Security Protocols and Verification

Description of the Bourget-Saunier-Werck Protocol

Description of the Bourget-Saunier-Werck Public-Key Protocol

The Bourget-Saunier-Werck public key protocol is described as follows:

$$\begin{aligned}
\mathrm{A} \to \mathrm{S}: &\ \mathrm{A}, \{\,|\, \mathrm{B}, N_{\mathrm{a}},\ \{\,\mathrm{K}\,\}_{\mathrm{pub(B)}} \,|\,\}_{\mathrm{K}_{as}} \\
\mathrm{S} \to \mathrm{B}: &\ \{\,|\, \mathrm{A}, N_{\mathrm{a}},\ \{\,\mathrm{K}\,\}_{\mathrm{pub(B)}} \,|\,\}_{\mathrm{K}_{bs}} \\
\mathrm{B} \to \mathrm{A}: &\ \mathrm{B}, \{\,|\, \mathrm{ACK} \,|\,\}_{\mathrm{K}}
\end{aligned}$$

Initial knowledge. When an agent receives a nonce, they compare it to their list of previously received nonces to check if a replay attack has been tried.

Values generated during execution. N_{a} is a nonce freshly generated by A, and ACK is an integer (1) sent back for the confirmation.

Protocol description.

- **Step 1 (A→S).** A generates K and N_{a}, encrypts K for B as $\{\,K\,\}_{\mathrm{pub}(B)}$, then wraps $(\mathrm{B}, N_{\mathrm{a}}, \{\,K\,\}_{\mathrm{pub}(B)})$ under the A–S channel key K_{as}; the cleartext A tells S which key to use. S then checks if a replay attack happened.
- **Step 2 (S→B).** S decrypts with K_{as} and forwards $(\mathrm{A}, N_{\mathrm{a}}, \{\,K\,\}_{\mathrm{pub}(B)})$ to B encrypted under K_{bs}. B then checks if a replay attack happened by comparing the nonce he just received with the list of the previously received nonces.
- **Step 3 (B→A).** B decrypts with K_{bs} to obtain $\mathrm{A}, N_{\mathrm{a}}, \{\,K\,\}_{\mathrm{pub}(B)}$, recovers K using $\mathrm{prv}(B)$, and confirms by sending B, $\{\,\mathrm{ACK}\,\}_K$ to A.

Security properties.

- **Authentication (A→B).** If B completes a run of the protocol and obtains a key K, then K was indeed generated and sent by A. This follows since K is always transmitted encrypted under $\mathrm{pub}(B)$ and only A can initiate such a message through the server S.
- **Authentication (B→A).** If A receives the confirmation message $\{\,\mathrm{ACK}\,\}_{\mathrm{K}}$, then B has successfully decrypted $\{\,\mathrm{K}\,\}_{\mathrm{pub}(B)}$ and thus possesses K. Hence, A can be assured that B has received the correct key.
- **Secrecy.** The session key K remains secret between A and B (and possibly the server S). An attacker cannot learn K, as it is always transmitted encrypted under $\mathrm{pub}(B)$.
- **Freshness.** B checks nonces to detect and reject replayed messages. Thus, old protocol runs cannot be reused by an adversary to mislead honest agents.

Cost of the protocol. For reference:

$$\begin{aligned}
\text{Step 1:}\ & 1+10+50+50+1+1+1+1+1+1 = 117,\\
\text{Step 2:}\ & 10+50+50+1+1+1+1+1+1 = 116,\\
\text{Step 3:}\ & 10+1+1+1 = 13.\\
\text{Total:}\ & 117+116+13 = 246.
\end{aligned}$$