Security Protocols 3

Security Principles
Gavin Lowe

Encrypted Key Exchange

The Encrypted Key Exchange (EKE) protocol aims to authenticate a user of a client to a server, and establish a session key for subsequent communication.

The user a and the server b share a secret password $p(a, b)$. However, the password might be poorly chosen, say an English word.

We want to ensure that the intruder cannot deduce the password from observing a protocol exchange.

How not to do it

Consider a protocol that starts as follows:

Msg 1. $a \to b : \{a, b, k_{ab}\}_{p(a,b)}$.

Suppose the intruder sees the message $\{a, b, k_{ab}\}_{p(a,b)}$ and guesses the password. He can then verify his guess by decrypting the message with his guess, and seeing whether the result starts with a, b.

Alternatively he can write a program to try every word in an online dictionary in turn.

EKE

The client a creates an asymmetric key pair (k_1, k_2).

Msg 1. $a \to b : a, \{k_1\}_{p(a,b)}$
Msg 2. $b \to a : \{\{k_{ab}\}_{k_1}\}_{p(a,b)}$
Msg 3. $a \to b : \{n_a\}_{k_{ab}}$
Msg 4. $b \to a : \{n_a, n_b\}_{k_{ab}}$
Msg 5. $a \to b : \{n_b\}_{k_{ab}}$.

Note that an intruder cannot carry out a guessing attack. If he guesses the password, he can obtain

k_1 and $\{k_{ab}\}_{k_1}$

but he cannot use these to verify his guess.