ENSIAS

Sécurité physique et carte à Puces

Mohamed Senhadji
senhadji@ensias.ma

Objectifs Généraux du cours

ENSIAS

- L'objectif général à atteindre, c'est qu'au terme de ce cours l'étudiant doit être capable de monter une solution de sécurité physique basé sur des composants technologiques pour maitriser le mouvement du personnel et des équipements à l'intérieur d'une entreprise.
- Pour ce faire, un certains nombre de cahiers de charges (études de cas) seront proposés aux étudiants en tant que projets à traiter

Objectifs Spécifiques

- Les objectifs spécifiques à atteindre lors de ce cours consistent à maitriser les techniques et technologies permettant d'assurer la sécurité physique :
  1- Utilisation des supports d'identification (badges, biométrie, etc….)
  2- Sécurisation des supports d'identification
  3- Mécanisme de contrôle d'accès physique
  4- Technologie de vidéosurveillance, ronde de surveillance et détection d'intrusion
  5- Sécurité du personnel, des biens mobilier et immobilier (incendie, vol, catastrophe naturelle, etc..)

Plan du cours

- Sécurité Physique
  - Ce module traite la sécurité physique selon les certifications connues dans le monde de la sécurité IT : CISSP (Certified Information System Security Professional), CISM (Certified Information Security Manager), CISA (Certified Information Systems Auditor) & CEH (Certified Ethical Hacher)
- Sécurité RFID
  - Ce module traite la sécurité des RFID après une introduction complète aux techniques RFID, les vulnérabilités seront présentés et plusieurs techniques d'attaques seront utilisées. Les travaux pratiques permettront de mieux maitriser ces techniques et faciliter la mise en œuvre de solutions sécurisées basées sur ces cartes
- Travaux Pratiques et travaux dirigés
  - Des travaux pratiques et des travaux dirigés seront dispensé durant ce cours à la fin de chaque module
- Mini Projets
  - A la fin de cet élément de module les étudiants se verront affectés des mini projets dans le domaine de la sécurité physique en utilisant des cartes RFID ou à puce.

Sommaire

ENSIAS

- Statistiques sur la sécurité
- Sécurité Physique
- Besoin en sécurité physique
- Facteurs affectant la sécurité physique
- Sécurité physique-liste de contrôle
- Obstacles Physiques
- Wireless Security
- Vols des Laptops
- Défis pour mettre en œuvre la sécurité Physique
- Techniques d'espionnage
- Les mécanismes de sécurité de l'information
- Sécurité du système de l'information
- EPS (Electronic Physical Security)

Sécurité en quelques chiffres

ENSIAS

- Alarmes 28%
- Contrôle d'accès avec cartes d'identification 90%
- Badges visiteurs ou laisser passer 93%
- Détecteur d'explosion 9%
- Agents de sécurité 56%
- Détecteur de métaux pour les visiteurs 7%
- 260 disparitions de matériel informatique par jour
- Coût moyen d'un incident de sécurité est de 40.000 E
- 3/4 des entreprises françaises estiment avoir une dépendance très forte vis-à-vis de leur SI
- 1/4 des entreprises ont mis en place une politique de sécurité

- Statistiques sur la sécurité
- Sécurité Physique
- Besoin en sécurité physique
- Facteurs affectant la sécurité physique
- Sécurité physique-liste de contrôle
- Obstacles Physiques
- Wireless Security
- Vols des Laptops
- Défis pour mettre en œuvre la sécurité Physique
- Techniques d'espionage
- Les mécanismes de sécurité de l'information
- Sécurité du système de l'information
- EPS (Electronic Physical Security)

Comprendre la sécurité physique ?

ENSIAS

- Depuis que l'être humain dispose de chose précieuses à protéger, il a toujours chercher les moyens pour le faire
- Les Egyptiens étaient les premiers à concevoir une serrure
- La Sécurité physique décrit les mesures pour empêcher ou dissuader des intrus d'accéder aux installations, ressources, ou support de stockage d'information,
- La sécurité physique est une composante très importante pour la sécurité informatique
- Les points suivants doivent être pris en considération dans la sécurité physique :
  - Empêcher les attaques contre les données stockées dans les ordinateurs
  - La sécurité physique est une couche de la sécurité du réseau
  - Protéger les ordinateurs des catastrophes et des intrus qui cherchent le moyen d'accéder aux ordinateurs.

Définition de la Sécurité Physique

ENSIAS

- La sécurité Physique décrit les moyens et les techniques utilisées pour assurer la protection des biens, des personnes et des systèmes contre les menaces accidentelles et délibérées.

  Les moyens mis en œuvres en sécurité physique peuvent être :
  - Physique
  - Techniques
  - Opérationnels

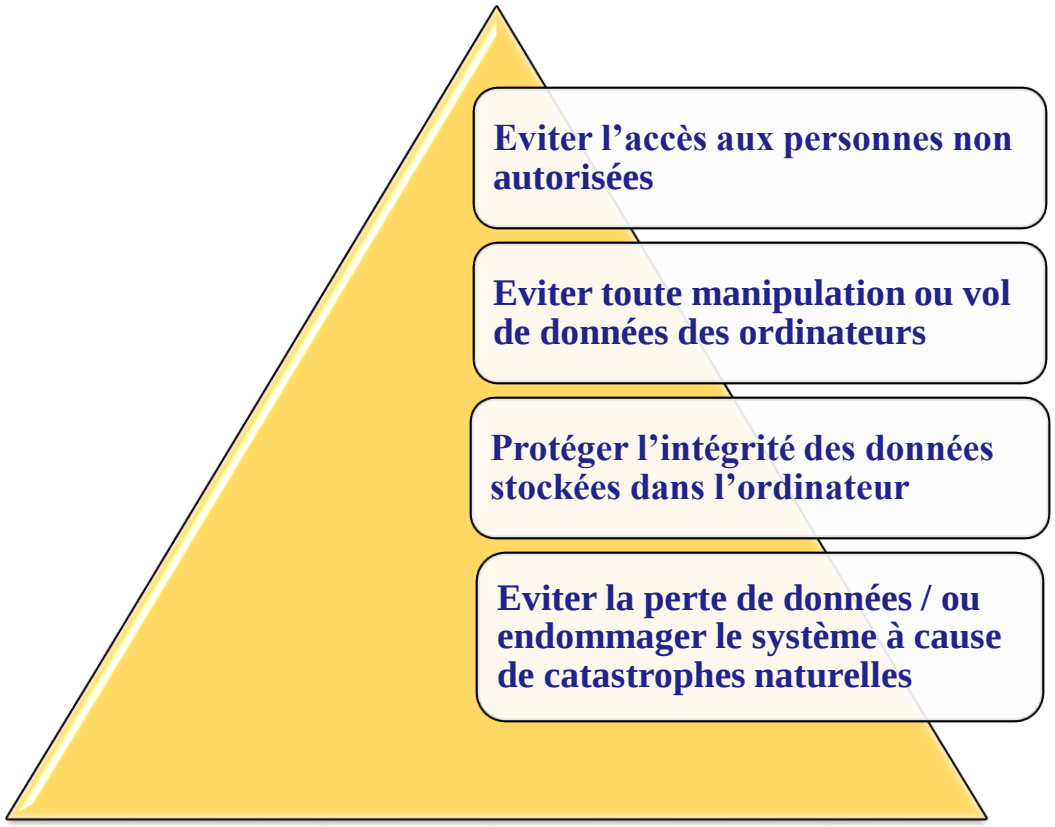
Définition suite

- Physiques : les moyens physiques sont utilisés pour protéger les biens :
  - Déployer des agents de sécurité
  - Barrières, clôtures
- Techniques : les moyens techniques sont utilisés pour sécuriser les services et les systèmes d'informations (serveurs, salle machine, réseau, BD etc….)
  - solution de contrôle d'accès, badges, biométrie, IDS, Capteurs,
- Opérationnels : les mesures communes de sécurité qui sont prises avant de procéder :
  - analyse et identification des menaces,
  - évaluation des risques et études des contre mesures appropriés.

- Statistiques sur la sécurité
- Sécurité Physique
- Besoin en sécurité physique
- Facteurs affectant la sécurité physique
- Sécurité physique-liste de contrôle
- Obstacles Physiques
- Wireless Security
- Vols des Laptops
- Défis pour mettre en œuvre la sécurité Physique
- Techniques d'espionnage
- Les mécanismes de sécurité de l'information
- Sécurité du système de l'information
- EPS (Electronic Physical Security)

Les besoins en sécurité physique

Pour le SI



Les besoins : suite

- La sécurité physique ne consiste pas à sécuriser juste le SI, elle implique aussi la sécurisation :
  - des environs de la société, les locaux, ou toute zone propre à la société,
  - des postes de travail,
  - du réseau,
  - Accès distant
  - Poubelles

Responsabilité de la sécurité physique

- En général, la sécurité touches plusieurs corps de métiers. Par conséquent, plusieurs compétences peuvent intervenir dans la sécurité,
- Les personnes impliquées dans la sécurité physique et sécurité du SI sont :
  - Les services d'ordre d'accès aux locaux de la société
  - Service de protection du personnel (incendies, accident, contamination, etc)
  - Le DSI, responsable système, responsable réseau
- La politique de sécurité physique doit fixer les responsabilités de chacun des corps de métier pour tout type de violation.

Responsabilité : suite

- Les personnes suivantes doivent avoir la responsabilité de la sécurité physique et sécurité du SI de la société :
  - Service sécurité gardiennage est responsable de :
    - filtrer l'accès physique au locaux de la société
    - formation des gardiens, rondiers et veilleurs de nuit
  - Service protection des agents est responsable de :
    - Protection contre l'incendie et mesure à prendre
    - Contamination, inondation, catastrophes naturelles, etc….
  - Administrateur du SI est responsable de :
    - L'accès au SI,
    - L'accès au réseau et l'accès distant

Responsabilité : suite

L'ensemble de ces corps de métiers doivent faire parti d'un comité piloté par un responsable sécurité qui cadre la politique de sécurité de la société et détermine le rôle de chacun des corps de métiers

- Statistiques sur la sécurité
- Sécurité Physique
- Besoin en sécurité physique
- Facteurs affectant la sécurité physique
- Sécurité physique-liste de contrôle
- Obstacles Physiques
- Wireless Security
- Vols des Laptops
- Défis pour mettre en œuvre la sécurité Physique
- Techniques d'espionnage
- Les mécanismes de sécurité de l'information
- Sécurité du système de l'information
- EPS (Electronic Physical Security)

Facteurs affectant la sécurité physique

ENSIAS

- Vandalisme :
  - employé mécontent, (modification des MDP)
  - troubles civiles, etc….
- Vol : gardien, serrures, antivol et IDS
- Poussière :
  - Diminue les performances du système (composant hardware),
  - Réduit la faculté des composants à se refroidir,
  - Même si le PC n'a jamais été ouvert, la poussière peut entrer par les ouvertures des connecteurs et ventilateurs,
  - Il faut utiliser régulièrement un compresseur d'air pour souffler la poussière déposée sur la carte mère et les autres composants,

Facteurs affectant la sécurité physique

ENSIAS

- Catastrophes naturelles :
  - tremblement de terre (bâches, plastique à bulles),
  - Feu : toujours erreurs humaine
    - détection incendie (extincteurs),
    - séparer les zones fumeurs
  - Inondation :
    - détecteur d'eau,
    - inspection des infiltrations (rondiers)
  - éclaire & tonnerre : parafoudre
    - surcharge électrique soudaine,
    - fluctuation de voltage qui peut endommager le système
    - tous les PC doivent avoir un onduleur et/ou un stabilisateur

Facteurs affectant la sécurité physique

ENSIAS

- Eau
  - Les PC ne doivent pas être placés près de sources d'eau, éviter l'éclaboussement ou l'écoulement d'eau sur le PC,
  - Les PC ne doivent pas être placé près de fenêtre,
- Explosion
  - Destruction massive
  - Les produits chimiques doivent être stocké dans des zones isolés
- Attaques terroristes
  - Peuvent arriver même si tout a été prévue en matière de sécurité physique
  - Tout activité suspecte doit être reportée aux responsables de la sécurité

<u>Les Détecteurs doivent être inspectés régulièrement</u>

- Statistiques sur la sécurité
- Sécurité Physique
- Besoin en sécurité physique
- Facteurs affectant la sécurité physique
- Sécurité physique-liste de contrôle
- Obstacles Physiques
- Wereless Security
- Vols des Laptops
- Défis pour mettre en œuvre la sécurité Physique
- Techniques d'espionnage
- Les mécanismes de sécurité de l'information
- Sécurité du système de l'information
- EPS (Electronic Physical Security)

Sécurité physique – Check list

- Les environs de la société
- Locaux
- Réception
- Serveur
- Station de travail
- Wireless access points
- D'autres équipements : fax, media amovible
- Contrôle d'accès
- Maintenance des équipements informatiques
- Ecoute électronique
- Accès distant

Sécurité physique(1)-contournement

- Les accès aux locaux de la société doivent être contrôlées (uniquement aux personnes autorisées),
- Pour sécuriser le périmètre de la société :
  - Clôtures (intérieur, extérieur 4,5 à 9m)
  - Portails : accès à l'entreprise
    - filtre des visiteurs,
    - barrières automatiques
  - Murs : séparation des différentes zones de l'entreprise :
    - Gardiens avec chiens

Portails, Barrières

Contournement : suite

- Pour sécuriser le périmètre de la société :
  - Gardiens, deux types de gardiens :
    - Gardien interne : connais mieux la société
    - Sté de gardiennage : sous contrat, en cas de non respect des mesures, le gardien est remplacé.
  - Alarmes : pour indiquer
    - Niveau d'eau (en cas d'inondation),
    - Feu,
    - Contamination chimique,
    - Tornades,
    - Intrusion
    - Antivol

Sécurité physique (2)-locaux

- Les locaux peuvent être protégé par :
  - La vérification des toitures, plafonds, canalisations,
  - Utilisation des cameras CCTV avec écran monitoré (temps réel) et enregistreur (différé), différents types de Cameras,
  - Système de détection d'intrusion,
  - Bouton de panique : (réceptionniste, caisse)
  - Système antivol : pour éviter le déplacement de certains appareils

Liste de contrôle-camera CCTV

Sécurité physique(3)-Réception

ENSIAS

- La réception est l'endroit par lequel transit les visiteurs de la société, elle doit être protégée :
  - Fichiers, documents, support amovibles : ne doivent pas être conservés à la réception,
  - La réception doit être conçus pour filtrer l'accès aux locaux des personnes étrangères à la société
  - L'écran du PC doit être positionné de telle façon qu'il ne soit pas visible pour un visiteur,
  - Le système doit être « logged off » lorsque la ou le réceptionnist(e) n'est pas à son poste
  - Logiciel de gestion visiteurs

Liste de contrôle-Réception

ENSIAS

- La salle d'attente doit être à une distance telle que les visiteurs n'entendent pas les conversations des réceptionnistes
- Les visiteurs qui restent longtemps à la réception doivent être interrogés sur l'objet de leur visite. Auquel cas il faut les notifier de quitter pour des raisons de sécurité.

Sécurité physique(4)-Salle Machine

ENSIAS

- La salle machine contiens les serveurs qui sont les éléments les plus importants d'un réseau (système d'information). Elle doit disposer d'un niveau très élevé de sécurité,
- Elle doit être bien éclairé
- Le(s) serveur(s) doi(ven)t être sécurisé par :
  - Fermé et verrouillé pour éviter tout déplacement
  - Ne pas permettre à un intrus de booter à distance les serveurs (supprimer DOS du serveur),
  - Désactiver les différents lecteurs (Floppy disk, CD-ROM, USB, etc…) en supprimant les drivers

Sécurité physique(5)- Stations de travail

ENSIAS

- C'est la zone de travail de la majorité des employés,
- Les employés doivent être informés sur les règles de sécurité pour sécuriser leur espace de travail (house kepping),
- Les documents doivent être détruits avant de les mettre dans la poubelle
- Les stations de travail doivent être sécurisées :
  - Des cameras,
  - Ecran et PC doivent être verrouillés,
  - Aménagement de l'espace (pas de vis-à-vis),
  - Eviter les lecteurs amovibles
  - Seule une station par rangée doit avoir ces drives mais ne doit être utilisée pour autre chose

Sécurité physique(6)- Acces Point

- Si un intrus accède au réseau de l'entreprise via un AP, il peut faire tout ce qu'il veut
- Les AP doivent être sécurisés :
  - Utilisation du cryptage WEP/WPA (chiffrement)
  - SSID ne doit pas être révélé
  - AP doit être protégé par un PASSWORD,
  - Le mot de pass doit être robuste pour ne pas être craqué facilement

Sécurité physique(7)-Autres équipements

ENSIAS

- Autres équipements : Fax, lecteurs amovibles, phone, modems, etc….
  - Un téléphone ne doit pas être laissé sans surveillance
  - En cas d'absence du réceptionniste le standard doit être verrouillé par un code PIN
  - S'assurer que le téléphone n'est pas sous écoute,
  - Les fax qui se trouvent dans la réception doivent être verrouillés en cas d'absence du réceptionniste,
  - Les fax reçus doivent être rangés correctement,
  - Les faxes à jeter doivent être broyés
  - Les lecteurs amovibles ne doivent pas traîner partout,

Sécurité Physique(8) -Contrôle d'accès

ENSIAS

- Un système de contrôle d'accès est utilisé pour réguler et surveiller l'accès à des zones sensibles,
- Séparation des zones de travail
  - Chaque service ou département doit avoir une zone de travail séparée
  - Les accès entre les zones doivent être bien défini pour pouvoir les contrôler
  - Les règles d'accès entre les zones doivent être bien définies pour élaborer les profils des différentes autorisations
  - Ceci permet l'identification des employées ainsi que leurs services
- Cartes d'accès (différencie un employé / visiteur)

Contrôle d'accès – technologies ?

- Les technologies utilisées dans le contrôle d'accès électronique :
  - Identification des personnes : Inductif, Code barre, Piste magnétique, RFID, Biométrie,
  - Lecteurs : Badge, Biométrie, etc…
  - Contrôleurs
  - Obstacles physiques, SAS (Mantraps)
  - Middleware
  - Backoffice

Contrôle d'accès- RFID Smart card

ENSIAS

- Une carte à puce et un badge en plastique au format carte de crédit avec une puce qui peut être chargé par des données,
- Ces cartes peuvent être utilisées :
  - Téléphones portables,
  - Application de porte monnaie électronique
  - Contrôle d'accès, Passeport bio,
  - Carte Nationale, Permis de conduire, carte grise, sante
  - Carte d'étudiant, club de sport,
  - Transport, autoroute,
  - Carte abonnement, carte de fidélité, Satellite TV,
  - etc….
- Elle peut être programmée pour plusieurs applications

Contrôle d'accès-Biométrie

- La biométrie est la science qui permet de mesurer et d'analyser les données biologiques qui sont propre à chaque personne,
- Les lecteurs biométriques convertissent l'information saisie en format digital pour l'analyser et la comparer avec les données préenregistrées dans une base de données
- Il existe différents lecteurs biométriques :
  - Empreinte digitale, faciale
  - Rétine, Iris
  - Forme de la main, structure des veines,
  - Reconnaissance vocale.

Contrôle d'accès-Empreinte digitale

ENSIAS

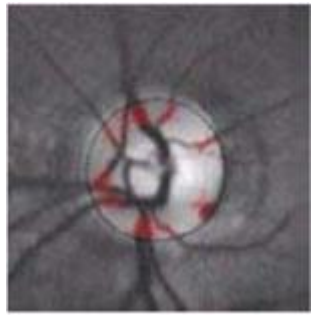
- Les empreintes des doigts peuvent être utilisées pour identifier une personne
- C'est la méthode biométrique la plus ancienne
- Chaque individu a une empreinte propre à lui
- Cette technique a été développée pour remplacer les Password, ID Cards ou d'autres méthodes pour contrôler l'accès aux PC, locaux, salles, etc…
- Utilisation des creux et des bosses de la surface du doigt
- Enrôlement des empreintes (base de donnée)
- Taux d'erreur $1/10^7$
- Falsifiable facilement

Contrôle d'accès-Reconnaissance de la rétine ou de l'Iris

- **Iris :**

  Analyse la couleur de l'œil derrière la cornée
  - L'iris de l'œil humain a un motif de texture propre a chaque personne

- **Rétine :**
  - Analyse les vaisseaux sanguins de l'œil



- L'identification prends plus de temps
- Plus difficile à falsifier que l'empreinte
- Taux d'erreur $1/10^9$

Contrôle d'accès-Forme de la main structure des veines

ENSIAS

- Forme de la main :
  - La main est scannée en 3D, la taille, la forme des doigts et articulations sont analysés,

- Structure des veines :
  - La disposition, l'emplacement et l'épaisseur des veines sont considérés

Contrôle d'accès - Reconnaissance faciale & vocale

La reconnaissance faciale consiste à reconnaitre l'empreinte du visage

La reconnaissance de la parole est la transformation d'un signal de parole en une séquence de symboles représentative du contenu du signal.

- Basée sur l'identification des fréquences vocales
- Reconnaissance mono-locuteur
- Pas fiable : cas d'une personne enrhumé

Contrôle d'accès-centrale ou contrôleur

ENSIAS

- Permet de gérer les lecteurs (interface entre le host et les lecteurs : badges, bio, etc…..)
- Envoie les signaux d'alarmes
- Récupère les signaux de contacts
- Distribue les commandes aux obstacles physiques
- Supporte plusieurs interfaces : Ethernet, WiFi, Wiegant, RS232, RS485, USB,etc…

Contrôle d'accès-Obstacles physiques

Quelques considérations concernant les obstacles physiques :

- L'activation se fait par contact sec :
- Logique positive/négative
- Verrouillage poigné (si accès seulement)
- En cas de porte : amortisseur ou ferme porte
- Barre anti-panique
- Contact magnétique pour contrôler durée ouverture
- Bouton poussoir pour ouverture d'urgence

Contrôle d'accès-Obstacles physiques

- Gâches
- Ventouses
- Electro serrures
- Motoverrous
- Tourniquets
- Tripodes
- Couloir
- Portillon

Obstacle physique : SAS(Mantrap)

ENSIAS

- Un **SAS** est un caisson muni de deux portes étanches. C'est un passage sécurisé pour les personnes dans certains bâtiments ou une porte technique d'un véhicule (bateau, sous-marin, vaisseau spatial) permettant le passage de deux milieux différents, ou un caisson permettant d'introduire des objets dans un lieu où règne des conditions particulières.

SAS Mantrap

- Il consiste à placer deux portes avec un espace fermé entre les deux,
- Il permet aux utilisateurs d'entrer par la 1er porte et exige une authentification pour sortir via la 2ème porte,
- La sécurité est fourni selon :
  - Poids, image
  - Evaluation de la personne avant l'accès
  - Permet l'accès à une seule personne à la fois

inBIO CONTROLLER

PC

Ethernet

Aux. Digital Input

Aux. Relay Output

Doorlock

Doorlock

Doorlock

Doorlock

F 11

Door

Exit button

MA300

Door

Exit button

SCR100

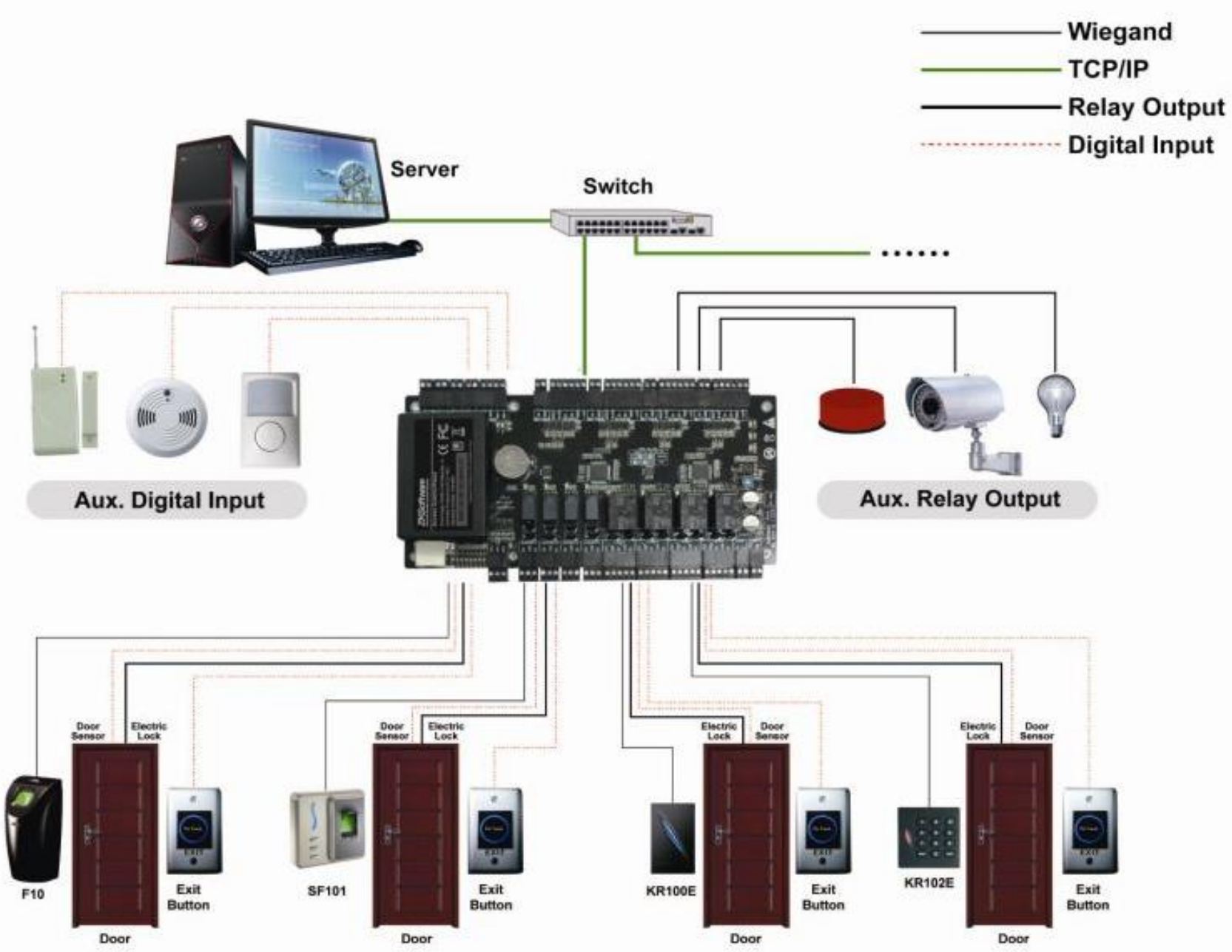
Door

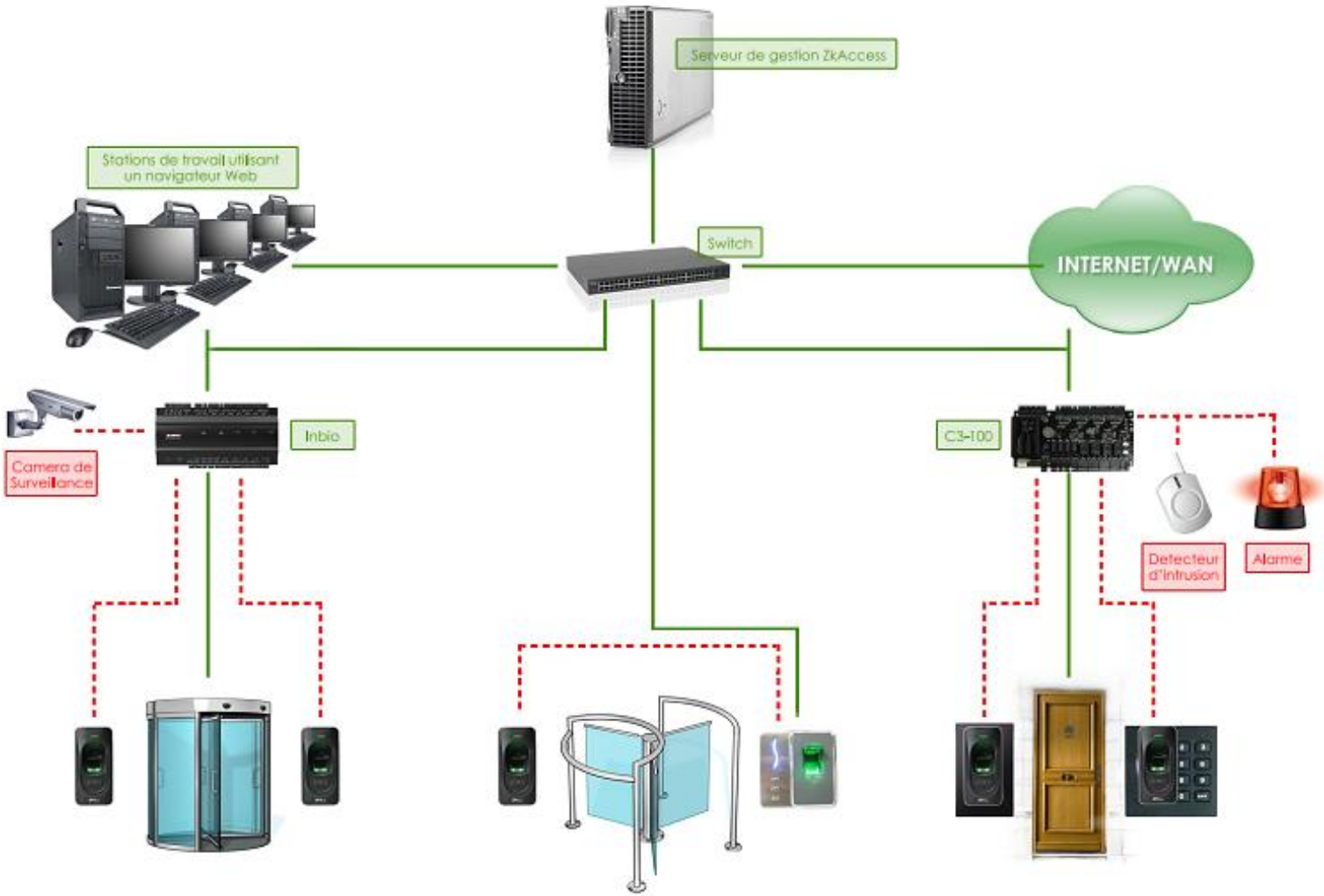
Exit button

FR1200

Door

Exit button


Wiegand
TCP/IP
Relay Output
Digital Input
Server
Switch
.....
Aux. Digital Input
Aux. Relay Output
Door Sensor
Electric Lock
Exit Button
Door
F10
SF101
KR100E
KR102E


Serveur de gestion ZkAccess
Stations de travail utilisant un navigateur Web
Switch
INTERNET/WAN
Camera de Surveillance
Inbio
C3-100
Detecteur d'intrusion
Alarme

Sécurité Physique(9)- Maintenance

- Nommer une personne qui s'occupera de la maintenance des équipements,
- Le matériel informatique qui est dans un entrepôt doit également être prix en compte,
- Le personnel du prestataire qui effectue le service de maintenance ne doit pas être laissé seul quand il viens pour l'entretien des équipements informatiques,
- Les boîtes à outils et les sacs du personnel du prestataire de maintenance doivent être soigneusement analysés pour éviter de compromettre la sécurité de l'entreprise.

Sécurité Physique(10)-Ecoute téléphonique

ENSIAS

- L'écoute électronique est l'action d'écouter secrètement les conversations d'autres personnes en connectant un appareil d'écoute à leur téléphone,
- Vous pouvez prendre les mesures suivantes pour s'assurer que personne n'écoute les communications :
  - Inspecter régulièrement toutes les données qui circulent dans les câbles
  - Utiliser des câbles blindés
  - Ne jamais laisser des câbles exposés

Sécurité Physique(11)-accès distant

ENSIAS

- L'accès distant est un moyen pour un employé de travailler depuis n'importe quel endroit en dehors des limites physiques de l'entreprise.
- L'accès distant au réseau de l'entreprise devrais être évité autant que possible
- Il est très facile pour un attaquant en utilisant l'accès distant de nuire au système d'information de l'entreprise
- L'accès distant est plus dangereux que l'accès physique puisque l'attaquant n'est pas dans le voisinage et la probabilité de l'attraper est moins.

Accès distant : suite

- Les données transféré durant un accès distant doivent être cryptées pour éviter l'interception
- L'accès distant doit être restreint pour des employés qui ont un niveau de responsabilité très important dans la compagnie
- Ils doivent avoir un compte (login) spécial pour l'accès distant, le mot de pass d'authentification doit être crypté pour éviter son piratage,
- VPN

- Statistiques sur la sécurité
- Sécurité Physique
- Besoin en sécurité physique
- Facteurs affectant la sécurité physique
- Sécurité physique-liste de contrôle
- Obstacles Physiques
- Wireless Security
- Vols des Laptops
- Défis pour mettre en œuvre la sécurité Physique
- Techniques d'espionnage
- Les mécanismes de sécurité de l'information
- Sécurité du système de l'information
- EPS (Electronic Physical Security)

Obstacles physiques

ENSIAS

- Gâches
- Ventouses
- Bandeaux et poignées ventouses
- Electro serrures
- Motoverrous
- Tourniquets
- Tripodes
- Couloir
- Portillon
- SAS

- Statistiques sur la sécurité
- Sécurité Physique
- Besoin en sécurité physique
- Facteurs affectant la sécurité physique
- Sécurité physique-liste de contrôle
- Obstacles Physiques
- Wireless Security
- Vols des Laptops
- Défis pour mettre en œuvre la sécurité Physique
- Techniques d'espionnage
- Les mécanismes de sécurité de l'information
- Sécurité du système de l'information
- EPS (Electronic Physical Security)

Wireless Security

ENSIAS

- Contrôle du trafic Wireless
- Activation cryptage :
  - WEP (Wired Equivalent Privacy), clé de 40, 128 bits
  - WPA (Wi-Fi Protected Access)
- Contrôle des adresses MAC
- Cryptage de bout en bout
  - SSL/SSH,
  - Utilisation de certificats
- VPN

Wireless Security

- Evaluation des AP
  - Les AP non autorisées doivent être contrôlés
  - Installation de firewalls et IDS sur les laptops
  - Analyse du système pour toute configuration incorrecte de sécurité
  - Verrouillage du système sur un nombre limité d'utilisateurs avec le minimum de droits possible
  - Supprimer les Broadcast des SSID

Wireless Security (M)

- Statistiques sur la sécurité
- Sécurité Physique
- Besoin en sécurité physique
- Facteurs affectant la sécurité physique
- Sécurité physique-liste de contrôle
- Obstacles Physiques
- Wireless Security
- Vols des Laptops
- Défis pour mettre en œuvre la sécurité Physique
- Techniques d'espionnage
- Les mécanismes de sécurité de l'information
- Sécurité du système de l'information
- EPS (Electronic Physical Security)

Vol de PC portable

ENSIAS

- Si un laptop est perdu :
  - Risque de divulguer des informations stratégiques :
    - Fusions de société
    - Résultat d'exploitation non finalisé
  - Risque de divulguer des informations tactiques :
    - Offres clients
    - Lecture des email,
    - Calendrier des RDV,
    - contacts,

Vol de PC portable : suite

ENSIAS

- Risque de divulguer des informations sur le réseau et l'infrastructure informatique :
  - Usernames & passwords
  - Adressage IP, DNS naming conventions,
  - Serveur entrant et sortant des mails
  - Ou tout autre détail qui permet de se connecter au réseau de la société
- Risque d'obtention des informations sur le propriétaire du laptop

Steel Cable Locks

Anti-Theft Tags

www.computersecurity.com

Tracking & Recovery Systems

StealthSignal

Portable Laptop Carts

Laptop Locker

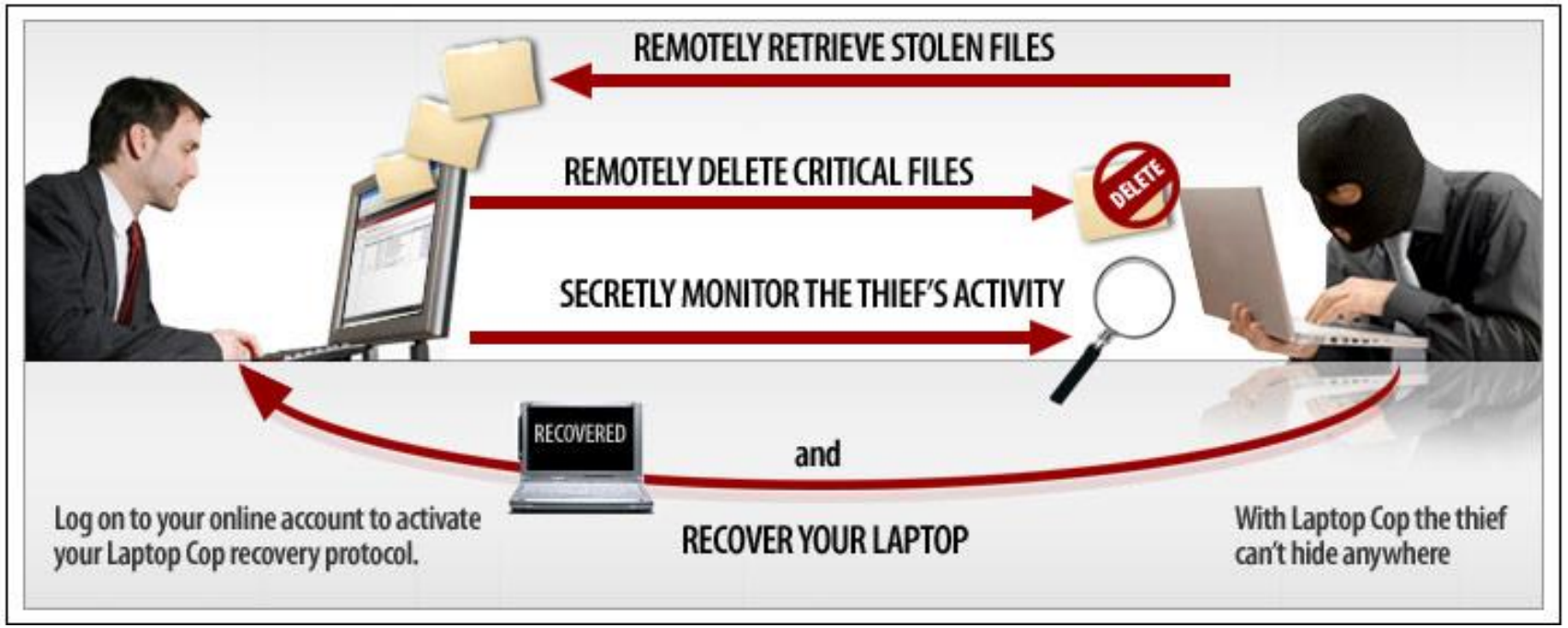
Laptop Tie-Down Brackets

Verrouillage des laptop

Suivi de PC portable : Xtool Computer Tracker

- Que se passe-t-il si vous perdez votre PC portable ?
- Voulez vous que votre PC vous appel et vous dit ou est ce qu' il se trouve ?
- XTOOL est un logiciel qui peut transmettre secrètement un signal furtif via une ligne téléphonique ou internet à un centre de contrôle pour suivre ça trace
- Chaque signal reçu par le centre de contrôle fourni suffisamment d'informations pour suivre la trace d'un PC :
  - chaque signal contient le numéro de téléphone ou l'adresse IP qui est utilisée par le signal transmis

Laptop COP



- Geo-locate laptops in real time
- Geo-location is determined by wi-fi signal, not IP address
- Lock down the stolen laptop if desired
- More accurate than GPS

Outils permettant de trouver les Portables volés

- Logiciels qui fournissent le lieu ou se trouve le PC volé,
- Ils utilisent la connexion internet :
  - Ztrace Gold : www.ztrace.com
  - CyberAngel : www.entryinc.com
  - ComputerPlus : www.computrace.com
  - Etc….

STOP Security Plates

- STOP plate « propriété perdue » et un N° téléphone gratuit pour vérifier l'identité du PC
- Le tatouage ne peut être effacé sans abîmer la toiture

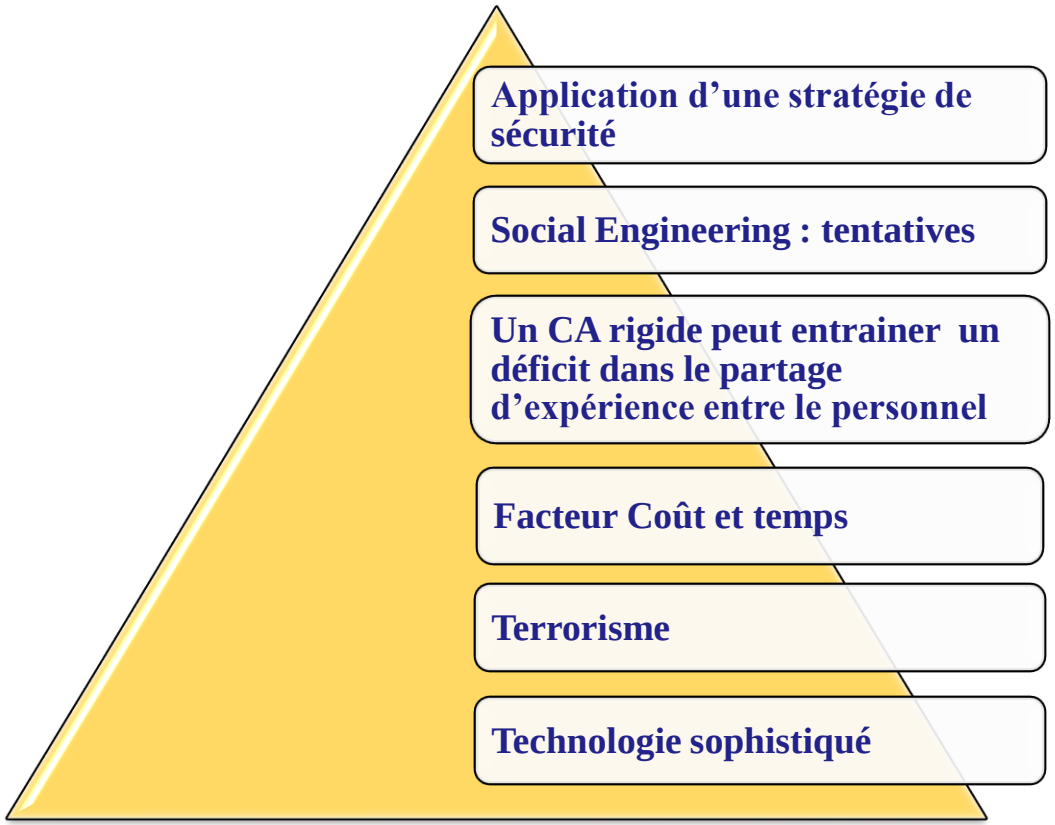
Cryptage du DD : TrueCrypt

ENSIAS

- TruCrypt est un logiciel qui permet de crypter (à la volée) une unité de stockage de données
- Les données sont automatiquement cryptées lors de la sauvegarde et décryptées lors de la restitution sans intervention de l'utilisateur
- C'est un logiciel OPEN SOURCE
- Ecryption algorithms : AES-256, Triple DES, Blowfish (448-bits key)

- Statistiques sur la sécurité
- Sécurité Physique
- Besoin en sécurité physique
- Facteurs affectant la sécurité physique
- Sécurité physique-liste de contrôle
- Obstacles Physiques
- Wireless Security
- Vols des Laptops
- Défis pour mettre en œuvre la sécurité Physique
- Techniques d'espionnage
- Les mécanismes de sécurité de l'information
- Sécurité du système de l'information
- EPS (Electronic Physical Security)

Défis pour mettre en œuvre la sécurité physique



- Statistiques sur la sécurité
- Sécurité Physique
- Besoin en sécurité physique
- Facteurs affectant la sécurité physique
- Sécurité physique-liste de contrôle
- Obstacles Physiques
- Wireless Security
- Vols des Laptops
- Défis pour mettre en œuvre la sécurité Physique
- Techniques d'espionnage
- Les mécanismes de sécurité de l'information
- Sécurité du système de l'information
- EPS (Electronic Physical Security)

Techniques d'espionnage

- Votre sécurité physique pourrais être mise en cause par des employés qui peuvent utiliser :
  - Cameras cachées ,
  - Enregistreur vocale,
  - Ecoute téléphonique,
  - GPS,
  - Désactivation des alarmes

- Statistiques sur la sécurité
- Sécurité Physique
- Besoin en sécurité physique
- Facteurs affectant la sécurité physique
- Sécurité physique-liste de contrôle
- Obstacles Physiques
- Wireless Security
- Vols des Laptops
- Défis pour mettre en œuvre la sécurité Physique
- Techniques d'espionnage
- Les mécanismes de sécurité de l'information
- Sécurité du système de l'information
- EPS (Electronic Physical Security)

Mécanismes de sécurité

ENSIAS

Contrôle d ’accès :

- Gestion des droits d ’utilisation
  - Accès légaux
  - Liste des personnes autorisées
  - Mots de passe
  - Règles d ’autorisation
  - Calendrier avec période et temps d ’accès
- Authentification

  Consiste à vérifier l ’identité d ’une entité (logique, matérielle ou humaine) par une autre à partir
  - d ’un élément supposé détenu ou connu de cette seule entité
  - ou de ses caractéristiques physiques spécifiques

Mécanismes de sécurité

ENSIAS

Sécurité des échanges par réseau :

Les problèmes de sécurité des échanges par réseaux peuvent être en 1ère approximation classés en 4 catégories non disjointes:

- Confidentialité:
  - Seuls les utilisateurs habilités doivent pouvoir prendre connaissance de l'information
  - Utilisateurs concernés ou à qui on veut vraiment envoyer l 'information
- Authentification: avoir la certitude que la personne avec qui on dialogue est bien celle que l'on croit
- Non répudiation: concerne les signatures

  comment prouver qu 'une personne
  - a bien envoyé un message
  - ou a bien reçu un message
- Contrôle d 'intégrité: comment être sûr que le message que l 'on reçoit est bien celui qui a été envoyé et qu 'il n 'a pas été altéré et modifié en cours de route

Les mécanismes d'authentification

L 'une des mesures les plus importantes et indispensables à l 'ensemble de la sécurité

- Accéder physiquement aux locaux
- Accéder physiquement aux éléments du réseau, terminaux, lignes ou ordinateurs centraux, serveurs
- Accéder logiquement à tous ces éléments

Deux étapes:

- Identification (login): on peut identifier un groupe
- Preuve : pour une et une seule personne

Comment ?

Les mécanismes d'authentification

ENSIAS

- Ce que connaît l 'entité : mot de passe, code confidentiel, etc..
- Ce que détient l 'entité : carte traditionnelle, clé physique, etc..
- Connaît et détient l 'entité : carte + clé privée ou code PIN

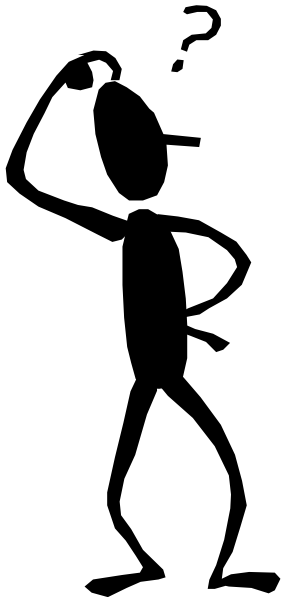
  avantage: le code PIN ne transite pas sur le réseau, vérification locale
- Ce qu 'est l 'entité ou l 'utilisateur

  Caractéristiques physiques : biométrie
  - Fond de l 'œil (Iris / Rétine)
  - Empreintes digitales
  - Forme de la main, structure des veines
  - Reconnaissance vocale

On suppose l'existence d 'un matériel sophistiqué et peu apprécié par l 'utilisateur

Les mécanismes de sécurité : Recap

ENSIAS



- processus à deux étapes:
  - Identification : login usuel
  - preuve ou « je le prouve »

- je connais : un mot de passe
- je possède : une carte
- je connais et je possède : smart card +clé privée et code confidentiel
- je suis : biométrie (empreintes digitales, fond de l ’œil, voix, etc …)

Les mécanismes de sécurité

Deux autres mécanismes de sécurité sont utilisés pour assurer les services de sécurité (complémentaire) :

- Cryptage ou chiffrement: assure la confidentialité
- Signature électronique : prouve l ’authentification, l ’intégrité et la non répudiation

Mécanisme de sécu : Cryptage/Décryptage

Deux classes de systèmes cryptographiques:

- Système symétrique ou à clé secrète
- Système asymétrique ou à clé publique

Mécanisme de sécu : Cryptage/Décryptage

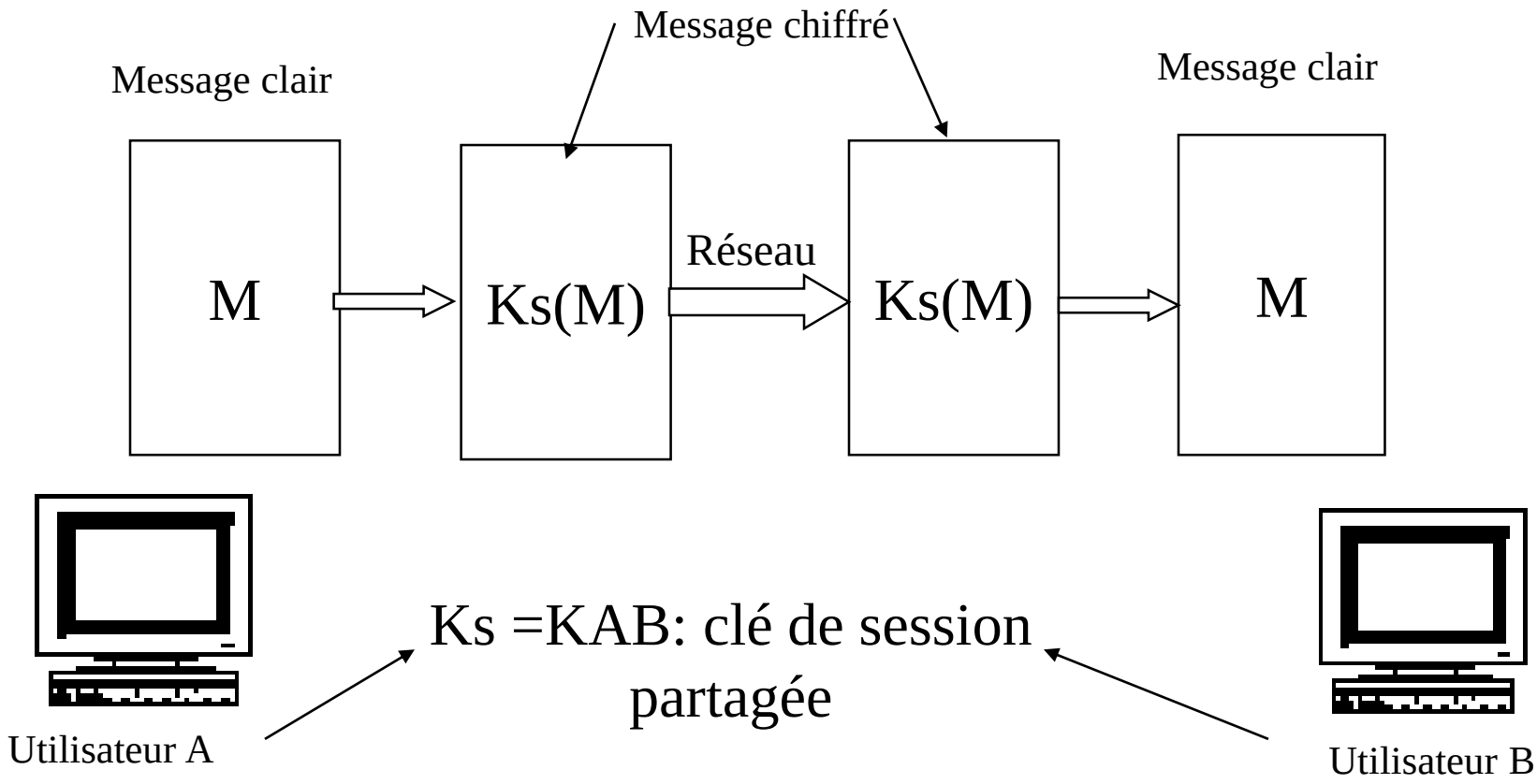
ENSIAS

Algorithme à clé secrète ou symétrique

- La même clé secrète(appelée aussi clé de session) est partagée entre les deux utilisateurs et utilisée aussi bien pour le cryptage que le décryptage
- Cette clé doit être échangée auparavant via un canal sûr
- Avantage: rapide
- Désavantage:
  - problème de stockage, distribution et gestion des clés
  - permet la confidentialité mais pas la signature (sauf en cas de notarisation)
- Exemples: AES, DES, 3DES, IDEA, ..

Mécanisme de sécu : Cryptage/Décryptage

Algorithme à clé secrète ou symétrique



Mécanisme de sécu : Cryptage/Décryptage

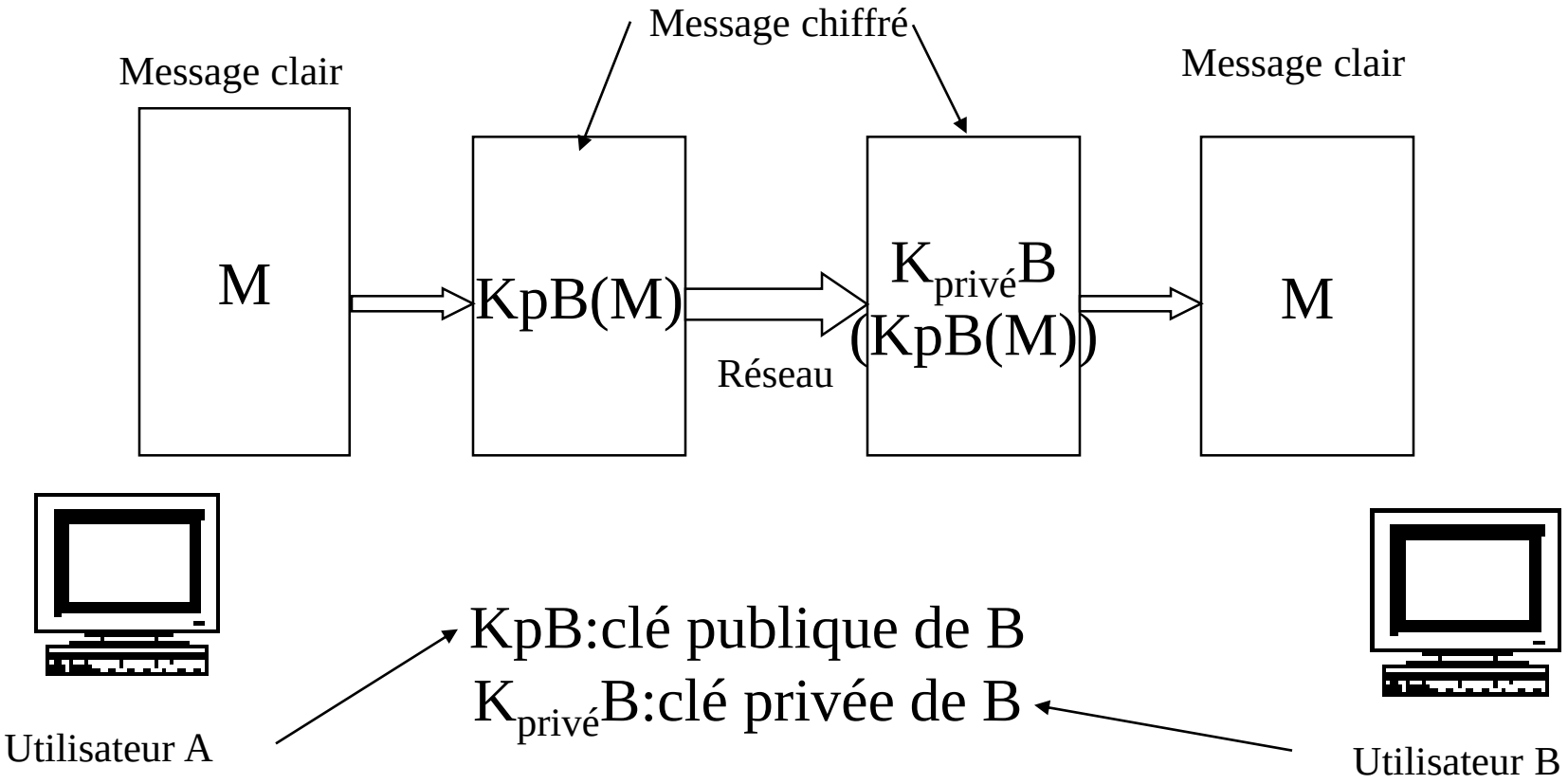
ENSIAS

Algorithme à clé publique ou asymétrique Principe

- Chaque utilisateur a une paire de clés, une clé publique P qui est distribuée et une privée (secrète) S
- Lorsque une clé crypte, seule l ’autre clé peut décrypter
- connaissant la clé publique ne permet pas de déduire la clé secrète correspondante
- Lent, mais peut être utilisé pour: intégrité, signature, authentification, distribution des clés (DES)
- Exemples: RSA, DSS, FIAT-SHAMIR, MD4

Mécanisme de sécu : Cryptage/Décryptage

Algorithme à clé publique



ENSIAS

Confidentialité avec clé publique

- pour envoyer un message confidentiel à B, A utilise la clé publique de B
- pour décrypter le message, B utilise sa clé privée
- personne à part B ne peut décrypter le message (même pas A)

Mécanisme de sécu : Signature digitale (1)

ENSIAS

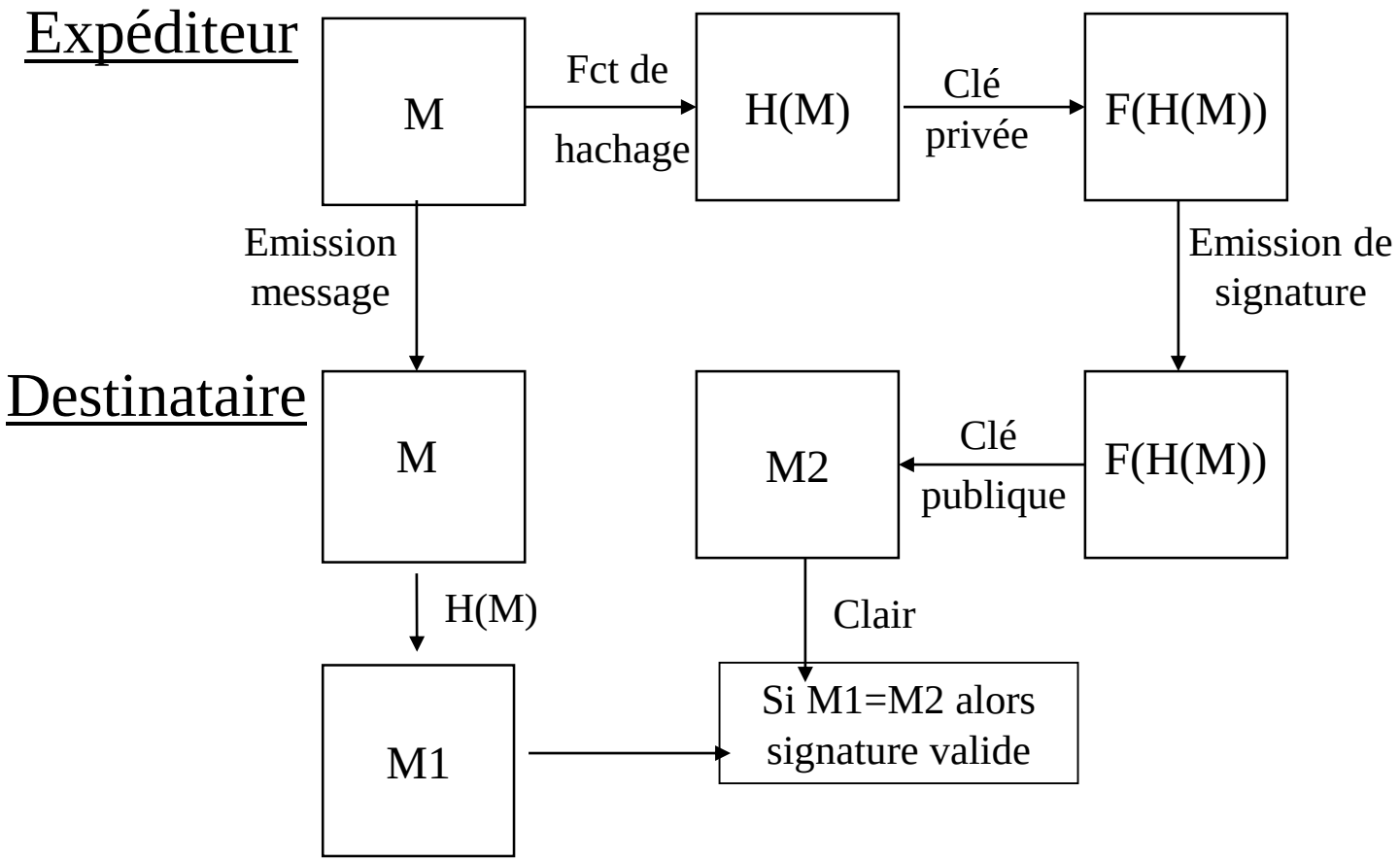
- Permet à l ’entité émettrice d‘ un message de prouver qu ’elle en est bien la productrice
- Offre au récepteur d ’un message les moyens de vérifier si celui-ci provient bien de l ’émetteur supposé
- La génération d ’une signature utilise des informations privées appartenant à l ’entité qui signe
- La vérification de la signature utilise des procédures et des informations publiques accessibles (annuaire) mais à partir desquelles on ne peut déduire les informations privées du signataire
- La signature doit être non forgeable

Mécanisme de sécu : Signature digitale (2)

- A applique sa clé privée (signe)
- B utilise la clé publique de A pour décrypter le message
- Pas de confidentialité

Mécanisme de sécu : Signature digitale (3)

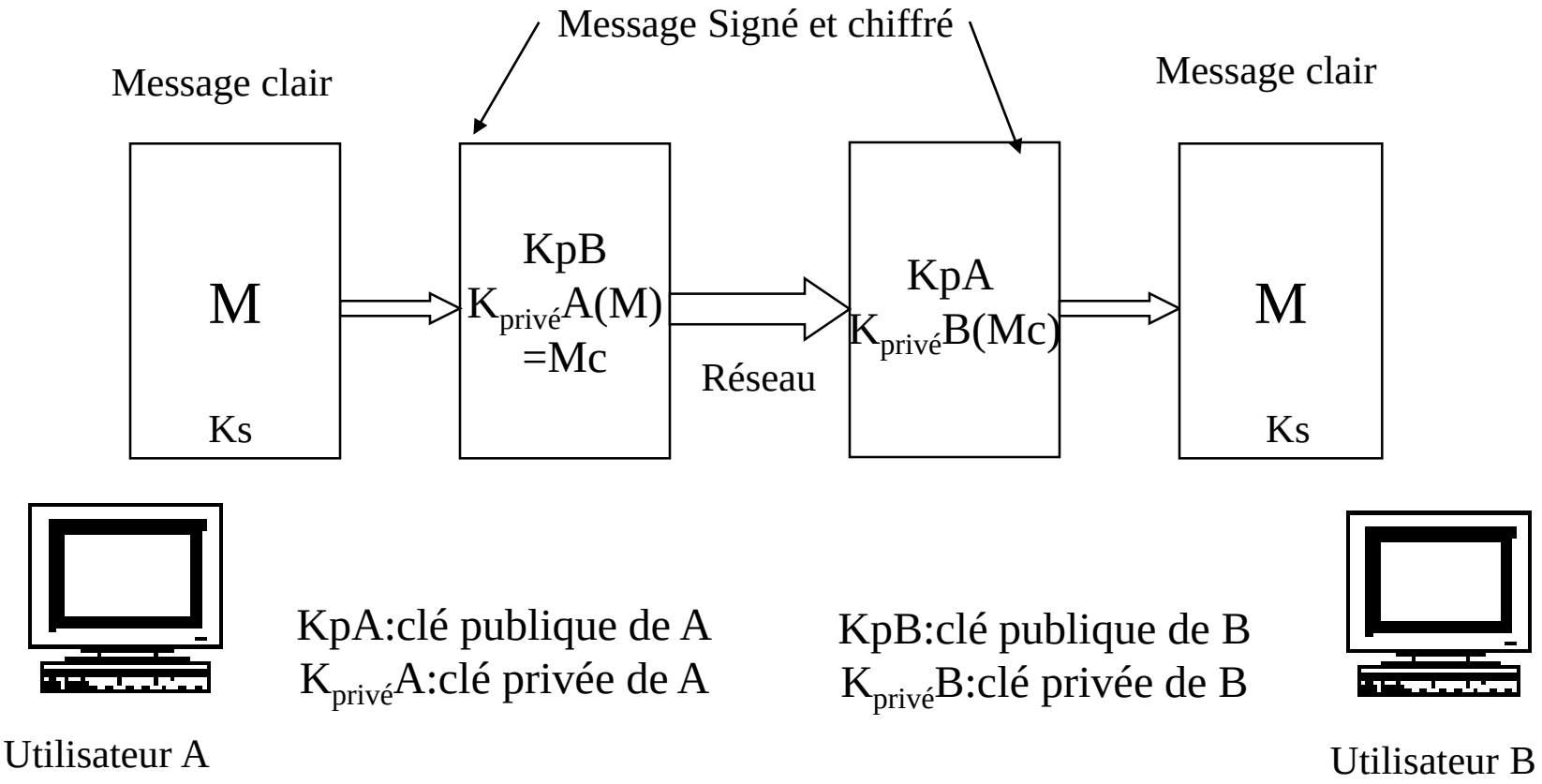
Signature digitale : vérification



Combinaison : confidentialité et signature

- A applique sa clé privée (signe)
- pour envoyer un message confidentiel à B, A utilise la clé publique de B
- pou décrypter le message, B utilise sa clé privée
- B utilise la clé publique de A pour vérifier la signature

Combinaison des 2 algorithmes : partage de Ks



Comparaison des 2 algorithmes

Type de chiffrement	Avantages	Inconvénients
Chiffrement symétrique	• Rapide • Facile à réaliser sur une carte à puce	• Même clé pour cryptage/décryptage • Gestion des clés lourde • Pas de signature électronique
Chiffrement asymétrique	• Une paire de clés • Facilite la distribution des clés • Garantie l'intégrité, la non répudiation et l'authentification (certificat)	• Lent et demande beucoup de calcul

- Statistiques sur la sécurité
- Sécurité Physique
- Besoin en sécurité physique
- Facteurs affectant la sécurité physique
- Sécurité physique-liste de contrôle
- Obstacles Physiques
- Wireless Security
- Vols des Laptops
- Défis pour mettre en œuvre la sécurité Physique
- Techniques d'espionnage
- Les mécanismes de sécurité de l'information
- Sécurité du système de l'information
- EPS (Electronic Physical Security)

Sécurité du SI

- Hiérarchie de sécurisation de l'information :
  - Protection des password / password complexe
  - Antivirus
  - Firewalls
  - IDS
  - Mise à jour régulière de l'OS
  - Verrouillage des ports inutiles (+Laptop)
  - Enregistrement de laptop (chez les fabriquants)
  - Cryptage des fichiers confidentiels/importants

- Statistiques sur la sécurité
- Sécurité Physique
- Besoin en sécurité physique
- Facteurs affectant la sécurité physique
- Sécurité physique-liste de contrôle
- Obstacles Physiques
- Wireless Security
- Vols des Laptops
- Défis pour mettre en œuvre la sécurité Physique
- Techniques d'espionnage
- Les mécanismes de sécurité de l'information
- Sécurité du système de l'information
- EPS (Electronic Physical Security)

EPS Electronic Physical Security

ENSIAS

- Système de détection d'incendie
- Système de suppression automatique de gaz
- Solution de vidéosurveillance (CCTV, IP Network, DVR/NVR, etc….
- Access Control : RFID-Biometric-Smart Card
- Gestion visiteurs
- IDS
- Système répressif : clôture du périmètre, barrières de sécurité, barrière hyperfréquence, barrière infrarouge,
- Solution de contrôle de ronde
- Solution contre le vol de PC portable et PDA

Schéma de principe de la solution intégrée