Protocoles Cryptographiques

Yannick Chevalier
Université de Toulouse
CSA M1, Security

Plan

Introduction

Buts

TLS

PKI

Protocoles *vs.* Primitives

Primitives

- opérations de transformations sur les données
- des garanties sont fournies sur les transformations possibles et impossibles

Protocoles cryptographiques

- séquence de messages dont le contenu a été produit par l'application de primitives cryptographiqes
- un protocole cryptographique a un **but**, qui est une assurance donnée à un participant s'il respecte les règles du protocole

Suite du cours

- buts habituels
- notation simple pour les protocoles cryptographiques
- analyse basique d'un protocole cryptographique

Plan

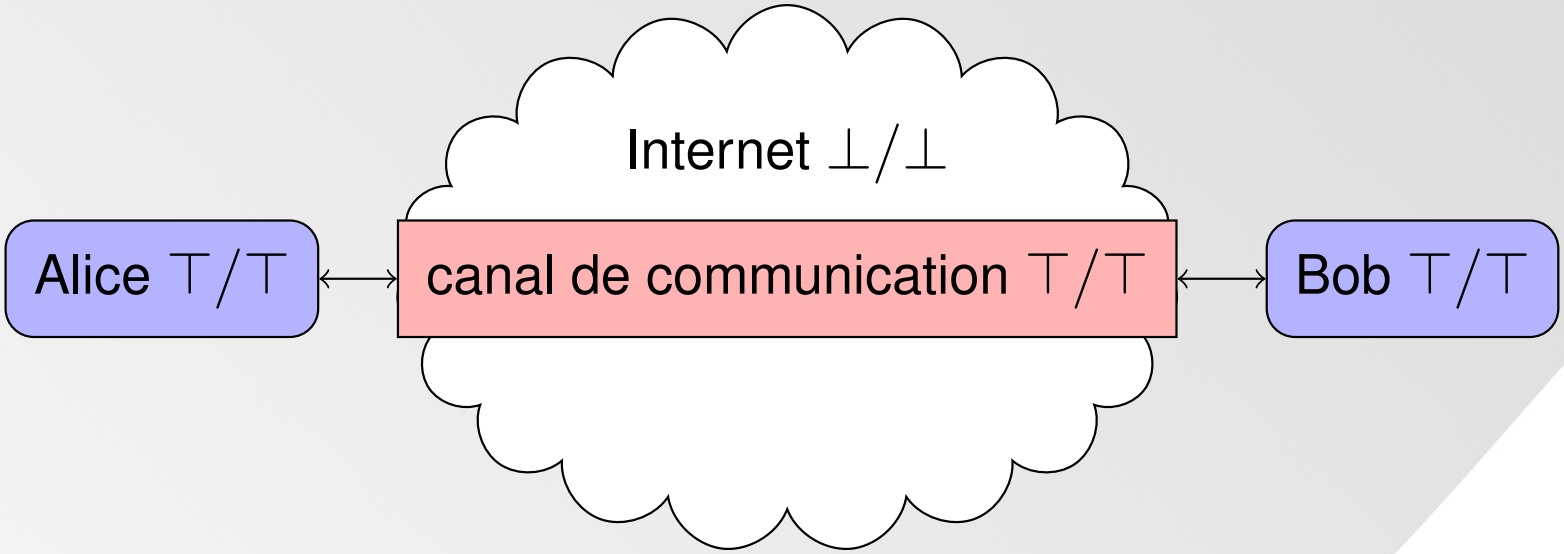
Introduction

Buts

TLS

PKI

Analyse d'une communication



Communication à travers Internet

- par défaut, aucune sécurité sur Internet
- protocole cryptographique = mise en place d'un canal protégeant les communications du reste d'Internet (séparation)
- Buts possibles :
  - intégrité : pas d'écriture sur le canal à partir d'Internet
  - confidentialité : pas de lecture sur le canal à partir d'Internet

Formulation locale des buts

Expression des buts

- selon les protocoles, le pair n'est pas toujours connu
- un sujet ne doit poser des buts que sur ses actions propres

Pseudonymes et identité

- identité : identifiant global d'un sujet
- pseudonyme : identifiant local (à une exécution du protocole) d'un sujet :
  - numéro de session d'un client
  - hôte et ports de communication
  - pseudonyme obtenu par un protocole dédié
- identité cas particulier de pseudonyme (utilisation d'une identité globale dans une session)

Buts pour les protocoles cryptographiques

Intégrité

- d'après les niveaux d'intégrité, seulement lors de la réception de messages par un sujet
- contenu *a priori* inconnu : la propriété se réduit à demander que le message a été envoyé par sujet désigné
- identité inconnue : utilisation possible de pseudonymes

Confidentialité

- d'après les niveaux de confidentialité, seulement lors de l'émission de messages par un sujet
- dans ce cas, la propriété se réduit à demander que le message ne puisse être connu que par des sujets désignés
- identité inconnue : utilisation possible de pseudonymes

AUTHENTIFICATION

PREUVE D'AUTHENTIFICATION

- environnement distribué
- authentification repose sur une preuve
- la preuve ne peut être que le message reçu, ou une partie de ce message

CHALLENGE/RÉPONSE

- déjà vu pour les protocoles de transmission de mot de passe
- un sujet crée une valeur aléatoire r
- la présence de cette valeur dans un message doit garantir son origine

Rejeu (replay)

But d'authentification naïf

A authentifie *B* en se basant sur la preuve *Na* si, quand *A* reçoit un message contenant *Na*, ce message a précédement été envoyé par *B*

Rejeu

rejouer un message signifie, pour un attaquant :

- enregistrer le déroulement du protocole
- réutiliser ces messages pour se faire passer pour un des participants

Formulation naïve et rejeu

- lors d'un rejeu, le message reçu a été précédement envoyé par l'auteur légitime
- pour l'authentification, il faut compter le nombre de fois que le message a été envoyé/reçu

Buts d'authentification

Authentification faible

A authentifie *B* en se basant sur la preuve *Na* si, quand *A* reçoit un message contenant *Na*, ce message a précédement été envoyé par *B*

Authentification forte

A authentifie *B* en se basant sur la preuve *Na* si, le message contenant *Na* a été reçu par *A* moins souvent qu'il n'a été envoyé par *B*

CONFIDENTIALITÉ

BESOIN D'AUTHENTIFICATION

- l'information envoyée est destinée à certaines personnes
- il faut donc avoir la certitude de l'identité (ou de son pseudonyme) d'un pair avant de lui envoyé une donnée confidentielle

BUT DE CONFIDENTIALITÉ

Une partie d'un message envoyé par A ne peut être lue que par $B_1, \ldots, B_n$

Spécification simplifiée d'un protocole

Parties utilisées

Connaissances initiales : pour chaque sujet, une liste de valeurs connues

Échange : une suite de communications

1. $A \rightarrow B : M_1$
2. $B \rightarrow A : M_2$

$\vdots$

Buts : la description des buts de confidentialité et d'authentification

Note

Pour simplifier, on utiliser $\{\_\}\_$ pour le chiffrement symétrique, asymétrique, et la signature digitale. La clef utilisée indique l'opération utilisée.

Plan

Introduction

Buts

TLS

PKI

Historique

SSL

- débuts d'internet
- protocole proposé par Netscape (adresses `https`)
- plusieurs versions (v1,v2,v3)
- toutes buggées

TLS

- standardisation IETF de SSL
- TLS 1.0 = SSL v3 (sauf détails mineurs)
- version courante 1.2 (théorie), 1.1 en pratique

Fonctionnement de TLS

Négociation

- le client et le serveur s'entendent sur la version à utiliser et sur les algorithmes à utiliser dans les phases suivantes
- risque : attaque demandant d'utiliser une version buggée

Rendez-vous (handshake)

- phase d'authentification
- négociation d'un contexte de sécurité (clef secrète)

Utilisation

- chiffrement symétrique des messages échangés basé sur le contexte de sécurité
- on chiffre le flux de message, pas les messages individuels

Fin/renégociation

- lorsque la période de validité du contexte de sécurité se termine
- ou à la demande d'un des 2 participants

Négociation

Négociation initiale

- dans le protocole HTTP, demande de changement du protocole de transport (client ou serveur, mot-clef `Connection`)
- valeurs du champ `upgrade` : algorithmes supportés par le navigateur, par ordre de préférence

```
GET /hello.txt HTTP/1.1
Host: www.example.com
Connection: upgrade
Upgrade: HTTP/2.0, SHTTP/1.3, IRC/6.9, RTA/x11
```

Rendez-vous (Handshake)

Principe

- protocole d'authentification mutuelle, utilisation de certificats (voir plus loin)
- Diffie-Hellman le plus utilisé
- **mais** beaucoup d'implémentations ($\sim$ 90%) avec de mauvais paramètres

Protocole de Diffie-Hellman

A connait A, B, g, N, Na, et B connait A, B, g, N, Nb (Na, Nb aléatoires)

1. $A \rightarrow B : g^{Na} \mod N$
2. $B \rightarrow A : g^{Nb} \mod N$

But : $g^{Na \times Nb} \mod N$ est connu seulement de A et B

Explications Diffie-Hellman

Calcul du secret

- $g^{Na \times Nb} \mod N = g^{Na^{Nb}} \mod N$
- $g^{Na \times Nb} \mod N = g^{Nb^{Na}} \mod N$

Robustesse (jeu)

- on doit au joueur soit :
  - $(g^{Na} \mod N, g^{Nb} \mod N, g^{Na \times Nb} \mod N)$
  - $(g^{Na} \mod N, g^{Nb} \mod N, g^{r} \mod N)$, où r est un nombre aléatoire
- le joueur gagne si il devine correctement quel choix a été fait
- Hypothèse de Diffie-Hellman Décisionnel (DDH) : aucun joueur (machine de Turing) réaliste ne peut faire mieux que pile ou face
- Si un observateur peut calculer une partie du secret à partir de l'échange, il peut faire mieux que une chance sur deux

UTILISATION

CHIFFREMENTS DE FLUX

- soit chiffrement type Vernam, avec clair $\oplus$ nombre aléatoire
- soit chiffrement par bloc : la même clef est toujours utilisée, mais le block précédent est pris en compte
- il y a une attaque générique sur les chiffrements par blocs (mais faible probabilité de succès)

ALGORITHMES UTILISÉS

- par block : RCA, 3DES (seuls disponibles sur XP), AES,...
- par flux : Salsa, Chacha, blowfish,...

Plan

Introduction

Buts

TLS

PKI

Retour sur Diffie-Hellman

Pas d'authentification !

- un attaquant C peut s'immiscer dans un échange entre $A - B$ pour le remplacer par deux échanges $A - C$ et $C - B$
- on parle d'attaque par un intermédiaire (man-in-the-middle)
- il y a bien un secret partagé, mais on ne sait pas avec qui

Ajout de l'authentification

- pour authentifier la session, les messages sont signés par le client et le serveur en :
  - utilisant une clef de signature
  - la clef de validation correspondante est envoyée en même temps
- problème : comment relier la clef à une identité ?

CERTIFICATS

CERTIFICAT

Un certificat est un document signé digitalement par un sujet.

UTILISATION

- un sujet s'engage sur la véracité d'informations en signant ces informations
- 2 cas possibles :
  - soit le lecteur connait la clef de validation permettant de valider la signature
  - soit le lecteur doit obtenir la preuve que la clef à utiliser pour la validation est bien celle du sujet

INFRASTRUCTURES DE CLEFS PUBLIQUES

BUT : PROPAGATION DE LA CONFIANCE

- confiance : ensemble de certificats justifié par des certificats connus du lecteur
- http : justification existe = cadenas vert, pas de justification = cadenas rouge/avertissement

CONFIANCE DANS LES NAVIGATEURS

- chaque navigateur a une liste des certificats reconnus (certificats racines pour la confiances)
- pour être accepté, un site Internet doit obtenir un certificat qui peut être validé pour un certificat racine

Utilité et fragilité

Problème d'initialisation

il faut avoir confiance dans les entreprises qui émettent des certificats racines

Exemple : navigateurs d'entreprise

- des sociétés sont spécialisées dans l'émission de "faux" certificats
- ces certificats sont mis par des entreprises dans le navigateur de leurs employés
- celà permet à la société émettrice d'intercepter les communications https des employés (attaque Man-in-the-Middle par la société)
- avantage/désavantage : une entreprise a accès à l'historique de navigation de ses salariés
- Certificate Transparency : effort pour permettre aux internautes de savoir si les certificats qu'ils acceptent ont été réellement émis par le site