Multi-protocol attacks

Sometimes it is possible to replay an encrypted component from one protocol to another so as to cause an attack.

Such attacks would be prevented if it were possible to tell from which protocol a component came, for example by including a protocol identification field.

Type flaw attacks

Some protocols suffer from *type flaw attacks*, where a field of one type is interpreted as being of another type.

Example type flaw attack

The Woo and Lam Protocol π_1:

Msg 1. $a \to b : a$

Msg 2. $b \to a : nb$

Msg 3. $a \to b : \{a, b, nb\}_{shared(a,s)}$

Msg 4. $b \to s : \{a, b, \{a, b, nb\}_{shared(a,s)}\}_{shared(b,s)}$

Msg 5. $s \to b : \{a, b, nb\}_{shared(b,s)}$,

can be attacked as follows:

Msg 1. $I_A \to B : A$

Msg 2. $B \to I_A : N_b$

Msg 3. $I_A \to B : N_b$

Msg 4. $B \to I_S : \{A, B, N_b\}_{shared(B,S)}$

Msg 5. $I_S \to B : \{A, B, N_b\}_{shared(B,S)}$.