4/17/07

Key Management. IPsec

(1) Manual
(2) Automatic

ISAKMP/Oakley

Internet Security Association Key management Protocol

Oakley

Oakley - Modified form of Diffie-Hellman Key Exchange.

Diffie-Hellman

prime (large) q

primitive root of q α

q, e A ⟷ B q, e

A Creates a Secret Key X_A

Computes $Y_A = \alpha^{X_A} \bmod q$

$A \rightarrow B: \; Y_A$

B creates a Secret Key X_B

Computes $Y_B = \alpha^{X_B} \bmod q$

$B \rightarrow A: \; Y_B$

$$K = (Y_B)^{X_A} \bmod q = (\alpha)^{X_A X_B} \bmod q$$
$$= (Y_A)^{X_B} \bmod q = (\alpha)^{X_A X_B} \bmod q$$

Weaknesses DHKE

Man-in-the middle attack

No identity of sender

Computationally Expensive

q, α

Oakley algorithm.

Gronp

1) $q = 2^{768} - 2^{704} - 1 + 2^{64} \times \left(\lfloor 2^{638} \times \pi \rfloor + 149686 \right)$

$\alpha = 2$

2) $q = 2^{1024} - 2^{960} - 1 + 2^{64} \left(\lfloor 2^{894} \times \pi \rfloor + 129093 \right)$, $\alpha = 2$

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

Aggresive Key Exchange

Sender (Initiator) I

Receiver (Responder) R

$I \rightarrow R$:

$R \rightarrow I$:

$I \rightarrow R$:

$I \rightarrow R$: CKY_I - initiator Cookie

Ok. KeyX - Key exchange message type

GRP - Name of DHKE group for this exchange.

g^x - public key of the initiator

EHAO - Encryption, hash authentication function offered.

NIDP - Encryption not used in the remainder of the message

ID_I, ID_R

N_I - Random nonce

$S_{KI}[ID_I \| ID_R \| N_I \| GRP \| g^x \| EHAO]$

$R \rightarrow I$: 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

$S_{KR}[ID_R \| ID_I \| N_R \| N_I \| GRP \| g^Y \| g^X \| EHAS)$

$I \rightarrow R$:

ISAKMP

Exchanges

(1) Base exchange

(2) Identity Protection exchange

(3) Authentication only exchange

(4) Aggresive exchange

(5) Informational Exchange