Automated verification of protocols using low-entropy secrets

Stéphanie DELAUNE[1], Steve KREMER[2], Ludovic ROBIN[2]

[1]École Normale Supérieure de Cachan
[2]Laboratoire Lorrain en Informatique et Automatique

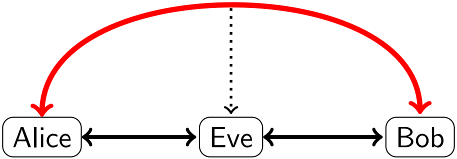
September 1, 2015

Motivation

Out of bands channels

Properties

- Authentication
- Asynchronous emission
- Short messages



Out of bands protocol example

n_w is a weak nonce.

A commitment before knowledge based protocol

$$\begin{array}{llll} A & \longrightarrow & B & : \langle m, \mathbf{hash}(\langle m, n_w \rangle)\rangle \\ B & \longrightarrow_O & A & : ack \\ A & \longrightarrow_O & B & : n_w \end{array}$$

n_w can be guessed before commitment !

Out of bands protocol example

n_w is a weak nonce.

A commitment before knowledge based protocol

$$\begin{array}{llll} A & \longrightarrow & B & : \langle m, \mathbf{hash}(\langle m, n_w \rangle)\rangle \\ B & \longrightarrow_O & A & : ack \\ A & \longrightarrow_O & B & : n_w \end{array}$$

n_w can be guessed before commitment !

n_s is a strong nonce.

A more secure one !

$$\begin{array}{llll} A & \longrightarrow & B & : \langle m, \mathbf{hash}(\langle m, n_s, n_w \rangle)\rangle \\ B & \longrightarrow_O & A & : ack \\ A & \longrightarrow & B & : n_s \\ A & \longrightarrow_O & B & : n_w \end{array}$$

Conclusion

Work in progress.

- Model the new capabilities of this attacker ;
- Automatically verify security properties using this attacker.

Future work.

- Complete proofs :-) ;
- Case studies : ISO standard, 3D-Secure ;
- Equivalence property ;
- Collisions on weak hash functions.