

VÉRIFICATION AUTOMATIQUE DE PROTOCOLES CRYPTOGRAPHIQUES

UN PEU DE PROSPECTIVE

HUBERT COMON-LUNDH & YASSINE LAKHNECH

ENJEUX ET SPÉCIFICITÉS DES PROBLÈMES

- Assurer des propriétés sécuritaires comme la confidentialité en utilisant des canaux publics.
- Les participants ont des ressources très limitées
- Les capacités mémoire d'un attaquant sont illimitées, ses moyens de calcul sont importants
- Les canaux publics ne sont pas fiables: un intrus peut intercepter des messages et envoyer des messages truqués.

CONTEXTE

- Développement de sémantiques depuis 1997 environ (Spi-calcul, modèles de traces, Strand spaces) **Pour les protocoles**
- Outils automatiques de preuve, notamment en France à Marseille, Nancy, Cachan, Grenoble, Paris.
- Concentration des outils sur les propriétés de confidentialité et certaines propriétés d'authentification, de manière ad hoc
- Indécidabilité du secret
- Hypothèse du chiffrement parfait

PROTOCOLS

Network | $P\sigma_1$ | $P\sigma_2$ | ... | $P\sigma_n$...

P is a process with k free variables called **roles**
 σ_i maps **roles** to **identities**, some of which are compromised.

Network is under control of the intruder

The confidentiality question:

$$\forall T, \forall a, b, T \not\vdash s(a, b)$$

PROBLÈMES DE SÉMANTIQUE

- Multiplicité des approches
- Certains points délicats ne sont toujours pas bien compris
- Comparaisons (e.g. spi-calcul vs traces)

QUELLES PROPRIÉTÉS DE SÉCURITÉ ?

- Qu'est ce que la confidentialité ?
- Qu'est ce que l'authentification ?
- Equité, délit d'initié, anonymat etc....

Un langage de définition des propriétés sécuritaires ?

Analogie des logiques temporelles pour la vérification des systèmes réactifs

AFFAIBLIR L'HYPOTHÈSE DU CHIFFREMENT PARFAIT

Hypothèse de chiffrement parfait (supposée par tous les outils existants):

Les chiffrés de deux messages syntaxiquement distincts sont distincts.

C'est une approximation: par exemple, l'associativité de la concaténation, les propriétés algébriques du ou exclusif,...

LE PETIT BOUT DE LA LORGNETTE

LE PETIT BOUT DE LA LORGNETTE

$$T \stackrel{?}{\vdash} m$$

T est un ensemble fini de termes et m est un terme.

Peut on déduire d'un ensemble fini de messages une donnée supposée rester confidentielle ?

INTRUDER CAPABILITIES: THE DOLEV-YAO MODEL

$$(A) \frac{}{T \vdash t} \quad \text{if } t \in T$$

$$(P) \frac{T_1 \vdash t_1 \quad T_2 \vdash t_2}{T_1, T_2 \vdash \langle t_1, t_2 \rangle}$$

$$(UL) \frac{T \vdash \langle t_1, t_2 \rangle}{T \vdash t_1}$$

$$(UR) \frac{T \vdash \langle t_1, t_2 \rangle}{T \vdash t_2}$$

$$(E) \frac{T_1 \vdash t_1 \quad T_2 \vdash t_2}{T_1, T_2 \vdash \{t_1\}_{t_2}}$$

$$(D) \frac{T_1 \vdash \{t_1\}_{t_2} \quad T_2 \vdash t_2}{T_1, T_2 \vdash t_1}$$

$$(H) \frac{T \vdash t}{T \vdash h(t)}$$

INTRUDER CAPABILITIES: THE DOLEV-YAO MODEL

$$\begin{array}{l}
 \text{(A)} \quad \frac{}{T \vdash t} \quad \text{if } t \in T \\
 \\
 \text{(P)} \quad \frac{T_1 \vdash t_1 \quad T_2 \vdash t_2}{T_1, T_2 \vdash \langle t_1, t_2 \rangle} \\
 \\
 \text{(UL)} \quad \frac{T \vdash \langle t_1, t_2 \rangle}{T \vdash t_1} \\
 \\
 \text{(UR)} \quad \frac{T \vdash \langle t_1, t_2 \rangle}{T \vdash t_2} \\
 \\
 \text{(E)} \quad \frac{T_1 \vdash t_1 \quad T_2 \vdash t_2}{T_1, T_2 \vdash \{t_1\}_{\text{pub}(t_2)}} \\
 \\
 \text{(D}_1\text{)} \quad \frac{T_1 \vdash \{t_1\}_{\text{pub}(t_2)} \quad T_2 \vdash \text{priv}(t_2)}{T_1, T_2 \vdash t_1} \\
 \\
 \text{(D}_2\text{)} \quad \frac{T_1 \vdash \{t_1\}_{\text{priv}(t_2)} \quad T_2 \vdash t_2}{T_1, T_2 \vdash t_1}
 \end{array}$$

EXAMPLE

$$T = \{s\}_{\{a\}_b}, \langle a, b \rangle$$

$$\begin{array}{c} \text{A} \frac{}{} \\ \text{UL} \frac{T \vdash \langle a, b \rangle}{T \vdash a} \\ \text{E} \frac{}{} \end{array} \quad \begin{array}{c} \text{A} \frac{}{} \\ \text{UR} \frac{T \vdash \langle a, b \rangle}{T \vdash b} \\ \text{D} \frac{T \vdash \{a\}_b}{T \vdash s} \end{array} \quad \begin{array}{c} \text{A} \frac{}{} \\ \text{A} \frac{}{} \end{array}$$

A FIRST SIMPLE RESULT

Theorem:

$T \stackrel{?}{\vdash} s$ can be decided in linear time and is PTIME-complete for the Dolev-Yao intruder

The Dolev-Yao intruder theory is **Local** (McAllester, JACM 1993).

INCLUDING SOME INTRUDER'S KNOWLEDGE

Theorem (Monniaux, Goubault-Larrecq,...)

If T is a recognizable set of trees, then $\{s, \mid T \vdash s \text{ is derivable}\}$ is an effectively recognizable set of trees

Proof: Consider the following definite set constraint:

$$\begin{array}{l} \mathcal{R} \subseteq I \quad \langle I, I \rangle \subseteq I \quad I \cap \langle \text{All}, \text{All} \rangle \subseteq \langle I, I \rangle \\ \{I\}_I \subseteq I \quad h(I) \subseteq I \quad I \cap \{\text{All}\}_I \subseteq \{I\}_{\text{All}} \end{array}$$

The least solution is the set of terms that can be derived from T by the intruder.

INCLUDING SOME ALGEBRAIC PROPERTIES

$$\text{XOR} \left\{ \begin{array}{l} x \oplus y = y \oplus x \\ (x \oplus y) \oplus z = x \oplus (y \oplus z) \\ x \oplus 0 = x \\ x \oplus x = 0 \end{array} \right.$$

$$\text{AG} \left\{ \begin{array}{l} x + y = y + x \\ (x + y) + z = x + (y + z) \\ x + (-x) = 0 \\ x + 0 = x \\ - - x = x \end{array} \right.$$

INTRUDER CAPABILITIES: INCLUDING XOR

$$\begin{array}{ll} \text{(A)} \quad \frac{}{T \vdash t} \quad \text{if } t \in T & \text{(P)} \quad \frac{T_1 \vdash t_1 \quad T_2 \vdash t_2}{T_1, T_2 \vdash \langle t_1, t_2 \rangle} \\ \text{(UL)} \quad \frac{T \vdash \langle t_1, t_2 \rangle}{T \vdash t_1} & \text{(UR)} \quad \frac{T \vdash \langle t_1, t_2 \rangle}{T \vdash t_2} \\ \text{(E)} \quad \frac{T_1 \vdash t_1 \quad T_2 \vdash t_2}{T_1, T_2 \vdash \{t_1\}t_2} & \text{(D)} \quad \frac{T_1 \vdash \{t_1\}t_2 \quad T_2 \vdash t_2}{T_1, T_2 \vdash t_1} \end{array}$$

INTRUDER CAPABILITIES: INCLUDING XOR

$$\begin{array}{ll}
 \text{(A)} \quad \frac{}{T \vdash t} \quad \text{if } t \in T & \text{(P)} \quad \frac{T_1 \vdash t_1 \quad T_2 \vdash t_2}{T_1, T_2 \vdash \langle t_1, t_2 \rangle} \\
 \text{(UL)} \quad \frac{T \vdash \langle t_1, t_2 \rangle}{T \vdash t_1} & \text{(UR)} \quad \frac{T \vdash \langle t_1, t_2 \rangle}{T \vdash t_2} \\
 \text{(E)} \quad \frac{T_1 \vdash t_1 \quad T_2 \vdash t_2}{T_1, T_2 \vdash \{t_1\}t_2} & \text{(D)} \quad \frac{T_1 \vdash \{t_1\}t_2 \quad T_2 \vdash t_2}{T_1, T_2 \vdash t_1} \\
 \text{(\oplus)} \quad \frac{T_1 \vdash t_1 \quad T_2 \vdash t_2}{T_1, T_2 \vdash t_1 \oplus t_2} & \frac{T_1 \vdash t_1 \oplus t_2 \quad T_2 \oplus t_2}{T_1, T_2 \vdash t_1} \\
 \text{(C)} \quad \frac{T \vdash t_1 \oplus t_2}{T \vdash t_2 \oplus t_1} & \text{(AL)} \quad \frac{T \vdash t_1 \oplus (t_2 \oplus t_3)}{T \vdash (t_1 \oplus t_2) \oplus t_3}
 \end{array}$$

RESULTS AND QUESTIONS

Theorem (Comon, Shmatikov 2002)

$T \vdash^? s$ is NP-complete when **XOR** or **AG** is added to the intruder's capabilities

Question:

For which Intruder's theories is $T \vdash^? s$ decidable ?

ANALYSE STATIQUE DE PROTOCOLES

Beaucoup d'attaques (ex: SSL) viennent de problèmes de réalisation logicielle.

- Rejoint les problèmes de sécurité du code mobile
- Techniques de typage et d'abstraction → entrée des outils existants

PROBLÈMES STRUCTURELS

- Absence de structure à l'heure actuelle
- Absence de visibilité (en particulier des outils)
- Base d'exemples (cf. Clark & Jacob, 1997)

EBAUCHE DE PLAN DE TRAVAIL

- Nouveau catalogue. *Mise en service prochaine d'un site ouvert*. Liste de diffusion:
Florent.Jacquemard@lsv.ens-cachan.fr
pour être ajouté.
- Site national prochainement en service à Grenoble
- 2 réunions annuelles dont une spécifique aux protocoles
- Etats de l'art et questions prospectives. Typiquement répertoire des outils.