

# IP Security II

Dr. Arjan Duresi  
Louisiana State University  
Baton Rouge, LA 70810  
Duresi@csc.lsu.edu

These slides are available at:

<http://www.csc.lsu.edu/~duresi/csc4601-04/>



- Key Management
  - Concept
  - Manual Exchange
  - Internet Key Exchange
- IPsec Strengths & Weaknesses
- Implementation of IPsec

## Key Management

- ❑ AH and ESP require encryption and authentication keys
- ❑ Process to negotiate and establish IPSec SA's between two entities
- ❑ Handles key generation & distribution
- ❑ Typically need 2 pairs of keys
  - 2 per direction for AH & ESP

## Key Management

- ❑ Manual key management
  - sysadmin manually configures every system
- ❑ Automated key management
  - automated system for on demand creation of keys for SA's in large systems
  - has Oakley & ISAKMP elements

## Concepts

- ❑ PFS: Perfect Forward Secrecy
  - Obtaining one key does not give access to all data, only data protected by that one key
  - Keys not derived from predecessors
- ❑ Nonces: locally generated pseudorandom numbers

## Manual Key Management

- ❑ Mandatory
- ❑ Useful when IPSec developers are debugging
- ❑ Keys exchanged offline (phone, email, etc.)
- ❑ Set up SPI and negotiate parameters

## Internet Key Exchange - IKE

- ❑ IKE
  - Mutual authentication
  - Establishing a shared secret key to create a IPsec SA
- ❑ Used when an outbound packet does not have an SA
- ❑ Two phases:
  - Establish an IKE SA
  - Use that SA to negotiate IPsec SAs
- ❑ IKE SA used to define encryption & authentication of IKE traffic
- ❑ Multiple IPsec SAs can be established with one IKE SA
- ❑ IKE SA bidirectional

## IKE Specifications

- ❑ ISAKMP Internet Security Association and Key Management Protocol – RFC 2408
- ❑ IKE RFC 2409
- ❑ DOI – Domain of Interpretation RFC 2407

## IKE Phase I – Create IKE SA

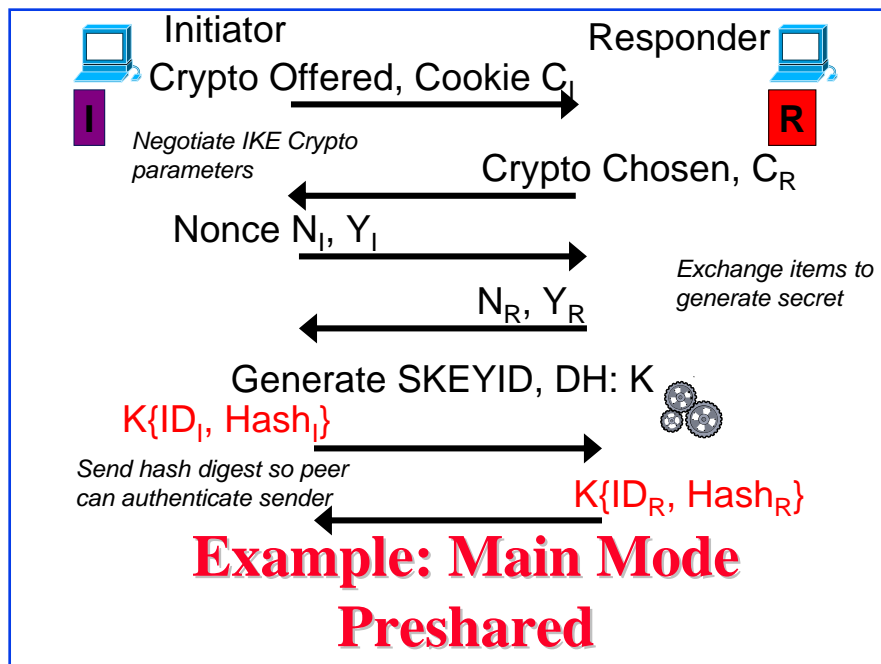
- ❑ Negotiate protection suite
- ❑ Use Diffie-Hellman to establish shared secret
- ❑ Authenticate the shared secret , IKE SA
  - Preshared keys (secret)
  - Digital signatures
  - Public-keys

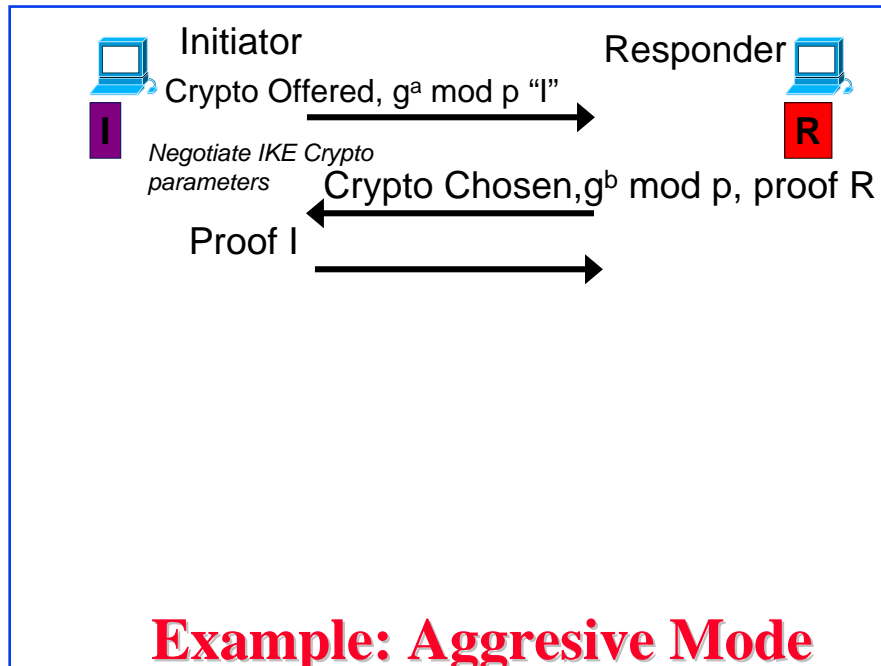
## Mode Exchanges

- ❑ Phase I
  - Main Mode – flexible, 6 messages
    - ❑ Checks cookies before DH work
  - Aggressive mode – faster, 3 messages
    - ❑ Open to clogging DoS, doesn't check cookie before DH work
- ❑ Phase II - Quick Mode

## Concepts - Cookies

- Requirements
  - Depend on specific parties
  - Only the issuing entity can generate acceptable cookies – implies issuer using local secret
  - Cookie generation and verification must be fast
- Hash over IP Src/Dest; UDP Src/Dest; local secret





## Key Types

- There are three types of keys used in a phase 1 IKE
  - Preshared secret key
  - Public key – a pair of public keys use for encryption and decryption
  - Public signature – used for signing and signature verification

## Main Mode Preshared

- ❑ PRF, Pseudo-Random Function, for example DES CBC
- ❑ *SKEYID* root secret  
=PRF(preshared-key, $N_I|N_R$ )
- ❑ *SKEYID\_d* for IPSec SA  
=PRF(SKEYID, $K|C_I|C_R|0$ )  
K is the secret generated by DH
- ❑ *SKEYID\_a* for IKE message data auth & integrity  
= PRF(SKEYID, $SKEYID_d|K|C_I|C_R|1$ )
- ❑ *SKEYID\_e* use to encrypt IKE messages  
= PRF(SKEYID, $SKEYID_a|K|C_I|C_R|2$ )

## Main Mode Preshared: Hashes

- ❑ To authenticate each other, each entity generates a hash digest that only the peer could know

*Hash-I*=PRF(SKEYID, $Y_I|Y_R|C_I|C_R|$ Crypto Offer|ID<sub>I</sub>)

*Hash-R*=PRF(SKEYID, $Y_R|Y_I|C_I|C_R|$ Crypto Offer|ID<sub>R</sub>)

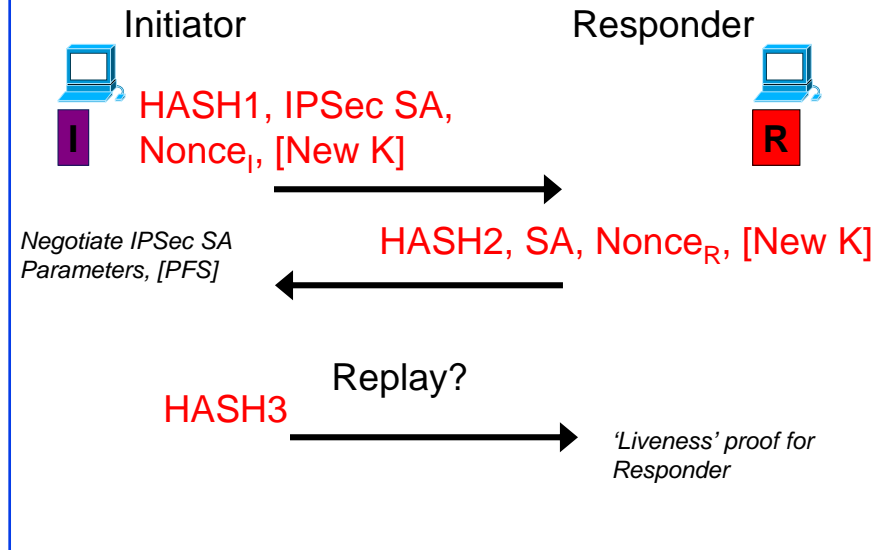
## IKE Phase II – Keys

- ❑ Default: no PFS
  - Keys for IPsec SA derived from IKE shared secret
- ❑ With PFS: use nonces

## Phase II

- ❑ What traffic does SA cover ?
- ❑ *Initiator* specifies which entries (selectors) in SPD are for this IPsec SA, sends off to *responder*
- ❑ Keys and SA attributes communicated with the Phase I - IKE SA
  - Passes encrypted & authenticated

## Example: Quick Mode



## IPSec

- ❑ Key exchange and encryption are separate
  - New encryption algorithms can be added
- ❑ Complex – a lot of flexibility & options
- ❑ Best VPN standard we've got

## The ANX: Realworld IPsec

- ❑ Automotive Networking eXchange
- ❑ Private network for Big 3 Auto Manufactures and their suppliers
- ❑ Uses IPsec to secure communication
- ❑ Certification for ANX turned standards into reality
- ❑ See
  - <http://www.anx.com>
  - <http://www.infosecuritymag.com/apr99/ANX%20SIDEBAR.htm>
  - <http://www.internetwk.com/indepth/indepth101899.htm>

## Summary



- ❑ Key Management
  - Concept
  - Manual Exchange
  - Internet Key Exchange
- ❑ IPsec Strengths & Weaknesses
- ❑ Implementation of IPsec