

Formal Computational Unlinkability Proofs of RFID Protocols

Hubert Comon, Adrien Koutsos

January 7, 2019

Motivations

Security protocols

Distributed programs which aim at providing some security properties.

The KCL⁺ RFID protocol

$$R : n_R \xleftarrow{\$}$$

$$T_A : n_T \xleftarrow{\$}$$

$$1 : R \longrightarrow T_A : n_R$$

$$2 : T_A \longrightarrow R : \langle A \oplus H(n_T, k_A), n_T \oplus H(n_R, k_A) \rangle$$

Security Properties

- Security protocols are short: few lines of specification.
 - Security properties are complex: the attacker controls the network.
- ⇒ Need to use formal methods.

The problem

Given a protocol P and a class of attackers \mathcal{C} , show that:

$$\forall \mathcal{A} \in \mathcal{C} \quad (P \mid \mathcal{A}) \text{ satisfies } \phi_{\text{sec}}$$

Attacker Models

Models

	Dolev Yao	Computational
Messages representation:	Abstract terms	Bitstrings
Adversaries capabilities:	Explicitly specified through a TRS	Polynomial Time Probabilistic TMs

Advantages and drawbacks

Dolev Yao	Computational
Good proof automation	Few proof automation
Not a realistic model	Strong security guarantees But with implicit hypothesis

The Complete Symbolic Attacker Model

The Complete Symbolic Attacker Model [Bana,Comon 2012]

- A first-order logic.
- Axioms specifying what the adversary *cannot* do.
- Security of a protocol expressed as a goal formula.

Advantages

- All hypotheses appear explicitly in the axioms.
- Possible proof automation.
- Security implies computational security.

Two logics

- Reachability properties: [Scerri 2016]
- We focus on the **indistinguishability** logic.

- 1 Motivations
- 2 The Complete Symbolic Attacker Model
 - Syntax
 - Computational semantics
- 3 Axioms
 - Structural Axioms
 - Pseudo Random Function
- 4 Case Studies: Security of Two RFID Protocols
- 5 Conclusion

Syntax

Term algebra

- Control flow function symbols:

$\text{if_then_else_}, \text{EQ}(_; _), \text{true}, \text{false}$

- Protocol function symbols:

$\{\langle _, _ \rangle, \pi_1(_), \pi_2(_), \text{H}(_, _), _ \oplus _ \}$

- Adversarial function symbols \mathcal{G} .
- A set of names \mathcal{N} .
- A set of variables \mathcal{X} .

Formulas

$\phi ::= \vec{u} \sim \vec{v} \mid \phi \wedge \phi \mid \neg \phi \mid \perp \mid \forall x. \phi$

where \vec{u}, \vec{v} are sequences of terms

Example

The KCL⁺ protocol

1 : $R \longrightarrow T_A$: n_R

2 : $T_A \longrightarrow R$: $\langle A \oplus H(n_T, k_A), n_T \oplus H(n_R, k_A) \rangle$

Example

- **Terms:**

$$m_A = \langle A \oplus H(n_T, k_A), n_T \oplus H(g(n_R), k_A) \rangle$$

- **Formula:**

$$n_R, m_A \sim n_R, m_B$$

Computational Semantics of Terms

Computational model \mathcal{M}_c : term interpretation

- $f/n \in \Sigma \cup \mathcal{G}$ interpreted as a polynomial time Turing Machine.
- $\mathbf{n} \in \mathcal{N}$ interpreted as a random sampling
- $\{\text{if_then_else_}, \text{EQ}(_; _), \text{true}, \text{false}\}$ interpretations are the expected ones.

Computational model \mathcal{M}_c : predicate interpretation

- \sim interpreted as computational indistinguishability.

Example

For every computational model \mathcal{M}_c we have:

$$\mathcal{M}_c \models A \oplus \mathbf{n}_1 \sim B \oplus \mathbf{n}_2$$

Proof Technique

Goal

- Ground formula $\vec{u} \sim \vec{v}$ expressing the security of the protocol.
- The formula is automatically obtained by folding the executions of the protocol [Bana,Comon 14].

Axioms \mathbb{A} : what the adversary *cannot* do

- Computationally valid structural axioms.
- Implementation and cryptographic axioms.

Soundness Theorem [Bana,Comon 14]

If $\mathbb{A} \wedge \vec{u} \not\sim \vec{v}$ is unsatisfiable then the protocol is computationally secure.
(under some cryptographic/implementation assumptions)

- 1 Motivations
- 2 The Complete Symbolic Attacker Model
 - Syntax
 - Computational semantics
- 3 Axioms
 - Structural Axioms
 - Pseudo Random Function
- 4 Case Studies: Security of Two RFID Protocols
- 5 Conclusion

Structural Axioms : Examples

Relation axioms

$$\frac{}{x \sim x} \text{ Refl} \quad \frac{x \sim y}{y \sim x} \text{ Sym} \quad \frac{x \sim y \quad y \sim z}{x \sim z} \text{ Trans}$$

\sim is not a congruence!

Counter-Example: $n \sim n$ and $n \sim n'$, but $n, n \not\sim n, n'$.

Function Application

If you cannot distinguish the arguments, you cannot distinguish the images.

$$\frac{x_1, \dots, x_n \sim y_1, \dots, y_n}{f(x_1, \dots, x_n) \sim f(y_1, \dots, y_n)} \text{ FunApp}$$

Pseudo Random Function

Definition

H is a *Pseudo Random Function* if for every PPTM adversary \mathcal{A} :

$$|\Pr(k : \mathcal{A}^{\mathcal{O}_{H(\cdot, k)}}(1^\eta) = 1) - \Pr(g : \mathcal{A}^{\mathcal{O}_{g(\cdot)}}(1^\eta) = 1)|$$

is negligible in η , where:

- k is drawn uniformly in $\{0, 1\}^\eta$.
- g is drawn uniformly in the set of all functions from $\{0, 1\}^*$ to $\{0, 1\}^\eta$.

Translation in the Logic

Axiom for one hash

$$H(s, k) \sim n$$

Where k does not appear in s .

Bad axiom for two hashes

If s and t are *syntactically* distinct,

$$H(s, k), H(t, k) \sim H(s, k), n$$

Counter-Example: $s = g(A)$, $t = g(B)$ and we interpret the attacker function g as a constant function.

Translation in the Logic

The PRF_2 Axioms

$$\begin{aligned} & H(s, k), \text{ if } EQ(t; s) \text{ then } 0 \text{ else } H(t, k) \\ \sim & H(s, k), \text{ if } EQ(t; s) \text{ then } 0 \text{ else } n \end{aligned}$$

where:

- H and k only occur in (s, t) as $H(s, k)$.
- n does not occur in (s, t) .

Theorem : Soundness

The $(PRF_n)_{n \in \mathbb{N}}$ axioms are valid in every computational model \mathcal{M}_c such that the interpretation of H satisfies the PRF assumption.

- 1 Motivations
- 2 The Complete Symbolic Attacker Model
 - Syntax
 - Computational semantics
- 3 Axioms
 - Structural Axioms
 - Pseudo Random Function
- 4 Case Studies: Security of Two RFID Protocols
- 5 Conclusion

Security Property

KCL⁺ Protocol: Unlinkability for 2 rounds (A, A vs. A, B)

$$\phi_2^{\text{sec}} \equiv n_R, m_1, n'_R, m_2^A \sim n_R, m_1, n'_R, m_2^B$$

where m_1, m_2^A are the terms:

$$m_1 = \langle A \oplus H(n_T, k_A), n_T \oplus H(g(n_R), k_A) \rangle$$

$$m_2^X = \langle X \oplus H(n'_T, k_X), n'_T \oplus H(g'(n_R, m_1, n'_R), k_X) \rangle$$

Unlinkability for n Rounds.

- A formula ϕ_n^{sec} expressing unlinkability for n rounds of a protocol can be automatically computed from the specification.
- If $\mathbb{A} \wedge \neg \phi_n^{\text{sec}}$ is unsatisfiable then the protocol satisfies Strong Privacy [Juels, Weis 2009] for n rounds.

Case Studies

Theorem: Unlinkability of KCL^+

Assuming PRF for the keyed hash function, the KCL^+ protocol verifies Strong Privacy for two agents and any number of rounds.

Theorem: Unlinkability of LAK^+

Assuming PRF for the keyed hash function, the LAK^+ protocol verifies Strong Privacy for two agents and two rounds.

- 1 Motivations
- 2 The Complete Symbolic Attacker Model
 - Syntax
 - Computational semantics
- 3 Axioms
 - Structural Axioms
 - Pseudo Random Function
- 4 Case Studies: Security of Two RFID Protocols
- 5 Conclusion

Conclusion

Contributions

- Designed and proved axioms for PRF, CR, XOR and PRNG.
- Formally expressed Strong Privacy [Juels, Weis 2009] in our model.
- Proved Strong Privacy of KCL^+ for an arbitrary number of rounds.
- Proved Strong Privacy LAK⁺ protocol for two rounds.
- Showed attacks against KCL^+ and LAK⁺ for weaker assumptions.

Future Work

- More examples, with more primitives (RFID or not).
- Automation through decidability of (a fragment of) the logic.
- Interactive/automatic prover.

Thanks for your attention