Sécurité et Internet

Didier DONSEZ

Université de Valenciennes

Institut des Sciences et Techniques de Valenciennes

e-mail : donsez@univ-valenciennes.fr

“CE NE SONT PAS LES MURS QUI PROTÈGENT LA CITADELLE, MAIS L’ESPRIT DE SES HABITANTS”

THUCYDITE

Sommaire

- Introduction: l’environnement réseau de l’entreprise
- Les problèmes
- Une réponse : la Cryptographie
- Echanges Sécurisés d’Information
- Les Protocoles
- Les Autorités Certifiantes
- La Preuve Electronique
- L ’Utilisation Légale des Outils de Chiffrage
- Les Accès Distants Sécurisés, Risques et Solutions

Introduction:
l'environnement « Réseau » de l'Entreprise

- Avant
  - Centralisé
  - Échange Papier
  - Pas d'Accès Distants

Introduction:
l'environnement « Réseau » de l'Entreprise

- Maintenant
  - Distribué sur plusieurs sites
    - siège, filiale, commerciaux, télé travailleurs
  - Extra entreprise ⇨ EDI - "Zéro Papier"
  - Intra entreprise ⇨ le Client-Serveur
  - Accès Distants
  - Multiplication des partenaires commerciaux
  - Mondialisation des échanges

Introduction:
l'environnement « Réseau » de l'Entreprise

- Futur
  - Clientèle : les « particuliers » informatisés
    - minitel, set top box, assistant personnel, PC, …
    - 3 000 000 000 d 'individus
  - Agents Commerciaux (Intelligents)
  - Réseaux sans Fil (GSM, …) , Internet

Les Risques liés aux Réseaux

- interception des messages
  - prise de connaissance des mots de passe
  - vol d'information
- intrusion des Systèmes
  - Vol d'information
  - Virus
  - Détournement de biens
- Faux client, Marchand escroc

- *ATTENTION : la fraude est souvent interne !!!!*

Les différentes facettes de la Sécurité

- l'Identification
  - Qui est-ce ?
- l'Authentification
  - Est-ce bien lui ?
- la Confidentialité
  - Est-ce qu'un autre nous écoute ?
- l'Intégrité
  - Le contenu est-il intact ?
    - altération, malveillance
- la Non Répudiation
  - Correspondant de Mauvaise Foi
    - nier ultérieurement une opération effectuée

Qui écoute ou falsifie ?

- Les Gouvernements
  - NSA (National Security Agency),

    CIA (Central Inteligence Agency), DGSE ...
- Le Crime Organisé
- Les Concurrents de votre Entreprise

Techniques de chiffrage

- Le Brouillage
- Le Chiffrage
  - à Clé symétrique
  - à Clé asymétrique

le Brouillage

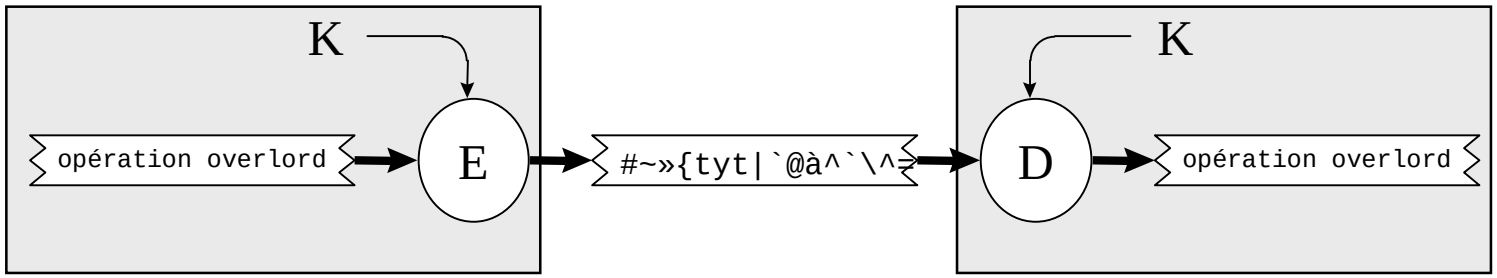
- algorithme privé
  - ex : code de César
    - i’bqnhr pt’b’drs bkzhq *j’crois qu’c’est clair*
    - hal *ibm (cf 2001 l’odyssée de l’espace)*
    - WNT *VMS*
  - ex : 1 bit sur 8 dans une image BMP
    - *la mafia s échangeait des photos de la « familia »*
  - WinZip possède une fonction de brouillage
  - *plus de secret si l ’algorithme est connu*

le Chiffrage (Cryptage)

- algorithme public
  - connu de tous
  - le secret est maintenue
    tant que la clé n'est pas connu
  - qui peut être propriétaire : royalties
- chiffrage à clé symétrique
  - (clé secrète)
- chiffrage à clé asymétrique
  - (clé publique / clé privée)

le Chiffrage à clé symétrique (clé secrète)

- 1 seule clé pour chiffrer et déchiffer



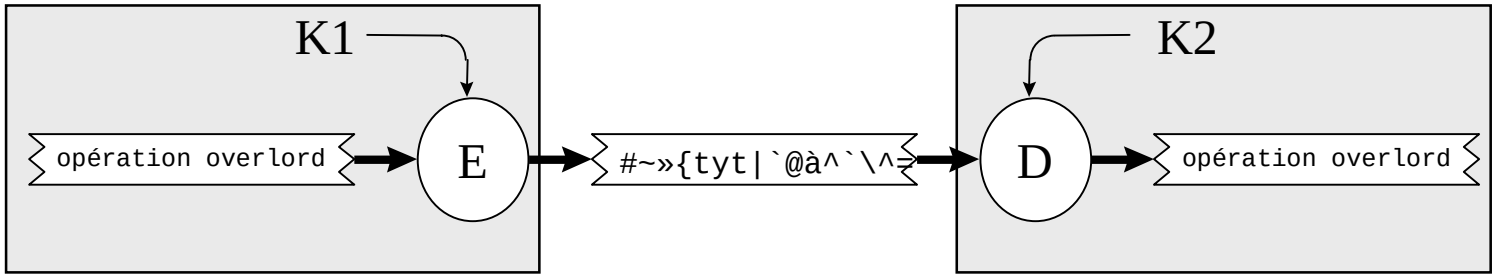
Le Gentil — Le Méchant — L'ami du Gentil

Le Truand — Les Gentils — Un Comparse du Truant

- DES (Decryption Encryption Standard - IBM 1977), IDEA

le Chiffrage à clé asymétrique (clé publique / clé privée)

- 2 clés K1 et K2
  - si chiffrage par K1, déchiffrage par K2
  - si chiffrage par K2, déchiffrage par K1
    - *Remarque : on ne peut pas trouver une clé à partir de l'autre*



- RSA (Rivest Shamir Akermann)

DES
(Decryption Encryption Standard)

- Principe
  - Succession de Rouleaux de Permutation
    - Machine ENIGMA

RSA
(Rivest Shamir Akermann)

Génération des Clés de B

B sélectionne p et q

B calcule $\gamma(N) = ppcm(p-1,q-1)$

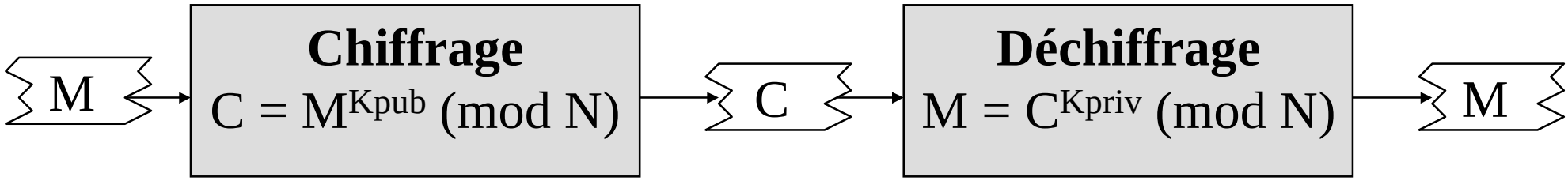
B tire la clé publique Kpub

B calcule la clé privée Kpriv

$$Kpriv * Kpub = 1 \ (mod(\gamma(N))$$

Privé
- *p, q nombres premiers*
- *Kpriv une clé secrète*

Public
- *N =p*q*
- *Kpub une clé publique*



RSA - Exemple

Génération des Clés de B

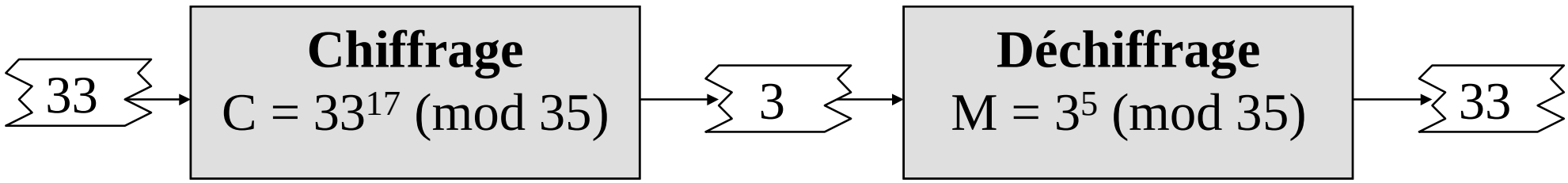
B sélectionne p=5 et q=7

B calcule $\gamma(N=35) = ppcm(4,6)=12$

B tire la clé publique Kpub=17

B calcule la clé privée Kpriv

$$Kpriv * 17 = 1 \pmod{12} \Rightarrow Kpriv=5$$



La CryptoAnalyse

- Attaque d'un chiffrage
  - l'attaquant cherche à connaître
    - le texte en clair
    - la clé « secrète ou privée » utilisée
  - à partir d'un texte encodé : très difficile
    - Paul Leyland et 1600 machines relèvent le Défi [1994]

      RSA : 129-digits (430 bits) -> 5000 Mips - Year

      « THE MAGIC WORDS ARE SQUEAMISH OSSIFRAGE »
  - à partir du texte clair et du texte encodé : faisable
    - Attention aux en-têtes de formulaires !!!!

Validité d'un Chiffrage

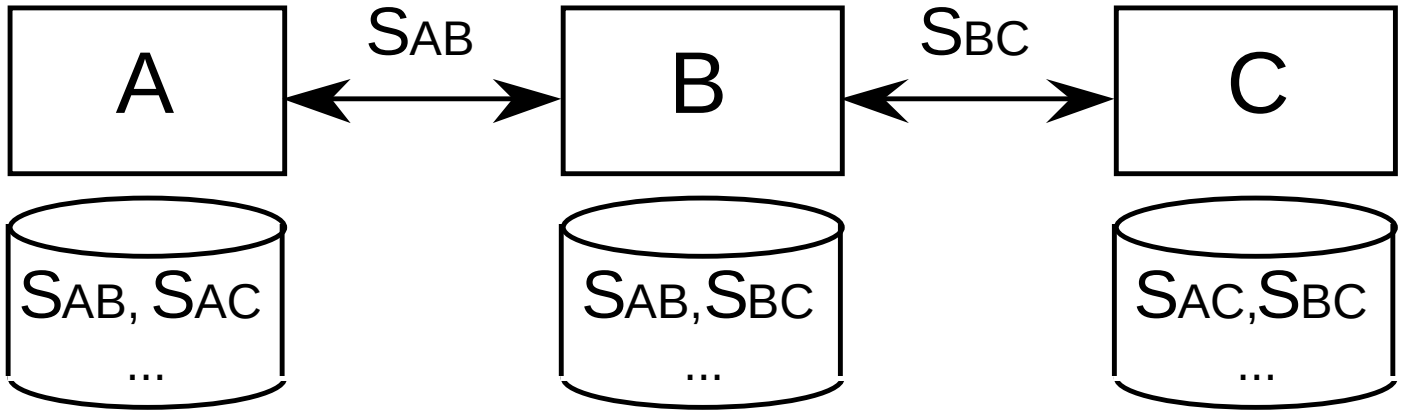
- dépendant de la nature de la donnée à protéger
  - transaction bancaire
    - quelques minutes
  - secret d'état, signature de contrat à long terme
    - 50 ans
- dimension de la clé
  - plus la clé est grande, elle est difficile à casser

Sécurisation des échanges d'information

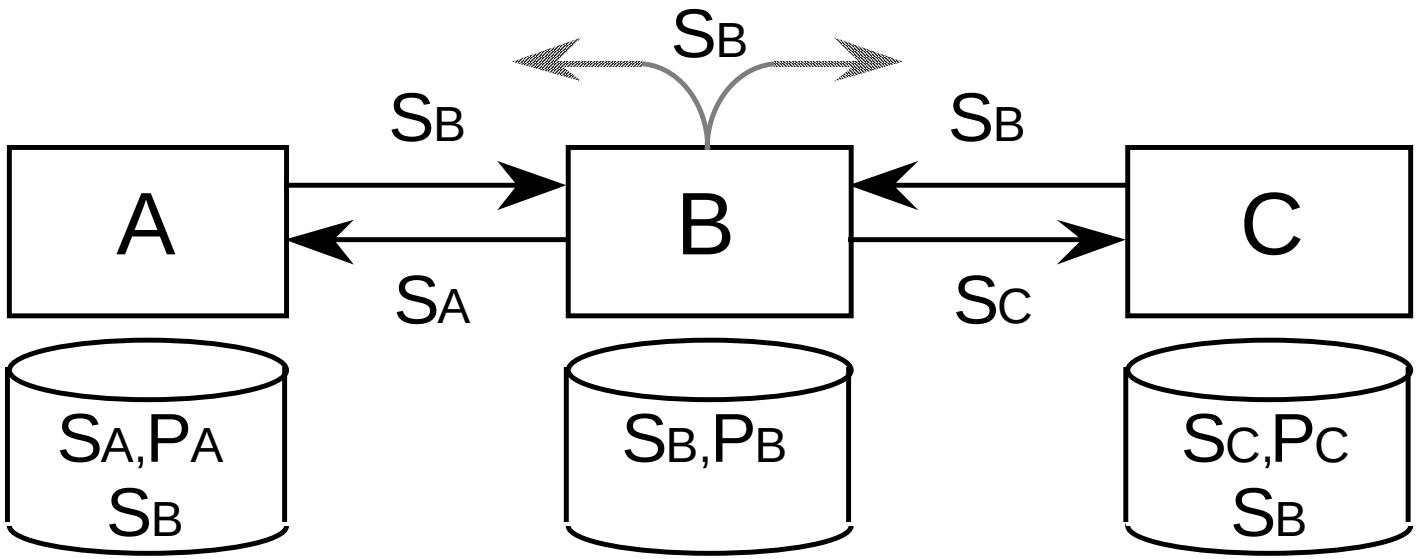
- Echange par clé secrète
  - Cryptographie à clé symétrique
- Echange par clé privée / clé publique
  - Cryptographie à clé asymétrique
- Echange hybride
  - Echange d'une clé secrète K
    par Cryptographie à clé asymétrique
  - Echange par clé secrète (K)

Echange par clé secrète

- Gestion exponentielle des Clés
- Échange “sûr” des clés entre les partenaires
- risque de Trahison : *mais qui est le traître ?*



Echange à clé publique / clé privée



Shared (Clé Publique) Private (Clé Privée)

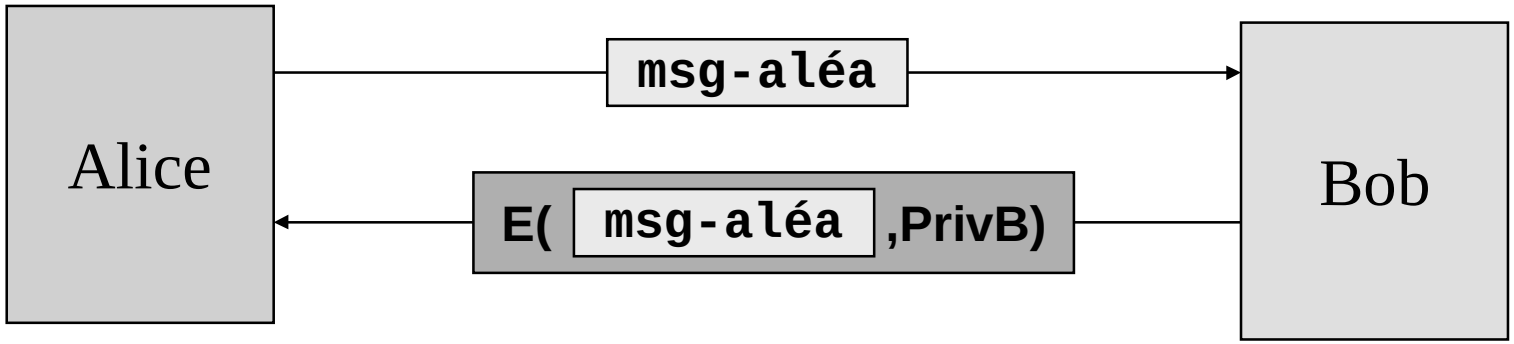
- Utilisé pour le courrier électronique
- Fragilité de la clé privée

Echange Sécurisé d'information

- Protocole
  - Phase 1 : authentification des partenaires
    - certification
  - Phase 2 : échange sécurisé d 'une clé secrète pour la session
  - Phase 3 : échange sécurisé des messages
    - algorithme à clé secrète
    - intégrité et sans playback

L’authentification

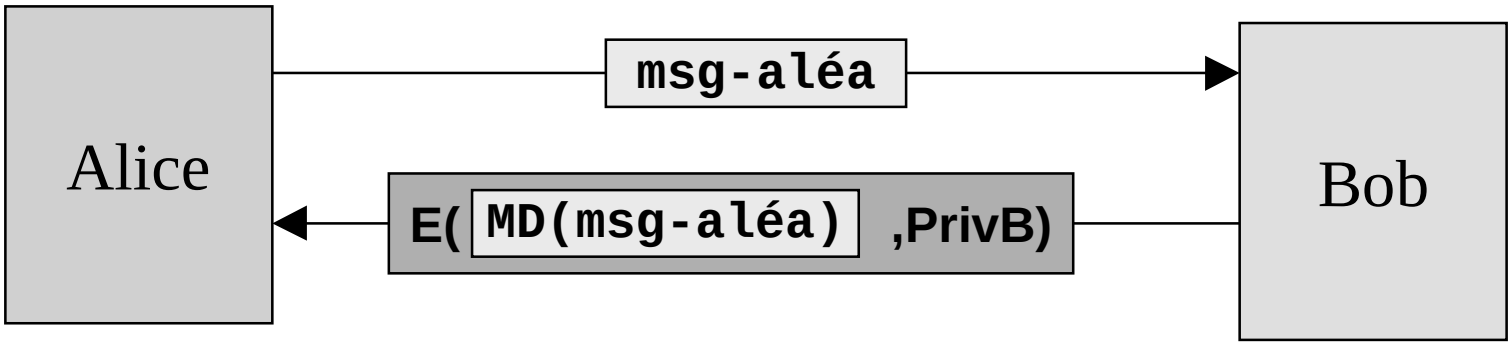
- proposition
  - Protocole



  - Problème
    - attaque de la clé privée de B à partir du message en clair et de son chiffrement.

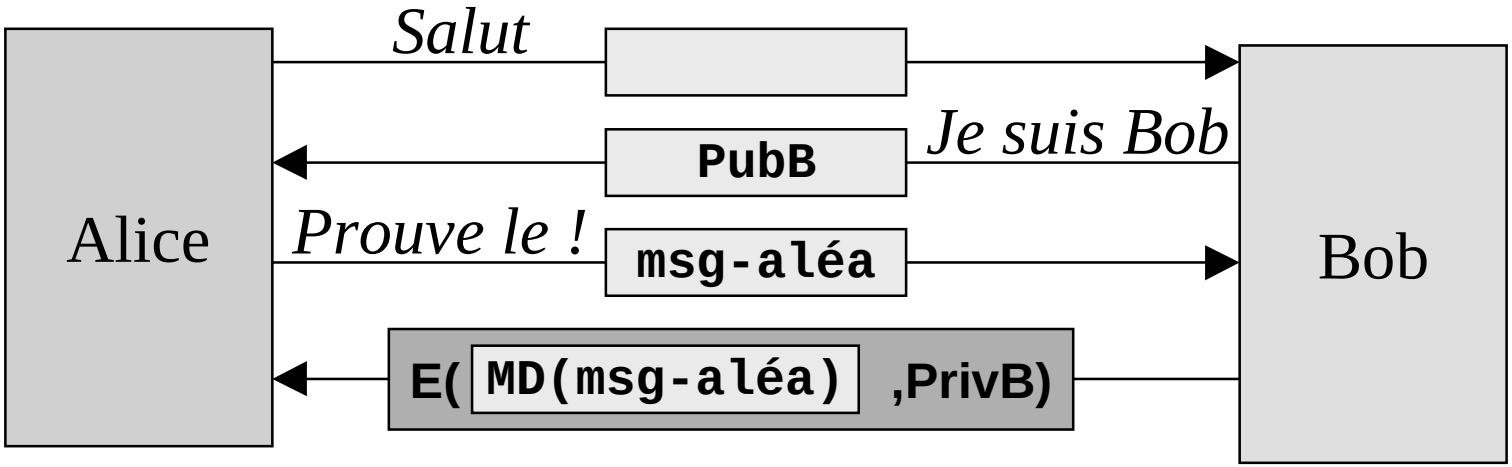
Correction

- Technique:
  - calculé un résumé (digest) difficile à “inverser”.
    - fonctions sécurisées de hachage
      - MD4, MD2, MD5 (Message Digest)



L’identification

- Proposition



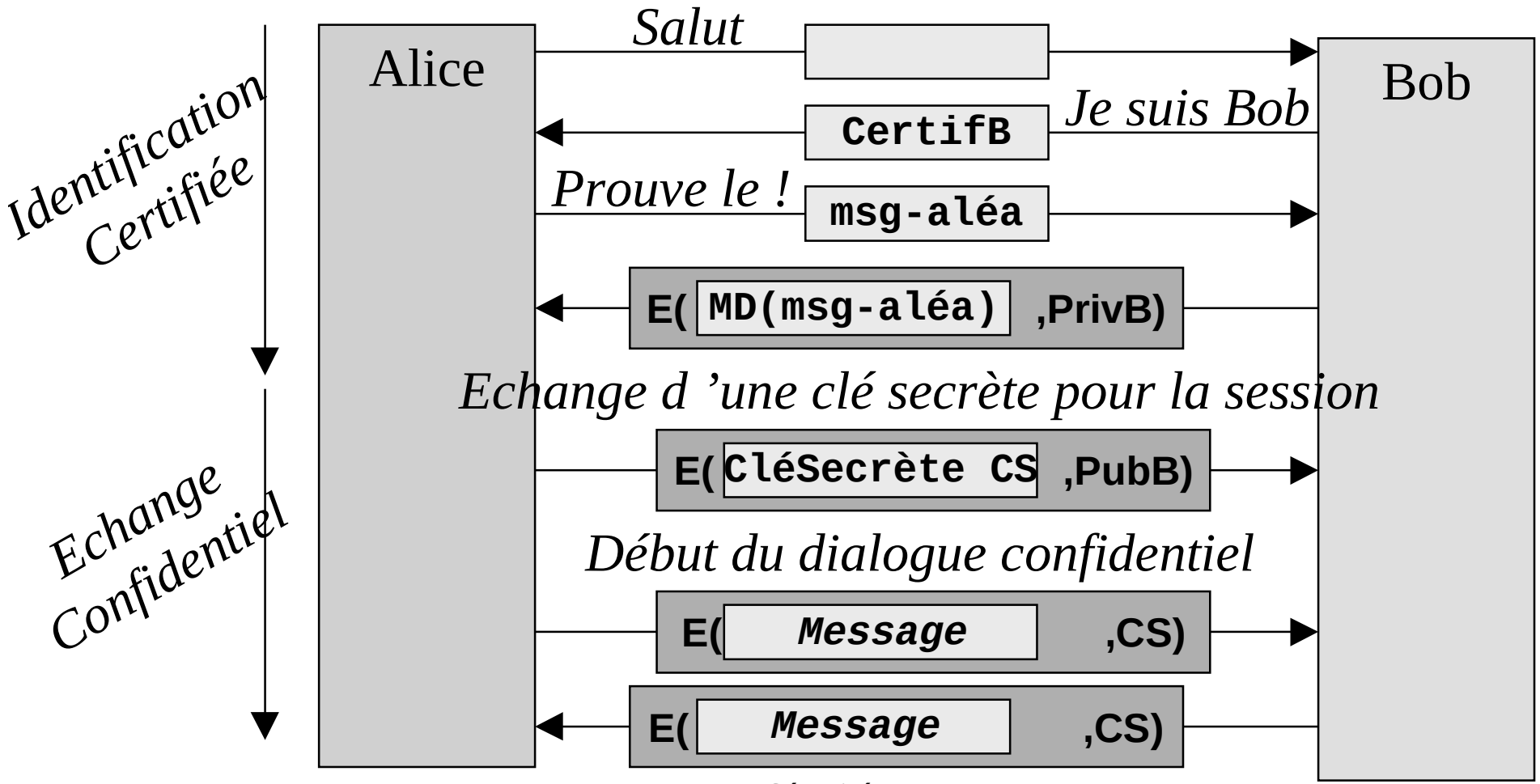
- Problème
  - n’importe qui peut se faire passer pour Bob
    et communiquer une fausse clé publique.

La Certification

- Technique:
  - communiquer son certificat émis et signé
    par une tierce partie CA (Certifying Authority)
    - Le certificat (ISO X509)

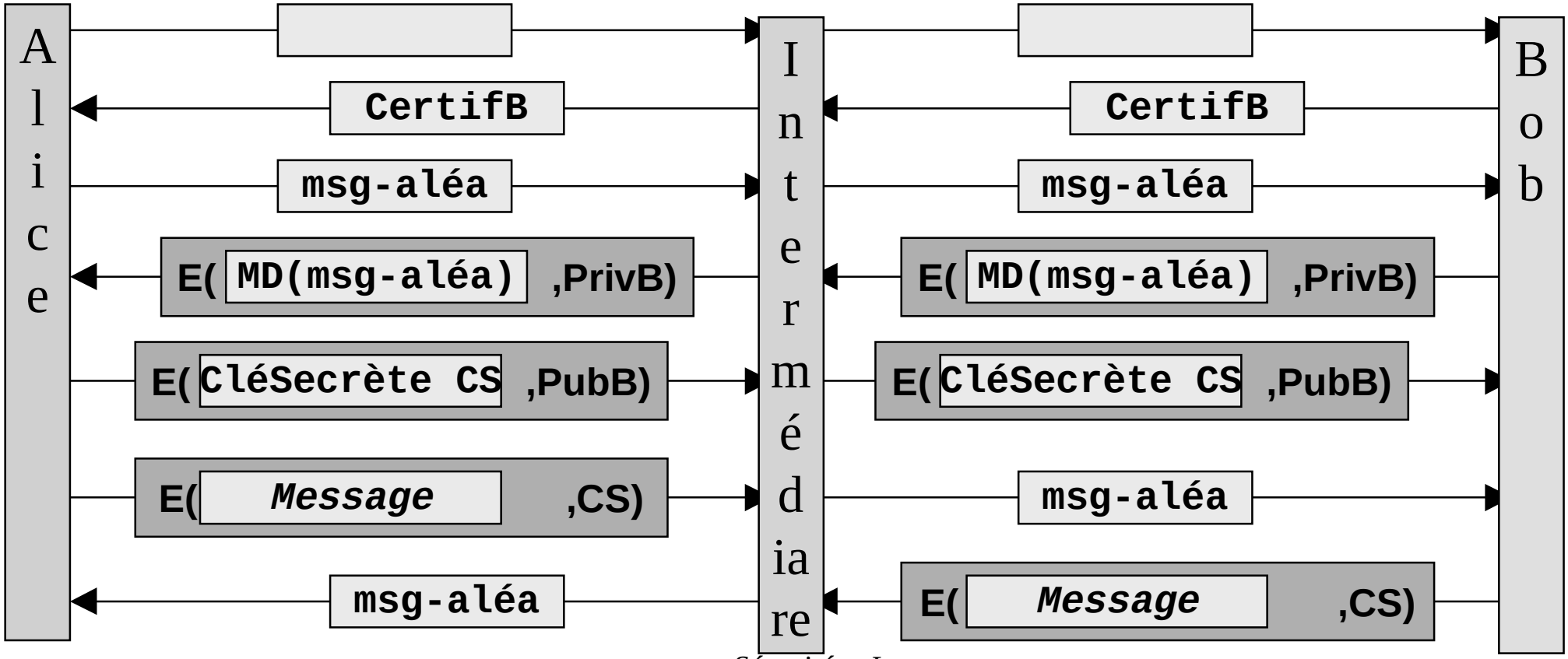
- Le certificat est signé par le Certifieur
- Tout le monde connaît la clé publique du Certifieur

L’Identification Certifiée



L’intégrité de la Conversation

- Problème : l’interception des messages



L’intégrité

- Correction
  - MAC : Message Authentification Code
    - ajouter au message échangé
      une authentification du message
    - MAC : = MD [conversation, clé_secrète]
- Protection contre le playback
    - un numéro de séquence de message
      ou un numéro aléatoire

Certifying Authorities (CA)

«Notaire Electronique»

- Service de délivrance de Certificat (X509)
- Service de Datation de Documents

- Des Acteurs :
  - VeriSign, Canada Postal Service, GTE, CommerceNet ...
- Des Produits :
  - Certificate Server de Netscape
    - génération et gestion propre des certificats

Service de Certification (i)

- commercialise et émet des certificats
  à la norme ISO X509

– Procédure de délivrance des certificats
  – définit par le CA (pièces notariales, ...)
– CIS (Certificate Issuing System)
  – processus sécurisé de fabrication des certificats
  – plusieurs opérateur humains indépendants

Service de Certification (ii)

- CRL (Certificate Revocation List)
  - liste des certificats corrompus ou invalidés
  - certificat “cassé”
  - certificat d’un employé licencié
- Problème
  - validité d’un certificat dans les contrats long terme.

Service de Datation

- DTS (Digital Time Stamp)
  - DTS(Document, Date)
    = { Document+ Date } clé_privée_du_CA
  - Processus Confidentiel de Datation:
    - A envoie un **digest** de son document au CA
    - CA retourne une DTS (**digest** , date_garantie_par_le_CA)
  - Problème
    - validité d'une DTS pour un contrat long terme
      => attaque d'un testament ... 15 ans après

Échanges Sécurisés

- Applications sans Connexion (ou Datagramme)
  - Authentification et Intégrité avec/sans Confidentialité de courriers électroniques
- Applications avec Connexion
  - dialogue entre deux applications
  - Authentification et Intégrité avec/sans Confidentialité

Échanges Sécurisés en mode datagramme (i)

- PGP (Pretty Good Privacy)
  - Auteur: Phil Zimmermann
  - RSA et IDEA
  - Freeware MIT, produits ViaCrypt et RSA Data Security
- PEM (Privacy Enhanced Mail)
  - RSA et DES, Certificats X509
  - assez compliqué à mettre en oeuvre
- PGP/MIME
  - RSA et IDEA, étudié par l'IETF

Échanges Sécurisés en mode Datagramme (ii)

- S/MIME
  - RC2 et DES, proposé par RSA Data Security, étudié par l'IETF
- MOSS (MIME Object Security Services)
  - étudié par l'IETF (RFC 1847-8)
- MSP (Message Security Protocol)
  - environnement X400 puis environnement IP
  - étudié du NSA (National Security Agency), norme NIST
  - RSA et DES

Échanges Sécurisés en mode datagramme (ii)

- Gestion des Clés (KMP)
  - Key Management Protocol
    - SKIP (Simple Key management for IP)
      - développé par Sun,
      - public, soumis à l'IETF et l'ANSI.
    - PSKMP (Photuris Session KMP)
      - développé par le WG IPSec de l'IETF.
    - ISAKMP (Internet Security Association KMP)
      - supporté par la NASA.

Échanges Sécurisés en mode connecté

- 2 approches
  - SSL
  - S-HTTP
- 1 compromis
  - SecureNet

SSL (Secure Socket Layer)

- Netscape, MasterCard, Bank of America, MCI et SGI
  - “au dessus” d’un protocole fiable de niveau transport : TCP
  - “en dessous” des protocoles de “haut niveau” : HTTP, FTP, TELNET, POP, NNTP
- Canaux de communication sécurisés
  - authentifié
  - serveur toujours / client optionel
  - confidentiel
  - chiffrage par clé symétrique (DES, RC4)
  - intègre (MAC par MD2, MD5)

S-HTTP (Secure HTTP)

- Terisa System fondé par RSA et EIT
  et soutenu par
  America Online, Compuserve,
  Prodigy, IBM, CommerceNet
- Sécurisation du protocole HTTP (niveau 7)
- Potentiel supérieur à SSL

SecureNet

- Terisa System et Netscape
- But:
  - supporter à la fois
    SSL et S-HTTP

La Preuve Electronique

- Dématérialisation du Papier
  le “Zéro Papier”
  - Nécessité d’une preuve électronique
    non répudiable
    - Signature et Datation

La Preuve Electronique aux USA

- en cours de légalisation
  dans les états de Californie, NewYork et Utah.
- Principe d'un contrat papier avec signature manuscrite amenant les deux parties à accepter la signature digitale des futurs documents à échanger.
  - le contrat papier spécifie également la méthode de signature et la taille minimum des clés utilisées.

La Preuve Electronique en France

Utilisation Légale des Outils de Chiffrage

- Usage:
  - Certification et Intégrité ("Signature Electronique")
  - Confidentialité
- Dans le Monde
  - Remarque:
    - les USA interdisent l’exportation de matériel de chiffrage performant (DES < 56 bits est autorisé à l’export depuis le 1/1/97 par le NSA)

Situation actuelle en France (i)

- 2 organismes
  - SCSSI : Service Central de la Sécurité des Systèmes Informatiques
    - relevant du Premier Ministre
      - contrôle du chiffrage
  - CNIL : Commission Nationale de l'Informatique et des Libertés
    - maintien de la confidentialité dans le secteur médicale
      - impose le chiffrage des données personnelles

Commission
Nationale
de l'Informatique
et des Libertés

Situation actuelle en France (ii)

- Intégrité, Authentification, Signature
  - Déclaration au SCSSI
- Confidentialité (i.e. chiffrage)
  - Demande au SCSSI : réponse lente, très lente.
  - Les outils doivent plutôt fonctionner
    suivant le **principe du séquestre des clés**
    - Exemple
      - Interdiction de télécharger PGP
        - 6 mois de prison et 200 000 FF d'amende

Exemple de mise en œuvre d ’un réseau sécurisé

- Réseau de médecins de Ville (Annecy, Armentières, ...)
  - RC4 (faible)
    - autorisé par le SCSSI
    - non autorisé par la CNIL
  - DES 56 (fort)
    - non autorisé par le SCSSI
    - autorisé par la CNIL
  - STOOL de CESIR, Solution MatraNet, ...
    - autorisé par la CNIL et le SCSSI
    - basé sur les clés de séquestre
    - mais propriétaire donc non standard et cher en général

Le Futur en France

- *On attend la loi ...*
- Tiers de Confiance
  - algorithme permettant le séquestre des clés
    - clé publique / clé privée
    - clés de session !!!
  - TC : “notaire” conservant les clés
  - probablement 1 par secteur d’activité
    - santé, bancaire, assurance ...

Les réseaux d’accès distants

- Qui et Comment ?
- La fraude
- La réponse

Qui et Comment

- Utilisateurs nomades / distants
  - Commerciaux, Télétravailleurs
  - Matériel
    - PC, PC Portable, PDA, ...
      + Modem (RTC, RNIS, GSM, ...)
      - Remarque : l'interface Air du GSM est chiffré.
    - Un point d'accès au réseau d'entreprise
  - Connexion vers réseau IP
    - PPP, SLIP

La fraude

- l’écoute de la ligne
    - capture du mot de passe, ...
- le vol du terminal
    - configuration automatique de la connexion

La réponse

- Mot de Passe
  - PPP (RFC1334)
  - PAP (Password Authentification Protocol)
    - les mots de passe circulent en clair
  - CHAP (Challenge Handshake Authentification Protocol)
  - PPTP (Point to Point Tunneling Protocol)
- Rappel Automatique
- Serveur d'Authentification: Kerberos, Netware, ...

Protection du Réseau privé

- Les Risques
  - l'Attaque de machines
    - Le ver de R.T. Morris en 1988 (systèmes BSD)
    - CRACK (/etc/passwd)
    - SATAN, Internet Scanner (teste les versions défaillantes de certains deamons IP)
  - les Virus
    - Import de fichiers (DK, CD, FTP, HTTP…)
    - Réception de fichiers attachés par mail

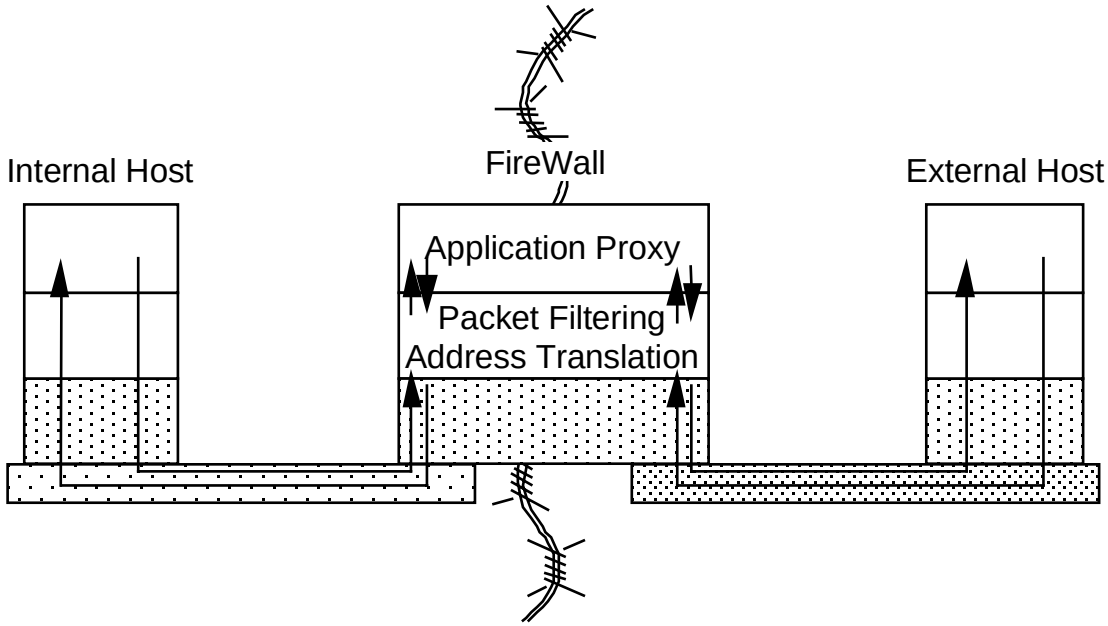
Protection du Réseau privé

- La Réponse
  - Gardes Barrières
  - Identification sûr
  - Audit Sécurité

Les Gardes Barrières (i)

- FireWalls (Coupe Feu)
  - pour un réseau
    - Checkpoint Software Tech (*40% du marché*), BorderWare, SUN, IBM, DEC, Raptor.
  - Spoofing (usurpation d'adresses IP)
    - => Filtrage Dynamique
  - pour une machine : TCP Wrapper

Les Gardes Barrières (ii)



Les Virus et les Gardes Barrières

- Fichiers seuls, compressé, en archive
- Vecteur : HTTP, FTP, SMTP/MIME

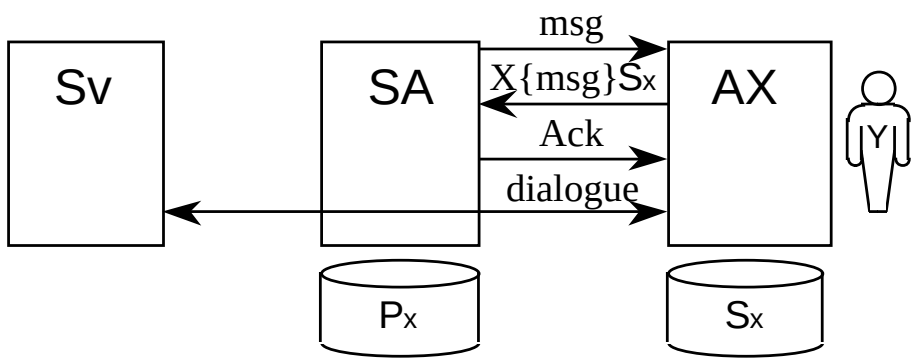
- CVP (Content Vectoring Protocol)
  - PlugIn AntiVirus pour FW

Identification

- auprès du réseau
  - coté réseau
    - serveur d'accès
      - parfois c'est une fonction du Firewall
  - Coté Terminal
    - Stockage de la clé privée
      - Fichier, Carte Magnétique, Carte à Puce, Calculette

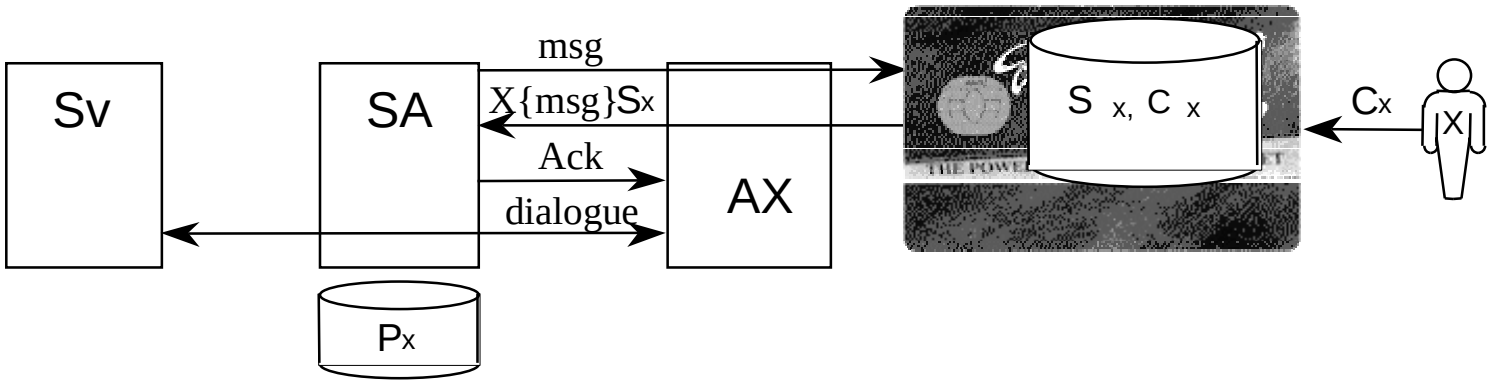
Stockage des Clés Privées (i)

- Fichier ou Carte Magnétique
  - Lecture du fichier contenant la clé privée, Perte/Vol
  - Duplication de la carte magnétique



Stockage des Clés Privées (ii)

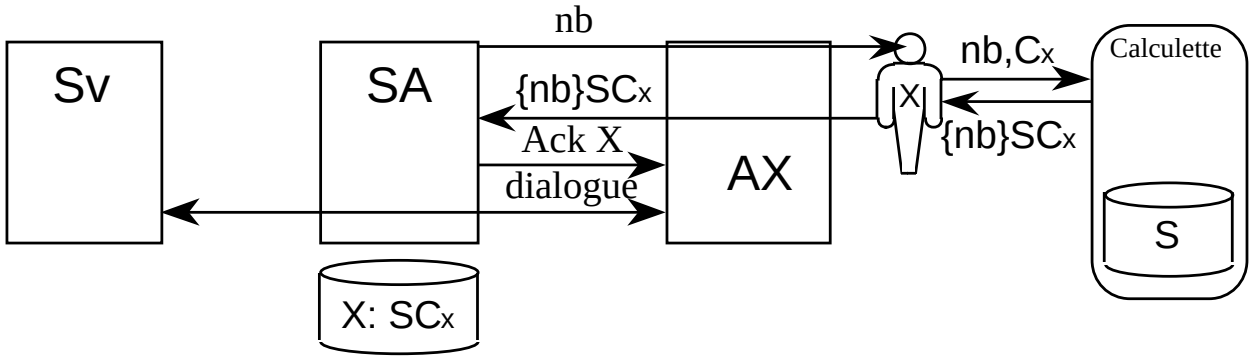
- Carte à Puce (GemPlus, Schlumberger, JavaCard Forum, ...)
  - Nécessité d'un lecteur ISO par ou sans Contact
  - \+ Lecteur ISO PCMCIA



Stockage des Clés Privées (iii)

- Calculette (ActivCard, SecurId, ...)
  - **-** Algorithmes souvent propriétaires
  - **-** Délai d'initialisation : lecture et 2 frappes sans erreur !
  - + Accès à des applications par des Serveur Vocaux

    NB: algorithme SecurID dans modems PCMCIA



La sécurité des codes mobiles (i)

Qu'est ce qu'un code mobile ?

- un code disponible sur un serveur de fichiers (httpd)
- le chargement de ce code sur votre client
    - pour installation ou mise à jour
        - HTTP
        - ou « push »
- l 'exécution de ce code sur votre client
    - en général, encaspuslé dans un page HTML joué par un butineur Web (browser)
- Risque
    - Virus, Usurpation d 'identité derrière un Firewall, ...

La sécurité des codes mobiles (ii)

- Java, CAML, TeleScript, JavaScript ...
  - bytecode interprété
    - contrôle de code au chargement
    - applications
      - applets (appliquettes en vf), servlets, « aglets » (agents mobiles), le « push »
  - bytecodes non signés
    - Bac à sable (Sandbox)
      - pas d ’accès aux ressources du poste
      - connexion réseau seulement vers le serveur d ’origine
  - bytecodes signés
- Activex
  - code objet signé :
    - ne désactivez pas le contrôle de la signature dans MS IE

La sécurité n’est pas statique !

- Liste de diffusion
  - CERT (Computer Emergency Response Team)
  - IETF (Internet Engeneering Task Force)
    - Alerte à Malibu !
- Audit Sécurité
  - 20% du budget “Sécurité” par an

Bibliographie (i)

- Cryptographie
  - Applied Cryptography, by Bruce Schneier (Wiley), ISBN 0-471-59756-2 (ISBN 2-84180-036-9 en VF)
- Législation
  - www.cnil.fr
  - Echange de Données Informatisé : Contrôle et audit d'un système EDI, AFNOR & EDIFRANCE 1994, ISBN 2-12-481312-9.
  - G. Beaure d'Augère, P. Bresse, S. Thuillier, «Paiement numérique sur Internet», Ed ITP France, 1997, ISBN 2-84180-160-8

Bibliographie (ii)

- Sécurité des Systèmes UNIX
  - Unix System Security: A Guide for Users and System Administrators by David Curry, O'Reilly
  - Practical Unix Security, by Simson Garfinkel and Gene Spafford,O'Reilly,ISBN 0-937175-72-2
- Internet Security Alerts
  - RISKS
    - Forum on Risks to the Public in Computers and Related Systems, http://catless.ncl.ac.uk/Risks
  - CERT
    - ftp://ftp.cert.org/pub/cert_advisories/

Bibliographie (iii)

- Sécurité des Serveurs Web
  - How to Set Up and Maintain a World Wide Web Site: The Guide for Information Providers, by Lincoln D. Stein (Addison-Wesley), ISBN 0-201-63389-2
  - Managing Internet Information Systems, by Cricket Liu, Jerry Peek, Russ Jones, Bryan Buus, and Adrian Nye (O'Reilly), ISBN 1-56592-051-1
- Firewalls
  - Firewalls and Internet Security: Repelling the Wily Hacker by William R. Cheswick and Steven M. Bellovin,Addison-Wesley, ISBN 0-201-63357-4
  - Building Internet Firewalls, by D. Brent Chapman and Elizabeth D. Zwicky, O'Reilly, 1st Edition September 1995, ISBN 1-56592-124-0

Bibliographie (iv)

- CORBA
  - CORBA 2.1, «Security Service Specifications», OMG 1997

Vos suggestions et vos remarques

- Merci de me les retourner à
  - Didier DONSEZ, donsez@univ-valenciennes.fr, Fax 03 27 14 11 83
- Avez vous trouvé ce cours instructif ?
  - Est il complet ?
  - Qu ’est qu ’il manque ?
  - Qu ’est que vous auriez aimé voir plus développé ?
  - Est il bien organisé ?
  - ...
- Quels sont votre fonction et votre domaine d ’activité ?