Overview

- Replay attacks in interactive protocols
- A symmetric protocol for key exchange (Needham–Schroeder Key Exchange Protocol)
- A symmetric protocol for key exchange (Diffie-Hellman-Merkle Protocol)
- The challenge of authentication (Needham–Schroeder Authentication Protocol)
- Putting it all together (TLS)
- Trust models (PKI)

Replay attacks