

ISA 666 Internet Security Protocols

IPSEC Key Management Wireless Security

ISA 666

By Dr. Xinyuan (Frank) Wang

1

Outline

- Key management
 - Security principles
 - Center-based key management
 - Peer-to-peer key management
- Internet key management
 - Manual exchange
 - SKIP
 - Oakley
 - ISAKMP
- Internet Key Exchange (IKE)

ISE at George Mason University

ISA 666 By Dr. Xinyuan (Frank) Wang

2

Key Management

- Why do we need key management
 - IPSEC SA needs keys
 - AH authentication key
 - ESP encryption key
 - What if key expires?
 - What if SA terminates?
 - What if the initiator and responder support different crypto algorithms or different key lengths?
- Need process to negotiate and establish IPSEC SA's between two entities
 - Handle key generation, distribution, extension.

ISE at George Mason University

ISA 666 By Dr. Xinyuan (Frank) Wang

3

Security Principles

- Basic security principle for session keys
 - Compromise of a session key
 - Doesn't compromise future session keys and long-term keys
 - The compromised session key could not be reused
- **Perfect forward secrecy (PFS)**
 - Compromise of current keys (session key or long-term key) does not compromise past session keys.
 - Concern for encryption key rather than authentication key
 - Not really "perfect" in the same sense as perfect secrecy for one-time pad.

ISE at George Mason University

ISA 666 By Dr. Xinyuan (Frank) Wang

4

Center-Based Key Management

- Key distribution center (KDC)
 - Communication parties depend on KDC to establish a pair-wise key
 - The KDC generates the cryptographic keys for the two entities
 - Pull based
 - Alice communicates with the KDC before she communicates with Bob
 - Push based
 - Alice communicates with Bob, and it's Bob's responsibility to contact the KDC to get the pair-wise key

ISE at George Mason University

ISA 666 By Dr. Xinyuan (Frank) Wang

5

Center-Based Key Management (Cont'd)

- Key translation center (KTC)
 - Similar to KDC
 - Difference
 - One of the participants generates the cryptographic; KTC only translates and forwards it to the other participant

ISE at George Mason University

ISA 666 By Dr. Xinyuan (Frank) Wang

6

Peer to Peer Key Management (Cont'd)

- Both communicating parties are involved in the key exchange, and reach agreement on key collaboratively
 - Example: Diffie-Hellman key exchange
 - Most peer-to-peer key management schemes are based on Diffie-Hellman key exchange with improvements

Internet Key Management

- Three major competing proposals
 - Photuris
 - Ephemeral D-H + authentication + cookie
 - The first to use cookie to thwart DoS attack
 - Simple Key Management for Internet Protocols (SKIP)
 - Proposed by Sun Microsystems, connectionless
 - ISAKMP (RFC-2408)
 - Proposed by NSA, a framework for key management and policy negotiation
 - Oakley (RFC-2412), authenticated D-H, work with ISAKMP
 - Skeme
 - IKE (RFC-2409)

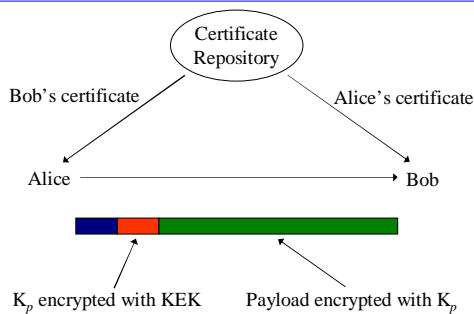
Manual Key Management

- Mandatory
- Useful when IPSEC developers are debugging
- Keys exchanged offline (phone, email, etc.)
- Setup SPI and negotiate parameters

SKIP

- Idea
 - IP is connectionless in nature
 - Use session-less key establishment
 - Does not establish SA
 - Packet-specific encryption key is included in each packet
 - Good for connectionless applications, but not for connection-oriented application (too much overhead)

SKIP (Cont'd)



SKIP (Cont'd)

- KEK should be changed periodically
 - Minimize the exposure of KEK
 - Prevent the reuse of compromised keys
- SKIP's approach
 - $KEK = h(K_{AB}, n)$, where h is a one-way hash function, where K_{AB} is the long-term key between A and B, and n is a counter.

SKIP (Cont'd)

- Limitations
 - No Perfect Forward Secrecy
 - Can be modified to provide PFS, but it will lose the sessionless property
 - No concept of SA; difficult to work with current IPSEC architecture
- Not the standard, but remains as an alternative

Oakley

- Oakley is a refinement of the basic Diffie-Hellman key exchange protocol
- What refinement?
 - Resource Clogging Attack
 - Replay attack
 - Man-in-the-middle attack
 - Choice of D-H groups

Resource Clogging Attack

- Attacker can send many bogus requests – with spoofed IP source address
 - Flood the stateful server
- Stopping requests is difficult
 - We need to provide services
- Ignoring requests is dangerous
 - Denial of service attacks

Resource Clogging Attack (Cont'd)

- Countermeasure
 - Cookie
 - Each side sends a pseudo-random number, the cookie, in the initial message, which the other side acknowledges
 - The acknowledgement must be repeated in the following messages
 - Do not begin D-H calculation until getting right acknowledgement from the other side
 - Cookies are used to thwart resource clogging attack
 - Thwart, not prevent

Requirements for Cookie Generation

- The cookie must depend on the specific parties
 - Prevent attacker from reusing cookies
- Impossible to forge
 - Use secret values
- Efficient
- Cookies are also used for key naming
 - Each key is uniquely identified by the initiator's cookie and the responder's cookie
 - Why?

Replay Attack

- The attacker can simply eavesdrop communication, record the cookie, and replay the cookie
- Countermeasure
 - Use nonce

Man-in-the-Middle-Attack

- The attacker can impersonate Alice to Bob and Bob to Alice at the same time
 - Alice thinks she is talking to Bob
 - Bob thinks he is talking to Alice
- Countermeasures
 - Authentication
 - Preshared secret key
 - Public key certificate

Oakley Groups

- 0 no group (placeholder)
- 1 MODP, 768-bit prime p , $g=2$
- 2 MODP, 1024-bit prime p , $g=2$
- 3 EC2N, 155-bit field size
- 4 EC2N, 185-bit field size
- 5 MODP, 1536 bit prime p , $g=2$
- Private group can be used

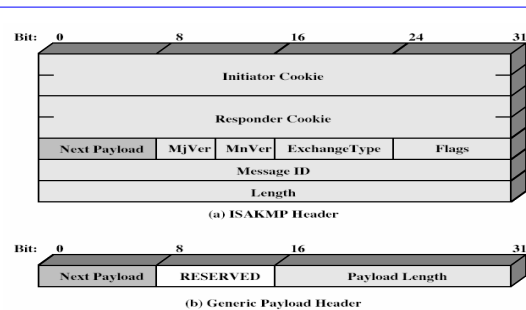
ISAKMP/Oakley

- ISAKMP
 - Security association and key management protocol
 - Define procedures and packet formats to establish, negotiate, modify and delete SAs
 - Defines payloads for security association
 - Independent from key exchange protocol, encryption algorithm and authentication method
- Oakley
 - Key exchange protocol
 - Developed for use with ISAKMP
 - Default for IPSEC key exchange

ISAKMP Message

- Fixed format header
 - 64 bit initiator and responder cookies
 - 8 bit exchange type
 - 8 bit next payload type
 - Flags: encryption, commit, authentication, etc.
 - 32 bit message ID
 - Resolve multiple phase 2 SAs being negotiated simultaneously
 - Variable number of payloads
 - Each has a generic header with
 - Payload boundaries
 - Next payload type (possible none)

ISAKMP Header



ISAKMP Phases

- Phase 1
 - Establish ISAKMP SA to protect further ISAKMP exchanges
 - Or use pre-established ISAKMP SA
 - ISAKMP SA identified by initiator cookie and responder cookie
- Phase 2
 - Negotiate security services in SA for target security protocol or application

ISAKMP

- Disadvantage
 - Additional overhead due to 2 phases
- Advantages
 - Same ISAKMP SA can be used to negotiate phase 2 for multiple protocols
 - ISAKMP SA can be used to facilitate maintenance of SAs

ISAKMP Domain of Interpretation (DOI)

- DOI defines
 - Payload format
 - Exchange types
 - Naming conventions for security policies, cryptographic algorithms
- DOI for IPSEC has been defined

IKE Overview

- IKE = ISAKMP + part of Oakley + part of SKEME
- A separate RFC (2409) has been published for IKE
- Request-response protocol
 - Initiator
 - Responder
- Two phases
 - Phase 1: establish an IKE (ISAKMP) SA
 - Essentially ISAKMP phase 1
 - Bi-directional
 - Phase 2: use the IKE SA to establish IPSEC SAs
 - Key exchange phase
 - Unidirectional

IKE Overview (cont'd)

- Several modes
 - Phase 1:
 - Main mode: 6 messages
 - Aggressive mode: 3 messages
 - Phase 2
 - Quick mode: 3 messages
 - Other modes
 - New group mode
 - Not in phase 1 or 2; follows phase 1
 - Establish a new group to use in future negotiation
 - Informational exchanges
 - ISAKMP notify payload
 - ISAKMP delete payload

IKE Phase 1

- Four types of keys for mutual authentication
 - Digital signature
 - Public key encryption
 - Public key encryption, revised
 - Pre-shared secret
- Eight variants of IKE Phase 1

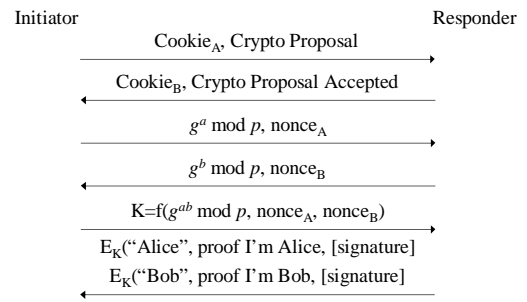
IKE Phase 1 (cont'd)

- IKE phase 1 goal:
 - Establish a shared secret SKEYID
 - With digital signature authentication
 - $SKEYID = \text{prf}(Ni_b | Nr_b, g^{xy})$
 - With public key encryption authentication
 - $SKEYID = \text{prf}(\text{hash}(Ni_b | Nr_b), CKY-I | CKY-R)$
 - With pre-share key authentication
 - $SKEYID = \text{prf}(\text{pre-shared-key}, Ni_b | Nr_b, g^{xy})$
 - Notations:
 - Prf: pseudo random function
 - CKY-I/CKY-R: I's (or R's) cookie
 - Ni_b/Nr_b: the body of I's (or R's) nonce

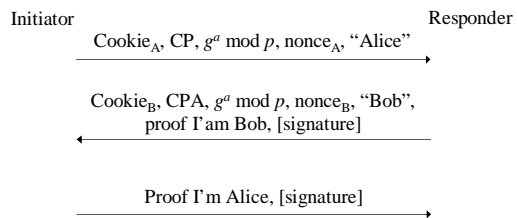
IKE Phase 1 (cont'd)

- Three groups of keys
 - Derived key for non-ISAKMP negotiations
 - $SKEYID_d = \text{prf}(SKEYID, g^{xy} \text{ mod } p | CKY-I | CKY-R | 0)$
 - Authentication key
 - $SKEYID_a = \text{prf}(SKEYID, SKEYID_d, g^{xy} \text{ mod } p | CKY-I | CKY-R | 1)$
 - Encryption key
 - $SKEYID_e = \text{prf}(SKEYID, SKEYID_a, g^{xy} \text{ mod } p | CKY-I | CKY-R | 2)$

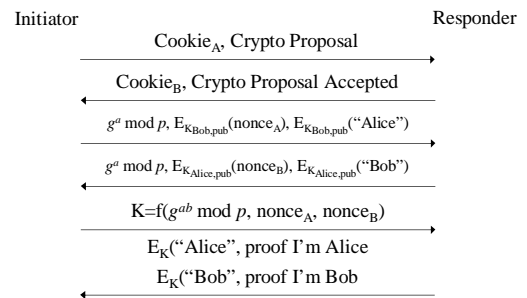
IKE Phase 1 Digital Signature, Main Mode



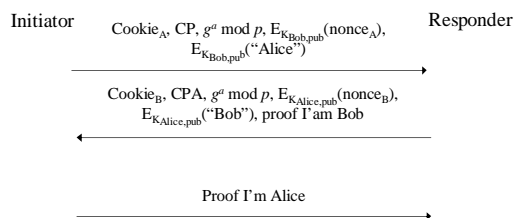
IKE Phase 1 Digital Signature, Aggressive Mode



IKE Phase 1 Public Encryption Key, Main Mode



IKE Phase 1 Public Encryption Key, Aggressive Mode



IKE Phase 1

- Public key encryption, revised, main mode
- Public key encryption, revised, aggressive mode
- Pre-shared key, main mode
- Pre-shared key, aggressive mode

IKE Phase 2 – Quick Mode

- Not a complete exchange itself
 - Based on phase 1 exchange
- Used to derive keys for IPSEC SAs
- Information exchange with quick mode must be protected by ISAKMP SA established in Phased 1
- Essentially a SA negotiation and an exchange of nonces
 - Generate fresh keys
 - Prevent replay attack

Wireless LAN Security

- Wireless LAN 802.11
 - Concepts and standards.
 - Current security services
 - Known threats and vulnerabilities.
 - Security improvements

Wireless LAN Standards

- IEEE ratified 802.11 in 1997.
 - Also known as Wi-Fi.
- 802.11 provides Layer 1 & Layer 2 of OSI model.
 - Physical layer
 - Data link layer
- Wireless LAN at 1 Mbps & 2 Mbps.
- Wi-Fi Alliance formed to promote interoperability.
- 802.11b ratified in 1999 adding 5.5 Mbps and 11 Mbps.

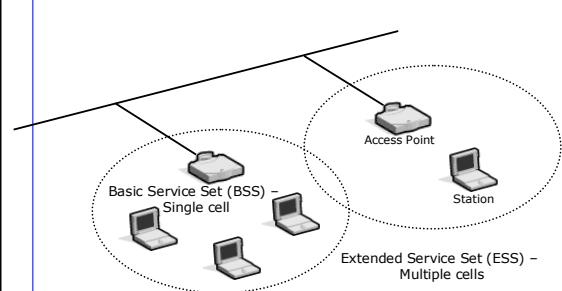
Wireless LAN Standards (Cont'd)

- 802.11a
 - Ratified 2001
 - 5 Ghz radio spectrum.
 - Maximum speed 54 Mbps.
 - In practice about 20Mbps
 - More energy efficient, less battery drain, better range
- 802.11g
 - Ratified June 2003
 - 2.4Ghz spectrum again
 - Maximum speed 54 Mbps
 - In practice from 10 to 20Mbps

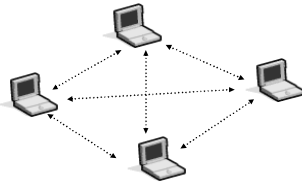
802.11 Modes

- Infrastructure mode
 - Basic Service Set
 - One access point
 - Extended Service Set
 - Two or more BSSs forming a single subnet.
 - Most corporate LANs in this mode.
- Ad-hoc mode
 - Also called peer-to-peer.
 - Independent Basic Service Set
 - Set of 802.11 wireless stations that communicate directly without an access point.
 - Useful for quick & easy wireless networks.

Infrastructure Mode



Ad-hoc Mode



Independent Basic Service Set (IBSS)

Open System Authentication

- Service Set Identifier (SSID)
- Station must specify SSID to Access Point when requesting association.
- Multiple APs with same SSID form Extended Service Set.
- APs can broadcast their SSID
 - But this can be turned off
- Some 802.11b clients allow * as SSID.
 - Associates with strongest AP regardless of SSID.

MAC Address Based Access Control

- Access points have Access Control Lists (ACL).
- ACL is list of allowed MAC addresses.
 - E.g. Allow access to:
 - 00:01:42:0E:12:1F
 - 00:01:42:F1:72:AE
 - 00:01:42:4F:E2:01
- But MAC addresses are sniffable and spoofable.
- Access Point ACLs are ineffective control.

Further issues

- Access Point configuration
 - Mixtures of SNMP, web, serial, telnet.
 - Community strings, default passwords.
- Evil Twin Access Points
 - Stronger signal, capture user authentication.
- Hub broadcasts
 - If AP connected to hub, all broadcasts transmitted.
- Renegade Access Points
 - Unauthorised wireless LANs.

802.11b Security Services

- Two security services provided:
 - Authentication
 - Shared Key Authentication
 - Encryption
 - Wired Equivalence Privacy (WEP)

Wired Equivalence Privacy

- Shared key between
 - Wireless stations.
 - An Access Point.
- Extended Service Set
 - All Access Points will have same shared key.
- No key management
 - Shared key entered manually into
 - Stations
 - Access points
 - Key management nightmare in large wireless LANs

RC4

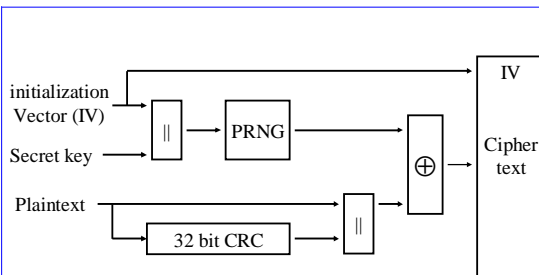
- Ron's Code number 4
 - Symmetric key encryption
 - RSA Security Inc.
 - Designed in 1987.
 - Trade secret until leak in 1994.
- RC4 can use key sizes from 1 bit to 2048 bits.
- RC4 generates a stream of pseudo random bits
 - XORed with plaintext to create ciphertext.



WEP – Sending

- Compute Integrity Check Vector (ICV).
 - Provides integrity
 - 32 bit Cyclic Redundancy Check.
 - Appended to message to create plaintext.
- Plaintext encrypted via RC4
 - Provides confidentiality.
 - Plaintext XORed with long key stream of pseudo random bits.
 - Key stream is function of
 - 40-bit secret key
 - 24 bit initialization vector
- Ciphertext is transmitted.

WEP Encryption



WEP – Receiving

- Ciphertext is received.
- Ciphertext decrypted via RC4
 - Ciphertext XORed with long key stream of pseudo random bits.
 - Key stream is function of
 - 40-bit secret key
 - 24 bit initialization vector (IV)
- Check ICV
 - Separate ICV from message.
 - Compute ICV for message
 - Compare with received ICV

Shared Key Authentication

- When station requests association with Access Point
 - AP sends random number to station
 - Station encrypts random number
 - Uses RC4, 40 bit shared secret key & 24 bit IV
 - Encrypted random number sent to AP
 - AP decrypts received message
 - Uses RC4, 40 bit shared secret key & 24 bit IV
 - AP compares decrypted random number to transmitted random number
- If numbers match, station has shared secret key.

WEP Safeguards

- Shared secret key required for:
 - Associating with an access point.
 - Sending data.
 - Receiving data.
- Messages are encrypted.
 - Confidentiality.
- Messages have checksum.
 - Integrity.
- But SSID still broadcast in clear.

Initialization Vector

- IV must be different for every message transmitted.
- 802.11 standard doesn't specify how IV is calculated.
- Wireless cards use several methods
 - Some use a simple ascending counter for each message.
 - Some switch between alternate ascending and descending counters.
 - Some use a pseudo random IV generator.

WEP attacks

- Statistical attack
 - If 24 bit IV is an ascending counter,
 - If Access Point transmits at 11 Mbps,
 - All IVs are exhausted in roughly 5 hours.
- Passive attack:
 - Attacker collects all traffic
 - Attacker could collect two messages:
 - Encrypted with same key and same IV
 - So XORed with same key stream
 - Ciphertext 1 XOR Ciphertext 2 = Plaintext 1 XOR Plaintext 2
 - Statistical attacks to reveal plaintext
 - More than two messages with same key and same IV...

More WEP attacks

- If attacker knows plaintext and ciphertext pair
 - Key is known.
 - Attacker can create correctly encrypted messages.
 - Access Point is deceived into accepting messages.

Limited WEP keys

- Some vendors allow limited WEP keys
 - User types in a password
 - WEP key is generated from passphrase
 - Passphrases creates only 21 bits of entropy in 40 bit key.
 - Reduces key strength to 21 bits = 2,097,152
 - Remaining 19 bits are predictable.
 - 21 bit key can be brute forced in minutes.
 - <http://www.lava.net/~newsham/wlan/>

Brute Force Key Attack

- Capture ciphertext.
 - IV is included in message.
- Search all 2^{40} possible secret keys.
 - 1,099,511,627,776 keys
 - ~100 days on a modern machine
- Find which key decrypts ciphertext to plaintext.

128 bit WEP

- Vendors have extended WEP to 128 bit keys.
 - 104 bit secret key.
 - 24 bit IV.
- Brute force takes 10^{19} years for 104-bit key.
- Effectively safeguards against brute force attacks.

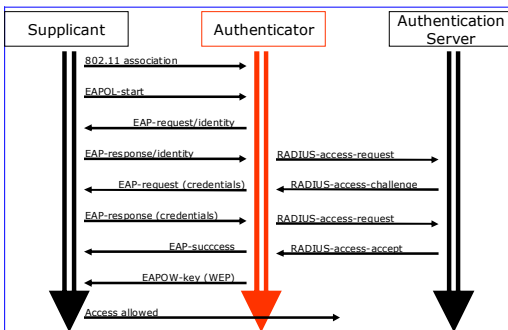
Wireless as Untrusted LAN

- Treat wireless as untrusted.
 - Similar to Internet.
- Firewall between WLAN and Backbone.
- Extra authentication required.
- Intrusion Detection
 - at WLAN / Backbone junction.
- Vulnerability assessments

802.1x Access Control for WLAN

- 802.1x (IEEE)
 - Data link layer protocol for port-based network access control
 - Independent of physical layer, so wired or wireless
- Uses EAP (RFC 2284)
 - Extensible Authentication Protocol
 - Allows choice of authentication methods
 - Authentication chosen by peers
 - Access point doesn't care about EAP methods
- Manages user and session WEP keys
 - Session key used for a limited time
 - User key for rekeying session key
- RADIUS server provides authentication service
 - Remote Authentication Dial In User Service
 - RFC 2138

802.11 + 802.1X/EAP



Association and Authentication

- 802.11 association happens first
 - Open authentication
 - Provides access to the AP and allows an IP address to be supplied
- Access beyond the AP is still prohibited
 - AP drops non-EAPOL traffic
- Authentication conversation between supplicant and authentication server
 - Wireless NIC and AP are pass through devices
- After authentication, AP allows traffic through

802.11i / WPA

- Draft standard
- Will apply to 802.11 a, b & g
- Uses 802.1X & EAP as authentication framework
- Temporal Key Integrity Protocol (TKIP)
 - RC4 still used
 - 128 bit temporal key shared with all clients
 - Per-packet key from temporal key, MAC address & 16 bit initialisation vector
 - Temporal key regenerated every 10,000 packets
 - Only firmware upgrade required
- AES
 - AES cipher replaces RC4
 - Will require new hardware