Intruder deduction problem in presence of guessing attacks

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

Example 1 - vote protocol

Consider this exchange:

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

with $vote \in \{v_1, v_2, ..., v_n\}$.

Example 1 - vote protocol

Consider this exchange:

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

with $vote \in \{v_1, v_2, ..., v_n\}$.

Description of the guessing attack:

Laboratoire Spécification et Vérification

Example 1 - vote protocol

Consider this exchange:

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

with $vote \in \{v_1, v_2, ..., v_n\}$.

Description of the guessing attack:

- guess the value choosen by A: v_i

Laboratoire Spécification et Vérification

Example 1 - vote protocol

Consider this exchange:

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

with $vote \in \{v_1, v_2, ..., v_n\}$.

Description of the guessing attack:

- guess the value choosen by A: v_i
- build the message $\{v_i\}_{pub(S)}$

Example 1 - vote protocol

Consider this exchange:

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

with $vote \in \{v_1, v_2, ..., v_n\}$.

Description of the guessing attack:

- guess the value choosen by A: v_i
- build the message $\{v_i\}_{pub(S)}$
- compare it with the intercepted message: $\{vote\}_{pub(S)}$.

Laboratoire Spécification et Vérification

Example 1 - vote protocol

Consider this exchange:

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

with $vote \in \{v_1, v_2, ..., v_n\}$.

Description of the guessing attack:

- guess the value choosen by A: v_i
- build the message $\{v_i\}_{pub(S)}$
- compare it with the intercepted message: $\{vote\}_{pub(S)}$.

Result:

the intruder knows $vote$, the presumed secret vote of A.

Laboratoire Spécification et Vérification

Example 2 - Nonce challenge

Consider the two-messages handshake transaction: [Gong 93]

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

where $k \in \{k_1, ..., k_n\}$ is a symmetrical key and n is a nonce.

Laboratoire Spécification et Vérification

Example 2 - Nonce challenge

Consider the two-messages handshake transaction: [Gong 93]

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

where $k \in \{k_1, ..., k_n\}$ is a symmetrical key and n is a nonce.

Description of the guessing attack:

- guess the value of k : k_i
- decrypt the two intercepted messages $\{n\}_k$ and $\{n+1\}_k$ with the key k_i
- verify if the second obtained value is the increment of the first one.

Laboratoire Spécification et Vérification

Example 2 - Nonce challenge

Consider the two-messages handshake transaction: [Gong 93]

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

where $k \in \{k_1, ..., k_n\}$ is a symmetrical key and n is a nonce.

Description of the guessing attack:

- guess the value of k : k_i
- decrypt the two intercepted messages $\{n\}_k$ and $\{n+1\}_k$ with the key k_i
- verify if the second obtained value is the increment of the first one.

Result:

the intruder knows the key k, and the challenge n.

Laboratoire Spécification et Vérification

Summary

Goal:

Capture such «guessing attacks» in a formal framework

Laboratoire Spécification et Vérification

Summary

Goal:

Capture such «guessing attacks» in a formal framework

Results:

- An inference system replacing the classical Dolev-Yao model
- A decidability and PTIME complexity result for the intruder deduction problem

Laboratoire Spécification et Vérification

Summary

Goal:

Capture such «guessing attacks» in a formal framework

Results:

- An inference system replacing the classical Dolev-Yao model
- A decidability and PTIME complexity result for the intruder deduction problem

Related Work:

- In [Gong, Lomas, Needham & Saltzer, 1993]:
  $\hookrightarrow$ *definition and examples of «guessing attacks».*
- In [Lowe, 2002]:
  $\hookrightarrow$ *generalization of the definition and a decision algorithm.*

The intruder deduction problem: $T \overset{?}{\vdash} s$

INPUT:

- A finite set of messages: T,
  $\hookrightarrow$ *typically, the messages that pass over the network*
- A message: s,
  $\hookrightarrow$ *typically, a data assumed to be secret*

OUTPUT:

- Can the intruder deduce the secret s from T ?

Laboratoire
Spécification
et
Vérification

The Dolev-Yao model

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

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

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

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

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

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

The Dolev-Yao model

Axiom (A) $\dfrac{u \in T}{T \vdash u}$

Pairing (P) $\dfrac{T \vdash u \quad T \vdash v}{T \vdash \langle u, v \rangle}$

Unpairing (UL) $\dfrac{T \vdash \langle u, v \rangle}{T \vdash u}$

Unpairing (UR) $\dfrac{T \vdash \langle u, v \rangle}{T \vdash v}$

Encryption (E) $\dfrac{T \vdash u \quad T \vdash v}{T \vdash \{u\}_v}$

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

Laboratoire Spécification et Vérification

The Dolev-Yao model

Axiom (A) $\dfrac{u \in T}{T \vdash u}$

Pairing (P) $\dfrac{T \vdash u \quad T \vdash v}{T \vdash \langle u, v \rangle}$

Unpairing (UL) $\dfrac{T \vdash \langle u, v \rangle}{T \vdash u}$

Unpairing (UR) $\dfrac{T \vdash \langle u, v \rangle}{T \vdash v}$

Encryption (E) $\dfrac{T \vdash u \quad T \vdash v}{T \vdash \{u\}_v}$

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

Laboratoire Spécification et Vérification

The Dolev-Yao model

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

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

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

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

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

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

Results

The intruder deduction problem in the Dolev-Yao model

Locality result:

The Dolev-Yao theory is local in the sense of [Mc Allester, 1993]:
If $T \vdash s$, then there is a proof that only uses subterms of terms in $T \cup \{s\}$ [Comon & Shmatikov, 2003].

Consequence:

The intruder deduction problem, $T \stackrel{?}{\vdash} s$, is PTIME-complete.

Laboratoire Spécification et Vérification

The new intruder deduction problem: $T/T' \stackrel{?}{\vdash} s$

Laboratoire Spécification et Vérification

The new intruder deduction problem: $T/T' \overset{?}{\vdash} s$

INPUT:

- A finite set of «strongly known messages»: T,
  $\hookrightarrow$ *typically, the messages that pass over the network*

Laboratoire Spécification et Vérification

The new intruder deduction problem: $T/T' \stackrel{?}{\vdash} s$

INPUT:

- A finite set of «strongly known messages»: T,
  $\hookrightarrow$ *typically, the messages that pass over the network*
- A finite set of atomic data, the «weakly known messages»: T',
  $\hookrightarrow$ *typically, the data which take value in a finite set known by the intruder*

Laboratoire Spécification et Vérification

The new intruder deduction problem: $T/T' \overset{?}{\vdash} s$

INPUT:

- A finite set of «strongly known messages»: T,
  $\hookrightarrow$ *typically, the messages that pass over the network*
- A finite set of atomic data, the «weakly known messages»: T',
  $\hookrightarrow$ *typically, the data which take value in a finite set known by the intruder*
- A message: s,
  $\hookrightarrow$ *a data assumed to be secret*

Laboratoire Spécification et Vérification

The new intruder deduction problem: $T/T' \overset{?}{\vdash} s$

INPUT:

- A finite set of «strongly known messages»: T,
  $\hookrightarrow$ *typically, the messages that pass over the network*
- A finite set of atomic data, the «weakly known messages»: T',
  $\hookrightarrow$ *typically, the data which take value in a finite set known by the intruder*
- A message: s,
  $\hookrightarrow$ *a data assumed to be secret*

OUTPUT:

- Can the intruder deduce the secret s from T and T' ?

The extended Dolev-Yao model

We introduce two forms of sequents:

The extended Dolev-Yao model

We introduce two forms of sequents:

- **Strong deduction:** $T/T' \vdash u$

  $\hookrightarrow$ *The intruder can «strongly» deduce u from T and T'*

Laboratoire Spécification et Vérification

The extended Dolev-Yao model

We introduce two forms of sequents:

- **Strong deduction:** $T/T' \vdash u$

  $\hookrightarrow$ *The intruder can «strongly» deduce u from T and T'*

- **Weak deduction:** $T/T' \vdash' u$

  $\hookrightarrow$ *The intruder can «weakly» deduce u from T and T'*

Laboratoire Spécification et Vérification

The extended Dolev-Yao model

We introduce two forms of sequents:

- **Strong deduction:** $T/T' \vdash u$
  $\hookrightarrow$ *The intruder can «strongly» deduce u from T and T'*
- **Weak deduction:** $T/T' \vdash' u$
  $\hookrightarrow$ *The intruder can «weakly» deduce u from T and T'*

Example - *the axiom rule*

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

Laboratoire Spécification et Vérification

The extended Dolev-Yao model

We introduce two forms of sequents:

- **Strong deduction:** $T/T' \vdash u$
  $\hookrightarrow$ *The intruder can «strongly» deduce u from T and T'*
- **Weak deduction:** $T/T' \vdash' u$
  $\hookrightarrow$ *The intruder can «weakly» deduce u from T and T'*

Example - *the axiom rule*

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

$$\swarrow \qquad \searrow$$

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

Laboratoire Spécification et Vérification

The extended Dolev-Yao model

We introduce two forms of sequents:

- **Strong deduction:** $T/T' \vdash u$

  $\hookrightarrow$ *The intruder can «strongly» deduce u from T and T'*

- **Weak deduction:** $T/T' \vdash' u$

  $\hookrightarrow$ *The intruder can «weakly» deduce u from T and T'*

Example - *the pairing rule*

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

$$\swarrow \qquad \searrow$$

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

The extended Dolev-Yao model

We introduce two forms of sequents:

- **Strong deduction:** $T/T' \vdash u$
  $\hookrightarrow$ *The intruder can «strongly» deduce* u *from* T *and* T'
- **Weak deduction:** $T/T' \vdash' u$
  $\hookrightarrow$ *The intruder can «weakly» deduce* u *from* T *and* T'

Example - *the weakening rule*

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

Strong deduction

(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) $$\frac{T/T_1' \vdash \{u\}_v \quad T/T_2' \vdash v^{-1}}{T/T_1' \cup T_2' \vdash u}$$

Laboratoire Spécification et Vérification

Weak deduction

(A′) $$\frac{u \text{ atomic term}}{T/u \vdash' u}$$

(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′) $$\frac{T/T_1' \vdash' \{u\}_v \quad T/T_2' \vdash' v^{-1}}{T/T_1' \cup T_2' \vdash' u}$$

The compare rule (1^{st} version)

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

where:

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

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

(iii). P_1 and P_2 are normal proofs

The compare rule (1^{st} version)

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

where:

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

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

(iii). P_1 and P_2 are normal proofs

The compare rule (1^{st} version)

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

where:

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

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

(iii). P_1 and P_2 are normal proofs

Laboratoire Spécification et Vérification

The compare rule (1^{st} version)

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

where:

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

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

(iii). P_1 and P_2 are normal proofs

Laboratoire Spécification et Vérification

The compare rule

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

where:

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

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

(iii). P_1 and P_2 are normal proofs

(iv). $R(u, v)$ where $R = Id \cup \{(k, k^{-1})|$ k is a key$\}$

Laboratoire Spécification et Vérification

Example 1 - vote protocol

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

$T = \{\{v\}_{pub(S)}, pub(S)\}$

$T' = \{v\}$

Laboratoire Spécification et Vérification

Example 1 - vote protocol

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

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

We have the following derivation:

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

Laboratoire Spécification et Vérification

Example 2 - Nonce challenge

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

Example 2 - Nonce challenge

$$
\begin{array}{lll}
A & \rightarrow B : & \{n\}_k \\
B & \rightarrow A : & \{n+1\}_k
\end{array}
\qquad\qquad
\begin{array}{l}
T = \{\{n\}_k, \{n+1\}_k\} \\
T' = \{k\}
\end{array}
$$

We have the following derivation:

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

Results

The intruder deduction problem in the extended Dolev-Yao model

Locality theorem:

The extended Dolev-Yao theory is local in the following sense: If $T/T' \vdash s$, then there is a proof that only uses subterms of terms in $T \cup T' \cup \{s\}$.

Consequence:

The intruder deduction problem, $T/T' \stackrel{?}{\vdash} s$, is in PTIME.

Laboratoire Spécification et Vérification

Summary & Future work

Summary:

A decidability and PTIME complexity result for the intruder deduction problem in presence of guessable values

Laboratoire Spécification et Vérification

Summary & Future work

Summary:

A decidability and PTIME complexity result for the intruder deduction problem in presence of guessable values

Future work:

Passive attacker:		**Active attacker:**
attacker can only observe the messages that pass on the network	$\rightsquigarrow$	attacker can send messages and initiate new sessions
intruder deduction problem	$\rightsquigarrow$	reachability problem with a bounded number of sessions