Réseaux

Chapitre 7 - Cryptographie et sécurité dans les réseaux informatiques

Claude Duvallet

Université du Havre
UFR Sciences et Techniques
25 rue Philippe Lebon - BP 540
76058 LE HAVRE CEDEX
Claude.Duvallet@gmail.com

Plan de la présentation

Introduction (1/2)

- Des réseaux de plus en plus larges et développés.
- De plus en plus de personnes possèdent des connexions à hauts débits leur permettant d'accéder à des ressources réseaux disponibles à travers le monde entier.
- De nombreuses entreprises fonctionnent grâce au réseau Internet :
  - la communication inter-agences et l'échange de documents électroniques,
  - les transactions bancaires en ligne ou par des réseaux plus restreints,
  - le commerce électronique (site de ventes en ligne, etc.).
- Certaines informations doivent rester du domaine privés : échanges effectués entre quelques utilisateurs.

Introduction (2/2)

- Les identifications doivent se faire sans que tout le monde puisse connaître votre mot de passe.
- Des besoins :
  - la sécurité des moyens de connexion,
  - la confidentialité des documents et des informations échangées,
  - l'authentification des moyens de connexions.

$\Rightarrow$ cryptographie = crypter les informations circulant sur Internet.

Les risques (1/2)

- L'acheminement erroné :
  - des données confidentielles parviennent à un autre utilisateur.
- Les analyseurs de protocole :
  - des logiciels qui analysent le trafic réseau non crypté.
- La bombe logique :
  - c'est la modification d'un programme informatique pour le faire réagir d'une certaine manière dans certaines circonstances (écrasement de fichiers à certaines dates, augmenter le salaire si je suis le salarié X, etc.).
- Le cheval de Troie :
  - c'est un programme qui semble effectuer une tâche mais qui en effectue une autre (à votre insu).

Les risques (2/2)

- La contrefaçon :
  - création de documents ou d'enregistrements illicites présentés comme de vraies pièces.
- La compromission :
  - cela concerne les fuites de signal par rayonnement électromagnétique.
- La fraude :
  - exploitation du système d'information d'une entreprise en vue d'abuser ou d'exploiter ses ressources.
- La mascarade :
  - c'est l'usurpation du code d'accès d'un utilisateur pour examiner ses données ou utiliser ses programmes, ressources, etc.
- La porte dérobée :
  - Le plus souvent, elle est mise en œuvre par le concepteur pour ajouter des fonctionnalités supplémentaires lui permettant de s'introduire dans le système.

Protocoles sécurisés et non sécurisés

- Les protocoles non sécurisés par couche OSI :
  - Couche 2 (liaison de données) : PPP.
  - Couche 3 (réseau) : IP.
  - Couche 4 (transport) : TCP.
  - Couche 7 (application) : FTP, HTTP, LDAP, SMTP, POP, IMAP.
- Les protocoles sécurisés par couche OSI :
  - Couche 2 (liaison de données) : L2TP, PPTP.
  - Couche 3 (réseau) : IPv6, IP-Sec.
  - Couche 4 (transport) : SSL, SOCKS, TLS.
  - Couche 7 (application) : PGP, S/HTTP, SET, etc.

Cryptographie (1/2)

- La cryptographie = deux actions :
  - le chiffrement : transformation d'un texte clair (M) en un texte indéchiffrable (C) sous le contrôle d'une clé et d'une fonction de transformation,
  - le déchiffrement : transformation d'un texte indéchiffrable en un texte clair compréhensible en utilisant la même fonction de transformation et une clé dite « clé de déchiffrement ».
- Le chiffrement et le déchiffrement sont deux opérations complémentaires effectuées en utilisant la même fonction de transformation et, selon les cas la même clé ou deux clés différentes mais complémentaires.

Cryptographie (2/2)

- Un procédé de chiffrement est défini par un quadruplet (T, C, K, F) où :
  - T est le texte en clair à chiffrer,
  - C est le cryptogramme résultant du processus de chiffrement,
  - K est la clé de chiffrement,
  - F est la fonction de transformation.
- Les fonctions de transformation, dites fonctions de calcul, varient d'une simple substitution ou transposition, à une suite d'opérations complexes et de fonctions mathématiques particulièrement bien choisies, de façon à assurer l'unicité et la justesse du cryptogramme généré à partir de n'importe quel texte en clair.

Algorithmes à clés secrètes (1/2)

- Un algorithme de chiffrement est dit à clé secrète, ou aussi algorithme symétrique, si la clé utilisée pour le chiffrement et déchiffrement est la même.
- Le cryptogramme ${M_k}^a$ est obtenu par chiffrement du texte en clair M en utilisant la même clé K.
- L'action de chiffrement est symboliquement représentée par "$encrypt_{cl}{}^{algo} M$" et celle de déchiffrement par $M = decrypt(encrypt({M_k}^a)_k{}^a)$.
- L'utilisation de tels algorithmes exige le partage d'une clé dite clé de communication entre l'émetteur et le récepteur.

Algorithmes à clés secrètes (2/2)

- D.E.S. : Data Encryption Standard
  - D.E.S. a été proposé par IBM et adopté par le bureau national des standards des États-Unis en 1977.
  - Basé sur l'utilisation d'une clé de 64 bits.
- I.D.E.A : International Data Encryption Algorithm
  - I.D.E.A. a été proposé en 1991 par Xuejia Lai et James Massy.
  - Basé sur l'utilisation de 128 bits.

Algorithmes à clés publiques (1/7)

- Définition d'une paire de clés pour chaque utilisateur : P et S.
- La clé S est la clé secrète : elle n'est jamais échangée ou communiquée à une tierce personne.
- P est la clé publique : elle est volontairement partagée et mise à disposition de tous les autres utilisateurs qu'ils soient légitimes ou intrus.
- Tout message chiffré par la clef secrète S d'un utilisateur A ne peut être déchiffrée que par la clef publique P qui lui est complémentaire et vice versa.
- La fiabilité des systèmes à clefs publiques repose sur la possibilité de trouver une paire de clés à la fois complémentaires et inviolable.

Algorithmes à clés publiques (2/7)

- Quel que soit le processus d'attaque, quelle que soit la technique de mise en œuvre, et quelle que soit la puissance des machines utilisées, la clé publique à elle seule ne doit théoriquement pas permettre d'en déduire la clé secrète.
- Le coût d'une telle opération doit être excessivement cher et donc infaisable.
- Contrairement aux algorithmes à clés symétriques, les algorithmes à clés publiques n'utilisent pas en général le même processus et cycle de calcul lors du chiffrement et du déchiffrement.
- Les fondements théoriques de cette technique supposent l'utilisation de deux fonctions complémentaires.
- Toute la performance des systèmes asymétriques repose sur la fiabilité des fonctions de calculs utilisées lors du chiffrement et du déchiffrement.

Algorithmes à clés publiques (3/7)

- Pour assurer cette caractéristique, certains fondements mathématiques sont utilisés. En effet, les fonctions de calcul et de transformation, utilisées dans ces algorithmes sont :
  - soit des fonctions de puissance dans un anneau d'entier modulo N,
  - soit des fonctions exponentielles dans un corps fini.
- L'algorithme R.S.A. (Rivest Shamir Adleman) est jusqu'à nos jours considéré comme la référence des algorithmes asymétriques.
  - Il a été développé au M.I.T. en 1977 par trois ingénieurs : Ronald Rivest, Adi Shamir et Leonard Adleman.
  - Le principe du R.S.A. a été, depuis, utilisé dans de nouveaux algorithmes, il est particulièrement adapté aux mécanismes de signatures numériques.
  - Le chiffrement et déchiffrement se basent sur l'application de deux équations :
    - Chiffrement : $C = M^p \ mod \ N$
    - Déchiffrement : $M = C^s = (M^p)^s \ mod \ N$

Algorithmes à clés publiques (4/7)

- L'action de chiffrement et de déchiffrement se basent sur une fonction de puissance modulo N.
- Le texte chiffré est obtenu en élevant le message en clair M à la puissance p modulo N.
- Le déchiffrement se base également sur la même fonction de puissance modulo N en utilisant la clé S inverse de la clé P.
- Principe d'une session de communication sécurisée :
  - On commence par générer sa propre paire de clés (P,S).
  - On communique sa clé publique P aux différents interlocuteurs.
  - La clé publique et la clé secrète sont composées de deux éléments résultant d'un calcul particulier.

Algorithmes à clés publiques (5/7)

- Suivant l'objectif de la session de communication on utilise soit la clé publique du récepteur comme clé de chiffrement soit la clé secrète de l'émetteur :
  - si l'émetteur désire que seul le récepteur puisse analyser et interpréter les messages qu'il va lui adresser, il doit utiliser la clé publique du destinataire pour chiffrer les messages,
  - si l'objectif est d'assurer l'authenticité du message, c'est-à-dire de fournir le moyen de vérifier l'identité de son émetteur, le message sera chiffré en utilisant la clé secrète de l'émetteur. Une clé publique d'un autre émetteur ne pourra jamais déchiffrer ce message d'où la garantie d'authentification.
- La génération de la paire des clés (P, S) nécessite la vérification de plusieurs conditions.

Algorithmes à clés publiques (6/7)

- L'algorithme de génération des clés R.S.A. est sommairement décrit comme suit :
  - Choisir une combinaison unique de nombres premiers (p, q) tels que : $p > q$.
  - Calculer le modulo N = $p \times q$.
  - Calculer la fonction d'Euler Φ appliquée à N : on ne peut pas calculer Φ si on ne connaît pas la décomposition de N en $p \times q$ $\Phi(N) = n \times [(1 - \frac{1}{P_1}) \times (1 - \frac{1}{P_2}) \times ... \times (1 - \frac{1}{P_n})]$ où $P_1 ... P_n$ représentent les facteurs premiers de l'entier N.
  - Cette décomposition est d'autant plus difficile à deviner que N devient grand.
  - L'utilisateur de R.S.A. doit ensuite déterminer la valeur e en fonction de $\Phi(N)$. Il faut que e soit premier et que le plus grand diviseur commun de e et $\Phi(N)$ soit égale à 1.

Algorithmes à clés publiques (7/7)

- Algorithme de génération des clés R.S.A. (suite) :
  - Une fois la valeur de e calculée, l'utilisateur n'a plus qu'à calculer le complément de e, c'est-à-dire la valeur d telle que d soit l'inverse multiplicatif mod $\Phi(N)$ de e.
  - Si par hasard, il arrive que e soit égale d, il est recommandé de trouver une autre combinaison (p, q).
  - Une fois ces phases terminées, l'utilisateur rends publique les paramètres e et N qui constituent la clé publique P.
  - Il garde secret q et d qui forment la clé secrète S.

R.S.A. : mise en œuvre (1/3)

- Déterminer une clé publique et une clé privée :
  - Pour déterminer ces deux clés, il faut d'abord trouver deux nombres premiers p et q suffisamment grand.
  - On calcul n le produit de ces deux nombres : $n = p \times q$. On estime que lorsque n est codé sur plus de 1024 bits, la sécurité est suffisante.
  - On trouve ensuite un nombre e tel qu'il soit premier avec $p-1$ et $q-1$.

Définition : a et b sont premiers entre eux s'ils n'ont aucun facteurs premiers en commun. Par exemple 12 est premier avec 35 car 12 = 3 $\times$ 2 $\times$ 2 et 35 = 7 $\times$ 5.

  - On calcul enfin d tel que $(d \times e)\ mod\ (p-1)(q-1) = 1$.
  - On peut :
    - soit choisir e en respectant la règle du paragraphe précédent et calculer d avec cette formule,
    - soit choisir d et calculer e avec cette formule.

R.S.A. : mise en œuvre (2/3)

- On a défini les nombres suivants p, q, n, e, d :
  - La clé publique est constituée du couple [e, n].
  - La clé privée est constituée du couple [d, n]. Le nombre d ne doit pas être communiqué.
  - Les nombres p et q ne doivent pas être communiqués.
- Crypter/Décrypter :
  - Soit m le nombre à crypter et c le nombre crypter :
    - pour crypter : $c = m^e \ mod \ n$.
    - pour décrypter : $m = c^d \ mod \ n$.
  - Tout le monde peut crypter avec la clé publique de son correspondant mais seul ce dernier peut lier le message.

Exemple :

- $p = 13$ (un nombre premier).
- $q = 31$ (un nombre premier).
- $n = 403$ (produit $p \times q = 13 \times 31$).
- $e = 11$ (e est premier avec $p - 1 = 12$ et $q - 1 = 30$.

R.S.A. : mise en œuvre (3/3)

- A veut envoyer à B le nombre $m = 18$. Tout le monde sait que B a pour clé publique $e = 11$ et $n = 403$. Il calcul
  $c = m^e \ mod \ n = 18^{11} \ mod \ 403$
  $c = 64268410079232 \ mod \ 403 = 307$.
- A envoi ce nombre $c = 307$ à B. Mais un personne indiscrète C arrive à capter ce nombre c. Heureusement seul B connaît sa clé privée, c'est-à-dire $d = 131$. Il est le seul à pouvoir calculer.
  $m = c^d \ mod \ n$
  $m = 307^{131} \ mod \ 403$
- Le nombre 307^{131} a 326 chiffres en base 10 !
- Les nombres p, q, n devrait être beaucoup plus grands pour s'assurer que C ne puisse pas décomposer $n = 403$ en 13×31.

Sécurisation des moyens de paiement (1/6)

- Plusieurs protocoles pour la gestion sécurisée ont été développés :
  - PGP : Pretty Good Privacy.
  - S-HTTP : extension sécurisée du protocole HTTP.
  - SSL : Secure Socket Layer.
- PGP :
  - PGP est un logiciel de chiffrement gratuit, simple à utiliser et fonctionnant sous de nombreuses plates-formes (Unix, Windows, mac, etc.).
  - PGP est interdit d'exportation des USA.
  - Le chiffrement est soumis à autorisation en France.
  - Ce logiciel protège des fichiers, soit lors de leur transmission sur le réseau (courrier électronique ou autre méthodes) soit en local.

Sécurisation des moyens de paiement (2/6)

- S-HTTP : une extension sécurisée de HTTP
  - Un protocole d'application conçu pour offrir les garanties de confidentialité, d'authenticité, d'intégrité et de non-désaveu.
  - La fonction d'intégrité des données assure la non altération des informations et la fonction de non-désaveu assure l'accord non réfutable de l'acheteur.
  - S-HTTP crypte les messages échangés et permet de leur adjoindre une signature, il est conçu comme une boîte à outil pour le WEB pouvant accueillir toutes les applications qui puissent un jour exister.
  - S-HTTP peut employer différents algorithmes de cryptage (DES, triple DES, DESX, IDEA, RC2, LDMF, etc.).
  - L'identification peut être réalisée par plusieurs méthodes d'identité certifiée, dont R.S.A., et également par KERBEROS.

Sécurisation des moyens de paiement (3/6)

- SSL : Secure Socket Layer, développé par Netscape
  - SSL peut servir de base à HTTP, FTP ou TELNET.
  - La phase de négociation au départ permet l'authentification du serveur et optionnellement celle du client.
  - Il repose sur l'algorithme de R.S.A. (Rivest, Shamir, Adleman).
  - Le fait que R.S.A. soit à clé publique ou asymétrique signifie que deux clés sont utilisées, une pour le verrouillage, l'autre pour le déverrouillage. Les clés publiques sont habituellement de grands nombres aléatoires tandis que les clés symétriques sont constituées de plusieurs nombres n'ayant aucun rapport entre eux.
- Fonctionnement de SSL (1/4) :
  - Au démarrage de la session le protocole SSL identifie le serveur, le client puis négocie les paramètres de cryptage.

Sécurisation des moyens de paiement (4/6)

- Fonctionnement de SSL (2/4) :
  - Durant la phase d'identification, le serveur expédie ses certificats et indique ses algorithmes de cryptage de prédilection.
  - Durant la session, SSL assure la confidentialité et la fiabilité des échanges, par des techniques de cryptage et d'identification des messages.
  - Le client génère aléatoirement une première clé dite « clé de session », qu'il crypte par la clé publique du serveur avant de la lui expédier.
  - Le serveur se fait connaître en retournant un message crypté par la clé de session. Les échanges qui suivent sont cryptés par des clés dérivées de la clé de session.
  - En cas d'identification du client (phase facultative), le serveur expédie au client un message quelconque et le client s'identifie en envoyant sa signature électronique sur ce message, accompagné de ses certificats.

Sécurisation des moyens de paiement (5/6)

- Fonctionnement de SSL (3/4) :
  - SSL peut employer différents algorithmes de cryptage. R.S.A. est employé durant la phase d'identification.
  - L'ensemble de ce processus est maintenant complètement transparent pour l'utilisateur.
  - Une nouvelle paire de clés est générée à chaque établissement de la communication entre le logiciel client de l'utilisateur et le logiciel serveur. La communication est donc entièrement sûre mais en aucun cas le serveur commercial ne pourra s'assurer de l'identité de l'utilisateur à l'autre extrémité.
  - Une façon de résoudre ce problème est de joindre à ce processus un système de validation comme par exemple NIP (Numéro d'identification Personnel) qui s'obtient par une pré-inscription préalable.

Sécurisation des moyens de paiement (6/6)

- Fonctionnement de SSL (4/4) :
  - La version SSL3 emploie les trois fonctions de négociation qui sont essentielles à l'exercice de transactions sûres :
    - l'authentification mutuelle des parties (client et serveur),
    - le chiffrement des données transmises,
    - l'intégrité de celles-ci au travers de la couche « transport ».

$\Rightarrow$ des moyens de paiement sécurisés et fiables.

$\Rightarrow$ seul gros problème : l'authentification du client.

$\Rightarrow$ solution : signature numérique.