ACI ROSSIGNOL

Denis LUGIEZ

www.cmi.univ-mrs.fr/~lugiez/aci-rossignol.html

- LIF (UMR 6166 University de Provence)
- LIX (INRIA FUTURS)
- LSV (UMR 8643 ENS Cachan)
- VERIMAG (UMR 5104)

Verification of Cryptographic Protocols:

No mathematical cryptography,

hardware aspect,

quantum computation,....

But find logical flaws in the design of cryptographic protocols.

Needham-Shroeder authentication protocol

$$
\begin{aligned}
A &\Rightarrow B : \{N_A\}_{K_B} \\
B &\Rightarrow A : \{N_A, N_B\}_{K_A} \\
A &\Rightarrow B : \{N_B\}_{K_B}
\end{aligned}
$$

Needham-Shroeder authentication protocol

$$
\begin{aligned}
A &\Rightarrow B : \{N_A\}_{K_B} \\
B &\Rightarrow A : \{N_A, N_B\}_{K_A} \\
A &\Rightarrow B : \{N_B\}_{K_B}
\end{aligned}
$$

Error found 17 years after the publication.

Critical programs for *e-society*: e-vote, e-business,...

Hard because of:

- concurrency (interleaving of multiple processes),
- infi nite state systems,
- modelization aspects (dedicated models).

Research Directions

- Semantics issues.
  - Probabilistic computations.
  - Unified framework.
- The intruder theory.
  - Fill the gap between abstract description and implementations.
- Verification methods.
  - Bounded/unbounded number of sessions,
  - Abstraction methods,
  - Algebraic properties.

THE SEMANTICS ISSUE I

Formal methods		Cryptographic models
Domains of nonces, keys,. . . infi nite		Finite objects
Non-deterministic adversary	$\leftrightarrow$	Probabilistic polynomial-time adversary
The adversary learns the secret		Probability of distinguishing the actual protocol from a perfect one is negligible
Reachability analysis		Observational equivalence

$\Rightarrow$ ACI RESEARCH Probabilistic models (Spi-Calculus and observational equivalence).

THE SEMANTICS ISSUE II

Many formalisms: process calculi, Strand basis, Horn Clauses, Higher-order logic, . . . and a jungle of defi nitions.

- Diffi cult to compare approaches
- Mainly secrecy and authentication.
- No separation between the operational semantics of protocols and the logic to express properties.

$\Rightarrow$ ACI RESEARCH: A uniform operational semantics and a logic for cryptographic properties.

THE INTRUDER THEORY ISSUE

Idea: close the gap between the Dolev-Yao model and the actual implementations.

- Enhance the computational power of the intruder. Algebraic properties of xor, exponential function, homomorphism,. . . .
- Dictionary attacks (weak passwords, nonces,. . .)
- . . .

$\Rightarrow$ ACI RESEARCH: New algebraic properties, combinations, dictionary attacks,....

THE VERIFICATION ISSUE

Goal: Decision procedures for protocols (exact or approximate)

- Bounded number of sessions: many approaches but
  - hard to compare (no generic model).
  - Effi ciency issues: state explosion problem.
- Unbounded number of sessions: undecidability results but
  - Restricted cases are decidable: ping-pong, one-memory protocols,. . . . . .
  - Approximation schemes: Tree automata, abstract interpretation, ...
  - Tagging protocols is successful.
- Secrecy and authentication mainly.

$\Rightarrow$ ACI RESEARCH: Decidability and effi ciency issues, investigation of new properties.

Thank You

Questions?