Avaimensopimisprotokollista

Timo Karvi

2.2013

Needham-Schroeder Public Key Protocol I

The Needham-Schroeder public key protocol was one the earliest published key establishment protocols along with its well-known companion using symmetric encryption. This version uses public key encryption.

$$
\begin{array}{lll}
1. & A \longrightarrow B: & E_B(N_A, A) \\
2. & B \longrightarrow A: & E_A(N_A, N_B) \\
3. & A \longrightarrow B: & E_B(N_B)
\end{array}
$$

In 1996, an attack was found with the help of the automatic analysing tool FDR:

$$
\begin{array}{lll}
1. & A \longrightarrow C: & E_C(N_A, A) \\
1'. & C_A \longrightarrow B: & E_B(N_A, A) \\
2'. & B \longrightarrow C_A: & E_A(N_A, N_B) \\
2. & C \longrightarrow A: & E_A(N_A, N_B) \\
3. & A \longrightarrow C: & E_C(N_B) \\
3'. & C_A \longrightarrow B: & E_B(N_B)
\end{array}
$$

Needham-Schroeder Public Key Protocol II

The correction is simple:

1. $A \longrightarrow B$: $E_B(N_A, A)$
2. $B \longrightarrow A$: $E_A(N_A, N_B, B)$
3. $A \longrightarrow B$: $E_B(N_B)$

Host Identity Protocol I

- HIP adds a new name space to the TCP/IP protocol stack. Network hosts are identified with new identifiers, host identifiers (HIs). The HIs are public cryptographic keys. Therefore, peer hosts authenticate directly by their HIs.
- HIP has been designed to be backwards compatible, i.e. no changes to the network infrastructure or to the applications are needed. In order to bind other names to the HI public key representations, the host identity tags (HITs), a variety of mechanisms, like DNSSEC, SPKI/SDSI, and X.509 certificates, are available.
- If an entity A wants to start a HIP connection with B, A first makes a DNS query in order to get B's IP address and B's host identity. In this query, A uses human-friendly host names. It is essential that A can trust the DNS response. If the data in the response is incorrect, then it might be possible that A communicates with a malicious entity without noticing it.

Host Identity Protocol II

- There can be only one HIP association between a pair of HITs. Therefore, the only way to support multiple associations between two hosts is to have several HITs per host. This leads to a situation where a host may have several RSA or DSA public/private key pairs.

I1.	$I \longrightarrow R$:	$\mathrm{HIT}(i)$, $\mathrm{HIT}(r)$
R1.	$R \longrightarrow I$:	$\mathrm{HIT}(r)$, $\mathrm{HIT}(i)$, puzzle, $DH(r)$, $K(r)$, [CERT], sig
I2.	$I \longrightarrow R$:	$\mathrm{HIT}(i)$, $\mathrm{HIT}(r)$, solution, $DH(i)$, $K(i)$, [CERT], hmac, sig
R2.	$R \longrightarrow I$:	$\mathrm{HIT}(r)$, $\mathrm{HIT}(i)$, hmac sig

Figure: Base Exchange

Host Identity Protocol III

- The HIP connection is negotiated by performing the Base Exchange protocol, see Fig.1. An initiator I starts the negotiation with a responder R.
- Message I1 is sent without signature, messages R1, I2, R2 are signed (sig). R1 and I2 contain Diffie-Hellman parameters ($DH(r)$, $DH(i)$), a puzzle (in R1), its solution (in I2), and a puzzle difficulty parameter K. R1 and I2 may contain certificates with certificate authority lists.
- Normally, the signature in R1 can be calculated beforehand, because the signature does not contain HIT(i) or the checksum, if a puzzle is used. After receiving R1 packet I can calculate the Diffie-Hellman secret and R can calculate the same secret after receiving I2 packet. The standard demands that this secret is used when calculating the compulsory hmac values in I2 and R2. The hmac value is checked before the signature is checked.

Host Identity Protocol IV

- The CERT parameter is optional. It is contained in the variable size part of the HIP packet. The maximum length of a HIP packet is 2040 bytes and the maximum length of the parameter field is 2008 bytes.