4/17/07

Key Management - IPsec

(1) Manual
(2) Automatic

ISAKMP/Oakley

Internet Security Association
Key management Protocol

Oakley

Oakley - 3 Modified form of Diffie-Hellman Key Exchange.
Diffie-Hellman

prime (large) \( q \)

primitive root of \( q \) \( \alpha \)

\( q, e \)

A \( \leftrightarrow \) B \( q, e \)

A

- Creates a Secret Key
- Computes \( Y_A = \alpha^{XA} \mod q \)

A \( \rightarrow \) B: \( Y_A \)

B

- Creates a Secret Key
- Computes \( Y_B = \alpha^{XB} \mod q \)

B \( \rightarrow \) A: \( Y_B \)

\[ K = (Y_B)^{XA} \mod q = (\alpha)^{XAXB} \mod q = (Y_A)^{XB} \mod q = (\alpha)^{XAXB} \mod q \]
Weaknesses DHKE

Man-in-the-middle attack
No identity of sender
Computationally expensive
\( q, \alpha \)
Oakley algorithm.

Group

\[ q = 2^{768} - 2^{704} - 1 + 2^{64} \times (2^{638} \times 11 + 149686) \]
\( \alpha = 2 \)

\[ q = 2^{1024} - 2^{960} - 1 + 2^{64} (2^{894} \times 11 + 129093) \]
\( \alpha = 2 \)
3) 1536
4) Elliptic curve $2^{155}$
5) Elliptic Curve $2^{185}$

---

Use nonce

Cookies

MD5 — IP Source & Dest
      UDP Source & Dest port
      & logally generated secret value.
Example
Aggressive Key Exchange

Send: (Initiator) I
Receive: (Responder) R

I → R:
R → C:
I → R:
I→R: CKYᵢ - initiate Cookie

OK, KeyX - Key exchange message type

GRP - Name of DHKE group for this exchange.

Gₓ - public key of the initiator

EHAO - Encryption, hash authentication function offered.

NIDP - Encryption not used in the remainder of the message

IDᵢ, IDᵣ

Nᵢ - Random nonce

Sᵢ [IDᵢ || IDᵣ || Nᵢ || GRP || Gₓ || EHАО]
$$R \rightarrow I: \ CKY_R, CKY_I$$

OK- Key X

GRP

$g_Y$ - public key of $R$

EHAS - Encryption, Hash authentication selected

NIDP

$ID_R, ID_I, N_R, N_I$

$$SK_R[ ID_R \| ID_I \| N_R \| N_I \| GRP \| g_Y \| g X \| EHAS)$$

$\rightarrow R$:
ISAKMP

Exchanges

(1) Base exchange

(2) Identity Protection exchange

(3) Authentication only exchange

(4) Aggressive exchange

(5) Informational Exchange