Scalable Verification of Systems with Cryptography

Birgit Pfitzmann (IBM Research, Zurich)
Joint work mainly with Michael Backes (Univ. Saarbrücken) and Michael Waidner (IBM Research & SWG)

Building Secure Systems
Cryptography: The Details

Crypto-Toolbox

- Encryption
- Hash function
- Signature
- Key exchange

Fact(p\times q) \quad DL(g^x)

Prob[\text{Attack}] \leq ...

Not scalable!
Prior Automated Crypto Protocol Proofs: The Big Picture

E.g.: Secure Channels like SSL (with mutual authentication)

- If you use them in a larger system, what would you assume about them, or how would you model them?

- E.g., as “ideal secure channel”

  \[
  S \quad m \quad R
  \]

- E.g., as a primitive in $\pi$-calculus etc.
Secure Channels, ctd.

- How correct is this compared with actual SSL?
- Not bad, but not quite correct:
  - Computational assumptions and error probabilities from crypto
  - Message length and traffic pattern leak
  - No availability

Always very similar ⇒ make part of semantics ("fulfillment" relation)

Special ⇒ extend specification

Rather general ⇒ can just be in asynchronous model

Reactive Simulatability (RSIM)

Here “General RSIM” variant

Indistinguishability of random variables
RSIM in Overall Design Process

- Vague requirements
- Formalization
- Designer(s)
- Refinement
- Composition theorems allow iterated refinement and modular build-up
- Implementation

RSIM as the cryptographic variant

Treating Properties Cryptographically

- Integrity requirements
- No information flow between certain system parts
- Secrecy of specific data

- Vague requirements
- Formalization
- Designer(s)
- Refinement
- Cryptographic Fulfillment
- Implementation

Compatible with RSIM refinement
Recent Work

• Extended prior results for “Dolev-Yao models” – specific term-algebra abstractions widely used in verification community
• Impossibility results for certain Dolev-Yao model variants
• BPW-Dolev-Yao model in Isabelle/HOL (with Ch. Sprenger and D. Basin)
• Attempt to apply to real-world Web Services