

Models and analysis of security protocols

1st Semester 2009-2010

Active Intruder

Lecture 8

Pascal Lafourcade

Université Joseph Fourier, Verimag

Master: October 12th 2009

Last Time (I)

Lecture

- ▶ Passive Intruder
- ▶ Undecidability

Outline of Today

Active Intruder: Security Problem

Bounded Number of Sessions

NP-Hardness for Bounded Number of Sessions

Conclusion

Outline

Active Intruder: Security Problem

Bounded Number of Sessions

NP-Hardness for Bounded Number of Sessions

Conclusion

The Intruder is the Network (Worst Case)



Listen

Passive: Intruder deduction problem

The Intruder is the Network (Worst Case)

Listen



Passive: Intruder deduction problem

Active Intruder Security problem

- ▶ intercept messages (add messages to his knowledge)
- ▶ Play messages from his knowledge
- ▶ Start new sessions

Execution tree has:

- ▶ infinite branching (size of messages is not bounded)
- ▶ infinite depth (number of sessions is not bounded)

Active Intruder with bounded number of sessions

- ▶ Theoretically: **decidable**
- ▶ Interesting **practically**:
 - ▶ **Find flaws**
 - ▶ Usually attacks use **few sessions** !

Dolev-Yao Deduction System

Deduction System : $T_0 \vdash^? s$

$$(A) \quad \frac{u \in T_0}{T_0 \vdash u}$$

$$(UL) \quad \frac{T_0 \vdash \langle u, v \rangle}{T_0 \vdash u}$$

$$(P) \quad \frac{T_0 \vdash u \quad T_0 \vdash v}{T_0 \vdash \langle u, v \rangle}$$

$$(UR) \quad \frac{T_0 \vdash \langle u, v \rangle}{T_0 \vdash v}$$

$$(C) \quad \frac{T_0 \vdash u \quad T_0 \vdash v}{T_0 \vdash \{u\}_v}$$

$$(D) \quad \frac{T_0 \vdash \{u\}_v \quad T_0 \vdash v}{T_0 \vdash u}$$

Model: actions, roles and protocol

Definition (Action)

An **action** is a couple $(recv(u), send(v))$ such that $u \in \mathcal{T}(\mathcal{F}, \mathcal{X}) \cup \{init\}$, $v \in \mathcal{T}(\mathcal{F}, \mathcal{X}) \cup \{stop\}$. Denoted $(u \rightarrow v)$.

Model: actions, roles and protocol

Definition (Action)

An **action** is a couple $(recv(u), send(v))$ such that $u \in \mathcal{T}(\mathcal{F}, \mathcal{X}) \cup \{init\}$, $v \in \mathcal{T}(\mathcal{F}, \mathcal{X}) \cup \{stop\}$. Denoted $(u \rightarrow v)$.

Definition (Role)

A **role** is a finite sequence of actions:

$$(u_1 \rightarrow v_1), \dots, (u_n \rightarrow v_n)$$

such that $vars(v_i) \subseteq \bigcup_{1 \leq j \leq i} vars(u_j)$.

Model: actions, roles and protocol

Definition (Action)

An **action** is a couple $(recv(u), send(v))$ such that $u \in \mathcal{T}(\mathcal{F}, \mathcal{X}) \cup \{init\}$, $v \in \mathcal{T}(\mathcal{F}, \mathcal{X}) \cup \{stop\}$. Denoted $(u \rightarrow v)$.

Definition (Role)

A **role** is a finite sequence of actions:

$$(u_1 \rightarrow v_1), \dots, (u_n \rightarrow v_n)$$

such that $vars(v_i) \subseteq \bigcup_{1 \leq j \leq i} vars(u_j)$.

Definition (Protocol)

A **protocol** P is a finite set of roles: $P = \{R_1, \dots, R_k\}$

1st Example:

Example (Needham-schroeder)

1. $A \rightarrow B : \{N_a, A\}_{pk(B)}$
2. $B \rightarrow A : \{N_a, N_b\}_{pk(A)}$
3. $A \rightarrow B : \{N_b\}_{pk(B)}$

Write down each agent's role description, this A talks with anybody.

$$R_A = (init, X_b \rightarrow \{N_a, A\}_{pk(X_b)}, \\ (\{N_a, X_{N_b}\}_{pk(A)} \rightarrow \{X_{N_b}\}_{pk(X_b)}),$$

$$R_B = (\{X_{N_a}, X_A\}_{pk(B)} \rightarrow \{X_{N_a}, N_b\}_{pk(X_A)}) \\ (\{N_b\}_{pk(B)} \rightarrow stop)$$

Scyther Notation

```
A:  const Na: Nonce;
     var Nb: Nonce;

     send(A,B, {Na,A}pk(B));
     recv(B,A, {Na,Nb}pk(A));
     send(A,B, {Nb}pk(B));

B:  const Nb: Nonce;
     var Na: Nonce;

     recv(A,B, {Na,A}pk(B));
     send(B,A, {Na,Nb}pk(A));
     recv(A,B, {Nb}pk(B));
```

Exercise

Denning-Sacco Protocol

1. $A \rightarrow S : \langle A, B \rangle$
2. $S \rightarrow A : \{ \langle \langle B, N_{AB} \rangle, \langle N_S, \{ \langle N_{AB}, \langle A, N_S \rangle \} \rangle_{K_{BS}} \rangle \} \}_{K_{AS}}$
3. $A \rightarrow B : \{ \langle N_{AB}, \langle A, N_S \rangle \} \}_{K_{BS}}$
4. $B \rightarrow A : \{ S_{AB} \}_{N_{AB}}$

$P_{DS} = \{R_A, R_B, R_S\}$ models one session of A, B and S .

Exercise

Denning-Sacco Protocol

1. $A \rightarrow S : \langle A, B \rangle$
2. $S \rightarrow A : \{ \{ \langle B, N_{AB} \rangle, \langle N_S, \{ \langle N_{AB}, \langle A, N_S \rangle \} \}_{K_{BS}} \} \}_{K_{AS}}$
3. $A \rightarrow B : \{ \langle N_{AB}, \langle A, N_S \rangle \} \}_{K_{BS}}$
4. $B \rightarrow A : \{ S_{AB} \}_{N_{AB}}$

$P_{DS} = \{R_A, R_B, R_S\}$ models one session of A, B and S .

$$R_A = (init, X_B \rightarrow \langle A, X_B \rangle, \\ (\{ \{ \langle X_B, X_{N_{AB}} \rangle, \langle X_{N_S}, Z_A \rangle \} \}_{K_{AS}} \rightarrow Z_A), \\ (\{ W_A \}_{X_{N_{AB}}} \rightarrow stop))$$

$$R_B = (\{ \{ Y_{N_{AB}}, \langle X_A, Y_{N_S} \rangle \} \}_{K_{BS}} \rightarrow \{ S_{AB} \}_{Y_{N_{AB}}})$$

$$R_S = (\langle X_A, X_B \rangle \rightarrow \{ \{ \langle X_B, N_{AB}, \langle N_S, \{ \langle N_{AB}, \langle X_A, N_S \rangle \} \}_{K_{BS}} \} \}_{K_{AS}})$$

Semantic

Definition (States and Transitions)

A **state** is a couple (T, P) where T is a set of ground terms (intruder knowledge) and P a protocol.

We define a **transition relation** between states $(T, P) \rightarrow (T', P')$ by:

- ▶ $R_i \in P, R_i = (u \rightarrow v)$
- ▶ $T \vdash u\sigma \quad (dom(\sigma) = vars(u))$
- ▶ $T' = T \cup \{v\sigma\}$
- ▶ $R'_i \in P', R'_i = (P \setminus \{R_i\}) \cup R_i\sigma$

Example

Example

Let $T = \{a, b, k_l\}$ and $P = \{R\}$ where
 $R = (\langle x, y \rangle \rightarrow \langle \{y\}_k, x \rangle), (z \rightarrow \langle x, \langle y, z \rangle \rangle).$

- ▶ $(T, P) \rightarrow (T \cup \{\langle \{b\}_k, a \rangle\}, \{(z \rightarrow \langle a, \langle b, z \rangle \rangle)\})$
- ▶ $(T, P) \rightarrow (T \cup \{\langle \{\{a\}_{k_l}\}_k, a \rangle\}, \{(z \rightarrow \langle a, \langle \{a\}_{k_l}, z \rangle \rangle)\})$
- ▶ $(T, P) \not\rightarrow (T \cup \{\langle \{\{a\}_k\}_k, a \rangle\}, \{(z \rightarrow \langle a, \langle \{a\}_k, z \rangle \rangle)\})$

Example

Example

Let $T = \{a, b, k_l\}$ and $P = \{R\}$ where

$R = (\langle x, y \rangle \rightarrow \langle \{y\}_k, x \rangle), (z \rightarrow \langle x, \langle y, z \rangle \rangle).$

- ▶ $(T, P) \rightarrow (T \cup \{\langle \{b\}_k, a \rangle\}, \{(z \rightarrow \langle a, \langle b, z \rangle \rangle)\})$
- ▶ $(T, P) \rightarrow (T \cup \{\langle \{\{a\}_{k_l}\}_k, a \rangle\}, \{(z \rightarrow \langle a, \langle \{a\}_{k_l}, z \rangle \rangle)\})$
- ▶ $(T, P) \not\rightarrow (T \cup \{\langle \{\{a\}_k\}_k, a \rangle\}, \{(z \rightarrow \langle a, \langle \{a\}_k, z \rangle \rangle)\})$

Each branch has a **finite depth**, but **possibly a infinite branching**.

Preservation of the secrecy

Definition (Secrecy)

Let T_1 be a ground set of terms (Initial knowledge of the intruder). A protocol P **does not preserve the secrecy** of a ground term s for T_1 if there does not exist a state (T', P') , such that

- ▶ $T' \vdash s$
- ▶ $(T_1, P) \rightarrow^* (T', P')$

where \rightarrow^* is the reflexive and transitive closure of \rightarrow .

If there does not exist a such state (T', P') we say that P **preserves the secrecy** of s for the initial intruder knowledge T_1 .

Interleaving

Definition (Partial Order $<_P$)

A protocol P define a **partial order** $<_P$ on actions of P , s.t

$$(u_i \rightarrow v_i) <_P (u_j \rightarrow v_j)$$

if $R \in P$, $R = (u_1 \rightarrow v_1) \dots (u_i \rightarrow v_i) \dots (u_j \rightarrow v_j) \dots (u_n \rightarrow v_n)$ ($1 \leq i \leq j \leq n$).

Interleaving

Definition (Partial Order $<_P$)

A protocol P define a **partial order** $<_P$ on actions of P , s.t

$$(u_i \rightarrow v_i) <_P (u_j \rightarrow v_j)$$

if $R \in P$, $R = (u_1 \rightarrow v_1) \dots (u_i \rightarrow v_i) \dots (u_j \rightarrow v_j) \dots (u_n \rightarrow v_n)$ ($1 \leq i \leq j \leq n$).

Definition (Execution Order $<_E$)

An execution order $<_E$ of P is a total order on the subset A of actions of P , compatible with $<_P$ and stable by predecessor, i.e.

$$\text{if } b \in A \text{ et } a <_P b \text{ then } a \in A \text{ and } a <_E b$$

It corresponds to an interleaving of roles.

Secrecy

Definition (Secrecy over \langle_E)

Let an execution order \langle_E of P . We assume that

$$(u_1 \rightarrow v_1) \langle_E \dots \langle_E (u_n \rightarrow v_n)$$

\langle_E does not preserve the secrecy of s , given T_1 if there exists $\sigma_1, \dots, \sigma_n$ such that

$$(P, T_1) \rightarrow (P_1, T_1 \cup \{v_1\sigma_1\}) \rightarrow \dots \rightarrow (P_n, T_1 \cup \{v_1\sigma_1, \dots, v_n\sigma_n\})$$

and $T_1 \cup \{v_1\sigma_1, \dots, v_n\sigma_n\} \vdash s$.

Outline

Active Intruder: Security Problem

Bounded Number of Sessions

NP-Hardness for Bounded Number of Sessions

Conclusion

Constraints System

Symbolic representation of execution tree by constraints system.

Definition (Constraints System)

A **constraint** is an expression $T \Vdash u$ where T is a set of terms and u a term.

A **constraints system** C is a finite set of constraints $\cup_{1 \leq i \leq n} T_i \Vdash u_i$ such that

- ▶ $T_i \subseteq T_{i+1}$ ($1 \leq i \leq n$)
- ▶ if $T_i \Vdash u_i \in C$ and $x \in \text{vars}(T_i)$ then $T_j = \min\{T' \mid T' \Vdash v \in C, x \in \text{vars}(v)\}$ exists and $j < i$

A substitution σ is a **solution** of C if $T\sigma \vdash u\sigma$ for all $T \Vdash u \in C$.

We denote by \perp a constraints system unsatisfiable.

From Protocols to Constraints system

Let P a protocol, $<_E$ an execution order of P and s a secret term.

$$(u_1 \rightarrow v_1) <_E (u_2 \rightarrow v_2) <_E \dots <_E (u_n \rightarrow v_n)$$

We associate C :

$$\begin{array}{rcl} T_1 & \Vdash & u_1 \\ T_2 = T_1 \cup \{v_1\} & \Vdash & u_2 \\ & \vdots & \\ T_n = T_{n-1} \cup \{v_{n-1}\} & \Vdash & u_n \\ T_{n+1} = T_n \cup \{v_n\} & \Vdash & s \end{array}$$

We show that C has a solution iff $<_E$ does not preserve the secret of the term s .

Exercises

Exercise 1

$A \rightarrow B : \langle A, N_A \rangle$

$B \rightarrow A : \{\langle N_A, N_B \rangle\}_{K_{ab}}$

$A \rightarrow B : N_B$

$B \rightarrow A : \{\langle K, N_B \rangle\}_{K_{ab}}$

$A \rightarrow B : \{s\}_K$

Intruder knows only identities of A and B .

- ▶ Give role specification of this protocol of an instance of execution between A and B .
- ▶ Give a constraint system associated to this protocol between A and B .

Solution

$$\begin{aligned}
 A \rightarrow B &: \langle A, N_A \rangle \\
 B \rightarrow A &: \{\langle N_A, N_B \rangle\}_{K_{ab}} \\
 A \rightarrow B &: N_B \\
 B \rightarrow A &: \{\langle K, N_B \rangle\}_{K_{ab}} \\
 A \rightarrow B &: \{s\}_K
 \end{aligned}$$

$T_1 =$

$\{A, B, \langle A, N_A \rangle, \{\langle N_A, N_B \rangle\}_{K_{ab}}, N_B, \{\langle K, N_B \rangle\}_{K_{ab}}, \{s\}_K, \text{init}, \text{stop}\}$

Roles

$$\begin{aligned}
 R_A = & (\text{init} \rightarrow \langle A, N_A \rangle), \\
 & (\{\langle N_A, X_{N_B} \rangle\}_{K_{(A, X_B)}} \rightarrow X_{N_B}), \\
 & (\{\langle X_K, X_{N_B} \rangle\}_{K_{(A, X_B)}} \rightarrow \{s\}_{X_K})
 \end{aligned}$$

$$\begin{aligned}
 R_B = & (\langle X_A, X_{N_A} \rangle \rightarrow \{\langle X_{N_A}, N_B \rangle\}_{K_{(X_A, B)}}) \\
 & (N_B \rightarrow \{\langle K, N_B \rangle\}_{K_{(X_A, B)}}), \\
 & (\{X_s\}_K \rightarrow \text{stop})
 \end{aligned}$$

Solution

$$\begin{aligned}
 A \rightarrow B &: \langle A, N_A \rangle \\
 B \rightarrow A &: \{\langle N_A, N_B \rangle\}_{K_{ab}} \\
 A \rightarrow B &: N_B \\
 B \rightarrow A &: \{\langle K, N_B \rangle\}_{K_{ab}} \\
 A \rightarrow B &: \{s\}_K
 \end{aligned}$$

$T_1 =$

$\{A, B, \langle A, N_A \rangle, \{\langle N_A, N_B \rangle\}_{K_{ab}}, N_B, \{\langle K, N_B \rangle\}_{K_{ab}}, \{s\}_K, \text{init}, \text{stop}\}$

Constraint System

T_1	\Vdash	init
$T_2 = T_1 \cup \{\langle A, N_A \rangle\}$	\Vdash	$\langle X_A, X_{N_A} \rangle$
$T_3 = T_2 \cup \{\{\langle X_{N_A}, N_B \rangle\}_{K_{(X_A, B)}}\}$	\Vdash	$\{\langle N_A, X_{N_B} \rangle\}_{K_{(A, X_B)}}$
$T_4 = T_3 \cup \{X_{N_B}\}$	\Vdash	N_B
$T_5 = T_4 \cup \{\{\langle K, N_B \rangle\}_{K_{(X_A, B)}}\}$	\Vdash	$\{\langle X_K, X_{N_B} \rangle\}_{K_{(A, X_B)}}$
$T_6 = T_5 \cup \{\{s\}_{X_K}\}$	\Vdash	$\{X_s\}_K$
$T_7 = T_6 \cup \{\text{stop}\}$	\Vdash	s

Resolution of Constraints systems

Definition (Rules of simplification: $C \rightsquigarrow_{\sigma} C'$)

R_1	$C \cup \{T \Vdash u\}$	\rightsquigarrow	C	if $T \cup \{x \mid T' \Vdash x \in C, T' \subset T\} \vdash u$
R_2	$C \cup \{T \Vdash u\}$	$\rightsquigarrow_{\sigma}$	$C\sigma \cup \{T\sigma \Vdash u\sigma\}$	$\sigma = mgu(t, u), t \in st(T),$ t, u no variables
R_3	$C \cup \{T \Vdash u\}$	$\rightsquigarrow_{\sigma}$	$C\sigma \cup \{T\sigma \Vdash u\sigma\}$	$\sigma = mgu(t_1, t_2), t_1, t_2 \in st(T),$ t_1, t_2 no variables
R_4	$C \cup \{T \Vdash \{u\}_v\}$	\rightsquigarrow	$C \cup \{T \Vdash u, T \Vdash v\}$	
R_5	$C \cup \{T \Vdash \langle u, v \rangle\}$	\rightsquigarrow	$C \cup \{T \Vdash u, T \Vdash v\}$	
R_6	$C \cup \{T \Vdash u\}$	\rightsquigarrow	\perp	if $T = \emptyset$ or $var(T) = var(u) = \emptyset$ and $T \not\vdash u$

Properties of simplification rules

Lemma (Preservation)

Simplification rules transform a constraints system into a constraints system.

Properties of simplification rules

Lemma (Preservation)

Simplification rules transform a constraints system into a constraints system.

Lemma (Correctness)

If $C \rightsquigarrow_{\sigma} C'$ then if θ is a solution of C' , $\sigma\theta$ is also a solution of C .

Properties of simplification rules

Lemma (Preservation)

Simplification rules transform a constraints system into a constraints system.

Lemma (Correctness)

If $C \rightsquigarrow_{\sigma} C'$ then if θ is a solution of C' , $\sigma\theta$ is also a solution of C .

Lemma (Termination)

Simplification rules always terminate: There does not exist infinite chain $C \rightsquigarrow_{\sigma_1} C_1 \rightsquigarrow_{\sigma_2} C_2 \rightsquigarrow_{\sigma_3} \dots$

Properties

Definition (Solved Form)

A constraints system C is in **solved form** if $C = \perp$ or if each constraint is of the following form $T \Vdash x$ where x is a variable $T \neq \emptyset$.

Lemma

All constraints systems in solved form different of \perp has at least one solution.

Properties

Definition (Solved Form)

A constraints system C is in **solved form** if $C = \perp$ or if each constraint is of the following form $T \Vdash x$ where x is a variable $T \neq \emptyset$.

Lemma

All constraints systems in solved form different of \perp has at least one solution.

Lemma (Completeness)

If C is a constraint system not in solved form and if σ is a solution of C then there exists θ, τ such that $C \rightsquigarrow_{\theta} C'$, $\sigma = \theta\tau$ and τ is a solution of C' .

Decidability

Theorem

Preservation of the secrecy for protocol with bounded number of sessions is decidable.

- ▶ Guess an interleaving and build constraints system associated.
- ▶ Using previous lemma C has a solution iff there exists C' in solved form such that $C' \neq \perp$ and $C \rightsquigarrow_{\tau} C'$
- ▶ Using termination lemma to conclude.

We also can show that the problem is in co-NP.

Exercises

Exercise 1

$$A \rightarrow B : \langle A, N_A \rangle$$

$$B \rightarrow A : \{ \langle N_A, N_B \rangle \}_{K_{ab}}$$

$$A \rightarrow B : N_B$$

$$B \rightarrow A : \{ \langle K, N_B \rangle \}_{K_{ab}}$$

$$A \rightarrow B : \{s\}_K$$

Intruder knows only identities of A and B .

- ▶ Use simplification rules to transform the system in solved form.
- ▶ There exists an easy attack, can you find it ?

Solution

$$T_1 = \{A, B, \langle A, N_A \rangle, \{\langle N_A, N_B \rangle\}_{K_{ab}}, N_B, \{\langle K, N_B \rangle\}_{K_{ab}}, \{s\}_K, \text{init}, \text{stop}\}$$

C_1	T_1	\Vdash	init
C_2	$T_2 = T_1 \cup \{\langle A, N_A \rangle\}$	\Vdash	$\langle X_A, X_{N_A} \rangle$
C_3	$T_3 = T_2 \cup \{\{\langle X_{N_A}, N_B \rangle\}_{K_{(X_A, B)}}\}$	\Vdash	$\{\langle N_A, X_{N_B} \rangle\}_{K_{(A, X_B)}}$
C_4	$T_4 = T_3 \cup \{X_{N_B}\}$	\Vdash	N_B
C_5	$T_5 = T_4 \cup \{\{\langle K, N_B \rangle\}_{K_{(X_A, B)}}\}$	\Vdash	$\{\langle X_K, X_{N_B} \rangle\}_{K_{(A, X_B)}}$
C_6	$T_6 = T_5 \cup \{\{s\}_{X_K}\}$	\Vdash	$\{X_s\}_K$
C_7	$T_7 = T_6 \cup \{\text{stop}\}$	\Vdash	s

Road book

Interleaving: $(u_1^A, v_1^A)(u_1^B, v_1^B)(u_2^A, v_2^A)(u_2^B, v_2^B)(u_3^A, v_3^A)(u_3^B, v_3^B)$

$$R_2 \quad C \cup \{T \Vdash u\} \rightsquigarrow_{\sigma} C\sigma \cup \{T\sigma \Vdash u\sigma\} \quad \sigma = \text{mgu}(t, u), t \in \text{st}(T), \\ t, u \text{ no variables}$$

- ▶ Apply nothing on C_1 , already in resolved form.
- ▶ Apply R_2 on C_2 give $\sigma_1 = \{X_{N_A} \leftarrow N_A, X_A \leftarrow A\}$ and R_1

Solution

$$T_1 = \{A, B, \langle A, N_A \rangle, \{\langle N_A, N_B \rangle\}_{K_{ab}}, N_B, \{\langle K, N_B \rangle\}_{K_{ab}}, \{s\}_K, \text{init}, \text{stop}\}$$

$$\begin{array}{lll}
 C_3\sigma_1 & T_3 = T_2 \cup \{\{\langle N_A, N_B \rangle\}_{K_{(A,B)}}\} & \Vdash \{\langle N_A, X_{N_B} \rangle\}_{K_{(A,X_B)}} \\
 C_4\sigma_1 & T_4 = T_3 \cup \{X_{N_B}\} & \Vdash N_B \\
 C_5\sigma_1 & T_5 = T_4 \cup \{\{\langle K, N_B \rangle\}_{K_{(A,B)}}\} & \Vdash \{\langle X_K, X_{N_B} \rangle\}_{K_{(A,X_B)}} \\
 C_6\sigma_1 & T_6 = T_5 \cup \{\{s\}_{X_K}\} & \Vdash \{X_s\}_K \\
 C_7\sigma_1 & T_7 = T_6 \cup \{\text{stop}\} & \Vdash s
 \end{array}$$

Road book $\sigma_1 = \{X_{N_A} \leftarrow N_A, X_A \leftarrow A\}$

► Apply R_2 on C_3 gives $\sigma_2 = \{X_{N_B} \leftarrow N_B, X_B \leftarrow B\}$ (or N_A) and R_1

Solution

$$T_1 = \{A, B, \langle A, N_A \rangle, \{\langle N_A, N_B \rangle\}_{K_{ab}}, N_B, \{\langle K, N_B \rangle\}_{K_{ab}}, \{s\}_K, \text{init}, \text{stop}\}$$

$$\begin{array}{lll} C_5\sigma_1\sigma_2 & T_5 = T_4 \cup \{\{\langle K, N_B \rangle\}_{K_{(A,B)}}\} & \Vdash \{\langle X_K, N_B \rangle\}_{K_{(A,B)}} \\ C_6\sigma_1\sigma_2 & T_6 = T_5 \cup \{\{s\}_{X_K}\} & \Vdash \{X_S\}_K \\ C_7\sigma_1\sigma_2 & T_7 = T_6 \cup \{\text{stop}\} & \Vdash s \end{array}$$

Road book $\sigma_1 = \{X_{N_A} \leftarrow N_A, X_A \leftarrow A\}$ $\sigma_2 = \{X_{N_B} \leftarrow N_B, X_B \leftarrow B\}$

- ▶ Apply R_2 on $C_5\sigma_1\sigma_2$ give $\sigma_3 = \{X_K \leftarrow N_A\}$
- ▶ Apply R_2 , on $\sigma_1\sigma_2\sigma_3C_6$ give $\sigma_4 = \{X_S \leftarrow s\}$

Solution

- 1 $A \rightarrow B : \langle A, N_A \rangle$
- 2 $B \rightarrow A : \{\langle N_A, N_B \rangle\}_{K_{ab}}$
- 3 $A \rightarrow B : N_B$
- 4 $B \rightarrow A : \{\langle K, N_B \rangle\}_{K_{ab}}$
- 5 $A \rightarrow B : \{s\}_K$

The resolution of constraint system gives the following attack:
Send 2nd message $\{\langle N_A, N_B \rangle\}_{K_{ab}}$ instead of the 4th message $\{\langle K, N_B \rangle\}_{K_{ab}}$. Hence A will replay $\{s\}_{N_A}$ because intruder knows N_A

Exercises

Exercise 2

$$A \rightarrow B : \{\langle A, K \rangle\}_{K_{ab}}$$

$$B \rightarrow A : \{s\}_{K_{ab}}$$

Intruder knows only identities of A and B . Show that the secret data s is preserved by one single session between A and B .

Solution

$$A \rightarrow B : \{\langle A, K \rangle\}_{K_{ab}}$$

$$B \rightarrow A : \{s\}_{K_{ab}}$$

$$T_1 = \{A, B, \{\langle A, K \rangle\}_{K_{ab}}, \{s\}_{K_{ab}}\}$$

Constraint System

C_1	T_1	\Vdash	$\{\langle A, X_K \rangle\}_{K_{ab}}$
C_2	$T_2 = T_1 \cup \{\langle A, X_K \rangle\}_{K_{ab}}$	\Vdash	$\{s\}_{X_{K_{ab}}}$
C_3	$T_3 = T_2 \cup \{s\}_{X_{K_{ab}}}$	\Vdash	s

Solution

$$\begin{array}{ll}
 C_1 & T_1 \qquad \qquad \qquad \Vdash \{ \langle A, X_K \rangle \}_{X_{K_{ab}}} \\
 C_2 & T_2 = T_1 \cup \{ \langle A, X_K \rangle \}_{X_{K_{ab}}} \quad \Vdash \{ s \}_{X_{K_{ab}}} \\
 C_3 & T_3 = T_2 \cup \{ s \}_{X_{K_{ab}}} \quad \Vdash s
 \end{array}$$

$$T_1 = \{ A, B, \{ \langle A, K \rangle \}_{K_{ab}}, \{ s \}_{K_{ab}} \}$$

Road book

- ▶ Apply nothing or R_4 or R_5 and R_2 on C_1 give $\sigma_0 = \{ X_K \leftarrow K, X_{K_{ab}} \leftarrow K_{ab} \}$
- ▶ Apply R_5 or nothing and R_2 , on $\sigma_0 C_2$ give $\sigma_1 = \{ X_{N_B} \leftarrow N_B \}$ (or N_A)

Each time you meet a solved form of the form \perp with R_6 .

Outline

Active Intruder: Security Problem

Bounded Number of Sessions

NP-Hardness for Bounded Number of Sessions

Conclusion

NP-hardness

Theorem

Decide if a protocol P does not preserve the secrecy of a ground term s from an initial knowledge T_1 is NP-difficult.

Recall 3-SAT Problem

Definition

Input: set of propositional variables $\{x_1, \dots, x_n\}$ and a conjunction of clauses with 3 literals.

$$f(\vec{x}) = \bigwedge_{1 \leq i \leq l} (x_{i,1}^{\epsilon_{i,1}} \vee x_{i,2}^{\epsilon_{i,2}} \vee x_{i,3}^{\epsilon_{i,3}})$$

where $\epsilon_{i,j} \in \{+, -\}$ and $x^+ = x, x^- = \neg x$.

Question : Does exist a valuation V of $\{x_1, \dots, x_n\}$, such that $V(f(\vec{x})) = \top$.

Theorem

3-SAT problem is NP-complete.

NP-difficulty

We build a protocol such that an intruder can deduce s iff $f(\vec{x})$ is satisfaisable.

$$g(x_{i,j}^{\epsilon_{i,j}}) = \begin{cases} x_{i,j} & \text{if } \epsilon_{i,j} = + \\ \{x_{i,j}\}_K & \text{if } \epsilon_{i,j} = - \end{cases}$$

$$\forall 1 \leq i \leq l : f_i(\vec{x}) = \langle g(x_{i,1}^{\epsilon_{i,1}}), g(x_{i,2}^{\epsilon_{i,2}}), g(x_{i,3}^{\epsilon_{i,3}}) \rangle$$

We suppose Initial intruder knowledge is $\{\perp, \top\}$.

$$A : \langle x_1, \langle \dots, x_n \rangle \rangle \rightarrow \{ \langle f_1(\vec{x}), \langle f_2(\vec{x}), \langle \dots, \langle f_n(\vec{x}), end \rangle \dots \rangle \rangle \}_p$$

$$\forall 1 \leq i \leq l :$$

$$B_i : \{ \langle \langle \top, \langle x, y \rangle \rangle, z \rangle \}_p \rightarrow \{z\}_p$$

$$\overline{B}_i : \{ \langle \langle \{ \perp \}_K, \langle x, y \rangle \rangle, z \rangle \}_p \rightarrow \{z\}_p$$

$$C_i : \{ \langle \langle x, \langle \top, y \rangle \rangle, z \rangle \}_p \rightarrow \{z\}_p$$

$$\overline{C}_i : \{ \langle \langle x, \langle \{ \perp \}_K, y \rangle \rangle, z \rangle \}_p \rightarrow \{z\}_p$$

$$D_i : \{ \langle \langle x, \langle y, \top \rangle \rangle, z \rangle \}_p \rightarrow \{z\}_p$$

$$\overline{D}_i : \{ \langle \langle x, \langle y, \{ \perp \}_K \rangle \rangle, z \rangle \}_p \rightarrow \{z\}_p$$

$$E : \{ end \}_p \rightarrow s$$

Outline

Active Intruder: Security Problem

Bounded Number of Sessions

NP-Hardness for Bounded Number of Sessions

Conclusion

Summary

Today

- ▶ Active Intruder
- ▶ Bounded Number of Sessions
- ▶ NP-Hardness
- ▶ Tools

Next Time

- ▶ Playing with Tools:
 - ▶ Scyther
 - ▶ Avispa: OFMC, CI-Atse, SATMC, TA4SP
 - ▶ Proverif

Thank you for your attention



Questions ?