Bezpečnostní protokoly

Protokol Woo Lam Π^f

Pavel Frýz

xfryzp00@stud.fit.vutbr.cz

Vysoké učení technické, Fakulta informačních technologií

Popis protokolu

- Vytvořen:
  - Thomas Y. C. Woo a Simon S. Lam
  - V roce 1994
- Zajišťuje:
  - Jednosměrnou autentizaci
  - Autentizuje účastníka komunikace A(iniciátor spojení) vůči B.
- Používá:
  - Symetrickou kryptografie
  - Důvěryhodný server
  - Princip úplných informací

Reprezentace protokolu

Textová reprezentace:

A, B, S: Subjekty

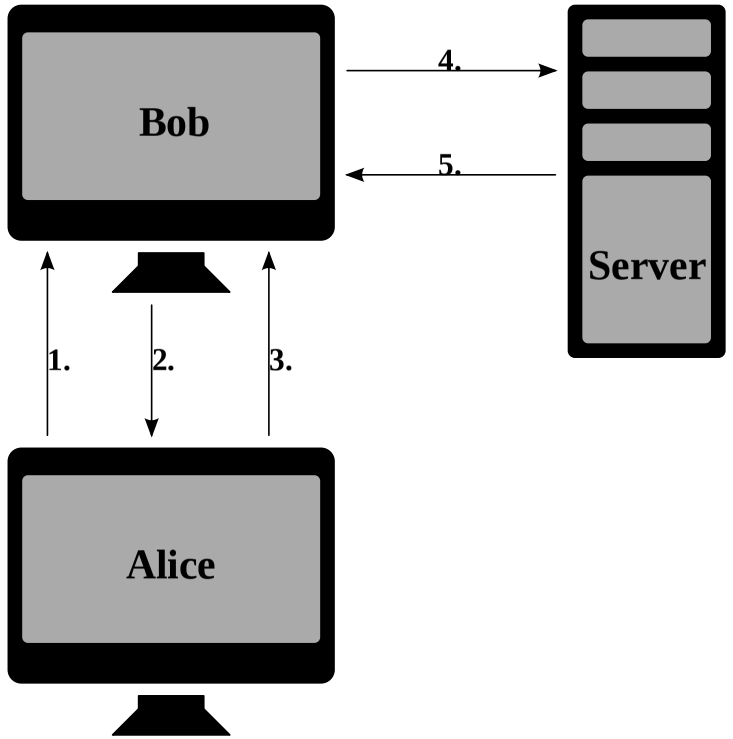
K_{AS}, K_{BS}: Sdílené klíče

N_B: Nonce

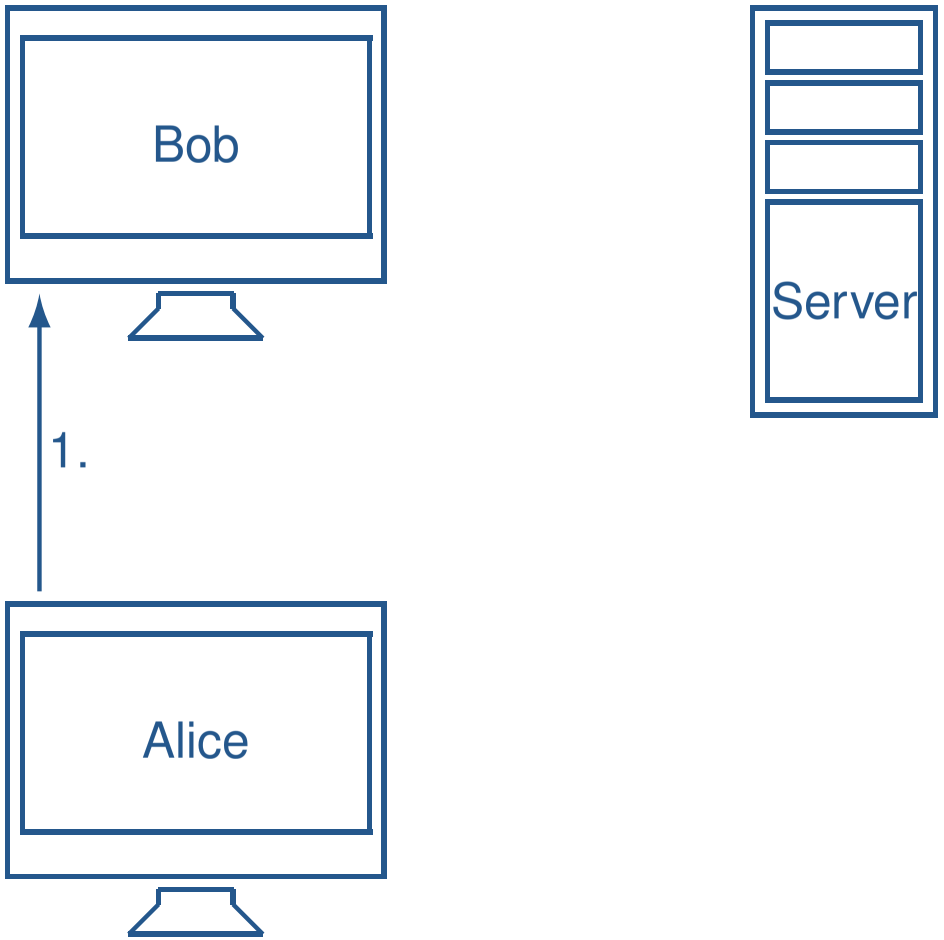
1. $A \rightarrow B: A$
2. $B \rightarrow A: N_B$
3. $A \rightarrow B: \{A, B, N_B\}_{K_{AS}}$
4. $B \rightarrow S: \{A, B, N_B, \{A, B, N_B\}_{K_{AS}}\}_{K_{BS}}$
5. $S \rightarrow B: \{A, B, N_B\}_{K_{BS}}$

Počáteční znalosti	
A	A, B, S, K_{AS}
B	B, S, N_B, K_{BS}
S	A, B, S, K_{AS}, K_{BS}

Grafická reprezentace:



Průběh komunikace



Použité zdroje

- Repozitář bezpečnostních protokolů:
  `http://www.lsv.ens-cachan.fr/Software/spore/index.html`