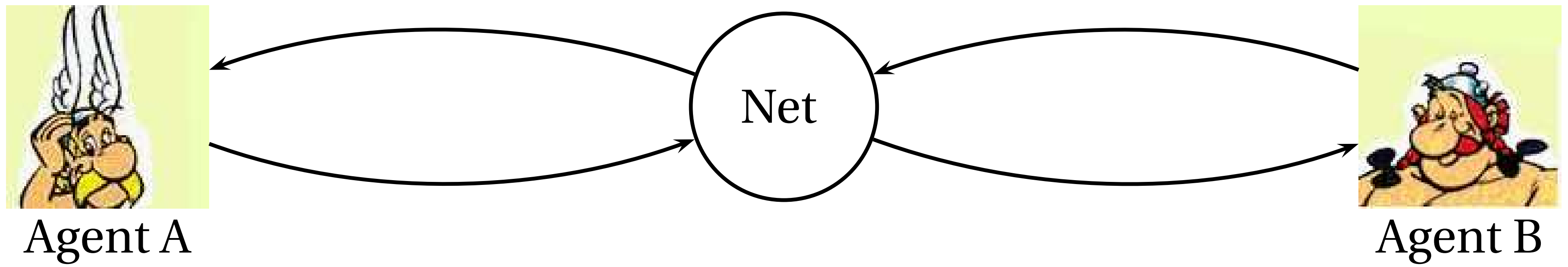
A Decision Procedure for the Verification of Security Protocols with Explicit Destructors

Stéphanie Delaune

LSV, CNRS UMR 8643, ENS de Cachan

France Telecom R&D

Cryptographic Protocols



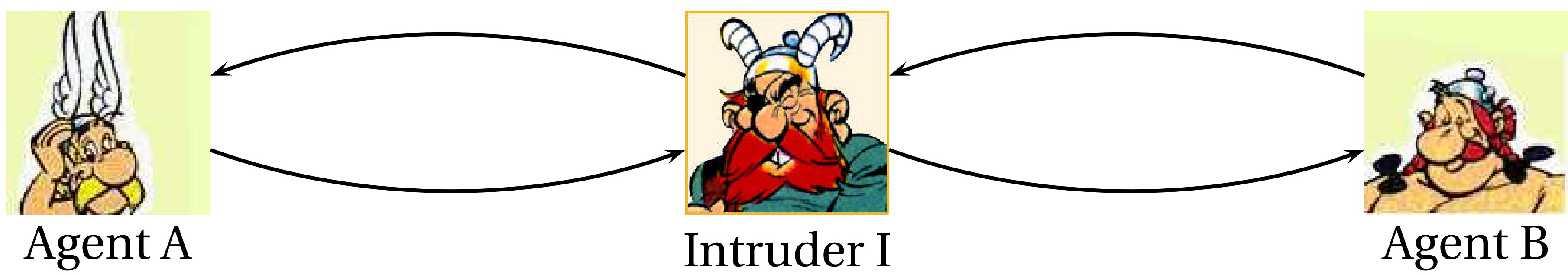
Protocol

$\hookrightarrow$ rules of message exchanges

Goal

$\hookrightarrow$ secure communications: *secrecy, authentication, anonymity* ...

Cryptographic Protocols



Messages $\rightsquigarrow$ ground terms built over a fixed signature $\mathcal{F} = \mathcal{VF} \cup \mathcal{PF}$

$\hookrightarrow$ pairing $\langle m_1, m_2 \rangle$

$\hookrightarrow$ encryption $\{m\}_k^s$, $\{m\}_k^a$ (symmetric /asymmetric)

$\hookrightarrow$ $\mathsf{pub}(a)$, $\mathsf{priv}(a)$, ...

Intruder $\rightsquigarrow$ inference system + (equational theory $\mathcal{E}$)

Attacker Model

Usually, the attacker power is a fixed theory:

- **Dolev-Yao intruder**: let u, v be terms and T be a finite set of terms.

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

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

- Recently, **new properties** have been added like the exclusive or $\oplus$, the modular exponentiation exp, ... [CLS03, CKRT03, ...]

Attacker Model

Usually, the attacker power is a fixed theory:

- **Dolev-Yao intruder**: let u, v be terms and T be a finite set of terms.

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

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

- Recently, **new properties** have been added like the exclusive or $\oplus$, the modular exponentiation exp, ... [CLS03, CKRT03, ...]

Here, we handle a **general class** of properties, represented by a class of equational theories (but not $\oplus$ or exp).

Protocol Specification (1)

Denning-Sacco Protocol (1981)

$$\begin{array}{rcll} A & \rightarrow & B : & A, \{\{K_{ab}\}^a_{\mathsf{priv}(A)}\}^a_{\mathsf{pub}(B)} \\ B & \rightarrow & A : & \{Secret\}^s_{K_{ab}} \end{array}$$

Protocol Specification (1)

Denning-Sacco Protocol (1981)

$$\begin{array}{rcll} A & \rightarrow & B: & A, \{\{K_{ab}\}^a_{\mathsf{priv}(A)}\}^a_{\mathsf{pub}(B)} \\ B & \rightarrow & A: & \{Secret\}^s_{K_{ab}} \end{array}$$

Usually, B's role: $x_A, \{\{x_{Kab}\}^a_{\mathsf{priv}(x_A)}\}^a_{\mathsf{pub}(b)} \quad \rightarrow \quad \{secret\}^s_{x_{Kab}}$

$\rightsquigarrow$ attack with 2 sessions between A/I and $I(A)/B$.

Protocol Specification (1)

Denning-Sacco Protocol (1981)

$$\begin{array}{rcll} A & \rightarrow & B: & A, \{\{K_{ab}\}^a_{\mathsf{priv}(A)}\}^a_{\mathsf{pub}(B)} \\ B & \rightarrow & A: & \{Secret\}^s_{K_{ab}} \end{array}$$

Usually, B's role: $x_A, \{\{x_{Kab}\}^a_{\mathsf{priv}(x_A)}\}^a_{\mathsf{pub}(b)} \quad \rightarrow \quad \{secret\}^s_{x_{Kab}}$
$\rightsquigarrow$ attack with 2 sessions between A/I and $I(A)/B$.

Here, B's role: $x \quad \rightarrow \quad \{secret\}^s_{da(da(\pi_2(x),\mathsf{pub}(b)^{-1}),\mathsf{pub}(\pi_1(x)))}$

Protocol Specification (1)

Denning-Sacco Protocol (1981)

$$\begin{array}{rcll} A & \to & B: & A, \{\{K_{ab}\}^a_{\mathsf{priv}(A)}\}^a_{\mathsf{pub}(B)} \\ B & \to & A: & \{Secret\}^s_{K_{ab}} \end{array}$$

Usually, B's role: $x_A, \{\{x_{Kab}\}^a_{\mathsf{priv}(x_A)}\}^a_{\mathsf{pub}(b)} \quad \to \quad \{secret\}^s_{x_{Kab}}$
$\rightsquigarrow$ attack with 2 sessions between A/I and $I(A)/B$.

Here, B's role: $x \quad \to \quad \{secret\}^s_{da(da(\pi_2(x),\mathsf{pub}(b)^{-1}),\mathsf{pub}(\pi_1(x)))} \qquad [\pi_1(x) = a]$

Protocol Specification (1)

Denning-Sacco Protocol (1981)

$$\begin{array}{rcll} A & \rightarrow & B: & A, \{\{K_{ab}\}^{a}_{\mathsf{priv}(A)}\}^{a}_{\mathsf{pub}(B)} \\ B & \rightarrow & A: & \{Secret\}^{s}_{K_{ab}} \end{array}$$

Usually, B's role: $x_A, \{\{x_{Kab}\}^{a}_{\mathsf{priv}(x_A)}\}^{a}_{\mathsf{pub}(b)} \quad \rightarrow \quad \{secret\}^{s}_{x_{Kab}}$

$\rightsquigarrow$ attack with 2 sessions between A/I and $I(A)/B$.

Here, B's role: $x \quad \rightarrow \quad \{secret\}^{s}_{da(da(\pi_2(x),\mathsf{pub}(b)^{-1}),\mathsf{pub}(\pi_1(x)))}$

$\rightsquigarrow$ attack with 1 session between $I(A)$ and B.

No ambiguities and **no implicit checks** allow us to found new attacks.

Protocol Specification (2)

Protocol [Tur03]

$$\begin{array}{rcl} A & \rightarrow & B: \quad \{M, B\}^s_K \\ B & \rightarrow & A: \quad B \\ A & \rightarrow & B: \quad K \\ B & \rightarrow & A: \quad M \end{array}$$

Protocol Specification (2)

Protocol [Tur03]

$$\begin{array}{rcl} A & \rightarrow & B : \quad \{M, B\}^s_K \\ B & \rightarrow & A : \quad B \\ A & \rightarrow & B : \quad K \\ B & \rightarrow & A : \quad M \end{array}$$

Usually, B's role can not be expressed.

Protocol Specification (2)

Protocol [Tur03]

$$\begin{array}{rcll} A & \rightarrow & B: & \{M, B\}^s_K \\ B & \rightarrow & A: & B \\ A & \rightarrow & B: & K \\ B & \rightarrow & A: & M \end{array}$$

Usually, B's role can not be expressed.

Here, B's role: $\begin{array}{rcll} x & \rightarrow & x_B & \\ y & \rightarrow & \pi_1(sd(x,y)) & \quad [\pi_2(sd(x,y)) = x_B] \end{array}$

Protocol Specification (2)

Protocol [Tur03]

$$\begin{array}{rcll} A & \rightarrow & B: & \{M, B\}^s_K \\ B & \rightarrow & A: & B \\ A & \rightarrow & B: & K \\ B & \rightarrow & A: & M \end{array}$$

Usually, B's role can not be expressed.

Here, B's role: $\begin{array}{rcll} x & \rightarrow & x_B & \\ y & \rightarrow & \pi_1(sd(x,y)) & \qquad [\pi_2(sd(x,y)) = x_B] \end{array}$

Explicit destructors and **equations** allow to address a broader class of protocol.

Insecurity Problems

Passive Attacker *intruder deduction problem*

Given a set of messages T and a message s, does there exist a proof of $T \vdash s$?

$\hookrightarrow$ PTIME–complete (in the Dolev-Yao model)

Active Attacker *insecurity problem for a finite number of sessions*

Given $\mathcal{P}$, s, $\mathcal{S}_0$ and T_0, does there exist a running sequence of protocol rules such that:

- at the end, the intruder's knowledge is T,
- there exists a proof of $T \vdash s$?

$\hookrightarrow$ NP–complete (in the Dolev-Yao model) [Rusinowitch&Turuani, 01]

Summary

Goal:

Decidability and complexity results for the insecurity problems for general equational theories:

- flexible intruder power: $sd(\{x\}_y, y) = x$
- flexible cryptographic properties: $\{\{x\}^s_y\}^s_y = x$

Summary

Goal:

Decidability and complexity results for the insecurity problems for general equational theories:

- flexible intruder power: $sd(\{x\}_y, y) = x$
- flexible cryptographic properties: $\{\{x\}^s_y\}^s_y = x$

Related Work:

- Many works for a fixed theory (ex: exclusive or theory): [Comon-Lundh&Shmatikov,03][Chevalier *et al.*,03].
- For general theories, very few results: [Comon&Treinen,03][Abadi&Cortier,04].
  $\hookrightarrow$ they only consider the intruder deduction problem
- Explicit destructors: [Millen,03][Lynch&Meadows,04].
- Equality tests: [Corin&Estalle,02].

Public-Collapsing Theories

We consider theories that can be represented by convergent public-collapsing rewriting systems, *i.e.* each rule $\ell \to r$ satisfies:

1. r is a variable or a ground term,
2. if $head(\ell) \in \mathcal{VF}$, then under each public symbol in ℓ, there is r.

Public-Collapsing Theories

We consider theories that can be represented by convergent public-collapsing rewriting systems, *i.e.* each rule $\ell \to r$ satisfies:

1. r is a variable or a ground term,
2. if $head(\ell) \in \mathcal{VF}$, then under each public symbol in ℓ, there is r.

Exemples:

Dolev-Yao theory: $sd(\{x\}^s_y, y) \to x, \;\; ad(\{x\}^a_y, y^{-1}) \to x, ad(\{x\}^a_{y^{-1}}, y) \to x$

$$\pi_i(\langle x_1, x_2\rangle) \to x_i \; (i = 1, 2), x^{-1^{-1}} \to x$$

Inverse-key theory: $\{sd(x, y)\}^a_y \;\to\; x, \{ad(x, y)\}^a_{y^{-1}} \to x, \{ad(x, y^{-1})\}^a_y \to x.$

Theory of involution: $\{\{x\}^a_y\}^a_{y^{-1}} \to x, \;\; \{\{x\}^a_{y^{-1}}\}^a_y \to x.$

Probabilistic encryption: $dec(enc(m, k, r), k) \to m$

Insecurity via Constraints Solving

Denning-Sacco Protocol (1981)

$$\begin{array}{lcll} A & \rightarrow & B: & A, \{\{K_{ab}\}^{a}_{\mathsf{priv}(A)}\}^{a}_{\mathsf{pub}(B)} \\ B & \rightarrow & A: & \{Secret\}^{s}_{K_{ab}} \end{array}$$

Insecurity via Constraints Solving

Denning-Sacco Protocol (1981)

$$
\begin{array}{lclll}
A & \rightarrow & B: & A, \{\{K_{ab}\}^a_{\mathsf{priv}(A)}\}^a_{\mathsf{pub}(B)} \\
B & \rightarrow & A: & \{Secret\}^s_{K_{ab}}
\end{array}
$$

Session $A = a; B = b; K_{ab} = k; Secret = s$

$$
\begin{array}{lllll}
(Role\ A) & \mathbf{a}: & & \rightarrow & \langle a, \{\{k\}^a_{\mathsf{pub}(a)^{-1}}\}^a_{\mathsf{pub}(b)}\rangle \\
(Role\ B) & \mathbf{b}: & x & \rightarrow & \{s\}^s_{da(da(\pi_2(x),\mathsf{pub}(b)^{-1}),\mathsf{pub}(\pi_1(x)))}
\end{array}
$$

Insecurity via Constraints Solving

Denning-Sacco Protocol (1981)

$$\begin{array}{lcll} A & \rightarrow & B: & A, \{\{K_{ab}\}^a_{\mathsf{priv}(A)}\}^a_{\mathsf{pub}(B)} \\ B & \rightarrow & A: & \{Secret\}^s_{K_{ab}} \end{array}$$

Session $A = a; B = b; K_{ab} = k; Secret = s$

$$\begin{array}{llccc} (Role\ A) & \mathbf{a}: & & \rightarrow & \langle a, \{\{k\}^a_{\mathsf{pub}(a)^{-1}}\}^a_{\mathsf{pub}(b)}\rangle \\ (Role\ B) & \mathbf{b}: & x & \rightarrow & \{s\}^s_{da(da(\pi_2(x),\mathsf{pub}(b)^{-1}),\mathsf{pub}(\pi_1(x)))} \end{array}$$

Constraint System $\mathcal{P}$

Insecurity via Constraints Solving

Denning-Sacco Protocol (1981)

$$\begin{array}{rcll} A & \rightarrow & B: & A, \{\{K_{ab}\}^a_{\mathsf{priv}(A)}\}^a_{\mathsf{pub}(B)} \\ B & \rightarrow & A: & \{Secret\}^s_{K_{ab}} \end{array}$$

Session $A = a; B = b; K_{ab} = k; Secret = s$

$$\begin{array}{llccl} (Role\ A) & \mathbf{a}: & & \rightarrow & \langle a, \{\{k\}^a_{\mathsf{pub}(a)^{-1}}\}^a_{\mathsf{pub}(b)}\rangle \\ (Role\ B) & \mathbf{b}: & x & \rightarrow & \{s\}^s_{da(da(\pi_2(x),\mathsf{pub}(b)^{-1}),\mathsf{pub}(\pi_1(x)))} \end{array}$$

Constraint System $\mathcal{P}$

$$T_1 = IK, \langle a, \{\{k\}^a_{\mathsf{pub}(a)^{-1}}\}^a_{\mathsf{pub}(b)}\rangle$$

Insecurity via Constraints Solving

Denning-Sacco Protocol (1981)

$$\begin{array}{lcll} A & \rightarrow & B: & A, \{\{K_{ab}\}^a_{\mathsf{priv}(A)}\}^a_{\mathsf{pub}(B)} \\ B & \rightarrow & A: & \{Secret\}^s_{K_{ab}} \end{array}$$

Session $A = a; B = b; K_{ab} = k; Secret = s$

$$\begin{array}{llccc} (Role\ A) & \mathbf{a}: & & \rightarrow & \langle a, \{\{k\}^a_{\mathsf{pub}(a)^{-1}}\}^a_{\mathsf{pub}(b)}\rangle \\ (Role\ B) & \mathbf{b}: & x & \rightarrow & \{s\}^s_{da(da(\pi_2(x),\mathsf{pub}(b)^{-1}),\mathsf{pub}(\pi_1(x)))} \end{array}$$

Constraint System $\mathcal{P}$

$$T_1 \Vdash x$$

$$T_1 = IK, \langle a, \{\{k\}^a_{\mathsf{pub}(a)^{-1}}\}^a_{\mathsf{pub}(b)}\rangle$$

$$T_2 = T_1, \{s\}^s_{da(da(\pi_2(x),\mathsf{pub}(b)^{-1}),\mathsf{pub}(\pi_1(x)))}$$

Insecurity via Constraints Solving

Denning-Sacco Protocol (1981)

$$\begin{array}{lcll} A & \rightarrow & B: & A, \{\{K_{ab}\}^a_{\mathsf{priv}(A)}\}^a_{\mathsf{pub}(B)} \\ B & \rightarrow & A: & \{Secret\}^s_{K_{ab}} \end{array}$$

Session $A = a; B = b; K_{ab} = k; Secret = s$

$$\begin{array}{lllll} (Role\ A) & \mathbf{a}: & & \rightarrow & \langle a, \{\{k\}^a_{\mathsf{pub}(a)^{-1}}\}^a_{\mathsf{pub}(b)}\rangle \\ (Role\ B) & \mathbf{b}: & x & \rightarrow & \{s\}^s_{da(da(\pi_2(x),\mathsf{pub}(b)^{-1}),\mathsf{pub}(\pi_1(x)))} \end{array}$$

Constraint System $\mathcal{P}$

$$T_1 \Vdash x \qquad\qquad T_1 = IK, \langle a, \{\{k\}^a_{\mathsf{pub}(a)^{-1}}\}^a_{\mathsf{pub}(b)}\rangle$$

$$T_2 \Vdash y \qquad y = s \qquad\qquad T_2 = T_1, \{s\}^s_{da(da(\pi_2(x),\mathsf{pub}(b)^{-1}),\mathsf{pub}(\pi_1(x)))}$$

Constraint Solving Problem

Input:

A finite set $\mathcal{P}$ of constraints:

- equations
- intruder contraints $s_1, \ldots, s_n \Vdash x$

Output:

Does there exist a $\mathcal{R}$-*solution*, *i.e.* a substitution θ such that:

- for each $t_1 = t_2 \in \mathcal{P}$, $t_1\theta =_{\mathcal{R}} t_2\theta$,
- for each $s_1, \ldots, s_n \Vdash x$ in $\mathcal{P}$, there exists a public context C such that $C[s_1\theta, \ldots, s_n\theta] =_{\mathcal{R}} x\theta$,

Constraint Solving System - $\mathcal{T}$

$$(\mathcal{P};\mathcal{C};\ \mathcal{S})$$

Constraint Solving System - $\mathcal{T}$

$$(\mathcal{P};\, \mathcal{C};\ \mathcal{S})$$

Narrowing
Unification Syntactic

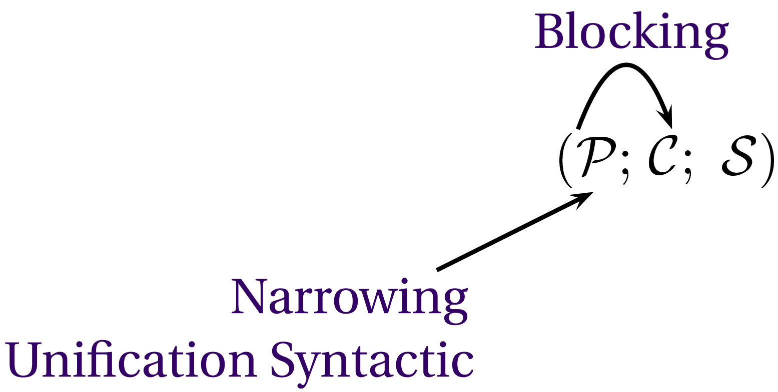
$$\frac{\mathcal{P} \cup \{e[u]\};\ \mathcal{C};\ \mathcal{S}}{\mathcal{P} \cup \{e[r]\};\ \mathcal{C}\eta;\ \mathcal{S}\eta \cup \eta}$$

Narrowing
e is an equation or an intruder constraint,
$l \to r$ is a fresh variant of a rule of $\mathcal{R}$,
$\eta = mgu(l\mathcal{S}, u\mathcal{S})$,
$root(l) = root(u)$.

$$\frac{\mathcal{P} \cup \{t_1 = t_2\};\ \mathcal{C};\ \mathcal{S}}{\mathcal{P};\ \mathcal{C}\eta;\ \mathcal{S}\eta \cup \eta}$$

Unification Syntactic
$\eta = mgu(t_1\mathcal{S}, t_2\mathcal{S})$.

Constraint Solving System - $\mathcal{T}$



$$\frac{\mathcal{P}\cup\{c\};\ \mathcal{C};\ \mathcal{S}}{\mathcal{P};\ \mathcal{C}\cup\{c\mathcal{S}\};\ \mathcal{S}}$$

Blocking
c is an intruder constraint.

Constraint Solving System - $\mathcal{T}$

Blocking

$$(\mathcal{P};\ \mathcal{C};\ \mathcal{S})$$

Narrowing
Unification Syntactic

Var. Elim.
Ground

$$\frac{\mathcal{P};\ \mathcal{C};\ \mathcal{S}}{\mathcal{P};\ \mathcal{C}[x \mapsto t];\ \mathcal{S}[x \mapsto t] \cup [x \mapsto t]}$$

Variable Elimination
$x \in vars(\mathcal{C}), t \in st(\mathcal{C}) \setminus vars(\mathcal{C})$,
there is no occurence of x in t.

$$\frac{\mathcal{P};\ \mathcal{C} \cup \{T \Vdash u\};\ \mathcal{S}}{\mathcal{P};\ \mathcal{C};\ \mathcal{S}}$$

Ground
if $T \vdash_R u$.

Constraint Solving System - $\mathcal{T}$

Blocking

$$(\mathcal{P};\, \mathcal{C};\ \mathcal{S})$$

Narrowing
Unification Syntactic

Var. Elim.
Ground

Solution

$$\frac{\mathcal{P};\ \mathcal{C};\ \mathcal{S}}{\mathcal{P};\ \mathcal{C}[x \mapsto t];\ \mathcal{S}[x \mapsto t] \cup [x \mapsto t]}$$

Variable Elimination
$x \in vars(\mathcal{C}), t \in st(\mathcal{C}) \setminus vars(\mathcal{C})$,
there is no occurence of x in t.

$$\frac{\mathcal{P};\ \mathcal{C} \cup \{T \Vdash u\};\ \mathcal{S}}{\mathcal{P};\ \mathcal{C};\ \mathcal{S}}$$

Ground
if $T \vdash_R u$.

Denning-Sacco Example

$$\begin{array}{ll}
\mathcal{P}: & IK, \langle a, \{\{k\}^a_{\mathsf{pub}(a)^{-1}}\}^a_{\mathsf{pub}(b)}\rangle \Vdash x; \\
 & IK, \langle a, \{\{k\}^a_{\mathsf{pub}(a)^{-1}}\}^a_{\mathsf{pub}(b)}\rangle, \{s\}^s_{da(da(\pi_2(x), \mathsf{pub}(b)^{-1}), \mathsf{pub}(\pi_1(x)))} \Vdash y; \\
 & y = s \\
\mathcal{C}: & \emptyset \\
\mathcal{S}: & \emptyset
\end{array}$$

Denning-Sacco Example

$$
\begin{array}{ll}
\mathcal{P}: & IK, \langle a, \{\{k\}^a_{\mathsf{pub}(a)^{-1}}\}^a_{\mathsf{pub}(b)}\rangle \Vdash x; \\
 & IK, \langle a, \{\{k\}^a_{\mathsf{pub}(a)^{-1}}\}^a_{\mathsf{pub}(b)}\rangle, \{s\}^s_{da(da(\pi_2(x),\mathsf{pub}(b)^{-1}),\mathsf{pub}(\pi_1(x)))} \Vdash y; \\
 & y = s \\
\mathcal{C}: & \emptyset \\
\mathcal{S}: & \emptyset
\end{array}
$$

Step 1: Unification Syntactic

$$\frac{\mathcal{P} \cup \{t_1 = t_2\};\ \mathcal{C};\ \mathcal{S}}{\mathcal{P};\ \mathcal{C}\eta;\ \mathcal{S}\eta \cup \eta} \qquad \eta = mgu(t_1\mathcal{S}, t_2\mathcal{S})$$

Denning-Sacco Example

$\mathcal{P}$: $IK, \langle a, \{\{k\}^a_{\mathsf{pub}(a)^{-1}}\}^a_{\mathsf{pub}(b)}\rangle \Vdash x;$

$IK, \langle a, \{\{k\}^a_{\mathsf{pub}(a)^{-1}}\}^a_{\mathsf{pub}(b)}\rangle, \{s\}^s_{da(da(\pi_2(x),\mathsf{pub}(b)^{-1}),\mathsf{pub}(\pi_1(x)))} \Vdash y;$

$\mathcal{C}$: $\emptyset$

$\mathcal{S}$: $y = s$

Step 1: Unification Syntactic

$$\frac{\mathcal{P} \cup \{t_1 = t_2\};\ \mathcal{C};\ \mathcal{S}}{\mathcal{P};\ \mathcal{C}\eta;\ \mathcal{S}\eta \cup \eta} \qquad \eta = mgu(t_1\mathcal{S}, t_2\mathcal{S})$$

Denning-Sacco Example

$\mathcal{P}$: $IK, \langle a, \{\{k\}^a_{\mathsf{pub}(a)^{-1}}\}^a_{\mathsf{pub}(b)}\rangle \Vdash x;$

$IK, \langle a, \{\{k\}^a_{\mathsf{pub}(a)^{-1}}\}^a_{\mathsf{pub}(b)}\rangle, \{s\}^s_{da(da(\pi_2(x),\mathsf{pub}(b)^{-1}),\mathsf{pub}(\pi_1(x)))} \Vdash y;$

$\mathcal{C}$: $\emptyset$

$\mathcal{S}$: $y = s$

Step 2: Narrowing with $\pi_2(\langle x_1, x_2\rangle) \rightarrow x_2$

$$\frac{\mathcal{P} \cup \{e[u]\};\ \mathcal{C};\ \mathcal{S}}{\mathcal{P} \cup \{e[r]\};\ \mathcal{C}\eta;\ \mathcal{S}\eta \cup \eta}$$

$l \rightarrow r$ is a fresh variant of a rule of $\mathcal{R}$,
$\eta = mgu(l\mathcal{S}, u\mathcal{S})$,
$root(l) = root(u)$.

Denning-Sacco Example

$\mathcal{P}$: $IK, \langle a, \{\{k\}^a_{\mathsf{pub}(a)^{-1}}\}^a_{\mathsf{pub}(b)}\rangle \Vdash x;$

$IK, \langle a, \{\{k\}^a_{\mathsf{pub}(a)^{-1}}\}^a_{\mathsf{pub}(b)}\rangle, \{s\}^s_{da(da(x_2,\mathsf{pub}(b)^{-1}),\mathsf{pub}(\pi_1(x)))} \Vdash y;$

$\mathcal{C}$: $\emptyset$

$\mathcal{S}$: $y = s,\ x = \langle x_1, x_2\rangle$

Step 2: Narrowing with $\pi_2(\langle x_1, x_2\rangle) \rightarrow x_2$

$$\frac{\mathcal{P} \cup \{e[u]\};\ \mathcal{C};\ \mathcal{S}}{\mathcal{P} \cup \{e[r]\};\ \mathcal{C}\eta;\ \mathcal{S}\eta \cup \eta}$$

$l \rightarrow r$ is a fresh variant of a rule of $\mathcal{R}$,
$\eta = mgu(l\mathcal{S}, u\mathcal{S})$,
$root(l) = root(u)$.

Denning-Sacco Example

$\mathcal{P}$: $IK, \langle a, \{\{k\}^a_{\mathsf{pub}(a)^{-1}}\}^a_{\mathsf{pub}(b)}\rangle \Vdash x;$
$IK, \langle a, \{\{k\}^a_{\mathsf{pub}(a)^{-1}}\}^a_{\mathsf{pub}(b)}\rangle, \{s\}^s_{da(da(x_2,\mathsf{pub}(b)^{-1}),\mathsf{pub}(\pi_1(x)))} \Vdash y;$

$\mathcal{C}$: $\emptyset$

$\mathcal{S}$: $y = s,\ x = \langle x_1, x_2\rangle$

Step 2: Narrowing with $\pi_2(\langle x_1, x_2\rangle) \to x_2$

$$\frac{\mathcal{P} \cup \{e[u]\};\ \mathcal{C};\ \mathcal{S}}{\mathcal{P} \cup \{e[r]\};\ \mathcal{C}\eta;\ \mathcal{S}\eta \cup \eta}$$

$l \to r$ is a fresh variant of a rule of $\mathcal{R}$,
$\eta = mgu(l\mathcal{S}, u\mathcal{S})$,
$root(l) = root(u)$.

. . . .

Denning-Sacco Example

Initial System

$\mathcal{P}$: $IK, \langle a, \{\{k\}^a_{\mathsf{pub}(a)^{-1}}\}^a_{\mathsf{pub}(b)}\rangle \Vdash x;$

$IK, \langle a, \{\{k\}^a_{\mathsf{pub}(a)^{-1}}\}^a_{\mathsf{pub}(b)}\rangle, \{s\}^s_{da(da(\pi_2(x),\mathsf{pub}(b)^{-1}),\mathsf{pub}(\pi_1(x)))} \Vdash y;$

$y = s$

$\mathcal{C}$: $\emptyset$

$\mathcal{S}$: $\emptyset$

Final System

$\mathcal{P}$: $\emptyset$

$\mathcal{C}$: $\emptyset$

$\mathcal{S}$: $y = s, x = \langle a, \{0\}_{\mathsf{pub}(b)}\rangle, \cdots$

Results

Given a convergent and public-collapsing system, we have the following results:

Termination:
The application of the inference rules terminates and the depth, the branching degree and the size of the node of the derivation tree are polynomially bounded.

Soundness:
The reduction rules do not introduce new solution.

Completeness:
If the initial constraint set is satisfiable then among all the simple constraints sets produced by $\mathcal{T}$, there is at least one satisfiable set.

Corollary:
The insecurity problem for a bounded number of sessions is NP-complete.

Conclusion & Future Works

Conclusion

Decidability and complexity results for the insecurity problems (passive and active attacker) for a class of equational theories.

Conclusion & Future Works

Conclusion

Decidability and complexity results for the insecurity problems (passive and active attacker) for a class of equational theories.

Future Works

- Extension of the decision procedure to deal with an AC symbol:
  $\rightsquigarrow$ exclusive or theory

$$\begin{aligned} x \oplus x &\rightarrow 0 \\ x \oplus 0 &\rightarrow x \\ x \oplus (x \oplus y) &\rightarrow y \end{aligned}$$

- Extension of the decision procedure to deal non equivalence static constraints:
  $\rightsquigarrow$ dictionary attacks