

Authentication Protocols

Mark Ryan

M.D.Ryan@cs.bham.ac.uk

Computer Security lecture notes

October 2009

<http://www.cs.bham.ac.uk/~mdr/>

Cryptographic protocols

A cryptographic protocol is a **distributed procedure** that employs cryptography to achieve a security goal.

Examples of participating agents:

- Client *and* Server
- Application *and* TPM
- VM₁ *and* VM₂
- Voter *and* Collector
- Phone *and* Network
- Base station *and* Network
- Peer *to* Peer
- Alice *and* Bob

Cryptographic protocols

A cryptographic protocol is a distributed procedure that employs cryptography to achieve a **security goal**.

Examples of “security goal”:

- Authentication
- Key agreement
- Secure communication
- Privacy
- Confidentiality management
- Attestation
- Non-repudiation
- Fair exchange
- Contract signing
- Secure storage
- Access control
- Voting

Protocols are usually simple, but often subtle. That makes them ideal for automated reasoning.

Attacker model

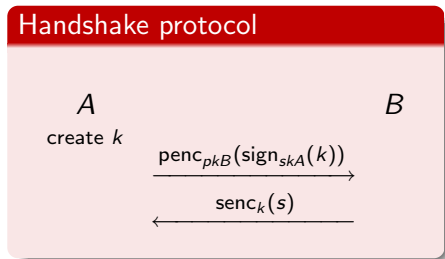
We model a very powerful attacker, with “Dolev-Yao” capabilities:



- it completely controls the communication channels, so it is able to record, alter, delete, insert, redirect, reorder, and reuse past or current messages, and inject new messages. (The *network* is the attacker.)
- manipulate data in arbitrary ways, including applying crypto operations **provided** has the necessary keys.
- It controls dishonest participants.

“It’s always better to assume the worst. Assume your adversaries are better than they are. Assume science and technology will soon be able to do things they cannot yet. Give yourself a margin for error. Give yourself more security than you need today.” - Bruce Schneier

Example: handshake protocol

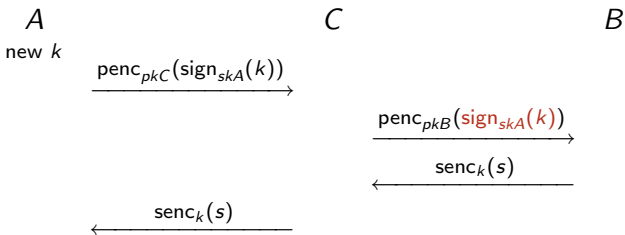


Alice and Bob know each other's public keys. They want to agree a session key for private communication of a **secret s** . They communicate on a channel which is controlled by the attacker.

Intended properties:

- If Alice has completed the protocol, apparently with Bob, then Bob has completed the protocol with her.
- If Bob has completed the protocol, apparently with Alice, then Alice has completed the protocol with him.
- Messages sent encrypted with the agreed key remain secret.

Handshake protocol attack



Intended properties:

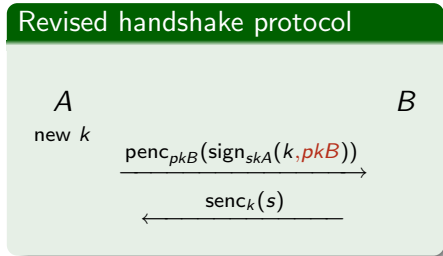
- If Alice has completed the protocol, apparently with Bob, then Bob has completed the protocol with her.
- If Bob has completed the protocol, apparently with Alice, then Alice has completed the protocol with him.
- Messages sent encrypted with the agreed key remain secret.

Handshake protocol fixed

The attack is avoided by making the package the initiator sends include the identity of the respondent.

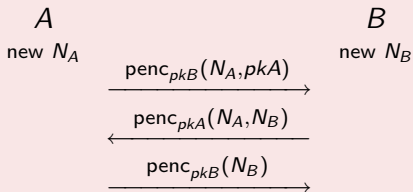
The three properties hold of the revised protocol, but not for the original one.

There are techniques and software tools that enable us to automatically establish these facts.



Example: Needham-Schroeder public key protocol

NSPK protocol



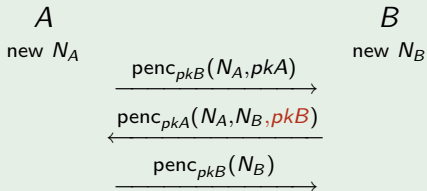
As before, A and B know each other's public keys, and want to agree a session key for private communication. They communicate on a channel which is controlled by the attacker.

- If Alice has completed the protocol, apparently with Bob, then Bob has completed the protocol with her.
- If Bob has completed the protocol, apparently with Alice, then Alice has completed the protocol with him.
- Messages sent encrypted with the agreed key (based on N_A, N_B) remain secret.

NSPK protocol fixed

The protocol (invented in 1978) was found to be flawed in 1995. The attack is avoided similarly as before, by including identity information in an encrypted package.

Revised NSPK



The three properties hold of the revised protocol, but not for the original one.

Go to next slides