Deciding knowledge under some e-voting theories

Mouhebeddine Berrima
Joint work with Narjes Ben Rajeb and Véronique Cortier

LIP2-FST, Tunis

Workshop VETO, June 2009

1. Introduction
2. Attacker Knowledge
3. The two e-voting theories
4. Decidability results
5. Conclusion

E-voting protocols

- Motivation:
  - Importance of voting to the society.
  - Limitations of manual voting (scalability, efficiency, cost, accuracy).
  - Move towards automated (electronic) means.
- Advantages:
  - Convenient and inexpensive.
  - Efficient facilities for tallying votes.
  - Must upheld the security properties of the classical paper vote.

Observations

Drawbacks:

- Difficulties to design.
- Such protocols are extremely error-pone.
- Risk of undetectable fraud.
- Definition of security properties are often insufficiently precise.

$\longrightarrow$ Needs to formal verification for developing provably correct systems.

Framework: Applied pi calculus

- Based on pi-calculus [Milner et al 92].
- Adds equational theory for terms.
- Transmitted messages are represented by terms.
- Cryptographic primitives are represented by function symbols.
- Algebraic properties are represented by equations.

Formalization of properties:

- Reachability-based.
- Equivalence-based.

Example: Privacy, Receipt-freeness, coercion-resistance [Delaune,Kremer,Ryan 06]

Applied pi-calculus on an example

Example: Theory E_{enc} of pairs and asymmetric encryption

Operations: pair(-,-), fst(-), snd(-), pk(-), sk(-), dec(-,-), enc(-,-)

Equations:

- fst(pair(x,y)) = x
- snd(pair(x,y)) = y
- dec(enc(x,pk(y)),sk(y)) = x

Terms: $pk(ska)$, $enc(pair(A, N_A), pk(ska))$, etc...

Notion of frame

The set of circulated messages is organized into a frame $\nu\widetilde{n}\sigma$, where

- $\nu\widetilde{n}$ is a finite set of names and,
- $\sigma \stackrel{\text{def}}{=} \{M_1/x_1, \ldots, M_k/x_k\}$ with $dom(\sigma) = \{x_1, \ldots, x_k\}$ and M_i are closed terms.

Motivation

The are two standard notions for expressing about knowledge of an attacker:

- Deduction: states whether an attacker can learn the value of a secret.
- Static equivalence: states whether an attacker can notice some difference between protocol runs with different values of the secret.

Deduction

Deduction problem

Given a set of messages, i.e frame ϕ, and a secret s, can an attacker compute s from ϕ ?

Deduction system:

$$\frac{}{\nu\tilde{n}.\sigma \vdash M} \text{ if } \exists x \in dom(\sigma) \text{ s.t } x\sigma = M \qquad \frac{}{\nu\tilde{n}.\sigma \vdash s} \text{ if } s \notin \tilde{n}$$

$$\frac{\phi \vdash M_1 \quad \phi \vdash M_k}{\phi \vdash f(M_1, \ldots, M_k)} \text{ if } f \in \Sigma \qquad \frac{\phi \vdash M \quad M =_E M'}{\phi \vdash M'}$$

Deduction

Lemma (Characterization of deduction) [Abadi, Cortier 06]

$\phi \vdash_E M$ if and only if there exists a term ζ such that $fn(\zeta) \cap \widetilde{n} = \emptyset$ and $\zeta\sigma =_E M$.

$\rightarrow$ Such a term ζ is called a recipe of the term M.

Example

Let $\phi = \nu k, s.\{enc(s,k)/x, k/y\}$. Then $\phi \vdash k$ and $\phi \vdash s$.

- $\zeta_k = y$ is a possible recipe recipe for k,
- $\zeta_s = dec(x,y)$ is a possible recipe for s.

Deduction is not always sufficient

Example

Let $\Sigma_0 = \{v_1, v_2\}$ (represents initial knowledge of an attacker), and $\phi = \nu.s\{enc(v_1, s)/x\}$.
The question $\phi \vdash v_1$ is not suitable.

$\rightarrow$ But we can ask if $\nu.s\{enc(v_1, s)/x\}$ is indistinguishable from $\nu.s\{enc(v_2, s)/x\}$.

Static equivalence $\approx_E$

- Introduced in the context of applied pi-calculus [Abadi and Fournet '2001].
- Focuses on the static aspect of protocol (i.e exchanged messages between participants).
- Intuitively: we say that two frames are statically equivalent if they satisfy the same equalities (tests).

Definition

$\phi \approx_E \psi$, when $dom(\phi) = dom(\psi)$ and when, for all terms M and N, we have $(M =_E N)\phi$ iff $(M =_E N)\psi$.

Example

Consider again the theory E_{enc}.
We have $\nu k.\{enc(s,k)/x\} \approx_{E_{enc}} \nu k.\{enc(s',k)/x\}$.

Existing results

Deduction: the problem of deduction is generally decidable due to a property of locality [McAllester 93].

- Intruder of Dolev-Yao: [Amadio, lugiez 00] [Rusinowitch, Turuani 01]
- Exclusive or: [Common-Lundh, Shmatikov 03]
- Exclusive or with distributive encryption: [Lafourcade, Lugiez, Treinen 05]
- Exclusive or with homomorphism: [Delaune 06]
- Subterms and "locally stable" theories: [Abadi, Cortier 06]

Static equivalence: is more complex than deduction.

- Subterms and "locally stable" theories: [Abadi, Cortier 06]

Our goal

$\longrightarrow$ Develop an algorithm for deciding about deduction and static equivalence under some e-voting theories:

- Lee *et al* theory
- Okamoto theory.

Protocol due to Lee *et al*

Relies on two cryptographic primitives.

- Re-encryption: allows to change the random coins (used in randomized encryption), without changing or revealing the plaintext.
- Designated verifier proofs (DVP): allows to prove that the two ciphertexts contain indeed the same plaintext.

Equational theory E_{Lee}

Modeling taken from [Delaune, Kremer, Ryan 09].

$$
\begin{aligned}
&(1)\ getpk(host(x)) = x\\
&(2)\ checksign(sign(x, y), pk(y)) = x\\
&(3)\ decrypt(penc(x, pk(y), z), y) = x\\
&(4)\ rencrypt(penc(x, pk(y), z), w) = penc(x, pk(y), f_0(z, w))\\
&(5)\ checkdvp(dvp(x, rencrypt(x, y), y, pk(z)), x, rencrypt(x, y), pk(z)) = ok\\
&(6)\ checkdvp(dvp(x, y, z, w), x, y, pk(w)) = ok
\end{aligned}
$$

Protocol due to Okamoto

Based on a trap-door bit commitment and blind signatures.

- A trap-door bit commitment: allows the agent who has performed the commitment to open it in many ways.
- Blind signature: allows a person to get a message signed by another party without revealing any information about the message to the other party.

Equational theory E_{Oka}

Modeling taken from [Delaune, Kremer, Ryan 09].

(1) $getpk(host(x)) = x$
(2) $checksign(sign(x, y), pk(y)) = x$
(3) $unblind(blind(x, y), y) = x$
(4) $unblind(sign(blind(x, y), z), y) = sign(x, y)$
(5) $open(tdcommit(x, y, z), y) = x$
(6) $tdcommit(x, f_1(y, z, w, x), w) \ = tdcommit(y, z, w)$

Modular approach for E_{Oka}

For this theory we proceed a modular approach.

- $E_{Oka} = E^1_{Oka} \uplus E^2_{Oka}$, where $E^1_{Oka} = \{(1), (2), (3), (4)\}$ and $E^2_{Oka} = \{(5), (6)\}$.
- We use the result of [Arnaud, Cortier, Delaune 07] for combining decidability for both deduction and static equivalence.
- E^1_{Oka} corresponds to the blind signatures for which both deduction and static equivalence have been proved decidable in polynomial time [Abadi, Cortier 06].

$\longrightarrow$ It remains to prove the decidability for E^2_{Oka}.
We simply write E_{Oka} instead of E^2_{Oka}.

Our approach for $\vdash_E$

Use the locality technique.

Principle of locality: the proof of $\phi \vdash_E M$ is local if it involves only terms in the set of subterms of $\phi \cup \{M\}$ (w.r.t an appropriate notion of subterms).

$\rightarrow$ We need to define an appropriate notion of subterms, that we use for proving the locality property.

Our notion of subterms St_{Lee}

Definition

St_{Lee} is defined as follows:

- $St_{Lee}(u) = u$ when u is a variable or a name,
- $St_{Lee}(penc(M_1, pk(M_2), f_0(M_3, M_4))) = \{penc(M_1, pk(M_2), f_0(M_3, M_4))\} \cup St_{Lee}(M_1) \cup St_{Lee}(pk(M_2)) \cup St_{Lee}(f_0(M_3, M_4)) \cup \{penc(M_1, pk(M_2), M_3)\}$,
- $St_{Lee}(sign(M_1, M_2)) = \{sign(M_1, M_2)\} \cup St_{Lee}(M_1) \cup St_{Lee}(pk(M_2))$,
- $St_{Lee}(f(M_1, \ldots, M_k)) = \{f(M_1, \ldots, M_k)\} \cup \bigcup_{i=1}^{k} St_{Lee}(M_i)$ otherwise

Our notion of subterms St_{Oka}

Definition

St_{Oka} is defined as follows:

- $St_{Oka}(u) = u$ when u is a variable or a name
- $St_{Oka}(f_1(M_1, M_2, M_3, M_4)) = \{f_1(M_1, M_2, M_3, M_4)\} \cup \bigcup_{i=1}^{4} St_{Oka}(M_i)$ $\cup \{tdcommit(M_1, M_2, M_3)\}$
- $St_{Oka}(f(M_1, \ldots, M_k)) = \{f(M_1, \ldots, M_k)\} \cup \bigcup_{i=1}^{k} St_{Oka}(M_i)$ otherwise

Locality result

Lemma

If $\phi \vdash_E M$ then there exists a term ζ_M, called local recipe, such that:

- $fn(\zeta_M) \cap \widetilde{n} = \emptyset$ *and* $\zeta_M\sigma =_E M$.
- *for all* $\zeta' \in St_E(\zeta_M)$, *for all* $\zeta'' \in St_E(\zeta')$ *we have* $\zeta''\sigma\downarrow \in St_E(\phi, \zeta'\sigma\downarrow) \cup \{\Sigma_0\}$. *Moreover, if* $\zeta'' = f(\zeta_1, \ldots, \zeta_k)$ *and* $f(\zeta_1\sigma\downarrow, \ldots, \zeta_k\sigma\downarrow) \xrightarrow{h} \zeta''\sigma\downarrow$ *by applying a subterm rule then we have* $\zeta''\sigma\downarrow \in St_E(\phi) \cup \{\Sigma_0\}$.

Proof.

First condition: from lemma of characterization of deduction.
Second condition: by induction on the size of ζ_M. □

Our algorithm for $\vdash_E$

Input: $\phi = \nu\tilde{n}.\{M_1/x_1, \ldots, M_k/x_k\}, M$
Output: true/false
$S := St_E(\phi, M) \cup \Sigma_0 \cup fn(\phi)$
1 $T := \{(M_i, x_i) \mid i \in \{1..k\}\} \cup \{(n, n) \mid n \in \Sigma_0 \cup fn(\phi)\}$
$T' := \emptyset$
while $T \neq T'$ **do**
  $T' := T$
  for *all* $(t_1, \zeta_1) \ldots, (t_n, \zeta_n) \in T'$ *and for every function symbol* f **do**
2   **if** $f(t_1, \ldots, t_n) \xrightarrow{h} t$ *and* $t \in S$ *and* $t \notin \{t \mid (t, \zeta_t) \in T\}$ **then**
      $(t, f(\zeta_1, \ldots, \zeta_n)) \in T$
    end
3   **if** $t = f(t_1, \ldots, t_n) \in S$ *and* $t \notin \{t \mid (t, \zeta_t) \in T\}$ **then**
      $(t, f(\zeta_1, \ldots, \zeta_n)) \in T$
    end
  end
end

If $(M, \zeta_M) \in T$ then return *true* else return *false*.

Main result for $\vdash_E$

Proposition

Let $\phi = \nu\tilde{n}\{M_1/x_1, \ldots, M_k/x_k\}$ be a frame, M be a term in normal form and T be the set computed by the Algorithm.

1. $\forall M' \in St_E(\phi, M)$ we have $\phi \vdash_E M'$ iff there exists a pair $(M', \zeta_{M'}) \in T$.
2. Moreover, the recipe $\zeta_{M'}$ computed by the algorithm is minimal and local.

Corollary

For every frame ϕ in normal form and for every closed term M in normal form, $\phi \vdash_E M$ is decidable in polynomial time.

Our approach for $\approx_E$ I

$\rightarrow$ Based on the result of [Abadi, Cortier 06].
Given a convergent rewriting system $\mathcal{R}_E$:

- Step 1: saturating frame
  We compute the set $sat_E(\phi)$ of deducible subterms of ϕ.
- Step 2: adding critical terms
  We compute the set $I_E(\phi)$ of deducible terms of ϕ satisfying some conditions.
- Step 3: introducing a finite set of equalities
  We compute a finite set $Eq_E(\phi)$ of equalities constructs by applying "small contexts" on the local recipes of terms in $sat_E(\phi) \cup I_E(\phi)$.

Our approach for $\approx_E$ II

- Step 1: saturating frame

$$sat_E(\phi) = \{M \mid \phi \vdash_E M \text{ and } M \in St_E(\phi) \cup \Sigma_0 \cup fn(\phi)\}$$

- Step 2: adding critical terms

$$I_{Lee}(\phi) = \{M \mid \phi \vdash_E M \text{ and } M \in M \in St_{Lee}(penc(M_1, M_2, M_3))\}$$

with $M_1, M_2, M_3 \in sat_{Lee}(\phi)$.

$$I_{Oka}(\phi) = \emptyset$$

Our approach for $\approx_E$ III

- Step 3: introducing a finite set of equalities
  Let $\mathcal{L}(\phi)$ be the set of local recipes that corresponds to the terms of $sat_E(\phi) \cup I_E(\phi)$.

Definition

The set $Eq_E(\phi)$ is the set of equalities

$$C_1[\zeta_{M_1}, \ldots, \zeta_{M_k}] = C_2[\zeta_{M'_1}, \ldots, \zeta_{M'_l}]$$

such that $(C_1[\zeta_{M_1}, \ldots, \zeta_{M_k}] =_E C_2[\zeta_{M'_1}, \ldots, \zeta_{M'_l}])\phi$, $|C_1|, |C_2| \leq c_E$, $M_i, M'_i \in sat_E(\phi) \cup I_E(\phi)$ and $\zeta_{M_i}, \zeta_{M'_i} \in \mathcal{L}(\phi) \cup dom(\sigma)$.

Main result for $\approx_E$

We show that it is actually sufficient to check for the set of equalities $Eq_E(\phi)$.

Proposition

We have $\phi \approx_E \phi'$ if and only if $\phi \models Eq_E(\phi')$ and $\phi' \models Eq_E(\phi)$.

Key lemmas

Lemma 1

Let $\phi = \nu\tilde{n}\sigma$ be a frame in normal form, ζ_M and ζ_N be local recipes of some term T, *i.e.* $\zeta_M\sigma\downarrow = \zeta_N\sigma\downarrow = T$. For every frame ϕ' such that $\phi' \models Eq_E(\phi)$, we have $(\zeta_M =_E \zeta_N)\phi'$.

Lemma 2

Let $\phi = \nu\tilde{n}\sigma$ be a frame in normal form, M be a deducible term in normal form and ζ_M a recipe of M. Then there exists a local recipe of M, denoted by $\widehat{\zeta_M}$, such that for every frame ϕ' such that $\phi' \models Eq_E(\phi)$, we have $(\zeta_M =_E \widehat{\zeta_M})\phi'$.

Conclusion

- Deduction is decidable in polynomial time for Lee *et al* and Okamoto theories.
- Static equivalence is decidable in polynomial time for Lee *et al* and Okamoto theories.

Further work:

- Generalize the construction of the set of critical terms.
- Design a decision procedure in the active case.