Vérification de protocoles de sécurité dans un modèle de l'intrus étendu

Stéphanie Delaune

delaune@lsv.ens-cachan.fr

Laboratoire de Vérification et de Spécification
CNRS UMR 8643
École Normale Supérieure de Cachan
CACHAN - France

Laboratoire Spécification et Vérification

Exemple 1 - protocole naïf de vote

Considérons l'échange suivant:

$$A \quad \rightarrow S : \quad \{vote\}_{pub(S)}$$

avec $vote \in \{v_1, ..., v_n\}$.

Laboratoire Spécification et Vérification

Exemple 1 - protocole naïf de vote

Considérons l'échange suivant:

$$A \quad \rightarrow S : \quad \{vote\}_{pub(S)}$$

avec $vote \in \{v_1, ..., v_n\}$.

Description de l'attaque:

Laboratoire Spécification et Vérification

Exemple 1 - protocole naïf de vote

Considérons l'échange suivant:

$$A \quad \to S : \quad \{vote\}_{pub(S)}$$

avec $vote \in \{v_1, ..., v_n\}$.

Description de l'attaque:

- deviner la valeur choisie par A: v_i

Laboratoire Spécification et Vérification

Exemple 1 - protocole naïf de vote

Considérons l'échange suivant:

$$A \quad \rightarrow S : \quad \{vote\}_{pub(S)}$$

avec $vote \in \{v_1, ..., v_n\}$.

Description de l'attaque:

- deviner la valeur choisie par A: v_i
- construire le message $\{v_i\}_{pub(S)}$

Exemple 1 - protocole naïf de vote

Considérons l'échange suivant:

$$A \quad \rightarrow S : \quad \{vote\}_{pub(S)}$$

avec $vote \in \{v_1, ..., v_n\}$.

Description de l'attaque:

- deviner la valeur choisie par A: v_i
- construire le message $\{v_i\}_{pub(S)}$
- le comparer avec le message intercepté: $\{vote\}_{pub(S)}$.

Laboratoire Spécification et Vérification

Exemple 1 - protocole naïf de vote

Considérons l'échange suivant:

$$A \quad \rightarrow S: \quad \{vote\}_{pub(S)}$$

avec $vote \in \{v_1, ..., v_n\}$.

Description de l'attaque:

- deviner la valeur choisie par A: v_i
- construire le message $\{v_i\}_{pub(S)}$
- le comparer avec le message intercepté: $\{vote\}_{pub(S)}$.

Conséquence:

l'intrus connaît le vote de A.

Laboratoire Spécification et Vérification

Exemple 2 - challenge

Considérons l'échange suivant: [Gong 93]

$$\begin{aligned} A &\to B: \quad \{n\}_k \\ B &\to A: \quad \{n+1\}_k \end{aligned}$$

où $k \in \{k_1, ..., k_n\}$ est une clef symétrique et n un nonce.

Exemple 2 - challenge

Considérons l'échange suivant: [Gong 93]

$$\begin{aligned} A &\to B : \quad \{n\}_k \\ B &\to A : \quad \{n+1\}_k \end{aligned}$$

où $k \in \{k_1, ..., k_n\}$ est une clef symétrique et n un nonce.

Description de l'attaque:

- deviner la valeur de k : k_i
- déchiffrer les deux messages interceptés, $\{n\}_k$ et $\{n+1\}_k$ avec la clef choisie k_i
- incrémenter la première des deux valeurs obtenues et comparer avec la deuxième.

Exemple 2 - challenge

Considérons l'échange suivant: [Gong 93]

$$\begin{aligned} A &\rightarrow B : \quad \{n\}_k \\ B &\rightarrow A : \quad \{n+1\}_k \end{aligned}$$

où $k \in \{k_1, ..., k_n\}$ est une clef symétrique et n un nonce.

Description de l'attaque:

- deviner la valeur de k : k_i
- déchiffrer les deux messages interceptés, $\{n\}_k$ et $\{n+1\}_k$ avec la clef choisie k_i
- incrémenter la première des deux valeurs obtenues et comparer avec la deuxième.

Conséquence:

l'intrus connaît la clef k, et le nonce n.

Objectifs

sur le plan de la modélisation

$\hookrightarrow$ *développer plusieurs modèles d'intrus étendus, pour prendre en compte:*

- les « attaques par prédictions »: [DEA]
- l'ajout de théories équationelles:
  $\oplus$ [Comon & Shmatikov, 2003]
- les propriétés algébriques des primitives cryptographiques:
  $\{\langle u, v\rangle\}_k = \langle\{u\}_k, \{v\}_k\rangle$ [Comon & Treinen, 2003].

Objectifs

sur le plan de la modélisation

$\hookrightarrow$ *développer plusieurs modèles d'intrus étendus, pour prendre en compte:*

- les « attaques par prédictions »: [DEA]
- l'ajout de théories équationelles:
  $\oplus$ [Comon & Shmatikov, 2003]
- les propriétés algébriques des primitives cryptographiques:
  $\{\langle u, v\rangle\}_k = \langle\{u\}_k, \{v\}_k\rangle$ [Comon & Treinen, 2003].

sur le plan de la vérification

$\hookrightarrow$ *développer des outils modulaires (et les modules d'intrus correspondant):*

- de recherche de preuves: (projet RNTL PROUVÉ)
- de recherche d'attaques: [DEA]

Laboratoire
Spécification
et
Vérification

Plan

I) **Modélisation des attaques par prédictions**

- Problème de déduction de l'intrus dans le modèle de Dolev-Yao
- Problème de déduction de l'intrus dans le modèle étendu

Laboratoire Spécification et Vérification

Plan

I) **Modélisation des attaques par prédictions**

- Problème de déduction de l'intrus dans le modèle de Dolev-Yao
- Problème de déduction de l'intrus dans le modèle étendu

II) **Vérification pratique des protocoles**

- Securify: un outil de vérification du secret
- Prototype: une procédure de recherche d'attaques

Laboratoire Spécification et Vérification

Plan

I) Modélisation des attaques par prédictions

- Problème de déduction de l'intrus dans le modèle de Dolev-Yao
  - ↪ Présentation du problème de déduction de l'intrus
  - ↪ Présentation du modèle de Dolev-Yao
  - ↪ Rappel des résultats
- Problème de déduction de l'intrus dans le modèle étendu

II) Vérification pratique des protocoles

- Securify: un outil de vérification du secret
- Prototype: une procédure de recherche d'attaques

Le problème de déduction de l'intrus: $T \overset{?}{\vdash} s$

ENTRÉE:

- Un ensemble fini de messages: T,
  ↪ *typiquement, les messages qui ont circulé sur le réseau*
- Un message: s,
  ↪ *le message pour lequel on veut vérifier le secret*

QUESTION:

- L'intrus peut-il déduire le secret s à partir de T ?

Le modèle de Dolev-Yao

Axiome (A) $$\frac{u \in T}{T \vdash u}$$

Déchiffrement (D) $$\frac{T \vdash \{u\}_v \quad T \vdash v^{-1}}{T \vdash u}$$

Projection (UL) $$\frac{T \vdash \langle u, v\rangle}{T \vdash u}$$

Chiffrement (E) $$\frac{T \vdash u \quad T \vdash v}{T \vdash \{u\}_v}$$

Projection (UR) $$\frac{T \vdash \langle u, v\rangle}{T \vdash v}$$

Paire (P) $$\frac{T \vdash u \quad T \vdash v}{T \vdash \langle u, v\rangle}$$

Laboratoire Spécification et Vérification

Le modèle de Dolev-Yao

Axiome (A) $$\frac{u \in T}{T \vdash u}$$

Déchiffrement (D) $$\frac{T \vdash \{u\}_v \quad T \vdash v^{-1}}{T \vdash u}$$

Projection (UL) $$\frac{T \vdash \langle u, v \rangle}{T \vdash u}$$

Chiffrement (E) $$\frac{T \vdash u \quad T \vdash v}{T \vdash \{u\}_v}$$

Projection (UR) $$\frac{T \vdash \langle u, v \rangle}{T \vdash v}$$

Paire (P) $$\frac{T \vdash u \quad T \vdash v}{T \vdash \langle u, v \rangle}$$

Laboratoire Spécification et Vérification

Le modèle de Dolev-Yao

Axiome (A)	$\dfrac{u \in T}{T \vdash u}$	Déchiffrement (D)	$\dfrac{T \vdash \{u\}_v \quad T \vdash v^{-1}}{T \vdash u}$
Projection (UL)	$\dfrac{T \vdash \langle u, v \rangle}{T \vdash u}$	Chiffrement (E)	$\dfrac{T \vdash u \quad T \vdash v}{T \vdash \{u\}_v}$
Projection (UR)	$\dfrac{T \vdash \langle u, v \rangle}{T \vdash v}$	Paire (P)	$\dfrac{T \vdash u \quad T \vdash v}{T \vdash \langle u, v \rangle}$

Le modèle de Dolev-Yao

Axiome (A) $$\frac{u \in T}{T \vdash u}$$

Déchiffrement (D) $$\frac{T \vdash \{u\}_v \quad T \vdash v^{-1}}{T \vdash u}$$

Projection (UL) $$\frac{T \vdash \langle u, v\rangle}{T \vdash u}$$

Chiffrement (E) $$\frac{T \vdash u \quad T \vdash v}{T \vdash \{u\}_v}$$

Projection (UR) $$\frac{T \vdash \langle u, v\rangle}{T \vdash v}$$

Paire (P) $$\frac{T \vdash u \quad T \vdash v}{T \vdash \langle u, v\rangle}$$

Laboratoire Spécification et Vérification

Rappel des résultats

Le problème de déduction de l'intrus dans le modèle de Dolev-Yao

Résultat de localité: [Comon & Shmatikov, 2003]

La théorie de Dolev-Yao est *locale* [Mc Allester, 1993]:
S'il existe une preuve de $T \vdash s$, alors il existe une preuve qui n'utilise que des sous-termes des termes de $T \cup \{s\}$.

Conséquence:

Le problème de déduction de l'intrus, $T \overset{?}{\vdash} s$, est PTIME complet.

Plan

I) **Modélisation des attaques par prédictions**

- Problème de déduction de l'intrus dans le modèle de Dolev-Yao
- Problème de déduction de l'intrus dans le modèle étendu

$\hookrightarrow$ Présentation du «nouveau» problème de déduction de l'intrus

$\hookrightarrow$ Présentation du modèle de Dolev-Yao étendu

$\hookrightarrow$ Résultats

II) **Vérification pratique des protocoles**

- Securify: un outil de vérification du secret
- Prototype: une procédure de recherche d'attaques

Laboratoire Spécification et Vérification

Le problème de déduction de l'intrus: $T/T' \overset{?}{\vdash} s$

Laboratoire Spécification et Vérification

Le problème de déduction de l'intrus: $T/T' \overset{?}{\vdash} s$

ENTRÉE:

- Un ensemble fini de messages «fortement connus»: T,
  $\hookrightarrow$ *typiquement, les messages qui ont circulé sur le réseau*

Le problème de déduction de l'intrus: $T/T' \overset{?}{\vdash} s$

ENTRÉE:

- Un ensemble fini de messages «fortement connus»: T,
  $\hookrightarrow$ *typiquement, les messages qui ont circulé sur le réseau*
- Un ensemble fini de données atomiques, «faiblement connues»: T',
  $\hookrightarrow$ *typiquement, les données qui prennent leur valeur dans un domaine fini connu de l'intrus*

Le problème de déduction de l'intrus: $T/T' \overset{?}{\vdash} s$

ENTRÉE:

- Un ensemble fini de messages «fortement connus»: T,
  $\hookrightarrow$ *typiquement, les messages qui ont circulé sur le réseau*
- Un ensemble fini de données atomiques, «faiblement connues»: T',
  $\hookrightarrow$ *typiquement, les données qui prennent leur valeur dans un domaine fini connu de l'intrus*
- Un message: s,
  $\hookrightarrow$ *le message pour lequel on veut vérifier le secret*

Laboratoire Spécification et Vérification

Le problème de déduction de l'intrus: $T/T' \overset{?}{\vdash} s$

ENTRÉE:

- Un ensemble fini de messages «fortement connus»: T,
  $\hookrightarrow$ *typiquement, les messages qui ont circulé sur le réseau*
- Un ensemble fini de données atomiques, «faiblement connues»: T',
  $\hookrightarrow$ *typiquement, les données qui prennent leur valeur dans un domaine fini connu de l'intrus*
- Un message: s,
  $\hookrightarrow$ *le message pour lequel on veut vérifier le secret*

QUESTION:

- L'intrus peut-il déduire le secret s à partir de T et T' ?

Laboratoire Spécification et Vérification

Le modèle de Dolev-Yao étendu

On introduit deux formes de séquent:

Laboratoire Spécification et Vérification

Le modèle de Dolev-Yao étendu

On introduit deux formes de séquent:

- **Déduction forte:** $T/T' \vdash u$

  $\hookrightarrow$ *L'intrus peut déduire «fortement»* u *à partir de* T *et* T'

Laboratoire Spécification et Vérification

Le modèle de Dolev-Yao étendu

On introduit deux formes de séquent:

- **Déduction forte:** $T/T' \vdash u$
  $\hookrightarrow$ *L'intrus peut déduire «fortement»* u *à partir de* T *et* T'
- **Déduction faible:** $T/T' \vdash' u$
  $\hookrightarrow$ *L'intrus peut déduire «faiblement»* u *à partir de* T *et* T'

Le modèle de Dolev-Yao étendu

On introduit deux formes de séquent:

- **Déduction forte:** $T/T' \vdash u$
  $\hookrightarrow$ *L'intrus peut déduire «fortement»* u *à partir de* T *et* T'
- **Déduction faible:** $T/T' \vdash' u$
  $\hookrightarrow$ *L'intrus peut déduire «faiblement»* u *à partir de* T *et* T'

Exemple - *la règle Axiome*

$$\frac{u \in T}{T \vdash u}$$

Le modèle de Dolev-Yao étendu

On introduit deux formes de séquent:

- **Déduction forte:** $T/T' \vdash u$

  $\hookrightarrow$ *L'intrus peut déduire «fortement» u à partir de T et T'*

- **Déduction faible:** $T/T' \vdash' u$

  $\hookrightarrow$ *L'intrus peut déduire «faiblement» u à partir de T et T'*

Exemple - *la règle Axiome*

$$\frac{u \in T}{T \vdash u}$$

$$\swarrow \qquad \searrow$$

$$\text{(A)} \quad \frac{u \in T}{T/\emptyset \vdash u} \qquad\qquad \frac{u \text{ terme atomique}}{T/u \vdash' u} \quad \text{(A}'\text{)}$$

Le modèle de Dolev-Yao étendu

On introduit deux formes de séquent:

- **Déduction forte:** $T/T' \vdash u$
  $\hookrightarrow$ *L'intrus peut déduire «fortement» u à partir de T et T'*
- **Déduction faible:** $T/T' \vdash' u$
  $\hookrightarrow$ *L'intrus peut déduire «faiblement» u à partir de T et T'*

Exemple - *la règle Paire*

$$\frac{T \vdash u \quad T \vdash v}{T \vdash \langle u, v \rangle}$$

Laboratoire Spécification et Vérification

Le modèle de Dolev-Yao étendu

On introduit deux formes de séquent:

- **Déduction forte:** $T/T' \vdash u$

  $\hookrightarrow$ *L'intrus peut déduire «fortement» u à partir de T et T'*
- **Déduction faible:** $T/T' \vdash' u$

  $\hookrightarrow$ *L'intrus peut déduire «faiblement» u à partir de T et T'*

Exemple - *la règle Paire*

$$\frac{T \vdash u \quad T \vdash v}{T \vdash \langle u, v\rangle}$$

$$\swarrow \qquad \searrow$$

$$(\mathrm{P}) \quad \frac{T/T'_1 \vdash u \quad T/T'_2 \vdash v}{T/T'_1 \cup T'_2 \vdash \langle u, v\rangle} \qquad\qquad \frac{T/T'_1 \vdash' u \quad T/T'_2 \vdash' v}{T/T'_1 \cup T'_2 \vdash' \langle u, v\rangle} \quad (\mathrm{P}')$$

Le modèle de Dolev-Yao étendu

On introduit deux formes de séquent:

- **Déduction forte:** $T/T' \vdash u$
  $\hookrightarrow$ *L'intrus peut déduire «fortement» u à partir de T et T'*
- **Déduction faible:** $T/T' \vdash' u$
  $\hookrightarrow$ *L'intrus peut déduire «faiblement» u à partir de T et T'*

Exemple - *La règle Affaiblissement*

$$(\mathsf{W}) \quad \frac{u \in T}{T/\emptyset \vdash' u}$$

Laboratoire Spécification et Vérification

Déduction forte

(A) $$\frac{u \in T}{T/\emptyset \vdash u}$$

(P) $$\frac{T/T'_1 \vdash u \quad T/T'_2 \vdash v}{T/T'_1 \cup T'_2 \vdash \langle u, v\rangle}$$

(UL) $$\frac{T/T' \vdash \langle u, v\rangle}{T/T' \vdash u}$$

(UR) $$\frac{T/T' \vdash \langle u, v\rangle}{T/T' \vdash v}$$

(E) $$\frac{T/T'_1 \vdash u \quad T/T'_2 \vdash v}{T/T'_1 \cup T'_2 \vdash \{u\}_v}$$

(D) $$\frac{T/T'_1 \vdash \{u\}_v \quad T/T'_2 \vdash v^{-1}}{T/T'_1 \cup T'_2 \vdash u}$$

Déduction faible

(A′) $$\frac{u \text{ terme atomique}}{T/u \vdash' u}$$

(P′) $$\frac{T/T'_1 \vdash' u \quad T/T'_2 \vdash' v}{T/T'_1 \cup T'_2 \vdash' \langle u, v \rangle}$$

(UL′) $$\frac{T/T' \vdash' \langle u, v \rangle}{T/T' \vdash' u}$$

(UR′) $$\frac{T/T' \vdash' \langle u, v \rangle}{T/T' \vdash' v}$$

(E′) $$\frac{T/T'_1 \vdash' u \quad T/T'_2 \vdash' v}{T/T'_1 \cup T'_2 \vdash' \{u\}_v}$$

(D′) $$\frac{T/T'_1 \vdash' \{u\}_v \quad T/T'_2 \vdash' v^{-1}}{T/T'_1 \cup T'_2 \vdash' u}$$

La règle Comparaison ($1^{ère}$ version)

$$
\dfrac{
P_1 \left\{ \dfrac{\dfrac{\vdots}{\vdash' x_1} \ldots \dfrac{\vdots}{\vdash' x_n}}{T/T'_1 \vdash' {\color{purple}v}} \;\text{(R1)} \right.
\qquad
P_2 \left\{ \dfrac{\dfrac{\vdots}{\vdash' y_1} \ldots \dfrac{\vdots}{\vdash' y_n}}{T/T'_2 \vdash' {\color{purple}v}} \;\text{(R2)} \right.
}{
T/T'_1 \cup T'_2 \vdash \ {\color{red}w}
} \;\text{(Comp)}
$$

où:

(i). $w \in T'_1 \cup T'_2$

(ii). R1 $\neq$ R2 ou $\{x_1, .., x_n\} \neq \{y_1, ..., y_n\}$

(iii). P_1 et P_2 sont des preuves en forme normale

La règle Comparaison ($1^{ère}$ version)

$$
\dfrac{
P_1 \left\{ \dfrac{\dfrac{\vdots}{\vdash' x_1} \cdots \dfrac{\vdots}{\vdash' x_n}}{T/T'_1 \vdash' v} \right. (\mathrm{R1})
\qquad
P_2 \left\{ \dfrac{\dfrac{\vdots}{\vdash' y_1} \cdots \dfrac{\vdots}{\vdash' y_n}}{T/T'_2 \vdash' v} \right. (\mathrm{R2})
}{
T/T'_1 \cup T'_2 \vdash w
} \ (\mathrm{Comp})
$$

où:

(i). $w \in T'_1 \cup T'_2$

(ii). R1 $\neq$ R2 ou $\{x_1, .., x_n\} \neq \{y_1, ..., y_n\}$

(iii). P_1 et P_2 sont des preuves en forme normale

La règle Comparaison ($1^{ère}$ version)

$$\dfrac{P_1 \left\{ \dfrac{\dfrac{\vdots}{\vdash' x_1} \cdots \dfrac{\vdots}{\vdash' x_n}}{T/T'_1 \vdash' {\color{purple}v}} \;(\text{R1}) \right. \qquad P_2 \left\{ \dfrac{\dfrac{\vdots}{\vdash' y_1} \cdots \dfrac{\vdots}{\vdash' y_n}}{T/T'_2 \vdash' {\color{purple}v}} \;(\text{R2}) \right.}{T/T'_1 \cup T'_2 \vdash \; {\color{red}w}} \;(\text{Comp})$$

où:

(i). $w \in T'_1 \cup T'_2$

(ii). R1 $\neq$ R2 ou $\{x_1, .., x_n\} \neq \{y_1, ..., y_n\}$

(iii). P_1 et P_2 sont des preuves en forme normale

Laboratoire Spécification et Vérification

La règle Comparaison ($1^{ère}$ version)

$$\dfrac{P_1 \left\{ \dfrac{\dfrac{\vdots}{\vdash' x_1} \ldots \dfrac{\vdots}{\vdash' x_n}}{T/T'_1 \vdash' v}\ (\mathsf{R1}) \right. \qquad P_2 \left\{ \dfrac{\dfrac{\vdots}{\vdash' y_1} \ldots \dfrac{\vdots}{\vdash' y_n}}{T/T'_2 \vdash' v}\ (\mathsf{R2}) \right.}{T/T'_1 \cup T'_2 \vdash\ w}\ (\mathsf{Comp})$$

où:

(i). $w \in T'_1 \cup T'_2$

(ii). R1 $\neq$ R2 ou $\{x_1, .., x_n\} \neq \{y_1, ..., y_n\}$

(iii). P_1 et P_2 sont des preuves en forme normale

La règle Comparaison

$$\dfrac{P_1 \left\{ \dfrac{\dfrac{\vdots}{\vdash' x_1} \cdots \dfrac{\vdots}{\vdash' x_n}}{T/T_1' \vdash' u} \text{(R1)} \right. \qquad P_2 \left\{ \dfrac{\dfrac{\vdots}{\vdash' y_1} \cdots \dfrac{\vdots}{\vdash' y_n}}{T/T_2' \vdash' v} \text{(R2)} \right.}{T/T_1' \cup T_2' \vdash \ w} \text{(Comp)}$$

où:

(i). $w \in T_1' \cup T_2'$

(ii). R1 $\neq$ R2 ou $\{v, x_1, .., x_n\} \neq \{v, y_1, ..., y_n\}$

(iii). P_1 et P_2 sont des preuves en forme normale

(iv). $R(u, v)$ où $R = Id \cup \{(k, k^{-1})|$ k est une clef$\}$

Exemple 1 - protocole naïf de vote

$A \to S : \{v\}_{pub(S)}$

$T = \{\{v\}_{pub(S)}, pub(S)\}$
$T' = \{v\}$

Laboratoire
Spécification
et
Vérification

Exemple 1 - protocole naïf de vote

$$A \rightarrow S : \{v\}_{pub(S)}$$

$$T = \{\{v\}_{pub(S)}, pub(S)\}$$
$$T' = \{v\}$$

Nous avons la dérivation suivante:

$$\dfrac{\dfrac{\{v\}_{pub(S)} \in T}{T/\emptyset \vdash' \{v\}_{pub(S)}}\,\mathsf{W} \qquad \dfrac{\dfrac{}{T/\{v\} \vdash' v}\,\mathsf{A}' \qquad \dfrac{pub(S) \in T}{T/\emptyset \vdash' pub(S)}\,\mathsf{W}}{T/\{v\} \vdash' \{v\}_{pub(S)}}\,\mathsf{E}'}{T/\{v\} \vdash v}\,\mathsf{C}$$

Exemple 2 - challenge

$$\begin{aligned} A &\rightarrow B: \quad \{n\}_k \\ B &\rightarrow A: \quad \{n+1\}_k \end{aligned}$$

$$T = \{\{n\}_k, \{n+1\}_k\}$$
$$T' = \{k\}$$

Laboratoire Spécification et Vérification

Exemple 2 - challenge

$$
\begin{aligned}
A &\to B : \quad \{n\}_k \\
B &\to A : \quad \{n+1\}_k
\end{aligned}
\qquad\qquad
\begin{aligned}
T &= \{\{n\}_k, \{n+1\}_k\} \\
T' &= \{k\}
\end{aligned}
$$

Nous avons la dérivation suivante:

$$
\dfrac{
\dfrac{
\dfrac{
\dfrac{\{n\}_k \in T}{T/\emptyset \vdash' \{n\}_k}
\qquad
\dfrac{}{T/\{k\} \vdash' k}
}{T/\{k\} \vdash' n}
}{T/\{k\} \vdash' n+1}
\qquad
\dfrac{
\dfrac{\{n+1\}_k \in T}{T/\emptyset \vdash' \{n+1\}_k}
\qquad
\dfrac{}{T/\{k\} \vdash' k}
}{T/\{k\} \vdash' n+1}
}{T/k \vdash k}\; C
$$

Résultats

Le problème de déduction de l'intrus dans le modèle étendu

Résultat de localité:

La théorie de Dolev-Yao étendu est *locale* :
S'il existe une preuve de $T/T' \vdash s$, alors il existe une preuve qui n'utilise que des sous-termes des termes de $T \cup T' \cup \{s\}$.

Conséquence:

Le problème de déduction de l'intrus, $T/T' \overset{?}{\vdash} s$, est PTIME.

Laboratoire Spécification et Vérification

Plan

I) **Modélisation des attaques par prédictions**

- Problème de déduction de l'intrus dans le modèle de Dolev-Yao
- Problème de déduction de l'intrus dans le modèle étendu

II) **Vérification pratique des protocoles**

- Securify: un outil de vérification du secret
  - $\hookrightarrow$ Présentation de Securify
  - $\hookrightarrow$ Principe de fonctionnement
  - $\hookrightarrow$ Amélioration de Securify
  - $\hookrightarrow$ Caractéristiques de Securify
- Prototype: une procédure de recherche d'attaques

Présentation de Securify

Outil disponible en ligne, à l'adresse: `http://www-eva.imag.fr/outils1.html`

Entrée:

- un protocole
- une propriété de secret

Sortie:

- la traduction du protocole dans le modèle Millen-Rueß
- la réponse à la question: «le secret est-il vérifié?»
  - ↪ si oui, l'arbre de preuve
  - ↪ si non, l'arbre d'échec de la preuve
  - ↪ pas de réponse, l'outil ne termine pas
- le temps d'exécution

Laboratoire Spécification et Vérification

Principe de fonctionnement

But:

Montrer inductivement que l'application d'une règle du protocole ne compromet aucun secret.

Tests élémentaires:

Conditions suffisantes pour conclure au secret, elles sont au nombre de 3:

- $\hookrightarrow$ New
- $\hookrightarrow$ Almost In
- $\hookrightarrow$ Secrets Disjoints

Procédure de recherche:

Recherche arrière en considérant toutes les instances des règles qui ont pu engendrer une partie des prémisses de la règle déjà considérée.

Laboratoire Spécification et Vérification

Amélioration de Securify

Amélioration apportée:

↪ généralisation des 3 tests élémentaires

Résultats:

Protocoles		Preuve dans	
		Securify	Securify amélioré
Otway-Rees		Oui	Oui
Needham-Schroeder-Lowe	*secret de Na, Nb*	Oui	Oui
	secret de Na	Non	Oui
	secret de Nb	Non	Oui
Needham-Schroeder	*secret de Na, Nb*	Non	Non
	secret de Na	Non	Oui
	secret de Nb	Non	Non
Yahalom		Non	Oui
RPC Secure		Non	Oui

Caractéristiques de Securify

Points forts:

- nombre de sessions en parallèle ou en séquence non borné
- capacité mémoire de l'intrus non bornée
- taille des messages non bornée
- chiffrement symétrique et asymétrique
- donne une preuve du secret

Points faibles:

- une seule propriété: le secret (long terme)
- clefs atomiques
- variables typées
- hypothèse du chiffrement parfait (modèle de Dolev-Yao)

Plan

I) **Modélisation des attaques par prédictions**

- Problème de déduction de l'intrus dans le modèle de Dolev-Yao
- Problème de déduction de l'intrus dans le modèle étendu

II) **Vérification pratique des protocoles**

- Securify: un outil de vérification du secret
- Prototype: une procédure de recherche d'attaques

$\hookrightarrow$ Présentation du prototype

$\hookrightarrow$ Structure du prototype

$\hookrightarrow$ Résultats

Présentation du prototype

But:

implémenter et expérimenter le nouveau modèle d'intrus

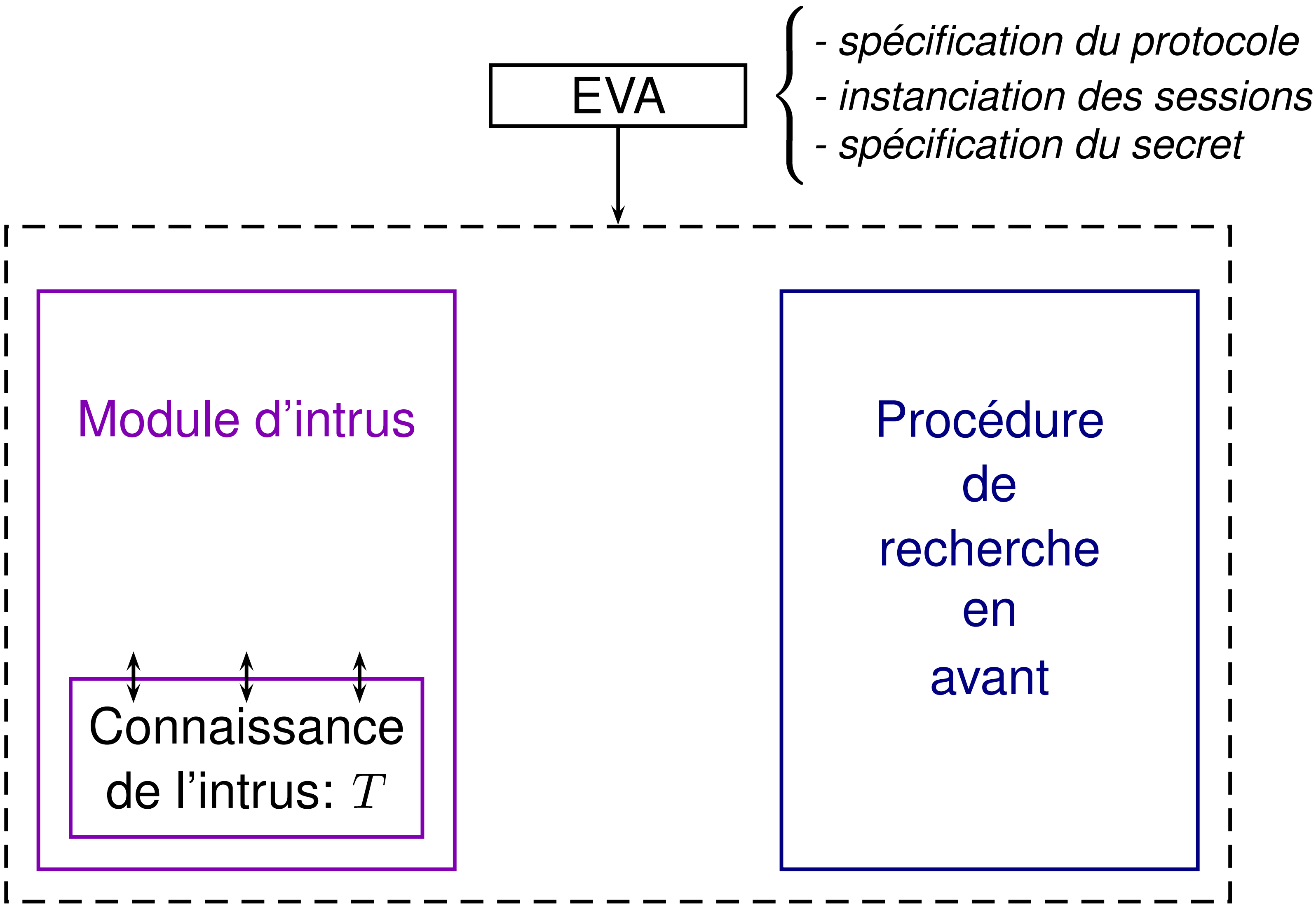
Entrée:

- un protocole
- les instances des sessions considérées
- une propriété de secret
- un module d'intrus

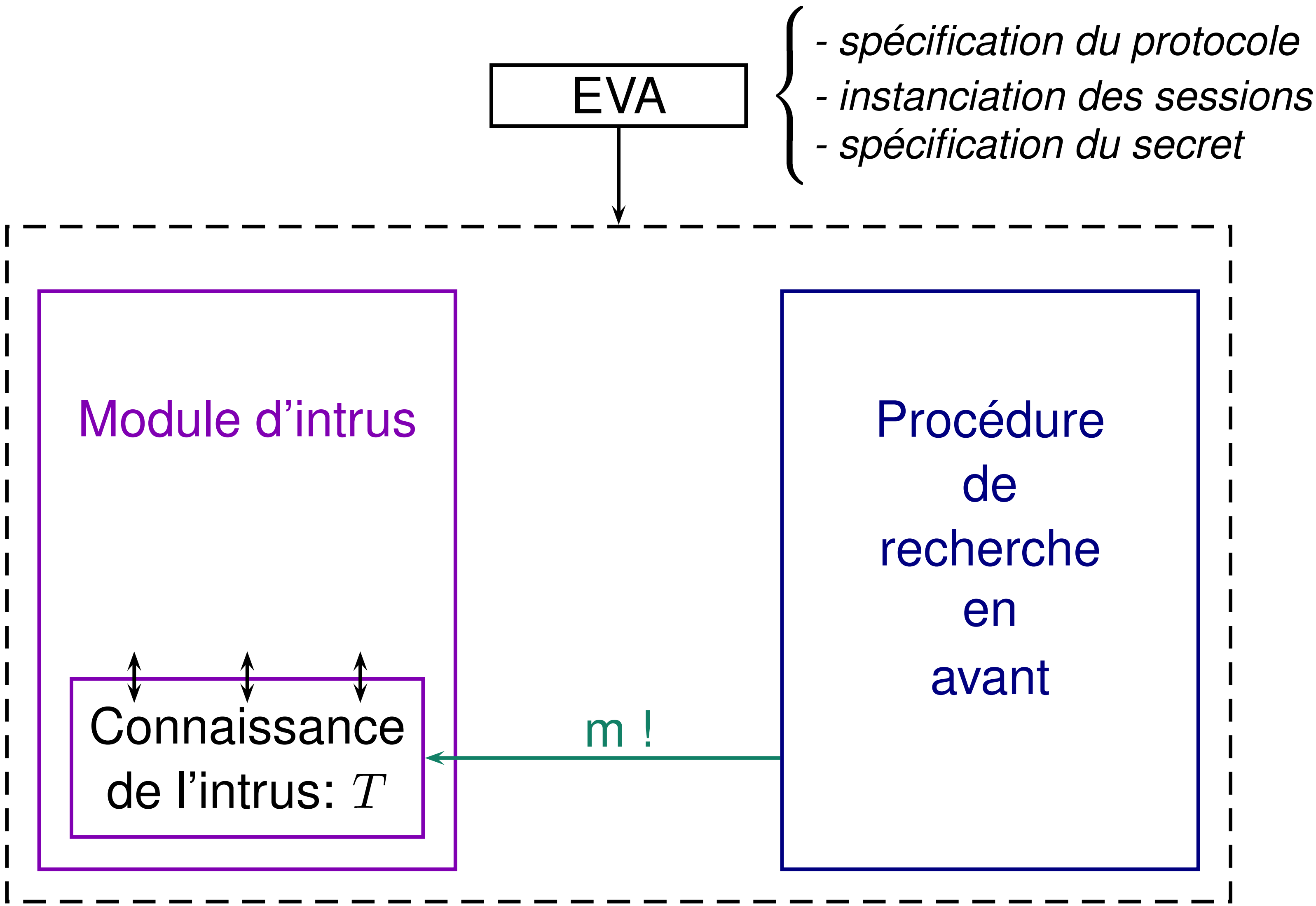
Sortie:

- la réponse à la question: «le secret est-il déductible par l'intrus»
  $\hookrightarrow$ si oui, description de l'attaque

Structure du prototype

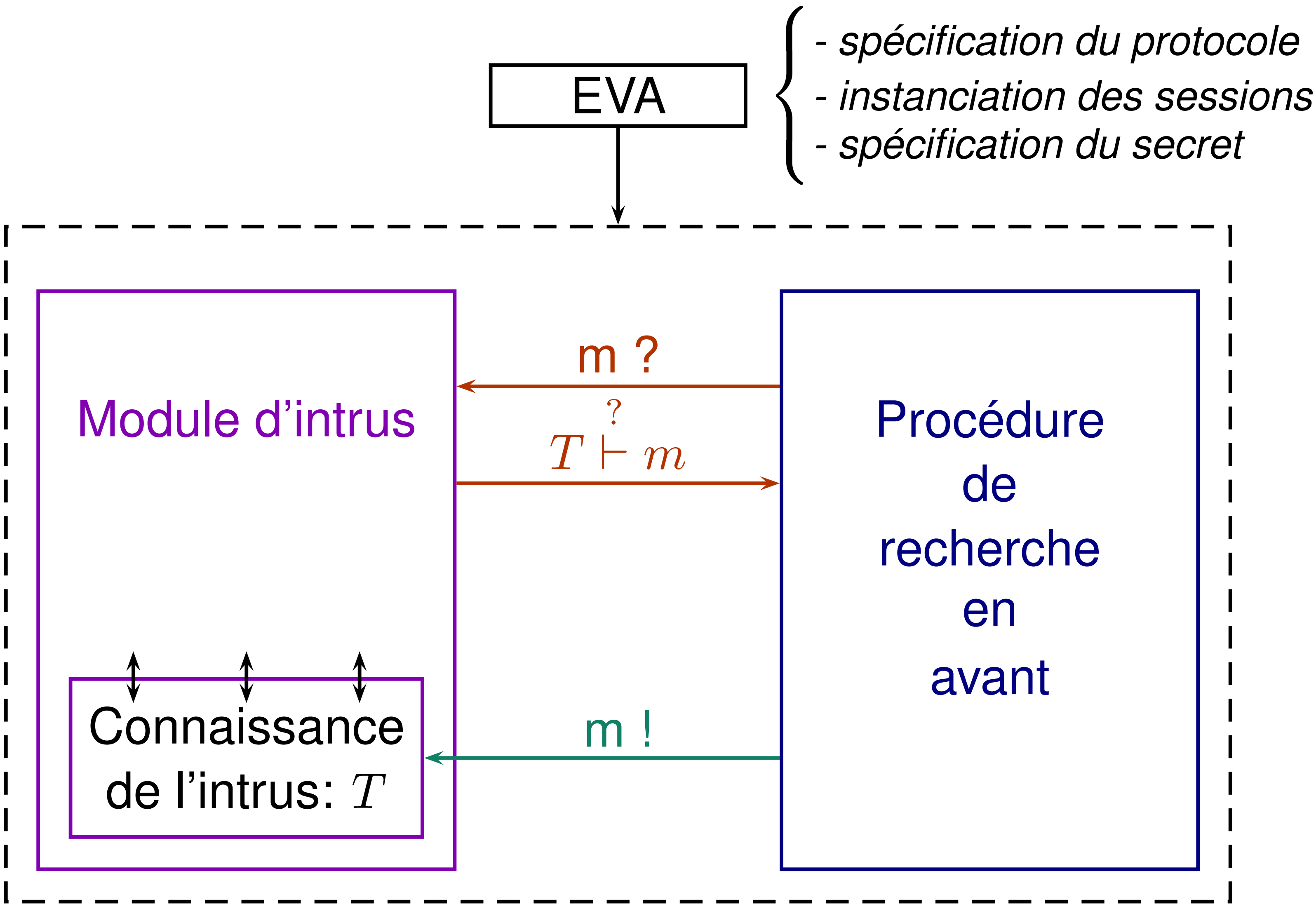


Structure du prototype



Laboratoire Spécification et Vérification

Structure du prototype



Laboratoire
Spécification
et
Vérification

Exemple - le protocole de Vote

```
Vote

constant keypair PK, SK (principal):number
parameter S, A : principal
parameter fresh N: weak
S knows S, PK, SK(S)
A knows A, S, N, PK

{ 1. A -> S : {N}_PK(S) }

value a, s: principal
value na:number
s1. session (A=a; S=s; N=na)

claim secret(na)
```

Laboratoire Spécification et Vérification

Résultats

↪ exécution normale d'une session du protocole

Protocole	Modèle d'intrus			
	Dolev-Yao standard		Dolev-Yao étendu	
	secret	temps (ms)	secret	temps (ms)
Vote	Oui	20	Non	20
Challenge	Oui	20	Non	20
Andrew Secure RPC	Oui	110	Non	60
Clefs asymétriques	Oui	20	Non	30
Echange Gong	Oui	60	Oui	310
Echange Gong modifié	Oui	30	Non	70
Bellovin et Merritt	Oui	50	Oui	220
Bellovin et Merritt modifié	Oui	50	Non	110

Laboratoire Spécification et Vérification

Protocole de Bellovin et Merritt (92)

But:

$\hookrightarrow$ échanger une clef de session Kab

$\hookrightarrow$ pw, mot de passe faible partagé entre les agents A et B (clef symétrique)

$\hookrightarrow$ pk, clef de session asymétrique fabriquée par A

Protocole:

$$
\begin{array}{lll}
A & \rightarrow B: & A, \{pk\}_{pw} \\
B & \rightarrow A: & \{\{Kab\}_{pk}\}_{pw} \\
A & \rightarrow B: & \{Na\}_{Kab} \\
B & \rightarrow A: & \{Na, Nb\}_{Kab} \\
A & \rightarrow B: & \{Nb\}_{Kab}
\end{array}
$$

Conclusion et Perspectives

Conclusion

- présentation d'un nouveau modèle d'intrus
- $T/T' \overset{?}{\vdash} s$ est PTIME
- prototype: une procédure de recherche d'attaques modulaire

Perspectives

- généraliser les résultats obtenus pour $T/T' \overset{?}{\vdash} s$, aux termes avec variables

  $\hookrightarrow$ résultat de décidabilité et de complexité pour un nombre borné de sessions
- considérer d'autres modèles d'intrus
- développer une procédure modulaire de recherche de preuves

Laboratoire Spécification et Vérification