Sécurité et Temps dans les Systèmes Répartis

- I – TERMINOLOGIE ET LIMITES IMPOSÉES
  - 1.1 Définitions
  - 1.2 Le droit
  - 1.3 La sécurité
  - 1.4 Le temps
  - 1.5 Sécurisation de l'ordre causal
- 2 – LES PROTOCOLES DE CRYPTOGRAPHIE
  - 2.1 Symétrie, asymétrie, hachage
  - 2.2 La signature électronique
  - 2.3 Preuve faible contre preuve forte
- 3 – DISCUSSION

Stephen Navarro

Bibliographie

- [Carrez98] C. Carrez, G. Florin, C. Toinard. Causally and totally ordered multicast protocols. 1998.
- [Fausse01] A. Fausse. La signature électronique. 2001.
- [Menezes96] A. Menezes. Handbook of Applied Crypto. 1996.
- [Mercadal93] B. Mercadal. Droit des affaires. 1993.
- [Natkin02] S. Natkin. Protocoles de sécurité d'Internet. 2002
- [Reiter99] M. Reiter. Securing causal relationship in distributed operating systems. 1999.
- [Tanenbaum98] A. Tanenbaum. Réseaux. 1998.

Définitions

- La sécurité représente la capacité d'un système à résister à des attaques menées à l'encontre de son dessein et de ses actifs.

Sûreté de fonctionnement	**Sécurité**
Probabiliste et prévisible	Aléatoire et imprévisible
MTBF MTTR MTTF	Virus, pirates, Cryptographie
La faute, l'erreur, la panne (dans cet ordre)	Intention délibérée de nuire au système

Politique de sécurité

- Le périmètre d'action : qui, où, quand ?
- Les droits : octroyés ou retirés,
- Les attaquants : nature, force,
- Les défaillances potentielles : nature.

- Politique discrétionnaire ou obligatoire.

- Les spécifications fonctionnelles sont énoncées avant les moyens mis en œuvre et non l'inverse.

Propriétés de la sécurité

- Authentification : suite à identification, êtes vous celui que vous prétendez être ?
- Confidentialité : êtes vous habilité à lire cette information à ce niveau ?
- Intégrité : êtes vous habilité à modifier cette information ?
- Non répudiation : origine et destination
- Auditabilité : détecter de façon infalsifiable les atteintes à la sécurité

Le droit

- La jurisprudence est adaptée pour réprimer la fraude et pour légitimer la force probante.

- Loi Godfrain : Art. 323 du Code Pénal,
  - Accés, atteinte, maintien,
- Signature électronique :
  - Art. 1316 du Code Civil : création, vérification,
  - Décrêt du 30 mars 2001 : loi applicable.

- Clefs de chiffrement :
  - France : DCSSI dépend du 1er ministre (40, 128),
  - Chine : le chiffrement est interdit,
  - États Unis : exportations contingentées (56).

Principes de bases de la sécurité

- Kerckhoff : (1863) la sécurité ne doit pas être procurée par l'obscurité et l'ignorance;
- Trusted clients : le niveau de sécurité est suffisant, donc le serveur fait confiance;
- Oracle : un problème A sous-ensemble d'un problème B, peut apporter le même type de solution, voire répondre oui ou non;
- Maillon faible : si une faiblesse existe quelque part, et si le système est investi, la sécurité s'écroule.

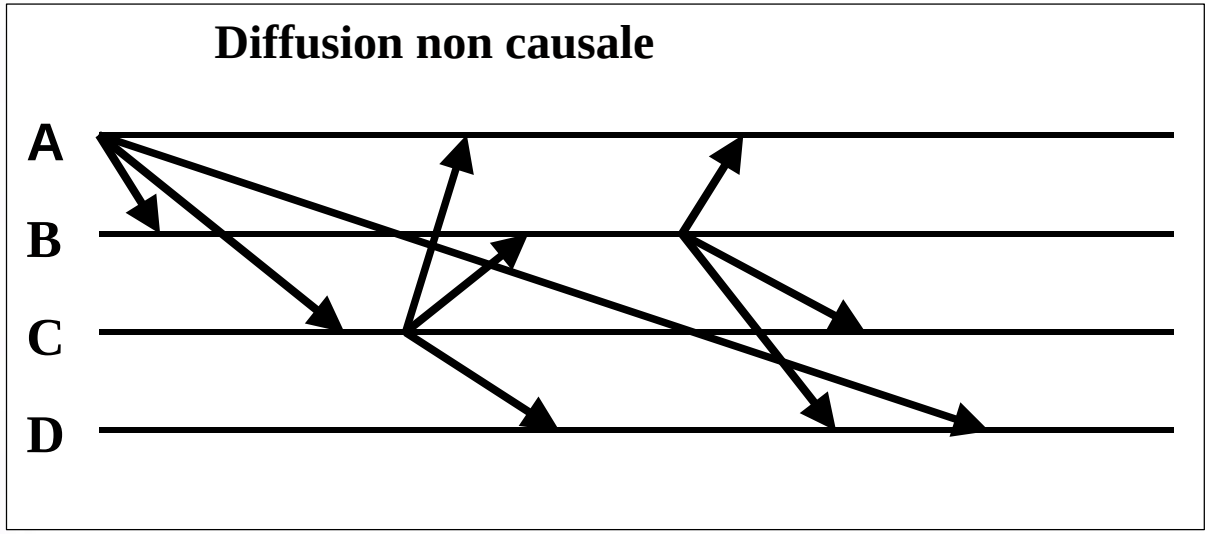
Types d'attaque

- Attaque active, attaque passive
- Attaque directe sur le chiffrement
- À partir de texte connu
- À partir de texte en clair choisi
- À partir de texte en clair choisi et adaptative
- À texte chiffré choisi
- À texte chiffré choisi et adaptative
- Attaque aléatoire, principe de l'oracle

Stephen Navarro

LE TEMPS

- Heure physique : U T C , T T S, N T P
- Diffusion causale, locale, totale :
  - émission, livraison, réception;
  - locale + causale ⇔ totale.



Stephen Navarro

Sécurisation de l'ordre causal

- Destruction de la causalité (DENIAL)
  - Prophylaxie par serveur de causalité
  - Prophylaxie par approche conservatrice
- Fabrication de la causalité (FORGERY)
  - Prophylaxie par horloges vectorielles
  - Prophylaxie par piggybacking

La clef

- La clef est formatée selon une norme de chiffrement de clef publique conformément à la RFC 2315;
- La clef est associé à une valeur, c'est un ensemble d'octets;
- La clef est la trappe d'un algorithme,
- La clef est privée, publique, session, secrète, interface, interne, management, racine, distribuées sur plusieurs machines, bi-clé.

Protocole Symétrique

- La clef est identique pour l'auteur (ALICE) et pour le destinataire (BOB). Clef = KAB
- Exemples : chiffre de Jules César, DES
- Chiffrement : $C = \{ M \}^{DES}_{KAB}$
- Déchiffrement : $M = \{ C \}^{DES}_{KAB}$
- Si l'espionne (ESTELLE) parvient à voler la clef commune, le secret est trahi.

Protocole Asymétrique

- Exemples : RSA, El Gamal, DSA

- Chaque acteur a un biclé (privée, publique)
- ALICE possède un bi-clé (KA , ka)
- BOB possède un bi-clé (KB , kb)
- Alice chiffre une clef de session

$$C = \{ \text{clef-session} \}_{\substack{\text{DSA} \\ \text{kb}}}$$

- Bob déchiffre la clef de session

$$\text{clef-session} = \{ C \}_{\substack{\text{DSA} \\ \text{KB}}}$$

- Mais, les temps de chiffrement sont longs.

Protocole à Fonction de Hachage

- Suite d'opérations à sens unique sans trappe.
- Fonction garantie sans collision.
- 2 messages proches, 2 empreintes différentes.
-
- Alice chiffre un message, obtient un résumé.
- Alice envoie le message et le résumé.
- Message = (M , $\{M\}^{MD5}$)
- Bob chiffre le message, obtient un résumé.
- Bob compare le résumé avec celui d'Alice.
- Si les deux résumés sont identiques,
- alors Estelle n'a-t-elle rien modifié ?

Signature électronique

- Le certificateur détient une clef avec laquelle il émet le certificat garantissant le lien entre la clef publique et la personne qui détient la clef privée correspondante.

- Le résumé du message est chiffré avec la clef privée de l'auteur fournie par le prestataire de service de certification (PSC).
- C'EST CELA UNE SIGNATURE.

- Le destinataire obtient la clef publique de l'auteur auprès du Prestataire de Certification.
- Le destinataire vérifie l'identité de l'auteur et l'intégrité des données qu'il a obtenues.

Stephen Navarro

Caractéristiques de la signature électronique

- Authentification : de l'auteur, avec la clef privée;
- Vérification : de l'auteur du message et de l'intégrité du message, avec la clef publique;
- Non répudiation : l'auteur doit reconnaître avoir signé le message, (sauf vol de clef privée);
- Unicité : il est impossible d'utiliser la signature pour un autre message;
- Scellement : une modification du message invalide la signature électronique.

Outil de gestion des clefs : KEYTOOL

- navarr_s@petitfour:~> keytool -v -list
- Enter keystore password: sel_toto
- Keystore type: jks
- Keystore provider: SUN
- Your keystore contains 1 entry:
- Alias name: navarr_s
- Creation date: Tue Feb 26 13:35:32 CET 2002
- Entry type: keyEntry
- Certificate chain length: 1
- Certificate[1]:
- Owner: CN=Stephen Navarro, OU=CEDRIC, O=CNAM, L=Paris, ST=idf, C=FR
- Issuer: CN=Stephen Navarro, OU=CEDRIC, O=CNAM, L=Paris, ST=idf, C=FR
- Serial number: 3c7b810a
- Valid from: Tue Feb 26 13:35:22 CET 2002
- until: Mon May 27 14:35:22 CEST 2002
- Certificate fingerprints:
- MD5: 22:D2:E1:26:B6:AE:55:8E:AE:E5:69:17:5D:BE:4F:0A
- SHA1: 34:1D:17:4F:43:AD:A8:E7:B7:8E:75:B5:DB:90:03:66:4D:72:45:85

Preuve Faible contre Preuve Forte

- **Preuve faible : Dans un schéma de preuve faible, l'approche est passive. {A} peut prouver que dans les opérations qui lui incombent, les exigences du protocoles ont été respectées.**

- **Preuve forte : Dans un schéma de preuve forte, l'approche est active. {B} ne peut pas altérer les propriétés d'ordre sans que cela soit décelable.**

  - **Un principal peut endosser les deux rôles.**
  - **Le comportement de {B} est byzantin.**

Le pays de cocagne, c'est par là …

- Construire un protocole de sécurité :
  - qui assure à long terme l'authenticité et l'intégrité d'un document électronique;
  - qui soit utilisable dans le contexte de la jurisprudence relative à la signature électronique;
  - qui permette la formalisation de contrats synallagmatiques sans intervention d'un tiers de confiance.

Stephen Navarro