Security protocol verification

Hands-on workshop

Martin Ukrop mukrop@mail.muni.cz

Faculty of Informatics, Masaryk University

CROCS
Centre for Research on Cryptography and Security

What are security protocols?

- Composition of cryptoprimitives
- *“Security protocols are three line programs that people still manage to get wrong.”*
  (Roger Needham)

Security protocols

- Having a good lock (cipher) is not enough.
- It has to be used properly.

Verification of security protocols

- Design flaw detection
- Constructing proof of correctness
- It's automatic!
- Assumption: perfect cryptoprimitives
- Specific attacker model (*"Dolev-Yao attacker"*)
- Verifying specified attributes
- Several tool available

Verification tools (some of them)

- The Scyther Tool
  – Intuitive, understandable, limited expressivness
- ProVerif
  – Well-known, stable, rather intuitive, expressive
- Tamarin Prover
  – Unintuitive, very expressive, semi-automated
- AVANTSSAR
  – Follow-up to AVISPA project, less known

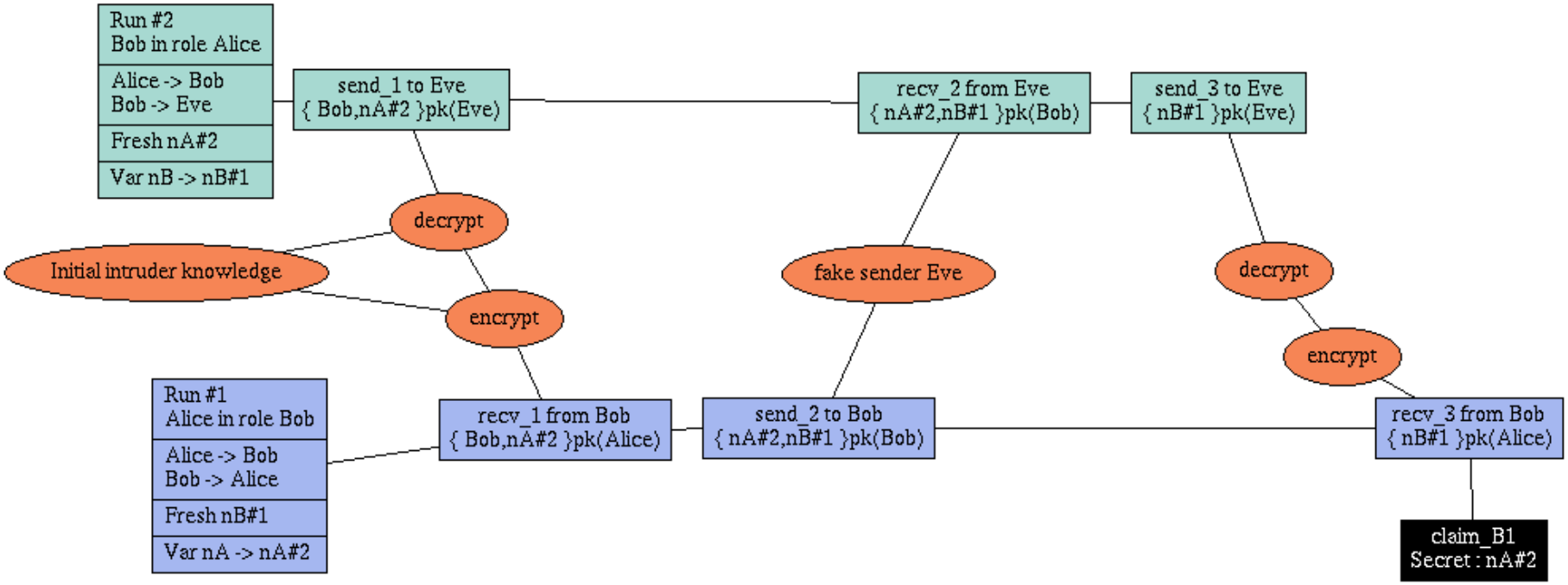
Needham–Schroeder protocol

- Simple (a)symmetric authentication protocol
- Designed by Roger Needham and Michael Schroeder in December 1978
- Works as follows:
  1. A -> B: $\{A, N_A\}_{pk(B)}$
  2. B -> A: $\{N_A, N_B\}_{pk(A)}$
  3. A -> B: $\{N_B\}_{pk(B)}$

Scyther syntax (needham-schroeder.spdl)

```
role Alice {
  fresh nA: Nonce;
  var nB: Nonce;
  send_1(Alice, Bob, {Alice, nA}pk(Bob) );
  recv_2(Bob, Alice, {nA, nB}pk(Alice) );
  send_3(Alice, Bob, {nB}pk(Bob) );
  claim_A1(Alice, Secret, nA);
  claim_A2(Alice, Secret, nB);
}
```

Man in the middle attack (Scyther)



- Attack discovered by Gavin Lowe after 17 years!

Needham–Schroeder–Lowe protocol

- Fixed in 1995 by Gavin Lowe
- Prevents the men-in-the-middle attack
- Works as follows:
  1. A -> B: $\{A, N_A\}_{pk(B)}$
  2. B -> A: $\{B, N_A, N_B\}_{pk(A)}$
  3. A -> B: $\{N_B\}_{pk(B)}$

Further exercises

- Verify NS-protocol along with NSL protocol
  - Why are there attacks on NSL now?
  - Implement protocol versioning
- More protocol examples in Scyther's demo folder
- More exercises available
  - Cas Cremer's exercise sheet
- Security Protocols Open Repository

What do the results actually mean?

It’s proven correct!

- (within the specified attacker model)
- (with respect to security features specified)
- (with the assumption of perfect cryptoprimitives)
- (with typing assumptions)
- (with…)

Conclusions

Negatives

- Specific attacker model
- Sensitive to precise specification
- Assumes perfect cryptoprimitives

Positives

- Automated process
- Prevents basic and some advanced design flaws
- Favours simple solutions

Image CC-BY-NC-SA-2.0 Luka Kladaric

Image CC-BY-NC-SA-2.0 Dustin Quasar

Thank you
for your attention.

Questions are welcome!

Martin Ukrop mukrop@mail.muni.cz

Faculty of Informatics, Masaryk University

CROCS
Centre for Research on Cryptography and Security