples:

- Ordre de virement électronique: 2 fois le même ordre de virement doit être honoré
- Commande par internet
- Utilisation de la signature électronique (Conseil de l'UE du 28/6/99)

Cadre juridique

- Nécessité de formalité préalable pour toute information nominative (collecte, enregistrement, conservation et non divulgation)
- Contrefaçons et droits d'auteurs (copie autre que pour sauvegarde)
- Exercice de droit d'accès et dispositions pénales de non respect (ex: dossier médical)
- Entrave au fonctionnement d'un système
- Accès frauduleux aux données
- Introduction de données

Règles d'usage de la cryptographie

- Demande d'autorisation concernant la confidentialité
- Déclaration concernant l'authentification et l'intégrité

Prof A. Chouarfia USTO-MB
Faculté FMI
Novembre 2010

Cas de la France (SCSSI)

- Libre utilisation des moyens de chiffrement de moins de 128 bits, ceux de plus de 48 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 ayant des clefs supérieures à 128 bits
- Demande d'autorisation pour l'exportation des produits de chiffrement

2 Système d’information d’abord

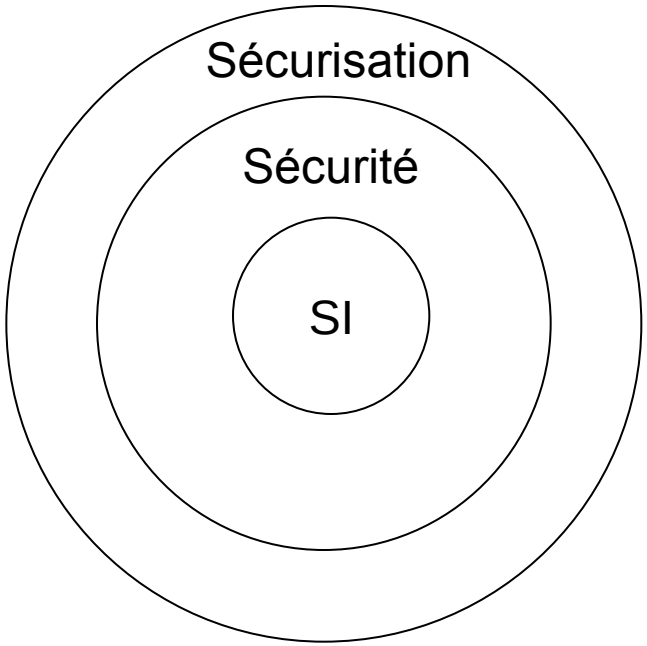
Prof A. Chouarfia USTO-MB
Faculté FMI
Novembre 2010

2.1 Similitude entre maintenance et sécurité

- Projeter en pensant maintenance
- Spécifier en pensant maintenance
- Concevoir en pensant maintenance
- Réaliser en pensant maintenance

- Projeter en pensant sécurité si nécessaire
- Spécifier en pensant sécurité si nécessaire
- Concevoir en pensant sécurité si nécessaire
- Réaliser en pensant sécurité si nécessaire

Donc l'entreprise doit avoir une politique de sécurité



L’entreprise doit s’assurer que son système d’information est fiable, sûr pour cela il faut :

- tester le Système d’information
- améliorer sa fiabilité
- gérer sa qualité

2.2 Fondement du test

- Objectif: Arriver à un produit ‘zéro défaut’
- Activité importante: 40%du budget est consacré aux tests
- Un bon test est celui qui met à jour une erreur/anomalie/exception/incohérence non encore rencontré
- Il vaut mieux que ce ne soit pas la même équipe (personne) qui développe et qui teste le produit
- Un test ne peut pas dire ‘qu’il n’y a pas d’erreur’, il teste le logiciel de façon poussive, plus que dans l’utilisation réelle
- Il existe plusieurs techniques de test qui dépendent de l’objectif du test. Aucune technique ne sera jamais complète

2.3 Techniques de test

- Test ‘Boite Blanche’
  - Métriques de McCabe (Structurelles)
    - détermination des chemins minimaux
    - un test par chemin
    - analyseurs statiques/dynamiques
  - Métriques de Halstead (Textuelles)
    - analyseurs statiques
  - Audit du code

- Test ‘Boite Noire’
  - Aspect fonctionnel du programme
  - Partitionnement du domaines en classes
  - Tests aux cas limites de classes

2.4 Fiabilité du logiciel

Probabilité de bien fonctionner (faire une opération) sans panne (arrêt) sur une durée de temps donnée pour un contexte donné

Elle est subjective, elle dépend de l'utilisateur et du contexte d'utilisation

Elle donne une mesure du degré de confiance

Elle mesure les conséquences d'une faute

Faute et défaut

- Une faute est une caractéristique statique du logiciel, elle provoque un défaut à l'exécution.
- Un défaut est du à la présence d'une faute, il est essentiellement dynamique.
- La même faute provoque le même défaut.
- La faute ne provoque pas nécessairement le défaut.

Amélioration de la fiabilité

Paradoxe: Plus on augmente la fiabilité, plus on réduit l'efficacité à cause du code ajouté

Vu la puissance et le prix des calculateurs, la fiabilité est privilégiée, l'efficacité devient de moins en moins nécessaire.

Métriques de la fiabilité

Probabilité d'une panne:

Probabilité que le logiciel se comporte de manière non souhaitée lorsqu'une requête est effectuée

ex: 1 défaut sur 1000 requêtes

Taux de panne:

Fréquence d'apparition d'un défaut

ex: 2 défauts sur 100 unités de temps

Temps moyen entre 2 pannes:

Temps écoulé entre 2 apparitions de défauts

ex: 500 unités de temps

Disponibilité:

Probabilité que le système soit opérationnel, il est tenu compte du temps de réparation éventuel

Unité de temps:

horloge interne pour un système non stop

temps calendaire pour un système à activité régulière

nombre de transactions pour un système fonctionnant à la demande

Classification des défauts

- Transitoire: ne se produit qu'avec certaines entrées
- Permanente: se produit avec toutes les entrées
- Réparable: ne nécessite pas d'intervention humaine
- Irréparable: nécessite une intervention humaine
- Non corruptrice: ne détruit, ni corrompt les données
- Corruptrice: Corrompt les données (**Inacceptable**)

2.5 Gestion de la qualité

- Elle a pour but de donner confiance aux clients pour certifier que le produit livré a une certaine qualité par l'entreprise

  - **Subjective/Relative**

- Elle vise à promouvoir le produit et/ou l'entreprise

- Elle implique
  - l'assurance,
  - la planification de la qualité
  - le contrôle de la qualité

Partie II: Sécurité

- Contexte d'économie mondialisée, les entreprises font aujourd'hui souvent évoluer leur organisation afin de se structurer par métier et non plus par pays
- Déploiement à l' échelle internationale implique une ouverture et une exposition davantage plus grande aux risques
- Information = ressource abstraite, impalpable, qui a de la valeur, à la fois difficile et facile à détourner
- Réseau Internet non sécuritaire, les indus accès sont aisés

Impact fort sur le management de la sécurité

La plupart des problèmes de sécurité sont le fait de personnes d'horizons divers, malintentionnées, intelligentes, ayant des moyens matériels et financiers illimités

Exemples:

Etudiant: s'amuser en fouinant dans le courrier électronique des autres ou voulant introduire des contradictions dans un cours en ligne ou encore modifiant les résultas des examens.

Cracker: Tester la sécurité d'un système d'information, dérober des informations

Agent commercial: Prétendre avoir une étendue plus grande ou exclusivité

Homme d'affaires: découvrir la stratégie marketing de ses concurrents

Ancien employé: se venger d'avoir été renvoyé

Comptable: opérer des détournements au détriment d'une entreprise

Espion: s'emparer de secrets militaires ou industriels

Arnaqueur: dérober des numéros de cartes de crédit

Oisif passionné

2.1. Concepts de sécurité

2.1.1 Menaces

Ensemble des actions de l'environnement pouvant entraîner des catastrophes financières, ce sont des résultantes d'actions et d'opérations du fait d'autrui

- Menaces relevant de problèmes non spécifiques à l'informatique: Techniques de protection assez bien maîtrisées

- Pannes et erreurs non intentionnelles: Ensemble des actions non intentionnelles inhérentes au système de sa spécification à son utilisation et sa maintenance peuvent entraîner des pertes financières

- Menaces intentionnelles: Ensemble des actions malveillantes constituant la plus grosse partie du risque qui devraient être l'objet principal de protection

  Menaces passives: atteinte à la confidentialité (prélèvement par copie, écoute de l'information sure les voies de communication, indiscrétions, elles sont souvent indétectable

  Menaces actives: nuisent à l'intégrité des données (modification, déguisement, interposition, virus, ver, etc.…)

Classification des menaces

1- Déguisement: se faire passer pour quelqu'un d'autre

2- Répétition(Replay, rejeu): espionner une interface, une voie de communication pour capter des opérations et obtenir une fraude

3- Analyse de trafic:observer le trafic des messages échangés pour en déduire (deviner) des informations sur des décisions futures

4- Inférence: obtenir des informations confidentielles (non divulgables) à travers des questions autorisées généralement de nature statistique

5- Déni de services: un émetteur ou récepteur affirme n'avoir pas respectivement émis ou reçu un ordre

6- Modification des données, des messages ou des programmes pour s'attribuer des avantages illicites

7- Modification à caractère de sabotage pour détruire des systèmes ou des informations

8- Attaque par saturation

2.1.2 Risques (Larousse)

Risque: danger, inconvénient possible, préjudice, sinistre éventuel

Risquer: (se) hasarder, (s') exposer à un danger

Menace: geste marquant l'intention de nuire, signe qui fait craindre quelque chose

Menacer: faire des menaces, chercher à intimider par des menaces, laisser craindre, laisser présager un risque ou une peur

Risques accidentels indépendants de tous les facteurs de l'entreprise

Risques structurels dépendants de l'organisation de l'entreprise

Classification des risques

- Acceptables: pas de conséquences graves sur l'entreprise (panne électrique, perte de liaison, congestion momentanée sur un réseau
- Courants: pas de préjudices graves, on peut réparer facilement (mauvaise configuration, erreur d'administration de réseau, etc.…)
- Majeurs: dus à des facteurs graves causant de gros dégâts mais récupérables (panne sèche d'un routeurs, perte des transactions d'une journée ou d'une semaine, etc.…)
- Inacceptables: fatales pour l'entreprise, ils peuvent entraîner le dépôt de bilan (perte d'information importante ou corruption, etc.…)

2.1.3 Sensibilité/vulnérabilité

Sensibilité: plus l'information est stratégique, plus elle a de la valeur, plus elle doit être confidentielle et plus elle est sensible

Vulnérabilité: Degré d'exposition au danger (on peut parler de fragilité, de faiblesse, de pauvreté du système de protection)

Le risque est estimé (apprécié) en fonction de la sensibilité et de la vulnérabilité

2.2 Avoir une de Politique de Sécurité (ISO17799)

1- être conscient des risques et des menaces éventuelles, de la nature de ces derniers et de la force des attaquants éventuels

2- délimiter le problème de sécurité ou de l'application
- Qui est concerné par la sécurité
- Où et à quel moment particulier, la sécurité doit s'appliquer

3- organiser la sécurité: établir des règles qui fixent les actions autorisées et interdites par les personnes et les systèmes

4- évaluer le coût d'une éventuelle attaque

5- choisir les contre-mesures adéquates

6- évaluer les coûts des contre-mesures

7- décider de mettre en oeuvre

ISO-17799

L'ISO-17799 présente un ensemble d'objectifs de sécurité très généraux et d'ordre théorique, et des bonnes pratiques concrètes à mettre en œuvre pour les atteindre

L'application de la norme peut être le résultat d'une série d'étapes:

1- que protéger et pourquoi? → liste des biens sensibles

2- de quoi les protéger? → liste des menaces

3- quels sont les risques? → liste des impacts et probabilités

4- comment protéger l'entreprise? → Liste des contre-mesures

ISO-17799 :Communication

Du représentant de la sécurité

A la direction générale:

- le besoin d'établir une politique de sécurité inspirée de l'ISO-17799

- la conformité des mesures de sécurité par rapport au cadre de la norme et des caractéristiques de l'entreprise

Aux restes de l'entreprise

- la sensibilisation des services et des personnels sur les meilleurs pratiques de la sécurité

- le bien fondé des mesures de sécurité à mettre en place

ISO-17799: Communication

De l'Entreprise à ses partenaires

- la cohérence de la démarche sécurité de l'entreprise avec la norme ISO-17799

- le bien fondé d'imposer des exigences de sécurité cohérentes avec la norme ISO-17799

Objectif : Marketing

2.3 Propriétés liées à la sécurité

2.3.1 Problématique

Assurer la sécurité informatique, relativement à une politique de sécurité, consiste à garantir que, à chaque instant, toutes opérations sur les objets informatiques (ressources matérielles et/ou logicielles) ne sont réalisables et réalisées que par des entités humaines ou informatiques (processus) habilitées.

Les bases de la réalisation de la sécurité sont:

Le confinement:

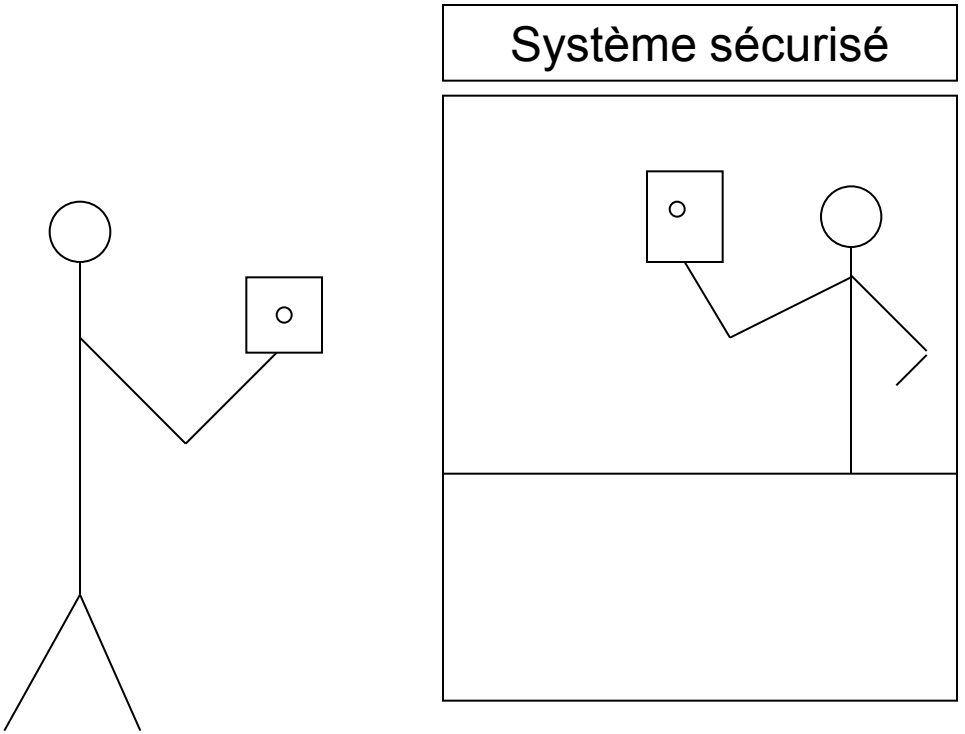
l'ensemble des objets sont maintenus dans des domaines étanches ainsi une entité ne peut interférer avec une autre à la suite d'une erreur volontaire ou involontaire.

exemple: violation d'espace mémoire d'un autre utilisateur.

Le principe du moindre privilège:

Pour qu'un système fonctionne en sécurité, il faut donner à ses utilisateurs exactement les droits dont ils ont besoins, ni plus ni moins.

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 un certificat attestant ses droits pour réaliser l'opération,

Elle réalise l'opération.

2.3.2 Propriétés

Confidentialité des données: elle assure que seules les entités habilitées, dans des conditions prédéfinies, ont accès aux informations

* droit de propriété d'une entreprise
  - des secrets de fabrication
  - des informations stratégiques

* droit des individus défini par la loi

* dossier médical

* dossier judiciaire

Intégrité des données:

elle assure que seules les entités habilitées, dans des conditions prédéfinies, peuvent modifier les données. Une modification doit maintenir le système d'information dans un état cohérent (vérification des contraintes d'intégrité)

Attention aux modifications temporaires

Authentification:

- elle assure que seules les entités autorisées ont accès au système,
- elle protège de l'usurpation d'identité, l'entité est reconnue à travers sa signature
- elle est un moyen clé de la sécurité pour assurer

    * la confidentialité:celui qui lit, modifie, exécute, crée ou détruit est bien celui dont le nom figure dans le certificat d'authentification

    * l'intégrité: celui qui lit, modifie, exécute, crée ou détruit est bien celui dont le nom figure dans la trace de l'opération

Pérennité:

elle caractérise le bon fonctionnement du système d'information, elle est estimée par

- la disponibilité: aptitude d'un système informatique à pouvoir être utilisé à un instant donné

- la fiabilité: aptitude d'un système d'information à fonctionner correctement de manière continue pendant une période de temps (quantité) donnée.

Rappel: les attaques de sabotage visent à rendre le système indisponible ou moins fiable

Auditabilité:

elle assure la capacité à détecter et à enregistrer de façon infalsifiable les tentatives de violations de la politique de sécurité

Non répudiation:

elle assure que l'auteur d'un acte ne peut nier l'avoir effectué.

une entité, à travers sa signature, est d'abord authentifiée et s'engage à honorer sa signature.

l'engagement est contractuel et juridique, l'entité ne peut pas revenir en arrière.

2.4 Mise en œuvre d'une politique de sécurité

2.4.1 les moyens

Avoir les moyens de sa politique

- **moyens organisationnels et procéduraux**:
  ensemble de règles qui doivent être mises en place et respectées

- **moyens matériels ou physiques**:
  architecture des bâtiments, les systèmes de contrôle d'accès,
  les destructeurs de documents, etc.…

- **moyens informatiques**:
  cryptographie: ensemble de méthodes de chiffrement
  cryptanalyse: ensemble de méthodes de casser le chiffrement

2.4.2 Caractéristiques des moyens

- **complets** dans le cadre des hypothèses considérées, quoiqu'il arrive, la politique est respectée,

- **complémentaires** entre eux et non contradictoires,

- **raisonnablement contraignants:** ils ne doivent pas constituer un obstacle à la réalisation d'une opération donnée prévue de l'entreprise,

- **homogènes** entre eux par rapport aux risques et aux attaques considérés (il est inutile de chiffrer tous les documents qui sortent de l'entreprise, s'ils partent en clair à la poubelle)

2.4.3 Caractéristiques des guichets d'accès

- être capable de vérifier la propriété de confidentialité
- être capable de vérifier la propriété d'intégrité des données
- être capable de vérifier la propriété d'authentification des entités et des guichets
- être capable de vérifier la propriété de non répudiation
- être capable de vérifier la propriété d'auditabilité
- être capable de vérifier la propriété de pérennité

- Pour pouvoir administrer un système sécurisé, il faut donner la possibilité de
  - Gérer les entités(personnes, processus,machine du réseau) par la création, la nomination, et la destruction de ces entités et par leurs données d'authentification,
  - Gérer les guichets incontournables et les données d'authentification de ces guichets
  - Gérer les droits d'accès de chaque entité

2.4.4 Modélisation du contrôle d'accès

Matrice de contrôle d'accès

pour une entité donnée et une ressources donnée, des autorisations (lecture,écriture, propriétaire, création, destruction) sont définies

Machines à anneaux (cas de VMS)

à chaque instant un processus s'exécute dans un contexte donné, les contextes étant hiérarchisés (anneaux de protection), un niveau est associé à chaque instruction machine et à chaque référence mémoire

Machines à domaines

chaque objet s'exécute dans un espace d'adressage propre (domaine). Les appels à l'intérieur du domaine ne sont pas contrôlés. Tout appel à l'extérieur du domaine est réalisé par passage de paramètres par valeur et passage d'une capacité (identité, droits).

Le domaine appelé contrôle la capacité avant d'exécuter la méthode et retourne le résultat par valeur

Sécurisation d'un réseau

1- sécuriser le routeur en autorisant que les services utiles pour l'entreprise

2- journaliser les transactions(@E, @D) mais pas les données, l'objectif est de retrouver la trace pour tout éventuel recours administratif

3- contrôler l'accès au routeur (l'idéal est qu'il ne soit pas configurable à distance)

FireWall (pare-feu)

Définition: **c'est un système ou ensemble de systèmes qui renforce la politique de sécurité d'une entreprise et Internet. C'est un mécanisme de filtrage des entrées de l'extérieur vers le réseau**

Le firewall détermine:

- quels services internes peuvent être accédés de l'extérieur,
- quels éléments extérieurs peuvent accéder aux services internes autorisés
- quels services externes peuvent être accédés par les éléments internes

Avantages d'un firewall

1- Il concentre la sécurité réseau en un seul point, à partir de ce point, l'administrateur réseau pour protéger le réseau dans sa totalité.

2-Il permet la génération d'alarmes et de monitoring, il est impératif que l'administrateur réseau évalue régulièrement le trafic pour s'assurer qu'il n'a pas été contourné ou cracké.

3- Il est l'endroit idéal pour monter un NAT.

4- Il est l'endroit parfait pour déployer un serveur WWW ou FTP ou autre. Il peut être configuré pour permettre l'accès à certains services tout en prévenant l'accès aux autres services du réseau privé.

5- Il est un point unique de panne, le réseau local continuera à fonctionner.

Limites du firewall

1-Cible privilégiée pour être saturé (étouffé) et mis hors service.

2- Il ne protège pas contre les attaques qui ne passent pas par lui.

3-Il ne prévient pas contre les fichiers infectés, il est difficile d'inspecter tous les fichiers entrants d'où l'utilité d'installer les antivirus sur les stations.

4- Supposons que le firewall bloque tous les fichiers ;doc de sortir, il suffit de les transformer en un autre format pour les faire sortir.

2.5.2 Les passerelles

Un code dédié, appelé service proxy) est installé sur la passerelle pour chaque application voulue (Telnet, WWW,…), il permet le filtrage au niveau de la couche application du modèle OSI.

L'utilisateur externe a accès au service proxy de manière transparente sans avoir accès à l'adresse IP de la passerelle.

Le service proxy intercepte la requête, il se connecte lui-même sur la passerelle et joue l'intermédiaire entre l'utilisateur et le serveur concerné.

Le service proxy peut être configuré suivant des règles prédéfinies par la politique de sécurité par l'administrateur réseau.

Avantages des passerelles

- La passerelle donne un contrôle complet sur chaque service par la restriction sur les commandes utilisables et l'accès aux hôtes internes par ces services.

- Un service est complètement bloqué si son service proxy est absent.

- L'administrateur a un parfait contrôle des services disponibles et des services non disponibles.

- Possibilité d'installer des procédures d'authentification très poussées.

- Les services proxy sont indépendants les uns des autres de manière à éviter de bloquer l'ensemble des services si un problème survenait.

Limitations des Passerelles

Les passerelles augmentent considérablement le coût des firewall.

Les passerelles ont tendance à réduire la qualité de service.

2.5.3 Les VPN

Un VPN est un réseau qui se superpose aux réseaux publics tout en conservant les avantages d'un réseau privé

Création de tunnels avec Internet en reliant les sites d'un même SA 2 à 2

Les tunnels sont réalisés avec IPsec

Lorsque le SA est actif, les firewalls se trouvant aux bouts des tunnels négocient les paramètres d'échange.

2.6 Solutions sécurisées

* IPsec
- PGP (Pretty Good Privacy)
- PEM (Privacy Enhanced Mail)
- S/MIME Secure Internet Multipupose Extension)
- DNSsec
- SSL (Secure Socket Layer)
- S-HTTP (Secure HTTP)
- Protocole TLS

2.7 Chiffrement

- Chiffrement par substitution
  Conserve l'ordre des caractères en les masquant

- Chiffrement par transposition
  Transforme l'ordre des caractères sans les masquer

Masques jetables (one pad time)
Choix d'une longueur donnée de bits
Ou exclusif entre le masque et la chaîne à crypter

Réputé incassable

Texte limité par la longueur de la clé

La clé ne s'utilise qu'une fois, donc le risque est limité dans le temps et dans l'espace

Si l'émetteur et le récepteur se désynchronisent, l'information résultante inintelligible
L'émetteur et le récepteur disposent d'une copie de la copie, problème de transport de la clé

2.7.1 Algorithmes à clés symétriques

La même clé est utilisée pour le chiffrement et le déchiffrement ou la clé de déchiffrement dérive de la clé de chiffrement

La clé est secrète, transport de la clé

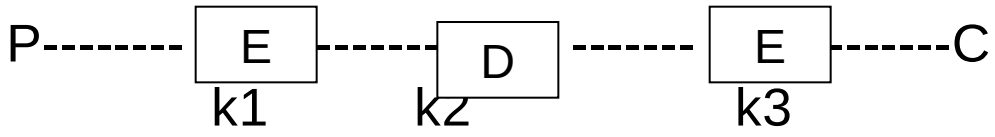
DES Data Encryption Standard) IBM 77

ISO8731 (DEA: Data Encryption Algorithm)

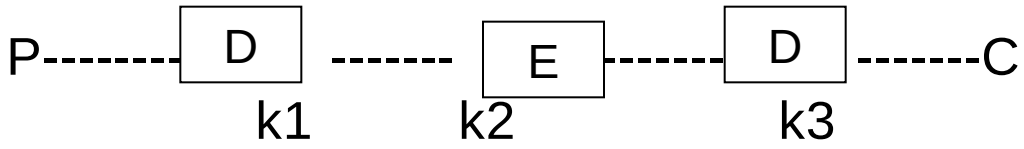
- Triple DES (ISO8732)

  - Clé de 128 bits au départ, ramenée à 56bits sur demande du NSA(National Security Agency),

  - IBM, convaincue que la clé est limitée, a conçu un moyen pour l'augmenter au moyen d'un triple chiffrement, 2 clés et 3 étapes



Triple chiffrement avec DES



Déchiffrement

- Pourquoi 2clés au lieu de 3?

  112 bits qu lieu de 168
- Pourquoi E-D-E?

  raisons de compatibilité

- AES : Advanced Encryption Standard

  Commande du NIST (National Institute of Standardisation and Technology) avec ses propres règles

  en 77, AES devint le standard américain FIPS197 (Federal Information Processing Standard)

2.7.2 Algorithmes à clés symétriques utilisés

Blowfish: Bruce Shneir 1 à 448 bits vieux et lent

DES: IBM 56 bits Trop faible actuellement

IDEA: Massey et Xuejia 128 bits efficace mais breveté

RC4: Ronald Rivest 1 à 2048 bits certaines clés sont faibles

RC5: Ronald Rivest 128 à 256 bits efficace mais breveté

Rijndael: Daemen & Rijmen 128 à 256 bits meilleurs choix

Serpent: Anderson, Biham et Knudsen 128 à 256 bits très fort

Triple DES: IBM 168 bits second meilleur choix

Twofish: Bruce Shneier 128 à 256 bits très fort largement utilisé

2.8 Modes de chiffrement

Mode ECB (Electronic Code Book Mode): Mode livre de codification électronique

Livre = ensemble d'enregistrements avec certaines rubriques en claires et d'autres chiffrées

Que se passe-t-il si un intrus capte l'information et permute les rubriques chiffrées?

Mode de Chiffrement avec chaînage de blocs (Cypher block chaining)

Solution à ECB

VI même nbre de bits que le bloc à chiffrer

généralement 64 bits

Mode de chiffrement avec rétroaction (caractère par caractère)

Le registre doit être initialisé (VI) pour les premiers caractères,

Si un bit d'octet est altéré au niveau du déchiffrement, seul l'octet correspondant sera altéré

Mode de chiffrement par flot (Stream Cypher Mode)

Pour le premier flot, on retient une VI, pour les flots suivants, VI devient respectivement E(VI,clé), E(E(VI,clé),clé),…….

Mode Compteur (Counter Mode)

On commence par chiffrer le VI auquel on ajoute une constante

Si la constante est 1; le rang d'un bloc est VIn-VI,

Si la constante est supérieure à 1, le rang d'un bloc est (VIn-VI)/constante

Comment déchiffrer?

2.9 Algorithmes à clés asymétriques (publiques)

Système radicalement différent (Diffie-Hellman 1976), deux clés totalement différentes, une pour le chiffrement et une autre pour le déchiffrement et l'une ne peut être déduite de l'autre

Les algorithmes doivent respecter 3 conditions simples

1- D(E(P))= P

2- Excessivement difficile de déduire D de E

3- E ne peut pas être cassé au moyen d'une attaque sur un texte en clair choisi

Si ces 3 conditions sont réunies, il n'y a aucune raison que la clé soit secrète

X souhaitant recevoir des messages chiffrés

X conçoit un algorithme de chiffrement E_x respectant les 3 conditions citées

X définit une clé K_{ex}

X rend publics E_x et K_{ex}

X conçoit un algorithme D_x et définit une clé K_{dx}

Une personne Y en fera pareil que X avec
E_y, K_{ey}; D_y et K_{dy}

X communique avec Y en lui envoyant le message P

X calcule $E_y(P,K_{ey})$

Y déchiffre $D_y(E_y(P,K_{ey}),K_{dy})=P$

Y répond à X Ex(R,Kex) R: réponse

X déchiffre $D_x(E_x(R,K_{ex}),K_{dx}) = R$

Personne ne peut lire les messages chiffrés, Dx et Dy supposés robustes et K_{dx} et K_{dy} clés secrètes

Méthode RSA(Rivest-Shamir-Adelman)

Non cassée depuis 25 ans

Théorie des nombres

Plusieurs systèmes de sécurité reposent sur RSA

Nécessite des clés d'au moins 1024 bits

Principe de RSA

1- Choisir 2 grands nbres premiers p et q en général de 1024 bits, p et q peuvent être égaux,

2- Calculer n = p*q et m=(p-1)*(q-1)

3- Choisir un nbre d tel que d et m soient premiers entre eux,

4- Trouver e tel que e*d = 1 mod m

Choisir p,q,n,m,d et e

P texte en clair à diviser en blocs de k bits tel que
$0 <= P <= n$

k étant le plus grand entier pour lequel la condition $2^k < n$ est vérifiée

Pour chiffrer P, on calcule $C= P^e \bmod n$

Pour déchiffrer C, on calcule $P=C^d \bmod n$

La clé publique est formée du couple (e,n)

La clé privée est formée du couple (d,n)

Exemple:

p=3, q=11, p et q premiers entre eux

n=p*q=33; m=(p-1)*(q-1)=20

d=7, d et m premiers entre eux

e=3, e*7=1 mod 20

P=MOHAMED

2.10 Signature à clés symétriques

Soit AC une Autorité Centrale

Chaque utilisateur définit sa clé secrète et l'apporte personnellement à AC

X avec sa clé secrète K_x

Y avec sa clé secrète K_y

X veut envoyer un message en clair P à Y

X génère $K_x(Y,R_x,t,P)$ qu'il adresse à AC

AC génère le message $K_y(X,R_x,t,P,K_{AC}(X,t,P))$ qu'il chiffre avec K_y de Y

L'utilité de t et de R_x?

Signature à clé publique

Qui peut être AC?

Structure gouvernementale, Avocat, Notaire; Banque, …..

Aucune structure n'inspire confiance, donc il est préférable de ne pas recourir à AC

D(E(P))=P propriété des algorithmes à clés publiques

Supposons que les algorithmes à clés publiques vérifient une 2° propriété E(D(P)) =P Cas de RSA

X transmet à Y $E_y(D_x(P))$ E_y clé publique de Y, D_x Clé privée de X

Y reçoit le message et le décrypte à l'aide de sa clé privée D_y

$D_y(E_y(D_x(P))) = D_x(P)$ suivant la 2° propriété

à $D_x(P)$, Y applique $E_x(D_x(P))=P$

Que se passe t-il si X nie avoir émis le message P à Y? Y présente P et $D_x(P)$ au juge

Le juge applique $E_x(D_x(P))$ si = P alors Y a raison

Inconvénients

- Que se passe-t-il si X ne garde pas D_x secrète?

  Y ne peut pas prouver que le message reçu provient de X

- Que se passe-t-il si X change son D_x?

  ce qui est fortement conseillé,

  Y ne peut pas prouver que le message reçu provient de X

Le NIST propose d'utiliser une variante de cet algorithme: El Gamel pour son standard

2.11 Protocoles d'authentification

Définition: Consiste à vérifier que, lors de l'établissement de la communication, le partenaire est bien celui qui prétend être et non un imposteur.

X contacte un serveur de fichier et demande à lire, écrire ou détruire le fichier F

Le serveur doit d'abord authentifier X (authentification), s'il est vrai; il vérifie les droits de X sur F (droits d'accès)

Pour s'authentifier, deux partenaires échangent plusieurs messages, cet échange de messages constituent le **protocole d'authentification**

Généralement ces messages sont chiffrés à l'aide de clés symétriques AES ou Triple DES

Authentification par clé secrète partagée K_{xy}

Principes admis par les protocoles d'authentification

X et Y interlocuteurs

R_x et R_y questions respectivement de X et de Y sous forme de grands nombres aléatoires de 128bits utilisés une seule fois (nonces n:nbre once: une fois)

K_x et K_y clés respectives de X et de Y

K_s clé de session

Protocole question-réponse

Le protocole contient au moins 5 messages

Si X et Y veulent créer une clé de session $K_{s,}$ X ou Y peut choisir une clé K_s et l'envoyer au partenaire chiffrée par K_{xy}

Peut-on améliorer ce protocole?

Oui en termes de nombre de messages

Non, attaque par réflexion (plusieurs sessions)

En ouvrant 2 sessions en même temps avec Y, Z est passé pour X et ainsi casser le protocole.

Moralité

1- Z doit prouver son identité avant que son interlocuteur ne le fasse. Y a communiqué $K_{xy}(R_z)$ sans avoir de preuve sur l'identité de X.

2- Les 2 interlocuteurs doivent utiliser des clés différentes K_{xy} et K'_{xy} pour cet échange.

3- X et Y doivent choisir leurs nombres dans des ensembles différents (ex pairs pour X et impairs pour Y).

4- Le protocole doit pouvoir résister aux attaques par réflexion (ex refus de 2 sessions d'un même interlocuteur)

Si une de ces règles est violée; le protocole peut être cassé

Solution à clé secrète partagée basée sur la signature numérique

Authentification à l'aide d'un centre de distribution de clés (KDC)

Le partage d'une clé secrète avec un partenaire peut fonctionner, mais pour échanger avec n partenaires, il faut n clés secrètes partagées qu'il est difficile à gérer pour un non initié.

D'où l'idée d'un KDC en qui tout le monde a confiance, il gère les authentifications et les clés de session

Chaque utilisateur a sa propre clé qu'il partage avec le KDC

Protocole d'authentification d'Otway&Rees

Prof A. Chouarfia USTO-MB Faculté FMI
Novembre 2010

Serveur d'authentification Kerberos

Le serveur AS contrôle les utilisateurs au cours de la connexion (login)

TGS serveur de vérification de ticket disposant d'une clé secrète K_{tgs} partagée avec AS, TGS délivre des preuves d'identité

L'émetteur X disposant d'une clé privée K_x connue d'AS et non stockée au niveau du poste de X

Le destinataire Y dispose d'une clé secrète K_y connue de AS Y peut être un serveur quelconque,

K_s clé de session délivrée par AS

Kxy clé de session créée par TGS pour le dialogue entre X et Y

Authentification par cryptographie à clé publique

Nécessité d'existence d'une PKI

2.12 Echange de clés de Diffie-Hellman

Le problème n'est pas l'authentification mais l'échange de clés secrètes partagées

X et Y ne peuvent se rencontrer pour échanger Kxy

X et Y ne peuvent pas le faire de vive voix, ils sont sous écoute

X et Y ne peuvent pas le faire par écrit, ils sont sous surveillance

Comment procéder?

X et Y se mettent d'accord sur 2 grands nombres publics n et g tel que

n et (n-1)/2 soient premiers

n et g sont choisis ou par X ou par Y; l'un les communiquera à l'autre

X choisit un grand nombre x de 128 ou 512 bits qu'il va garder secret, Y en fait pareil en choisissant un nombre y secret

g^{xy} mod n est la clé secrète partagée par X et Y

Exemple

n=47 (n-1)/2 = 23

g=3 x=8 y=10

Message 1 47, 3, 28 $(3^8 \bmod 47)=28$

Message 2 $(3^{10} \bmod 47) = 17$

X calcule $(3^{10} \bmod 47)^8 \bmod 47 = 17^8 \bmod 47$

$= 4$

Y calcule $(3^8 \bmod 47)^{10} \bmod 47 = 28^{10} \bmod 47 = 4$

$K_{xy} = 4$

Attaque par passeur de seau
X choisit x, Y choisit y, et l'intrus Z choisit z

n et g choisies par X ou par Y, n et g publics

Message 1 de X à Y <n,g, g^x mod n> intercepté par Z, Z calcule (g^x mod n)^z mod n)=g^{xz} mod n

Message 2 envoyé de Z à Y <n,g,g^zmod n>

Message 3 de Z à X <g^z mod n>, X calcule
(g^z mod n)^x mod n = g^{zx} mod n

Message 4 de Y à Z <g^y mod n>, Z calcule
(g^y mod n)^z mod n =g mod n

Z est arrivé à créer 2 clés secrètes partagées; g^{xz} mod n avec X et
g^{yz} mod n avec Y ➔Tout échange entre X et Y est intercepté par Z qui peut le garder ou le modifier à sa manière sans que X et Y ne se rendent compte

Conclusion

- Une question semble se poser: quelle solution adoptée pour quels besoins?
- IPsec : traitements spécifiques des entêtes par les routeurs, solution adaptée aux grandes entreprises.
- SSL plus simple à mettre en œuvre, solution adaptée aux entreprises moyennes et pas trop exigeantes en sécurité.
- Les solutions de niveau application semblent plus marginales et moins utilisées.

Bibliographie

- [GEM98]: J.C. Geffroy et G. Motet: Sûreté de fonctionnement des systèmes informatiques, Interéditions, Dunod, 1998
- [MON01]: J.L Montagnier: Construire son réseau d'entreprise, Eyrolles,2001
- [NAT02]: S. Natkin: Les protocoles de sécurité de l'internet, Dunod, 2002
- [PUJ02]: G. Pujolle: Initiation aux réseaux, Eyrolles, 2002
- [TAN03]: A. Tanenbaum: Réseaux 4° éditions, Pearson Education, 2003