Peut-on prouver la sécurité des communications ?

Hubert Comon
LSV, ENS Paris-Saclay

December 9, 2016

De quoi s'agit il ?

Communications

- internet
- sans fil
- réseaux ad-hoc

Téléphones, cartes a puces, cartes rfid, objets connectés...
la surface augmente.

De quoi s'agit il ?

Communications

- internet
- sans fil
- réseaux ad-hoc

Téléphones, cartes a puces, cartes rfid, objets connectés...
la surface augmente.

Les communications sont assurées par des protocoles qui s'appuient sur des bibliothèques cryptographiques.

cf. exposé de Stéphanie Delaune.

Exemple de protocole

$\longleftrightarrow$

Objectif: la porte s'ouvre si et seulement si la carte donne droit à l'accès.

Exemple de protocole (suite)

Une clef secrète k^{hcl} est partagée par ma carte et le CNRS.

$$\begin{array}{rcrl} L & \rightarrow & HCL: & \nu n_R.\quad n_R \\ HCL & \rightarrow & L: & \nu n_T.\quad HCL,\ n_T,\ \mathrm{H}(n_R \oplus n_T, k^{hcl}) \end{array}$$

Exemple de protocole (suite)

Une clef secrète k^{hcl} est partagée par ma carte et le CNRS.

$$\begin{array}{rcrl} L & \rightarrow & HCL: & \nu n_R.\quad n_R \\ HCL & \rightarrow & L: & \nu n_T.\quad HCL,\ n_T,\ \mathrm{H}(n_R \oplus n_T, k^{hcl}) \end{array}$$

programme L:

1. Engendrer un nombre aléatoire n_R, le mémoriser et l'envoyer à la carte X
2. Avec la réponse de la carte: id, x, y,
   - 2.1 rechercher la clef k^{id} correspondant à id. S'il n'y en a pas, échouer.
   - 2.2 calculer $\mathrm{H}(n_R \oplus x, k^{id})$. Vérifier que c'est égal à y. Si c'est le cas, ouvrir la porte et sinon échouer.

Exemple de protocole (3)

Une clef secrète k^{hcl} est partagée par ma carte et le CNRS.

$$\begin{array}{rcrl} L & \rightarrow & HCL: & \nu n_R.\quad n_R \\ HCL & \rightarrow & L: & \nu n_T.\quad HCL,\ n_T,\ \mathrm{H}(n_R \oplus n_T, k^{hcl}) \end{array}$$

Attaque:

Exemple de protocole (3)

Une clef secrète k^{hcl} est partagée par ma carte et le CNRS.

$$\begin{array}{rcrl} L & \rightarrow & HCL: & \nu n_R.\ \ n_R \\ HCL & \rightarrow & L: & \nu n_T.\ \ HCL,\ n_T,\ \mathrm{H}(n_R \oplus n_T, k^{hcl}) \end{array}$$

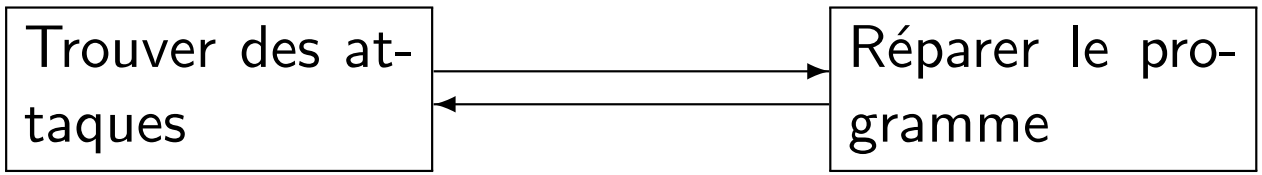
Attaque:

1. Intrus possède un lecteur et récupère les messages quand je passe
2. Intrus se présente à la porte avec une carte qui ne respecte pas le protocole:

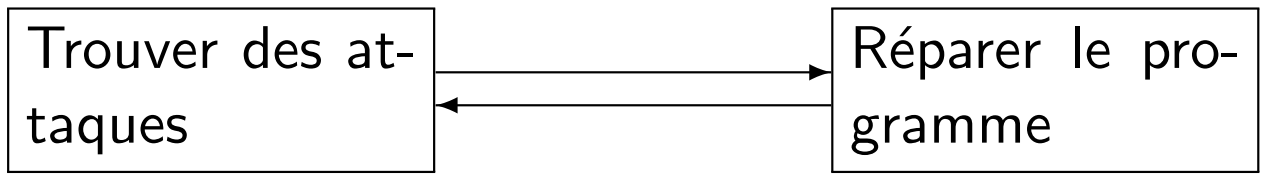
$$\begin{array}{rcrl} L & \rightarrow & Intrus: & \nu n'_R.\ \ n'_R \\ Intrus & \rightarrow & L: & HCL,\ \underbrace{n'_R \oplus n_R \oplus n_T}_{x},\ \mathrm{H}(n_R \oplus n_T, k^{hcl}) \end{array}$$

L vérifie que $\mathrm{H}(n_R \oplus n_T, k^{hcl}) = \mathrm{H}(x \oplus n'_R, k^{hcl})$, ce qui est le cas. Et donc ouvre la porte.

Computer and communication security



Computer and communication security



Rompre le cycle: preuves formelles de sécurité

Obstacles aux preuves formelles de sécurité (1)

Sources non disponibles

Obstacles aux preuves formelles de sécurité (1)

Sources non disponibles

La “sécurité par obscurité” est une erreur repérée depuis longtemps

Obstacles aux preuves formelles de sécurité (1)

Sources non disponibles

La “sécurité par obscurité” est une erreur repérée depuis longtemps

- principe de Kerckhoffs (19eme siècle).

Obstacles aux preuves formelles de sécurité (1)

Sources non disponibles

La “sécurité par obscurité” est une erreur repérée depuis longtemps

- principe de Kerckhoffs (19eme siècle).
- Machine Enigma

Obstacles aux preuves formelles de sécurité (1)

Sources non disponibles

La “sécurité par obscurité” est une erreur repérée depuis longtemps

- principe de Kerckhoffs (19eme siècle).
- Machine Enigma
- L’histoire de Cryptosense (G. Steel)

À l’inverse, TLS, SSL, https, sont (relativement) sûrs.

Obstacles aux preuves formelles de sécurité (2)

Objectif: prouver

$$\forall \mathcal{A}. \quad \mathcal{A} \parallel P \models \phi$$

Quel modèle de l'attaquant ?

Obstacles aux preuves formelles de sécurité (2)

Objectif: prouver

$$\forall \mathcal{A}. \quad \mathcal{A} \parallel P \models \phi$$

Quel modèle de l'attaquant ?

- Théorème de Shannon

Obstacles aux preuves formelles de sécurité (2)

Objectif: prouver

$$\forall \mathcal{A}. \quad \mathcal{A} \parallel P \models \phi$$

Quel modèle de l'attaquant ?

- Théorème de Shannon
- Attaquant symbolique

Obstacles aux preuves formelles de sécurité (2)

Objectif: prouver

$$\forall \mathcal{A}. \quad \mathcal{A} \parallel P \models \phi$$

Quel modèle de l'attaquant ?

- Théorème de Shannon
- Attaquant symbolique
- Attaquant calculatoire

Obstacles aux preuves formelles de sécurité (2)

Objectif: prouver

$$\forall \mathcal{A}. \quad \mathcal{A} \parallel P \models \phi$$

Quel modèle de l'attaquant ?

- Théorème de Shannon
- Attaquant symbolique
- Attaquant calculatoire
- Attaques par canaux auxilliaires
- ...

Quel attaquant ?

$$\begin{array}{rcrll} L & \rightarrow & HCL: & \nu n_R. & n_R \\ HCL & \rightarrow & L: & \nu n_T. & HCL,\ n_T,\ \mathsf{H}(\langle n_R, n_T \rangle, k^{hcl}) \end{array}$$

garantit il l'authentification ?

Quel attaquant ?

$$\begin{array}{rcrl} L & \rightarrow & HCL: & \nu n_R.\ \ n_R \\ HCL & \rightarrow & L: & \nu n_T.\ \ HCL,\ n_T,\ \mathsf{H}(\langle n_R, n_T \rangle, k^{hcl}) \end{array}$$

garantit il l'authentification ?

Cela dépend des propriétés de H (collision resistant?) et des capacités de l'attaquant (ressources polynomiales ?)

Oui, nous pouvons faire des preuves de sécurité...

... relatives

- Jeux cryptographiques: "Si $\mathcal{A}$ peut casser ma primitive, alors on peut construire $\mathcal{B}$ qui résoud un problème réputé difficile"
- Hypothèses sur les bibliothèques/attaquants: "Le protocole est sûr si on suppose qu'un attaquant ne peut pas distinguer $\mathrm{H}(m, k)$ de $\mathrm{H}(n, k)$."

Fixer un cadre d'utilisation précis, dans lequel la sécurité est assurée

Quelques outils

Pour des modèles d'attaquant spécifiques

ProVerif

Tamarin

Akiss, APTE

CryptoVerif

EasyCrypt

F⋆

...

Quelques outils

Pour des modèles d'attaquant spécifiques

ProVerif

Tamarin

Akiss, APTE

CryptoVerif

EasyCrypt

F⋆

...

Pour des familles de modèles d'attaquant

En développement Scary

La réponse à la question en résumé

- Ne pas cacher les programmes/protocoles
- Les preuves (automatiques) de sécurité sont possibles, mais sous des hypothèses précises sur l'attaquant et les bibliothèques utilisées.

Ces considérations dépassent le cadre des protocoles.