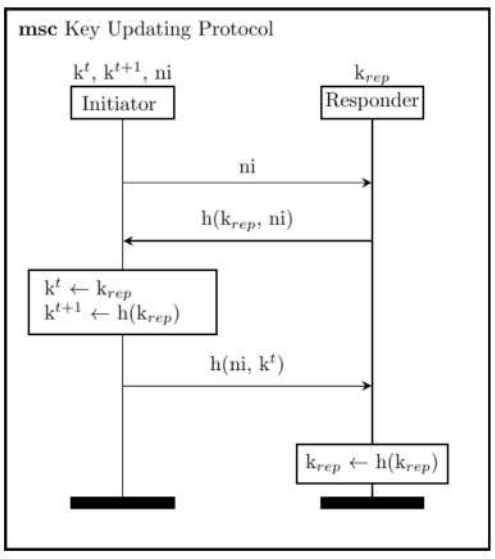
Automated Verification of Security Properties in RFID Communication Protocols

Zach Smith
University of Luxembourg

Introduction

- A communication protocol is a series of rules describing how a set of agents interact.
- A protocol has a set of specific goals: for example, authenticating the identity of the participants.
- We assume the presence of an *adversary*, who has complete control of the communication network.
- The aim: formally prove that the protocol will meet the security requirements regardless of adversary interference.



Desynchronisation

- Many protocols use a shared secret key that update between iterations.
- In order to maintain communication, the agents must update their keys synchronously.
- Providing a mathematical proof that a given communication protocol is immune to desynchronisation is an open problem.
- Some results can be achieved using automated verifiers built on rewrite logic.

Protocol Specification

$$\frac{\text{Agent}(A) \quad \text{Fr}(n)}{\text{Net}(n) \quad \text{Session}(A,n)}\ \texttt{Start}$$

$$\frac{\text{Agent}(B) \quad \text{Net}(n) \quad \text{Fr}(m)}{\text{Net}(n,m) \quad \text{Reply}(B,n,m)}\ \texttt{Reply}$$

Fig. 1: Protocol operation is broken down into a collection of rewrite laws

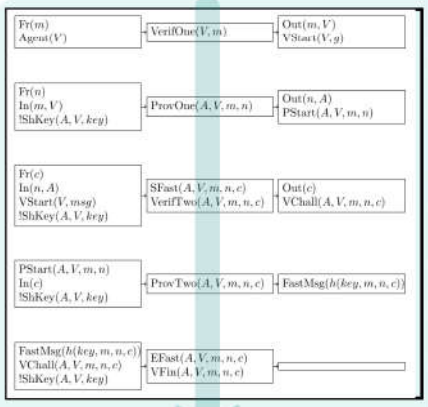
$$\frac{\text{Net}(n)}{\text{K}(n) \quad \text{Net}(n)}\ \texttt{AdvEavesdrop}$$

$$\frac{\text{K}(n)}{\text{Net}(n)}\ \texttt{AdvInject}$$

Fig. 2: Additional rules are added to model the capabilities of the adversary

Security Definitions

Fig. 3: Special 'marker' facts are added to protocol rules.




```
lemma dbsec:
  "
  All A V m n c #t. (
    Efast(A, V, m, n, c)@t ) ==>
    (
      Ex #t1 #t2. SFast(A, V, m, n, c)@t1 &
                  ProvTwo(A, V, m, n, c)@t2 &
                  (#t1 < #t2) &
                  (#t2 < #t)
    )
  "
```

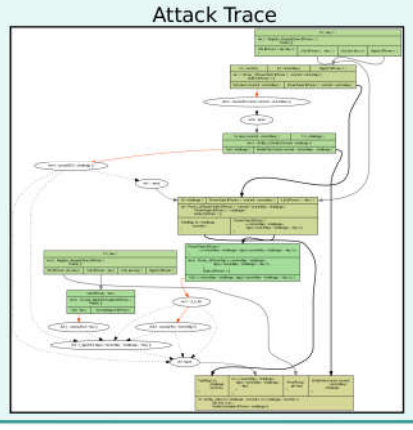
Fig. 4: Security properties are built from first-order logic statements on the marker facts

Property Verification

- The Tamarin prover tool is used to prove that the protocol rules obey the security properties.
- An equational theory allows for the modelling of functions such as hashing, encryption or XOR.
- Termination is not guaranteed, especially for unbounded protocols, but often works well.

Fig. 6: Machine verifiable proofs are constructed - or counterexamples are shown for false statements.

Attack Trace

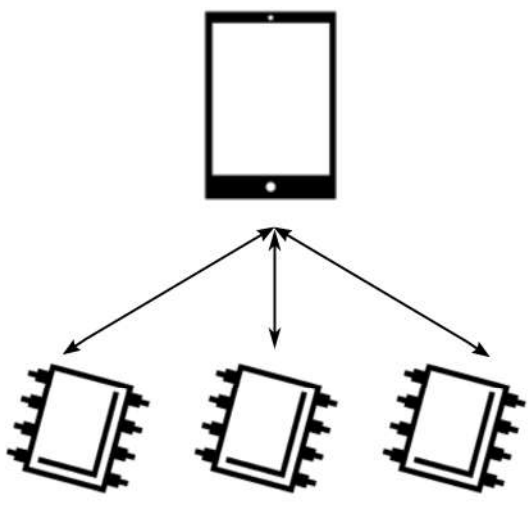


Tamarin Prover

Fig. 5: The Tamarin Prover tool is used to automatically verify properties

RFID Protocols

- Typically involve one reader interacting with one or more RFID tags.
- The reader uses the results of the protocol to interact with a secure server, which verifies the completion.
- The reduced computation power of RFID tags prevents them from using advanced cryptography.



Conclusions

- RFID protocols present unique challenges in their security requirements and the restrictions on how they are built.
- The use of automated verifiers allows for rapid construction of proofs (or presents counterexamples).
- Progress is still being made with respect to adapting proving engines to deal with equational theories.

References

[1] Schmidt, B., Meier, S., Cremers, C., & Basin, D. (2012, June). Automated analysis of Diffie-Hellman protocols and advanced security properties. In Computer Security Foundations Symposium (CSF), 2012 IEEE 25th (pp. 78-94). IEEE.

zach.smith@uni.lu