Needham Schroeder 1977

Sym key

\[
\begin{cases}
\text{(Client)} & \text{(Server)} \\
\text{Trent} & \text{Trent has A & B's} \\
\text{Alice} & \text{pub keys} \\
\text{Bob} & \text{Trent sends A B's} \\
A, B do key exchange \rightarrow \text{pub key A & vice versa}
\end{cases}
\]
key = (S, Consec S2)
Gonna party

4 will bring S to the comic 3

A can take S's

A

Frederick Party
Alice -> Authenticator

"Alice", KA-TGS, {"validity"} -> Authenticator

A-TGS

A-TGS

// KA-Alice = hash of password, clear passwd stored @ server

"Alice", KA-TGS, {"validity"} -> Authenticator

A-TGS

A-TGS

A-TGS

"Alice" user id.

"Alice" -> Authenticator

"Alice" -> Authenticator

oreandom # to be

"Clean text shows Alice password in..."
Alice sends to TGS, to get the session key KA-B, gets timestamp and lifetime.

Alice -> TGS: 

\{ "Alice", "Bob" \} \_K_{A-TGS}; \( \{ "Alice", \_K_{A-TGS}, validity \} \_K_{TGS} \)

//validity = requested lifetime

Server -> Alice: 

\{ \_K_{TGS}, Life, \_K_{A-B}, \_K_{A-TGS}, "Bob", \_K_{B-TGS} \} \_K_{A-TGS}

Alice sends to TGS, to get the session key KA-B, gets timestamp.

//validity = requested lifetime

TGS to Alice:

\{ \_K_{TGS}, Life, \_K_{A-B}, \_K_{A-TGS}, "Bob", \_K_{B-TGS} \} \_K_{A-TGS}

Alice to TGS:

\{ "Alice", "Bob", \_K_{A-TGS} \} \_K_{TGS}

//Servert Name

Server Name

and lifetime.
3. Alice establishes session key with Bob and Bob authenticates himself.

\[
\text{Alice} \rightarrow \text{Bob}, \{T_{GS}, L, K_{A-B}, \text{"Alice"} \} K_{B-TGS}, \{\text{"Alice", } T_{A}\} K_{A-B}
\]

\[
\text{Bob} \rightarrow \text{Alice}, \{T_{A} + 1\} K_{A-B}
\]

Alice establishes session key with Bob and Bob authenticates himself.
First consider sent

"inevitably & this is exactly

sent this"

- another identified (source did

- secret (enveloped)

Secret / Secret Communication

Secret / Secret Communication

secret / secret communication

secret / secret communication
\[ \text{msg, hash(msg)} \rightarrow A \]

\[ B \leftarrow \]
(msg, hash(mssg), K_A)

Message authentication

MAC

also for integrity

Purolity
2. Use hand drawn circle.

3. Use proper key. $A \rightarrow B \in \mathcal{E}$ (must)}

SECRET

\[ A \rightarrow B \in \mathcal{E} \]
How do I know if it's a key?
\( \{ x, y \} \) use as secret key

\[ E^{\prime}(L_s^2) \xrightarrow{\text{key}} A \]

\[ E^\oplus(L_s^2) \xleftarrow{\text{key}} A \]

need more

and keep

A \& B know each other