The IKE (Internet Key Exchange) Protocol

Sheila Frankel
Systems and Network Security Group
NIST
sheila.frankel@nist.gov

IKE Overview

- Negotiate:
  - Communication Parameters
  - Security Features
- Authenticate Communicating Peer
- Protect Identity
- Generate, Exchange, and Establish Keys in a Secure Manner
- Manage and Delete Security Associations

IKE Overview (continued)

- Threat Mitigation
  - Denial of Service
  - Replay
  - Man in Middle
  - Perfect Forward Secrecy (PFS)
- Usable by IPsec and other domains

IKE Overview (continued)

- Components:
  - Internet Security Association and Key Management Protocol (ISAKMP)
    RFC 2408
  - Internet Key Exchange (IKE)
    <draft-ietf-ipsec-ike-01.txt>
  - Oakley Key Determination Protocol
    RFC 2412
  - IPSec Domain of Interpretation (IPsec DOI)
    RFC 2407

Constructs Underlying IKE

- Security Association (SA)
- Security Association Database (SAD)
- Security Parameter Index (SPI)

IKE Negotiations - Phase 1

- Purpose:
  Establish ISAKMP SA (“Secure Channel”)
- Steps (4-6 messages exchanged):
  - Negotiate Security Parameters
  - Diffie-Hellman Exchange
  - Authenticate Identities
- Main Mode vs. Aggressive Mode vs. Base Mode

Phase 1 Attributes

- Authentication Method
  - Pre-shared key
  - Digital signatures (DSS or RSA)
  - Public key encryption (RSA or El-Gamal)
- Group Description (pre-defined)
- Group Type (negotiated)
  - MODP (modular exponentiation group)
  - ECP (elliptic curve group over GF[P])
  - EC2N (elliptic curve group over GF[2^N])

Phase 1 Attributes (continued)

- MODP Group Characteristics
  - Prime
  - Generator
- EC2N Group Characteristics
  - Field Size
  - Irreducible Polynomial
  - Generators (One and Two)
  - Curves (A and B)
  - Order

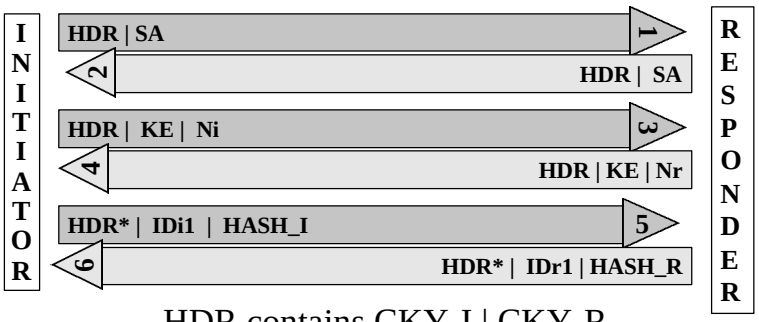
Phase 1 Attributes *(continued)*

- Encryption algorithm
  - Key Length
  - Block size
- Hash algorithm
- Life duration (seconds and/or kilobytes)

IKE's Pre-Defined Groups

- MODP
  - Prime: 768-bit, 1024-bit, 1536-bit
  - Generator: 2
- EC2N
  - GF[2^155], GF[2^185]
  - GF[2^163] (2 groups), GF[2^283] (2 groups)

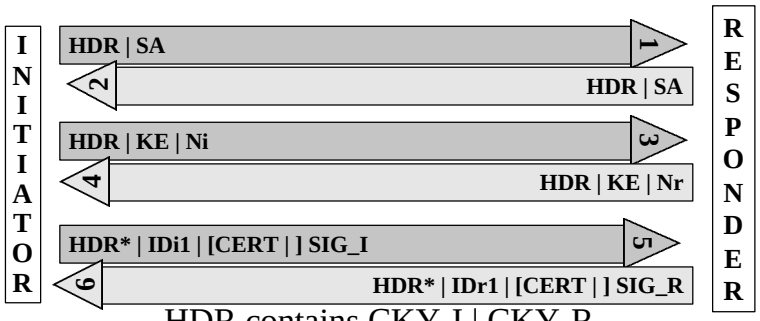
Main Mode:
Authentication with Pre-Shared Keys



HDR contains CKY-I | CKY-R

KE = g^i (Initiator) or g^r (Responder)

Main Mode:
Authentication with Digital Signatures



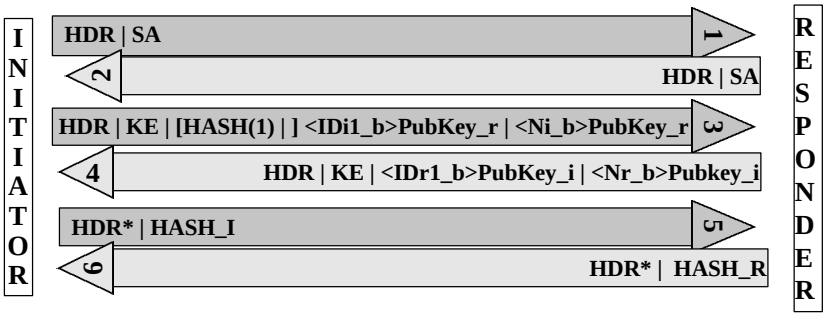
HDR contains CKY-I | CKY-R

KE = g^i (Initiator) or g^r (Responder)

SIG_I/SIG_R = digital sig of HASH_I/HASH_R

Main Mode:

Authentication with Public Key Encryption

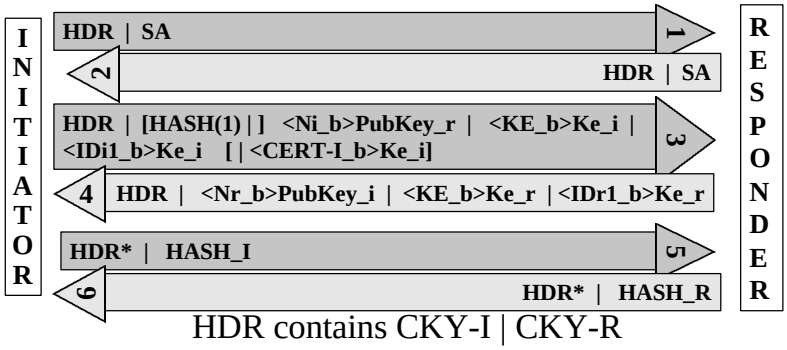


HDR contains CKY-I | CKY-R

KE = g^I (Initiator) or g^r (Responder)

Main Mode:

Authentication with Revised Public Key Encryption



HDR contains CKY-I | CKY-R

KE = g^I (Initiator) or g^r (Responder)

Ke_i/r = symmetric key from Ni/r_b and CKY_I/R

Key Derivation

- SKEYID
  - Pre-shared keys:
    HMAC_H(pre-shared-key, Ni_b | Nr_b
  - Digital signatures:
    HMAC_H(H(Ni_b | Nr_b), g^ir)
  - Public key encryption:
    HMAC_H(H(Ni_b | Nr_b), CKY-I | CKY-R)

Key Derivation (continued)

- SKEYID_d (used to derive keying material for IPsec SA):
  HMAC_H(SKEYID, g^ir | CKY-I | CKY-R | 0)
- SKEYID_a (auth key for ISAKMP SA):
  HMAC_H(SKEYID, SKEYID_a|g^ir|CKY-I|CKY-R|1)
- SKEYID_e (enc key for ISAKMP SA):
  HMAC_H(SKEYID, SKEYID_a|g^ir|CKY-I|CKY-R|2)

Hash Calculations

- HASH_I:

  HMAC_H(SKEYID, g^i | g^r | CKY-I | CKY-R | Sai_b | ID_i1_b)

- HASH_R:

  HMAC_H(SKEYID, g^r | g^i | CKY-R | CKY-I | Sai_b | ID_r1_b)

IKE Negotiations - Phase 2

- Purpose:

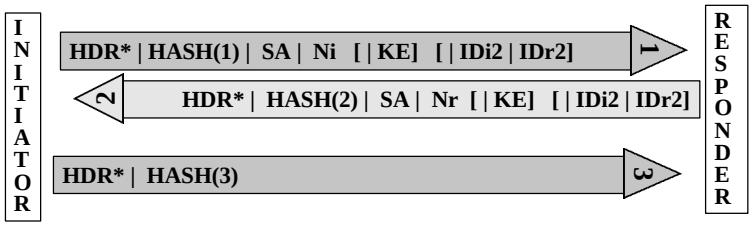
  Establish IPsec SA

- Steps (3-4 messages exchanged):
  - Negotiate Security Parameters
  - Optional Diffie-Hellman Exchange (for PFS)
  - Optional Exchange of Identities
  - Final Verification
- Quick Mode
- New Groups Mode

Phase 2 Attributes

- Group description (for PFS)
- Encryption algorithm (if any)
  - Key length
  - Key rounds
- Authentication algorithm (if any)
- Life duration (seconds and/or kilobytes)
- Encapsulation mode (transport or tunnel)

Quick Mode



HDR contains CKY-I | CKY-R

KE (for PFS) = g^I (Initiator) or g^r (Responder)

Key Derivation

- KEYMAT (no PFS):

  HMAC_H(SKEYID_d, protocol | SPI | Ni_b | Nr_b)

- KEYMAT (with PFS):

  HMAC_H(SKEYID_d, g^ir (QM) | protocol | SPI | Ni_b | Nr_b)

- Expanded KEYMAT (if needed):

  K2 = HMAC_H(SKEYID_d, KEYMAT | [g^ir (QM) |] protocol | SPI | Ni_b | Nr_b)

  K3 = HMAC_H(SKEYID_d, K2 | [g^ir (QM) |] protocol | SPI | Ni_b | Nr_b) etc.

Hash Calculations

- HASH(1) :

  HMAC_H (SKEYID_a | Message_ID | contents of Message #1)

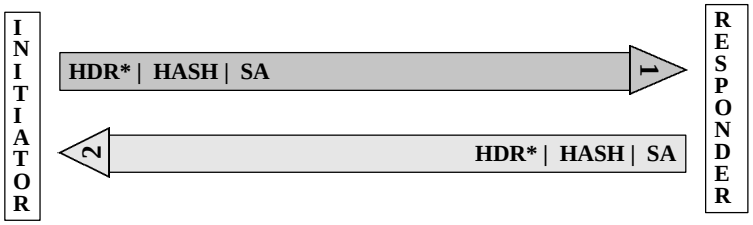
- HASH(2) :

  HMAC_H (SKEYID_a | Message_ID | Ni_b | contents of Message #2)

- HASH(3) :

  HMAC_H (SKEYID_a | 0 | Message_ID | Ni_b | Nr_b)

New Groups Mode



Contact Information

- For further information, contact:
  - Sheila Frankel: sheila.frankel@nist.gov