

# IPsec (AH, ESP), IKE

Guevara Noubir  
 CSG254: Network Security  
 noubir@ccs.neu.edu

---

---

---

---

---

---

---

---

# Securing Networks

Control/Management (configuration)	Applications Layer telnet/ftp: ssh, http: <b>https</b> , mail: <b>PGP</b> <b>(SSL/TLS)</b>	Network Security Tools: Monitoring/Logging/Intrusion Detection
	Transport Layer (TCP) <b>(IPsec, IKE)</b>	
	Network Layer (IP)	
	Link Layer <b>(IEEE802.1x/IEEE802.10)</b>	
	Physical Layer (spread-Spectrum, quantum crypto, etc.)	

CSG254: Network Security IPsec - IKE

---

---

---

---

---

---

---

---

# SSL vs. IPsec

- **SSL:**
  - Avoids modifying "TCP stack" and requires minimum changes to the application
  - Mostly used to authenticate servers
- **IPsec**
  - Transparent to the application and requires modification of the network stack
  - Authenticates network nodes and establishes a secure channel between nodes
  - Application still needs to authenticate the users

CSG254: Network Security IPsec - IKE

---

---

---

---

---

---

---

---

## IPsec Protocol Suite (IETF Standard)

- Provides inter-operable crypto-based security services:
  - Services: confidentiality, authentication, integrity, and key management
  - Protocols:
    - Authentication Header (AH): RFC2402
    - Encapsulated Security Payload (ESP): 2406
    - Internet Key Exchange (IKE)
  - Environments: IPv4 and IPv6
  - Modes:
    - Transport (between two hosts)
    - Tunnel (between hosts/firewalls)

CSG254: Network Security

IPsec - IKE

---

---

---

---

---

---

---

---

## IPsec

- Assumption:
  - End nodes already established a shared session key:
    - Manually or IKE
- Security Association:
  - Each secure connection is called a *security association (SA)*
  - For each SA: key, end-node, sequence number, services, algorithms
  - SA is unidirectional and identified by:
    - (destination-address, SPI = Security Parameter Index)
- Protocols:
  - Authentication Header: integrity protection
  - Encapsulated Security Payload: encryption and/or integrity

CSG254: Network Security

IPsec - IKE

---

---

---

---

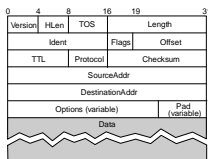
---

---

---

---

## IP Packets



CSG254: Network Security

IPsec - IKE

---

---

---

---

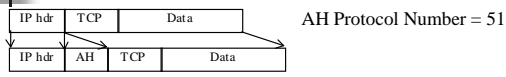
---

---

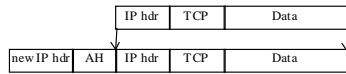
---

---

## AH Formatting



Transport mode



Tunnel mode

Next Header	Length (8)	Reserved (16)
Security Parameters Index (32)		
Sequence Number Field (32)		
Authentication Data (N*32)		

SN: for replay detection

CSG254: Network Security

IPsec - IKE

---

---

---

---

---

---

---

---

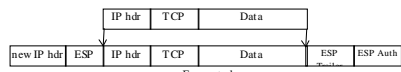
## ESP Formatting



← Encrypted →

← Authenticated →

Transport mode



← Encrypted →

← Authenticated →

Tunnel mode

CSG254: Network Security

IPsec - IKE

---

---

---

---

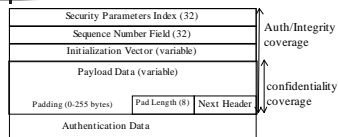
---

---

---

---

## ESP Header



CSG254: Network Security

IPsec - IKE

---

---

---

---

---

---

---

---

## Issues

- NAT boxes:
  - IPsec tunnel mode doesn't easily work
- Firewalls
  - IPsec encrypts information used by firewalls to filter traffic (e.g., port number)
- AH mutable/immutable/predictable fields:
  - Some fields get modified by the intermediate routers and can't be protected by the AH
  - Mutable: type of service, flags, fragment offset, TTL, header checksum
  - Why is PAYLOAD-LENGTH considered immutable (even if packets can be fragmented)? Why not fragment offset. Inconsistency!
  - Mutable but predictable fields are included in the AH computation using their expected value at the destination (e.g., destination address even when using source routing)

CSG254: Network Security

IPsec - IKE

---

---

---

---

---

---

---

---

## IPsec: Internet Key Exchange

- Goal:
  - Mutual authentication and establishment of a shared secret session key using:
    - Pre-shared secret key or public signature-only key, or public encryption key
  - Negotiation of features and cryptographic algorithms
- Specification documents:
  - ISAKMP (Internet Security Association and Key Management Protocol): RFC 2408
  - IKE: RFC 2409
  - DOI (Domain Of Interpretation): RFC 2407

CSG254: Network Security

IPsec - IKE

---

---

---

---

---

---

---

---

## Photuris

- Photuris goal: signed Diffie-Hellman exchange
  1.  $A \rightarrow B: C_A$
  2.  $B \rightarrow A: C_B, C_D$  crypto offered
  3.  $A \rightarrow B: C_B, C_D, g^a \text{ mod } p$ , crypto selected
  4.  $B \rightarrow A: C_B, C_D, g^b \text{ mod } p$
  5.  $A \rightarrow B: C_B, C_D, g^{ab} \text{ mod } p$ {A, signature on previous message}
  6.  $B \rightarrow A: C_B, C_D, g^{ab} \text{ mod } p$ {B, signature on previous message}
  - Role of  $C_A, C_B$ , and messages
  - Additional features: SPI selection
  - Why not sign messages 3 & 4...?

CSG254: Network Security

IPsec - IKE

---

---

---

---

---

---

---

---

## Simple Key-Management for Internet Protocol (SKIP)

- Uses long term Diffie-Hellman keys
- Parties assumed to know each other public keys (i.e.,  $g^p$  mod  $p$ ) or exchange certificates
- Session key  $X = g^{ab}$  mod  $p$  is established in 0 messages
- Each packet is encrypted using data key  $S$  and each packet contains:  $X\{S\}$ 
  - Same  $S$  can be used for several packets
- Later on PFS was added by periodically forgetting the keys and doing a new DH

CSG254: Network Security

IPsec - IKE

---

---

---

---

---

---

---

---

## ISAKMP (RFC2408)

- Proposed by NSA as a framework and accepted by IETF
  - Runs over UDP and allows to exchange fields to create a protocol
- IKE (RFC2409) based on OAKLEY & SKEME using ISAKMP syntax
- IKE phases:
  1. Mutual authentication and session key establishment (also called ISAKMP SA or IKE SA)
  2. AH/ESP SAs establishment
- Each source/destination/port has its own SA/keys otherwise ESP traffic not using integrity could be decrypted...

CSG254: Network Security

IPsec - IKE

---

---

---

---

---

---

---

---

## Phase 1 IKE

- Two modes:
  - Aggressive mode: mutual authentication and session key establishment in three messages
    - $A \rightarrow B$ :  $g^a$  mod  $p$ ,  $A$ , crypto proposal
    - $B \rightarrow A$ :  $g^b$  mod  $p$ , crypto choice, proof I'm  $B$
    - $A \rightarrow B$ : proof I'm  $A$
  - Main: additional features such as hiding end-points identities and negotiating crypto DH algorithm
    - $A \rightarrow B$ : crypto suite I support
    - $B \rightarrow A$ : crypto suite I choose
    - $A \rightarrow B$ :  $g^a$  mod  $p$
    - $B \rightarrow A$ :  $g^b$  mod  $p$
    - $A \rightarrow B$ :  $g^{ab}$  mod  $p$  ( $A$ , proof I'm  $A$ )
    - $B \rightarrow A$ :  $g^{ab}$  mod  $p$  ( $B$ , proof I'm  $B$ )

CSG254: Network Security

IPsec - IKE

---

---

---

---

---

---

---

---

## Phase 1 IKE

- Key types:
  - Pre-shared secret key
  - Public encryption key: fields are separately encrypted using the public key
  - Optimized public encryption key: used to encrypt a random symmetric key, and then data is encrypted using the symmetric key
  - Public signature key: used only for signature purpose
- ⇒ 8 variants of IKE phase 1: 2 modes x 4 key types
- Proof of Identity:
  - Required in messages 2-3 aggressive mode and 5-6 main mode
  - Proves the sender knows the key associated with the identity
  - Depends on the key type
  - Hash of identity key, DH values, nonces, crypto choices, cookies
  - Alternative: MAC of previous messages

CSG254: Network Security

IPsec - IKE

---

---

---

---

---

---

---

---

## Phase 1 IKE

- Negotiating cryptographic parameters:
  - A specifies suites of acceptable algorithms:
    - {(DES, MD5, RSA public key encryption, DH), (AES, SHA, pre-shared key, elliptic curve), ...}
  - The standard specifies a MUST be implemented set of algorithms:
    - Encryption=DES, hash=MD5/SHA, authentication=pre-shared key/DH
  - The lifetime of the SA can also be negotiated
- Session keys:
  - Key seed: SKEYID
    - Signature public keys:  $SKEYID = \text{prf}(\text{nonces}, g^v \text{ mod } p)$
    - Encryption public keys:  $\text{prf}(\text{hash}(\text{nonces}), \text{cookies})$
    - Pre-shared secret key:  $\text{prf}(\text{pre-shared secret key}, \text{nonces})$
  - Secret to generate other keys:  $SKEYID\_d = \text{prf}(SKEYID, (g^v, \text{cookies}, 0))$
  - Integrity key:  $SKEYID\_a = \text{prf}(SKEYID, (SKEYID\_d, (g^v, \text{cookies}, 1)))$
  - Encryption key:  $SKEYID\_e = \text{prf}(SKEYID, (SKEYID\_a, (g^v, \text{cookies}, 2)))$
- Message IDs:
  - Random 32-bits serves the purpose of a SN but in an inefficient manner because they have to be remembered

CSG254: Network Security

IPsec - IKE

---

---

---

---

---

---

---

---

## IKE Phase 1: Public Signature Keys, Main Mode

- Description:
  - Both parties have public keys for signatures
  - Hidden endpoint identity (except for ...?)
- Protocol:
  - A → B: CP
  - B → A: CPA
  - A → B:  $g^a \text{ mod } p, \text{ nonce}_a$
  - B → A:  $g^b \text{ mod } p, \text{ nonce}_b$
  - $K = \mathcal{K}(g^{ab} \text{ mod } p, \text{ nonce}_a, \text{ nonce}_b)$
  - A → B:  $K\{A, \text{proof I'm } A, [\text{certificate}]\}$
  - B → A:  $K\{B, \text{proof I'm } B, [\text{certificate}]\}$
- Questions:
  - What is the purpose of the nonces?
  - Can we make to protocol shorter (5 messages)? At what expense?

CSG254: Network Security

IPsec - IKE

---

---

---

---

---

---

---

---

### IKE Phase 1: Public Signature Keys, Aggressive Mode

- Protocol:
  - $A \rightarrow B$ :  $CP, g^a \text{ mod } p, \text{nonce}_A, A$
  - $B \rightarrow A$ :  $CPA, g^b \text{ mod } p, \text{nonce}_B, B, \text{proof I'm } B, [\text{certificate}]$
  - $A \rightarrow B$ : proof I'm  $A, [\text{certificate}]$

CSG254: Network Security

IPsec - IKE

---

---

---

---

---

---

---

---

### IKE Phase 1: Public Encryption Keys, Main Mode, Original

- Protocol:
  - $A \rightarrow B$ :  $CP$
  - $B \rightarrow A$ :  $CPA$
  - $A \rightarrow B$ :  $g^a \text{ mod } p, \{\text{nonce}_A\}_B, \{A\}_B$
  - $B \rightarrow A$ :  $g^b \text{ mod } p, \{\text{nonce}_B\}_A, \{B\}_A$
  - $K = f(g^{ab} \text{ mod } p, \text{nonce}_A, \text{nonce}_B)$
  - $A \rightarrow B$ :  $K\{\text{proof I'm } A\}$
  - $B \rightarrow A$ :  $K\{\text{proof I'm } B\}$

CSG254: Network Security

IPsec - IKE

---

---

---

---

---

---

---

---

### IKE Phase 1: Public Encryption Keys, Aggressive Mode, Original

- Protocol:
  - $A \rightarrow B$ :  $CP, g^a \text{ mod } p, \{\text{nonce}_A\}_B, \{A\}_B$
  - $B \rightarrow A$ :  $CPA, g^b \text{ mod } p, \{\text{nonce}_B\}_A, \{B\}_A, \text{proof I'm } B$
  - $A \rightarrow B$ : proof I'm  $A$

CSG254: Network Security

IPsec - IKE

---

---

---

---

---

---

---

---

### IKE Phase 1: Public Encryption Keys, Main Mode, Revised

- Protocol:
  - $A \rightarrow B$ :  $CP$
  - $B \rightarrow A$ :  $CPA$
  - $K_A = \text{hash}(\text{nonce}_{A'} \text{ cookie}_A)$
  - $A \rightarrow B$ :  $\{\text{nonce}_{A'}\}_B, K_A\{g^a \text{ mod } p\}, K_A\{A\}, [K_A\{A\} \text{ cert}]$
  - $K_B = \text{hash}(\text{nonce}_{B'} \text{ cookie}_B)$
  - $B \rightarrow A$ :  $\{\text{nonce}_{B'}\}_A, K_B\{g^b \text{ mod } p\}, K_B\{B\}$
  - $K = f(g^{ab} \text{ mod } p, \text{nonce}_{A'}, \text{nonce}_{B'}, \text{cookie}_{A'}, \text{cookie}_{B'})$
  - $A \rightarrow B$ :  $K\{\text{proof I'm } A\}$
  - $B \rightarrow A$ :  $K\{\text{proof I'm } B\}$

CSG254: Network Security

IPsec - IKE

---

---

---

---

---

---

---

---

### IKE Phase 1: Public Encryption Keys, Aggressive Mode, Revised

- Protocol:
  - $K_A = \text{hash}(\text{nonce}_{A'} \text{ cookie}_A)$
  - $A \rightarrow B$ :  $CP, \{\text{nonce}_{A'}\}_B, K_A\{g^a \text{ mod } p\}, K_A\{A\}, [K_A\{A\} \text{ cert}]$
  - $K_B = \text{hash}(\text{nonce}_{B'} \text{ cookie}_B)$
  - $B \rightarrow A$ :  $CPA, \{\text{nonce}_{B'}\}_A, K_B\{g^b \text{ mod } p\}, K_B\{B\}, \text{proof I'm } B$
  - $K = f(g^{ab} \text{ mod } p, \text{nonce}_{A'}, \text{nonce}_{B'}, \text{cookie}_{A'}, \text{cookie}_{B'})$
  - $A \rightarrow B$ :  $K\{\text{proof I'm } A\}$

CSG254: Network Security

IPsec - IKE

---

---

---

---

---

---

---

---

### IKE Phase 1: Shared Secret Keys, Main Mode

- Assumption  $A$  and  $B$  share a secret  $J$
- Protocol:
  - $A \rightarrow B$ :  $CP$
  - $B \rightarrow A$ :  $CPA$
  - $A \rightarrow B$ :  $g^a \text{ mod } p, \text{nonce}_{A'}$
  - $B \rightarrow A$ :  $g^b \text{ mod } p, \text{nonce}_{B'}$
  - $K = f(J, g^{ab} \text{ mod } p, \text{nonce}_{A'}, \text{nonce}_{B'}, \text{cookie}_{A'}, \text{cookie}_{B'})$
  - $A \rightarrow B$ :  $K\{\text{proof I'm } A\}$
  - $B \rightarrow A$ :  $K\{\text{proof I'm } B\}$

CSG254: Network Security

IPsec - IKE

---

---

---

---

---

---

---

---

## IKE Phase 1: Shared Secret Keys, Aggressive Mode

- Protocol:
  - $A \rightarrow B$ :  $CP, g^a \text{ mod } p, \text{nonce}_A, A$
  - $B \rightarrow A$ :  $CPA, g^b \text{ mod } p, \text{nonce}_B, B, \text{proof I'm } B$
  - $A \rightarrow B$ : proof I'm  $A$

CSG254: Network Security

IPsec - IKE

---

---

---

---

---

---

---

---

## IKE: Phase 2

- Also known as "Quick Mode": 3- messages protocol
  - $A \rightarrow B$ :  $X, Y, CP, \text{traffic}, SPI_A, \text{nonce}_A, [g^a \text{ mod } p]_{\text{optional}}$
  - $B \rightarrow A$ :  $X, Y, CPA, \text{traffic}, SPI_B, \text{nonce}_B, [g^b \text{ mod } p]_{\text{optional}}$
  - $A \rightarrow B$ :  $X, Y, \text{ack}$
- All messages are encrypted using SKEYID\_e, and integrity protected using SKEYID\_a (except  $X, Y$ )
- Parameters:
  - $X$ : pair of cookies generated during phase 1
  - $Y$ : 32-bit number unique to this phase 2 session chosen by the initiator
  - CP: Crypto Proposal, CPA: Crypto Proposal Accepted
  - DH is optional and could be used to provide PFS
  - Nonces and cookies get shuffled into SKEYID to produce the SA encryption and integrity keys

CSG254: Network Security

IPsec - IKE

---

---

---

---

---

---

---

---