Tutorial Notes

Mobile and Wireless Network Security

Michel Barbeau
Professor

School of Computer Science
Carleton University

October 8, 2003

2nd International Conference on AD-HOC Networks and Wireless (ADHOC-NOW'03)
Montréal, Canada

Contents

Insecurity of Mobile and Wireless Networks

Specific Threats

Wireless support	
Threats	***Methods of attack***
Eavesdropping	Using a radio receiver Using high gain directional antennas
	Interception of traffic on the Distribution System (infrastructure connecting Basic Service Sets, i.e. a WLAN) using sniffers
Unauthorized access/transmission MAC layer misbehavior	Frame injection
	Frame forging
	Jamming (Denial of service attack)
	Joining the WLAN
Identity malleability	Masquerading a valid user by changing the MAC address
Location determination	Networked sensors
Mobility support	
Threats	***Methods of attack***
Replay attack	On registration
Traffic redirection	On smooth handoff
Denial of service attack Hijacking attack	On binding update
Identity malleability	Spoofing
Location determination	Interception of registration messages and binding updates packets
Resource theft	Absence of access control, spoofing

References

- **Security of 802.11**

B. Potter and B. Fleck, 802.11 Security, O'Reilly, 2003.

- **Security flaws of 802.11**

N. Borisov, L. Golberg and D. Wagner, Intercepting Mobile Communications: The Insecurity of 802.11, In: Proceedings of the International Conference on Mobile Computing and Networking, July 2001, pp. 180-189.

R. Housley and W. Arbaugh, Security Problems in 802.11-based Networks, Communications of the ACM, May 2003, Vol. 46, No. 5, pp. 31-34.

N. Cam-Winget, R. Housley, D. Wagner and J. Walker, Security Flaws in 802.11 Data Link Protocols, Communications of the ACM, May 2003, Vol. 46, No. 5, pp. 31-34.

- **Breaking WEP**

S. Fluhrer, I. Mantin and A. Shamir, Weaknesses in the Key Schedule Algorithms of RCA, In: Proceedings of the 4th Annual Workshop on Selected Areas of Cryptography, 2001.

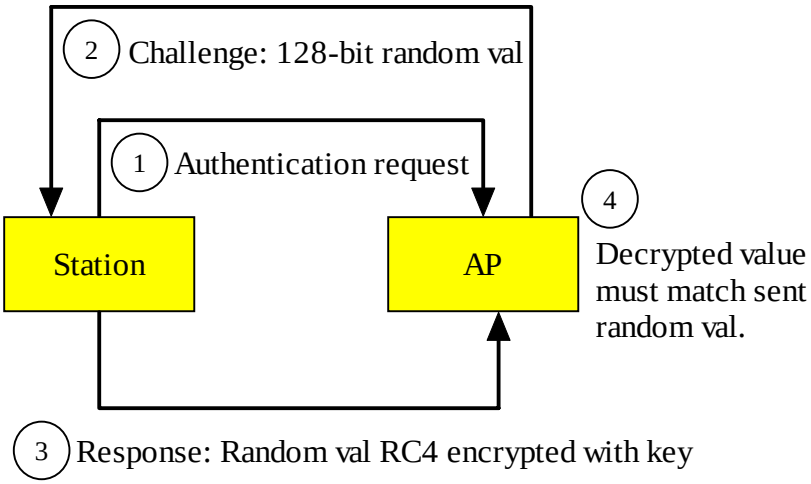
A. Stubblefield, I. Ioannidis and A. Rubin, Using the Fluhrer, Mantin and Shamir Attack to Break WEP, In: Proceedings of the 2002 Network and Distributed Systems Security Symposium, 2002, pp. 17-22.

AirSnort, http://airsnort.shmoo.com

Security and Security Flaws in 802.11

Station authentication during association with an AP

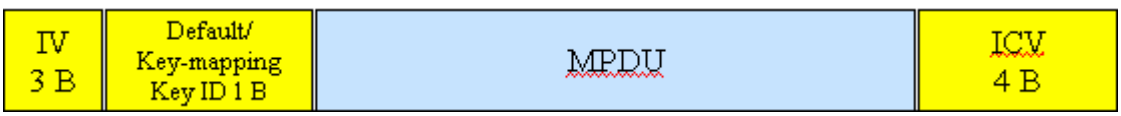
- Uses shared secret: 40-bit key or 104-bit key, distribution of keys is out the scope of 802.11
- Challenge/response exchange
- Easily compromised! Key can be obtained by XOR-ing random val. and its encrypted form



Authentication protocol of 802.11 (simplified)

Content protection

- Uses Wired Equivalent Privacy (WEP) with secret key
- Data is encrypted using IV and Default key or Key-mapping key
- Initialization Vector (IV): 24-bit random val. chosen by transmitter
- Default key: 40- or 104-bit key shared between AP and several stations
- Key-mapping key: 40- or 104-bit key shared between AP and one station
- Encryption: RC4
- Integrity (are frames intact?): CRC-32 Integrity Check Value (ICV)
- An exhaustive search can find the secret key in few hours
- Can be cracked by cryptanalysis [Fluhrer et al. 2001]: e.g. AirSnort



Encryption of Frames

WEP Replacements

IEEE 802.11 Task Group I (TGi), Temporal Key Integrity Protocol (TKIP)

- Interim solution
- A WEP patch for existing hardware: firmware and driver upgrade
- Highlights
  - Message Integrity Code (MIC): Michael, a 64-bit hash (shifts, XORs and additions) value computed from the data and a 64-bit key
  - Defense against replay attacks: 48-bit sequence num.
  - Per-packet RC4 encryption key based on a mixing function:
    - a combination of the 128-bit base key, MAC address and sequence num.
    - key is different from packet to packet, station to station

IEEE 802.11 Task Group I (TGi), Counter-Mode-CBC-MAC Protocol (CCMP)

- Supercedes WEP and TKIP
- 128-bit encryption with Advanced Encryption System (AES) from NIST
- 64-bit Message Integrity Code over the whole MSDU: Cipher Block Chaining Message Authentication Code (CBC-MAC)
- Defense against replay attacks: 48-bit sequence num.

Security in Bluetooth

The Official Bluetooth Website, Specification of the Bluetooth System, Specification Volume 1, Version 1.1, Chapter 14, February 22 2001, www.bluetooth.com.

- Security flaws of Bluetooth 1.0B

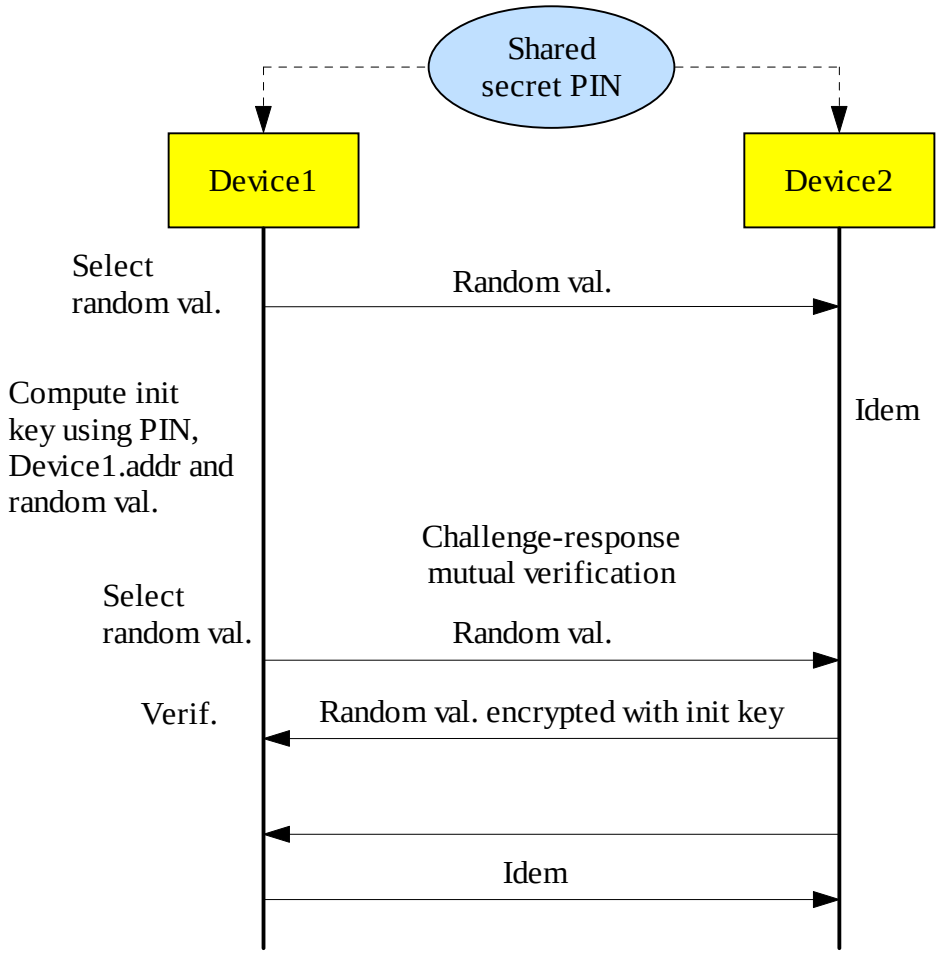
M. Jakobsson and S. Wetzel, Security Weaknesses in Bluetooth, In: D. Naccache(Ed.), CT_RSA 2001, LNCS 2020, 2001, pp. 176-191.

Bluetooth security

- Initialization key establishment protocol
- Link (session) key generation: Two protocols
- Ciphering algorithm

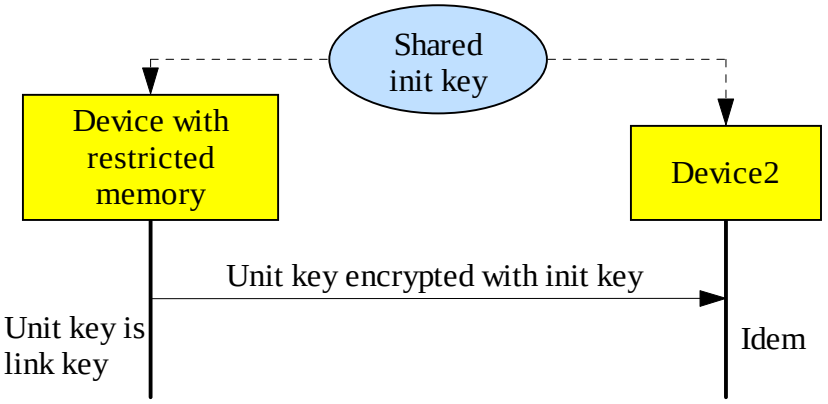
Initialization Key Establishment Protocol (Simplified)

Goal: Create a temporary key that will be used for encryption during the link key generation protocol.

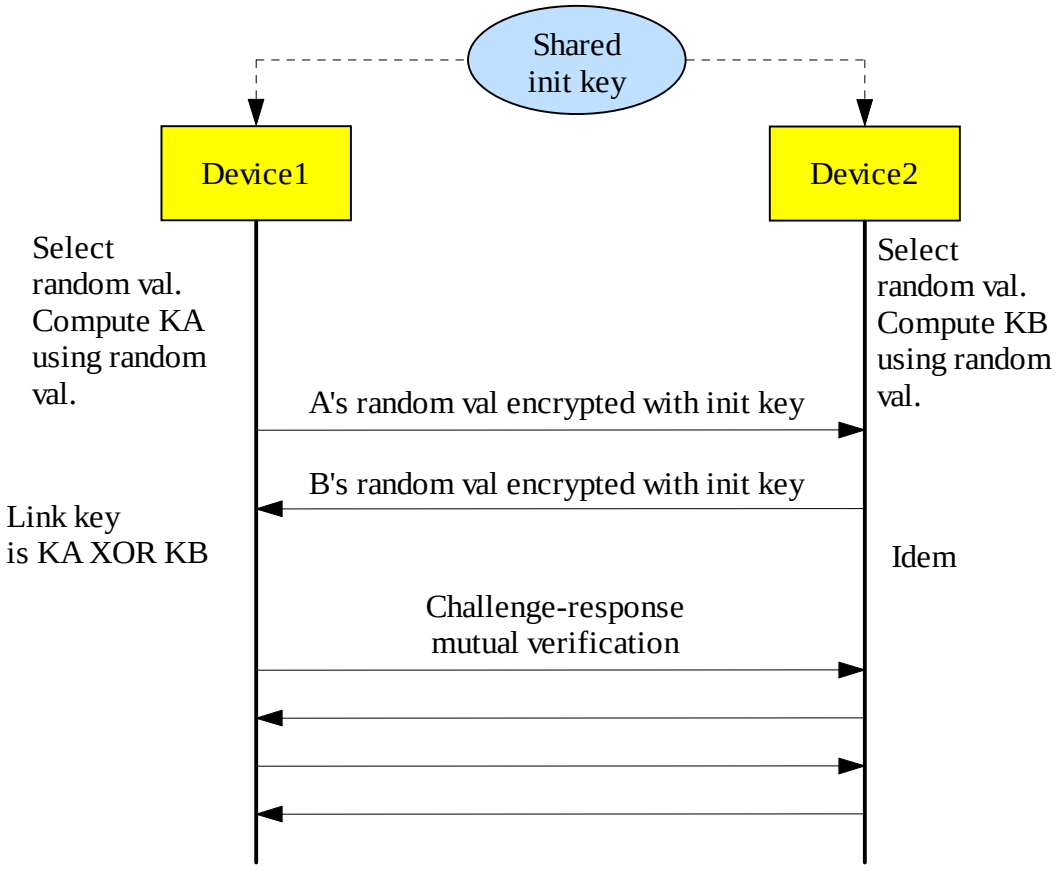


Link Key Generation Protocol 1

Unit key: unique symmetric long-term private key stored in persistent memory

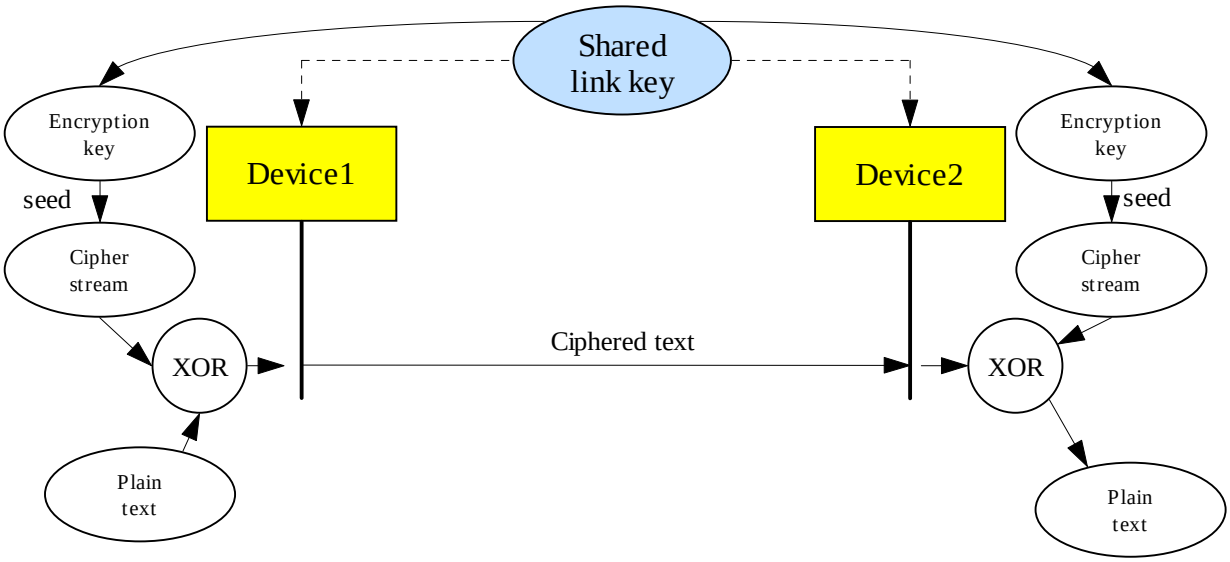


Link Key Generation Protocol 2



Ciphering algorithm (simplified)

Payload encryption only.



Vulnerabilities

Unit/Link/Encryption key disclosure

- Masquerading, eavesdropping, unauthorized access
- Method: exhaustive search, person in the middle attack
- Remedies: long keys (64+ bits), PK, security policies

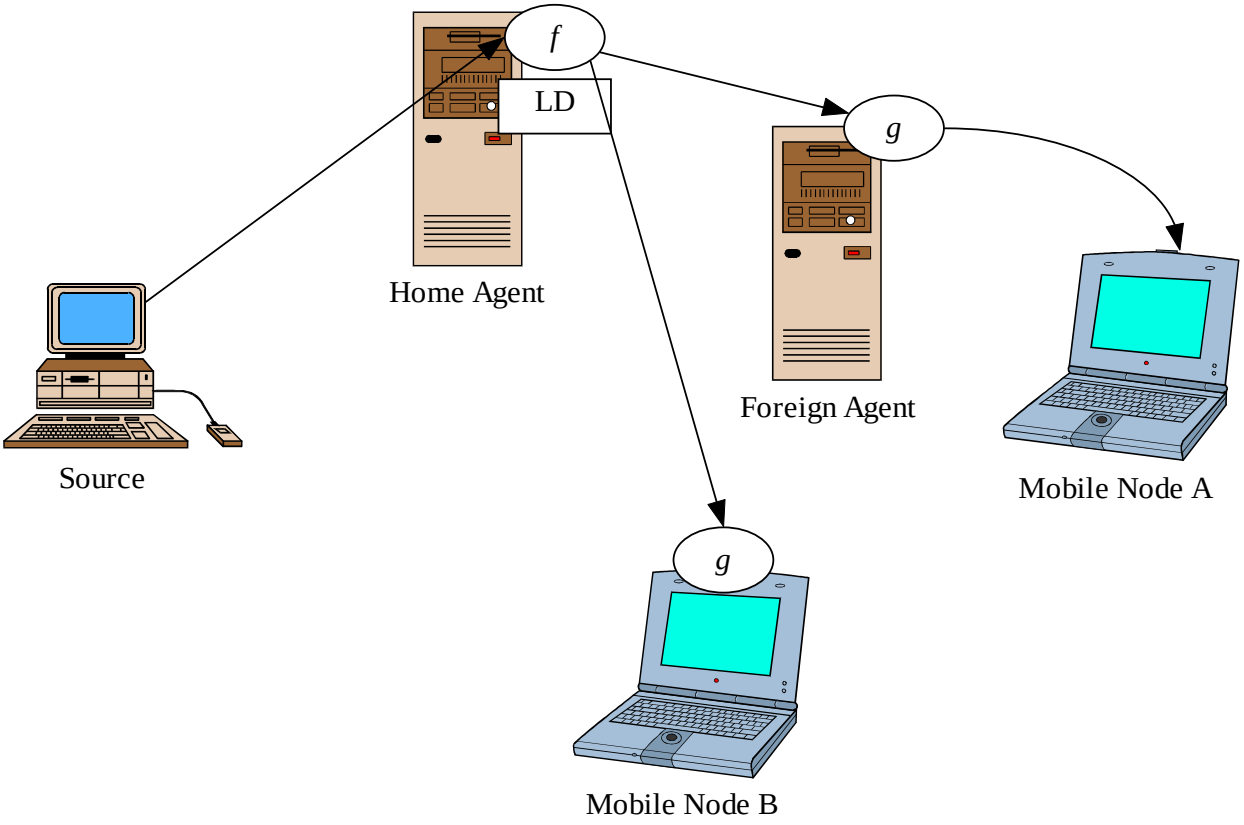
Location determination of a Bluetooth device

- Method: installing a large number of listening nodes/polling nodes (using the discovery protocol)
- Remedies: disable the inquiry mode, device cannot be discovered

Encryption

- If the plaintext sent in one direction is known, the plaintext sent in the other direction can be determined [Jakobsson and Wetzel, 2001].

Overview of Mobile IP



References

- **Replay attack on registration, PKI Authentication at registration**

Sufatrio and K. Y. Lam, Mobile IP Registration Protocol: A Security Attack and New Secure Minimal Public-Key Based Authentication, In: Proceedings of Fourth International Symposium on Parallel Architectures, Algorithms, and Networks (I-SPAN'99), Perth/Fremantle, Australia, 1999, pp. 364-369.

- **HA is a key distribution centre, HA is a key distribution centre**

C.E. Perkins, Mobile IP - Design Principles and Practices, Addison-Wesley Wireless Communications Series, 1998 (Chapter 6)

- **Public Key Infrastructure (PKI)**

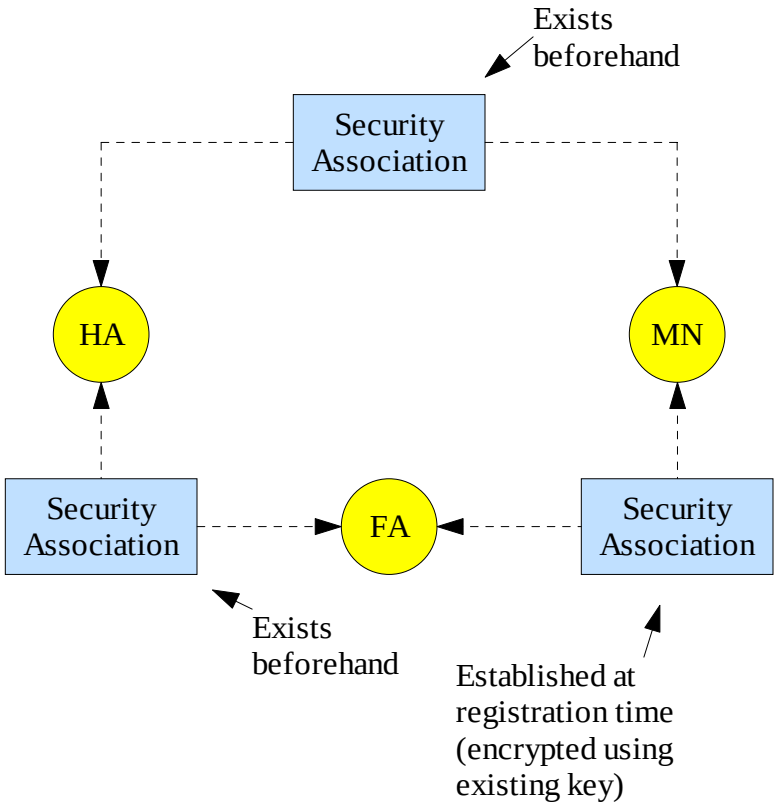
J. Zao, S. Kent, J. Gahm, G. Troxel, M. Condell, P. Helinek, N. Yuan, and I. Castineyra, A Public-Key Based Secure Mobile IP, Wireless Networks, 5 (1999), pp. 373-390.

- **Neither online trusted authority nor certificate repository**

S. Capkun, L. Buttyan, and J.-P. Hubaux, Self-Organized Public-Key Management for Mobile Ad Hoc Networks, IEEE Transactions on Mobile Computing, Vol. 2, No. 1, January-March 2003, pp. 52-64.

Current Security in Mobile IP

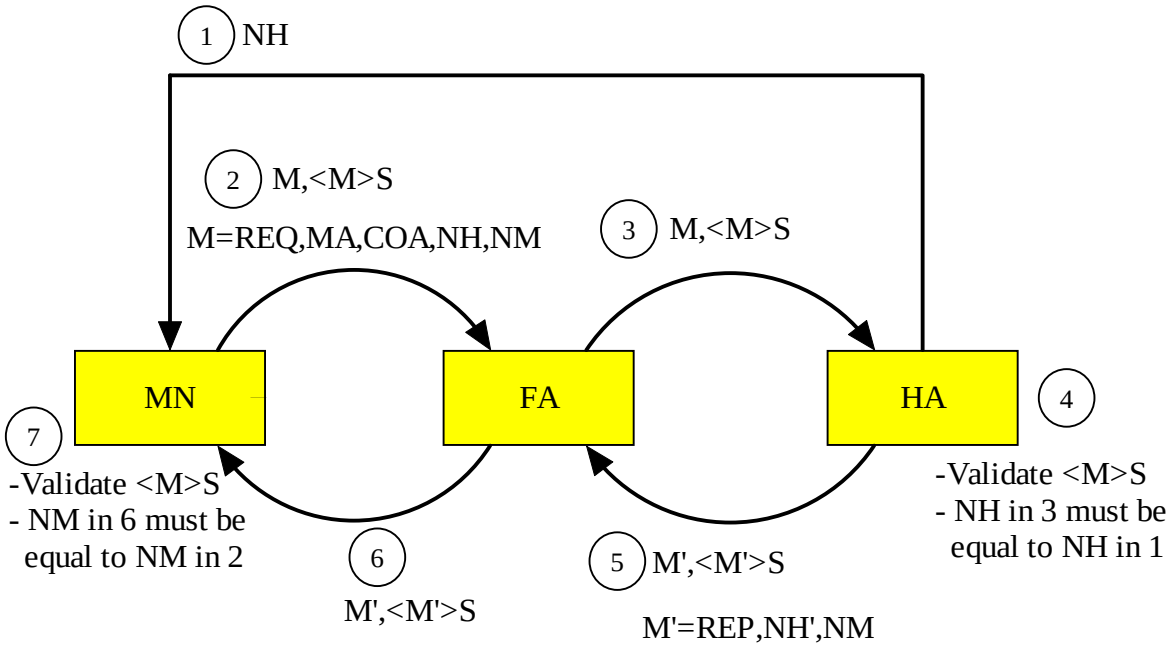
- Uses secret keys
- Difficulties:
  - scalability of key management
  - breaks if a node is lost, stolen or comprised
- Advantages (vs PKI):
  - No need to validate certificates (less communication overhead)
  - “1000 times” less computationally costly



Secret key model

Registration Using Nonces

- Uses a Message Authentication Code (MAC): i.e. authenticator, e.g. keyed MD5 in prefix-suffix mode
- Defense against replay attacks: nonce (pseudo-random number)



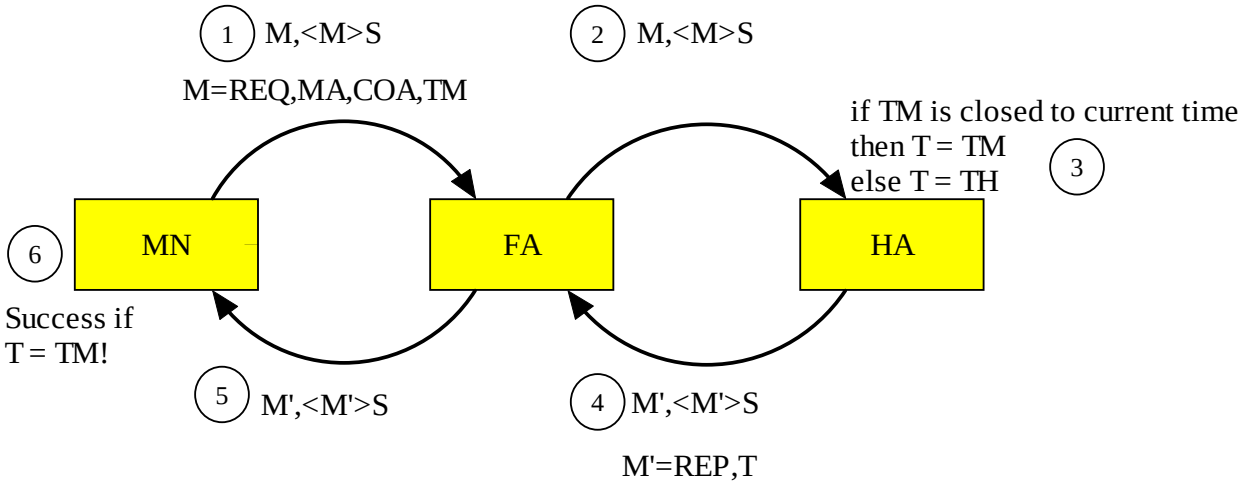
Registration protocol (simplified)

1. The protocol is self-synchronizing. A registration reply, either positive or negative, always provide a nonce for the next registration attempt.

REQ	Request
REP	Reply
MA	Home address of MN
COA	Care-of address
NM	Nonce of MN
NH	Nonce of HA
S	Shared secret between MN and HA
<M>S	MAC of message M under key S

Registration Using Timestamps

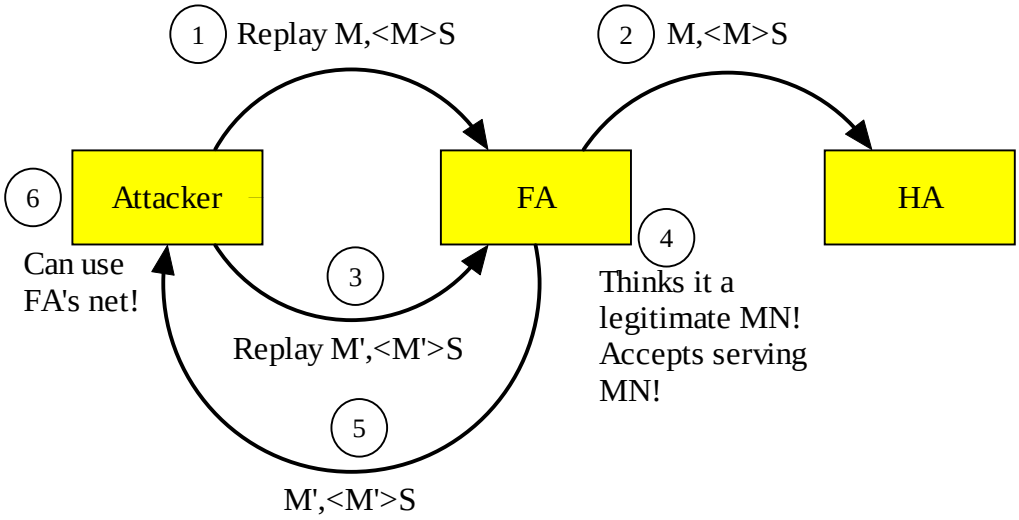
- Uses a Message Authentication Code (MAC): i.e. authenticator, e.g. keyed MD5 in prefix-suffix mode
- Defense against replay attacks: timestamp



Registration protocol (simplified)

REQ	Request
REP	Reply
MA	Home address of MN
COA	Care-of address
TM	Timestamp of MN
TH	Timestamp of HA
S	Shared secret between MN and HA
<M>S	MAC of message M under key S

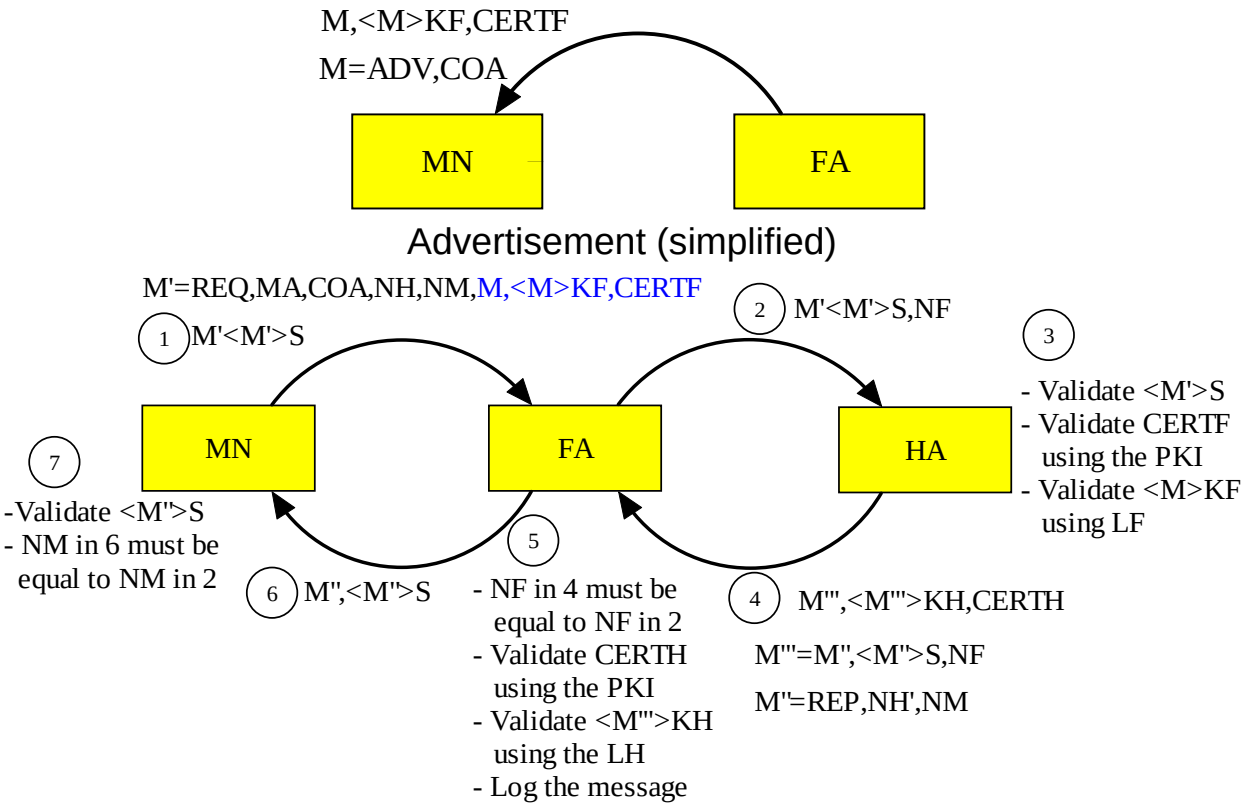
Replay Attack on Registration



Attacker spoofing the MN and the HA

Sufatrio and Lam' Proposal

Highlights:
Hybrid approach: Uses public key cryptography, while the MN performs only secret key operations
MN assumes HA is a trusted server, no need to retrieve a Certificate Revocation List (CRL) from a Certification Authority (CA)



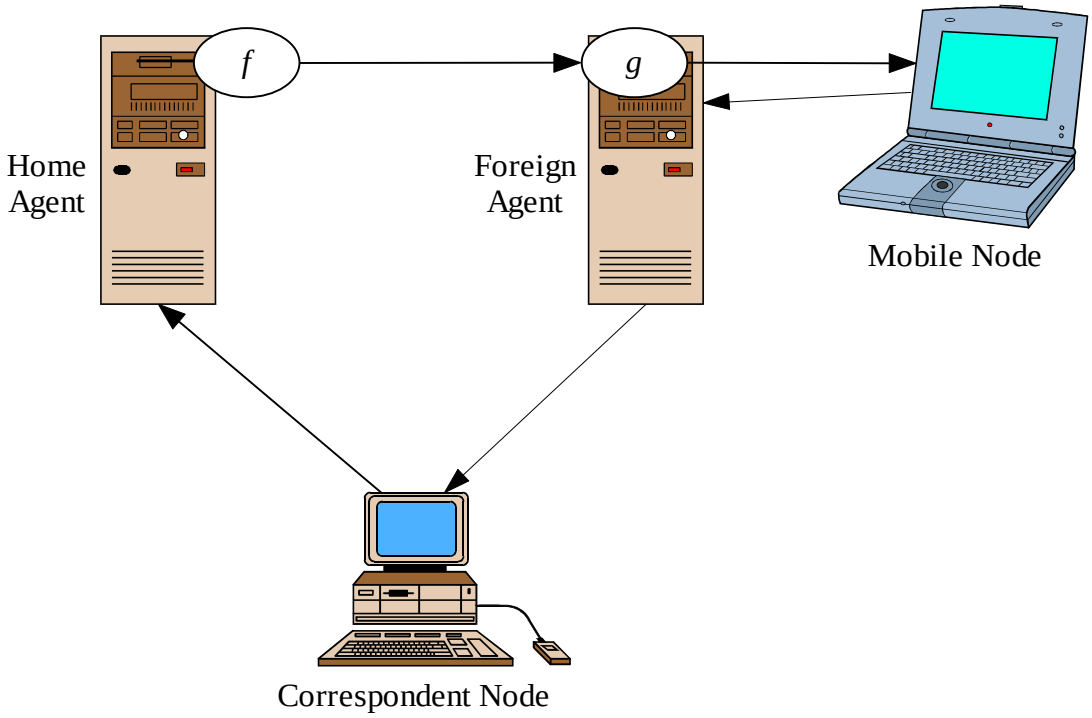
Advertisement (simplified)

Registration protocol (simplified)

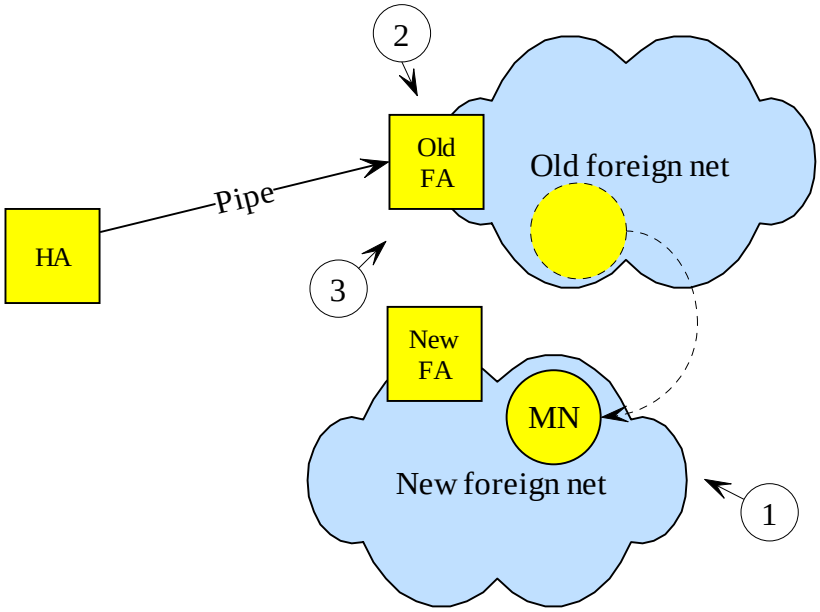
ADV	Advertisement
REQ	Request
REP	Reply
MA	Home address of MN
COA	Care-of address
KH/F	Private key of HA/FA
LH/F	Public key of HA/FA
CERTH/F	Certificate of HA/FA
NH/F/M	Nonce of HA/FA/MN
S	Shared secret between MN and HA
<M>S	MAC of message M under key S

Secure Route Optimization using PKI

Triangle Routing Problem



Lost of In-flight Packets During Handoff



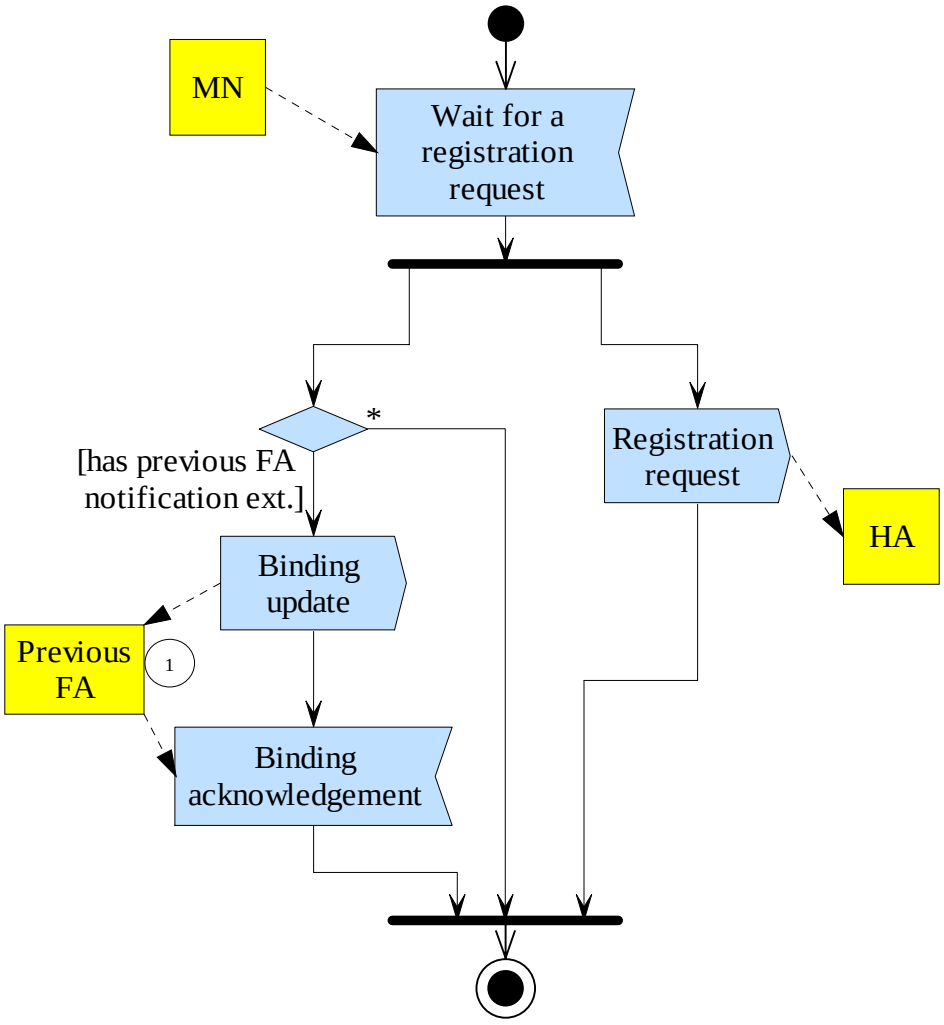
1. The mobile node (MN) has moved and is attached to a new foreign network. The registration process is not completed. The home agent (HA) is not aware of the new location of the MN and still tunnels packets to the old foreign agent (FA).

2. Packets destined to the MN and de-tunneled by the old FA are lost.

3. Resources might be allocated to the MN, but are unused, e.g. radio channel.

Smooth Handoff

The previous FA is made aware of the new location of the MN. De-tunneled packets are forwarded to the new FA.



Handling of a registration request by a FA.

1. Previous FA releases resources allocated to the MN, e.g. radio bandwidth.

Threat: Traffic redirection attacks

Secure route optimization: Establish a secret between an FA and an MN. Use it to authenticate binding updates from the MN to the old FA.

Assumption: It is assumed that most of the time, an FA and an MN don't have a mobility security association (MSA).

Registration Key

Def.: A shared secret between an FA and an MN established during registration time.

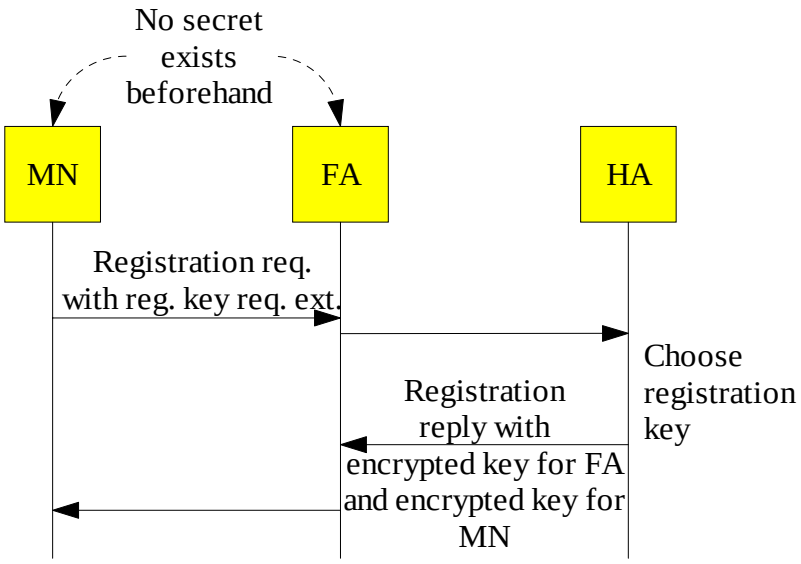
Purpose: authentication of binding update messages, sent by an MN and destined to an FA.

Stored is an FA’s visitor list.

Approaches

- HA is a key distribution centre
- Diffie-Hellman between MN and FA
- Public Key Infrastructure (PKI)

HA as a Key Distribution Centre



Encryption

- Compute $Expr_1 = MD5(Secret \| registration\ reply \| Secret) \oplus Key$.
- Put $Expr_1$ in registration reply extension.

Key recovery ($(A \oplus B) \oplus A = B$)

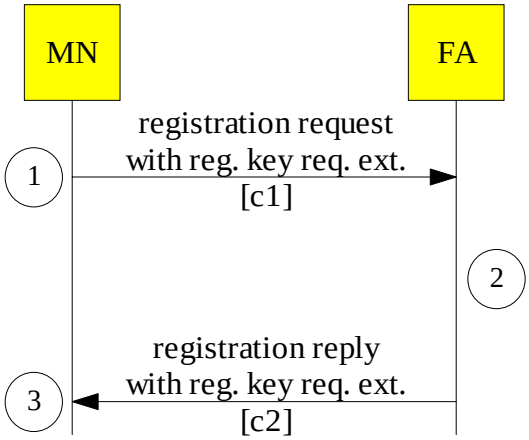
- Compute $Expr_2 = MD5(Secret \| registration\ reply \| Secret)$.
- Key is registration reply extension $\oplus Expr_2$.

Diffie-Hellman Between MN and FA

Public key cryptosystem: establishment of a key between two parties that don't share a secret a priori.

Public knowledge: p, a prime number; g, a generator.

Property: $(g^x)^y = (g^y)^x$.



1. Choose a private random number x and compute $c_1 = g^x \bmod p$.

2. Choose a private random number y and compute $c_2 = g^y \bmod p$. Secret key is $c_1^{\,y} \bmod p$.

3. Secret key is $c_2^{\,x} \bmod p$.

Weaknesses:

- Vulnerable to the person-in-the-middle attack (must be combined with an authentication procedure).
- Exponentiation of long numbers takes long time.

Using Public Key Infrastructure

Certificate:
- Identity and public key of an entity
- Serial number (certificate's ID)
- Validity: *not before*, *not after*
- Signature of an authority: mobile IP uses SHA-1 and RSA

Certification Authority (CA):
- Issues certificates to MNs and FAs
- Publishes invalid certificates: Certificate Revocation List (CRL)

DNS based certificate dispatch:
- Stored in a new type of resource records of DNS: X509CCRL
- Discovered by reverse DNS lookup: IP address to certificate mapping

Algorithm

Private values:
- MN's exponent: *i*
- FA's exponent: *j*

Public values:
- Prime modulus: *p*
- Base: *g*
- MN's public key: $g^i \bmod p$ (provided in MN's certificates, FA has to fetch them)
- FA's public key: $g^j \bmod p$ (provided in FA's certificates, MN has to fetch them)

Short Term Key Generation

1) Compute a long-term master key

Compute a long symmetric secret using Diffie-Helman:

$$S_{ij} = (g^i)^j \bmod p = (g^j)^i \bmod p$$

Fold S_{ij} to produce a long-term master key:

$$K_{ij} = \overset{M}{\oplus} \left[S_{ij} \right]_{Lk} \text{ with } M = \left\lceil \frac{Length(S_{ij})}{Lk} \right\rceil$$

- *Lk* is length of short-term key
- Break S_{ij} into fragments of length *Lk* (padding may be added after high order bits: 01010101)
- Take XOR of the *M* fragments

2) Prepare a transient value

Using 64-bit replay protection ID R_n (put in mobile IP control messages), prepare a 512-bit transient value (Repeated concatenation):

$$T_n = \overset{8}{|} R_n$$

The goal is to increase the number of changing bits for the next step.

3) Production of short-term keys

$$K_{auth} = MD5\left(K_{ij} \oplus P_1 \mid MD5\left(K_{ij} \oplus P_2 \mid T_n \right) \right)$$

Constants:

$$P_1 = \overset{48}{|} 36_{16}$$
$$P_2 = \overset{48}{|} 48_{16}$$

Note: SHA-1 can be used instead of MD5.

Cryptographically Generated Addresses

Outline

- References
- Background: Packet delivery in Mobility support for IPv6
- Threats
- Methods of attack
- Identifier ownership problem
- Cryptographically Generated Addresses (CGA)
- Montenegro and C. Castelluccia's proposal

References

Address Ownership Problem:

- Pekka Nikander, An Address Ownership Problem in IPv6, work in progress, Internet-Draft (expired), February 2001.

Original idea of CGA:

- G. Montenegro and C. Castelluccia, Statistically Unique and Cryptographically Verifiable Identifiers and Addresses, ISOC Symposium on Network and Distributed System Security (ISOC NDSS), San Diego, 2002.

Client puzzle:

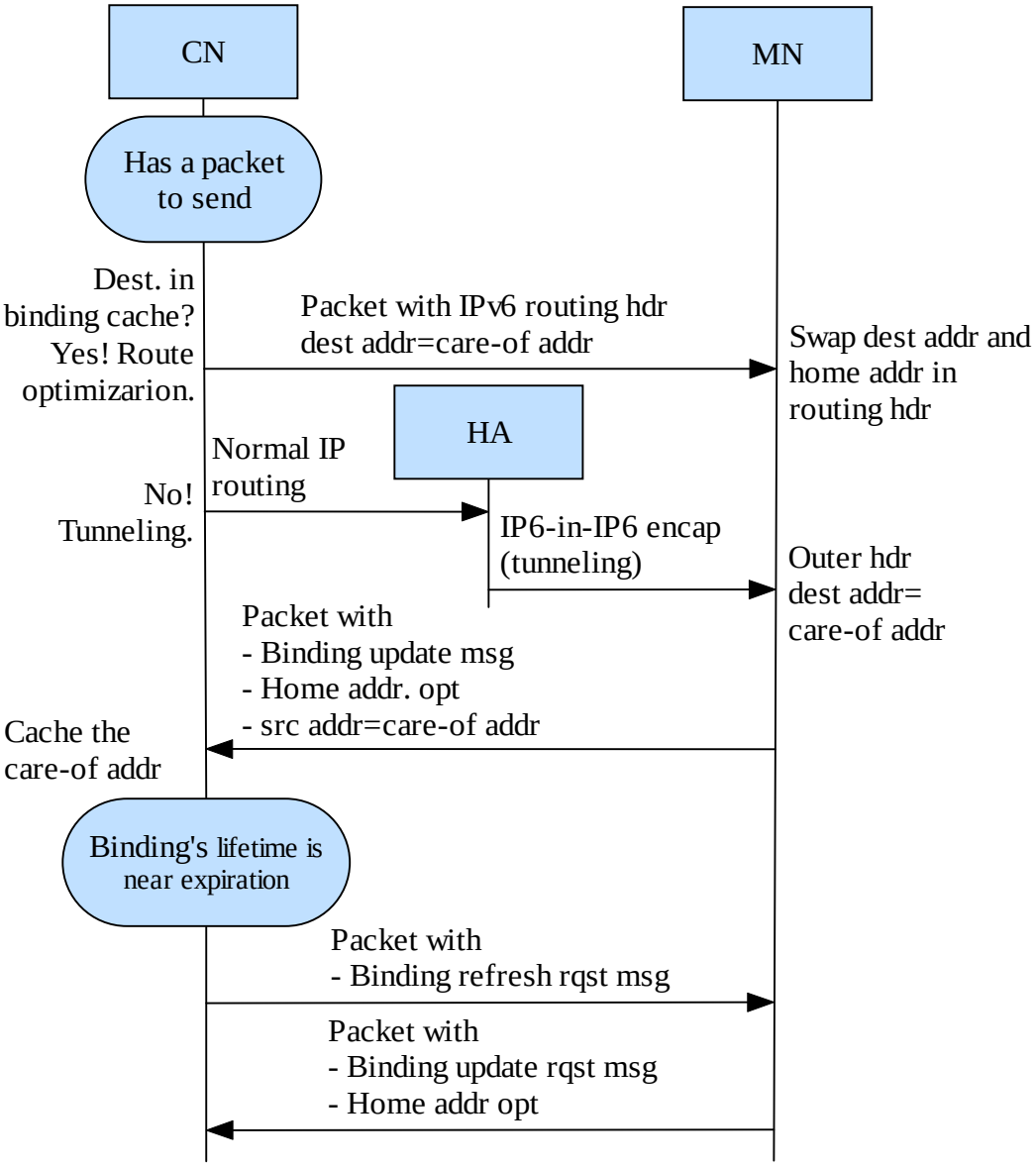
- Tuomas Aura and Pekka Nikander and Jussipekka Leiwo, DOS-Resistant Authentication with Client Puzzles, Lecture Notes in Computer Science, 2133, 2001.

Detailed design:

- Tuomas Aura, Cryptographically Generated Addresses (CGA), IETF Securing Neighbor Discovery WG, INTERNET DRAFT, February 2003.

Overview Packet Delivery in Mobility Support for IPv6

- IPv6 header destination option: Used by MNs to inform their CNs about MN's current location.
- CN to MN delivery: Packet with dest addr = care-of addr and Routing header containing home-of address.



Transmission of a packet by a CN

Role of HA in packet delivery: Whenever a moved is registered, inform all local nodes about new MAC address (Neighbor discovery: analogous to proxy/gratuitous ARP in IPv4).

Threats

- Hosts have the ability to change routing of packets to certain destinations.
- Redirection of traffic away from their legitimate destination:
    - Denial of service attack
    - Hijacking attack

Denial of Service and Hijacking Attacks

1) Denial of service attack

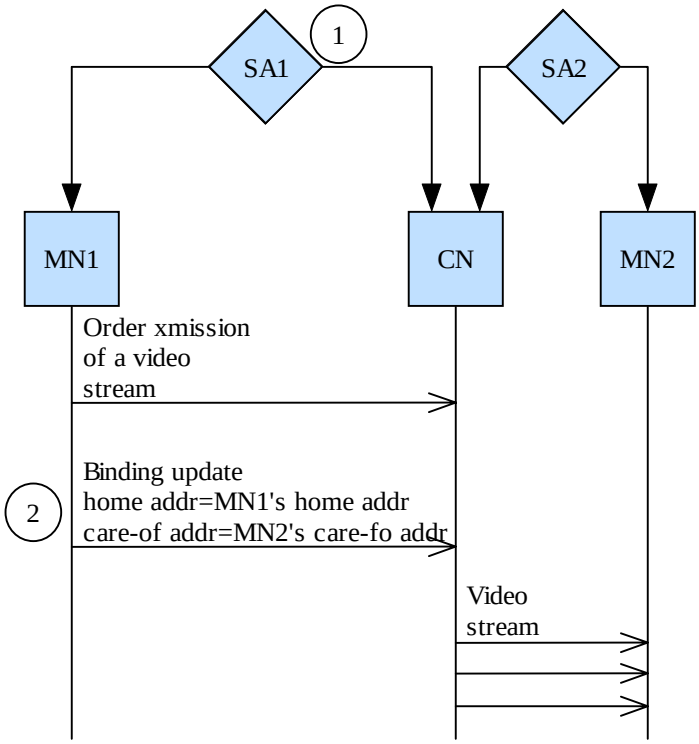
- MN1 starts a big file transfer from a server.
- MN1 sends to the server an update binding its home addr to the care-of addr of a victim.
- The file is sent to the victim.

2) Hijacking attack

- MN1 is corresponding with node CN
- MN2 sends an update binding MN1's home addr to MN2's care-of addr
- CN's traffic destined to MN1 is redirected to MN2

Does authentication solve the problems?

Identifier Ownership Problem [Nikander 2001]

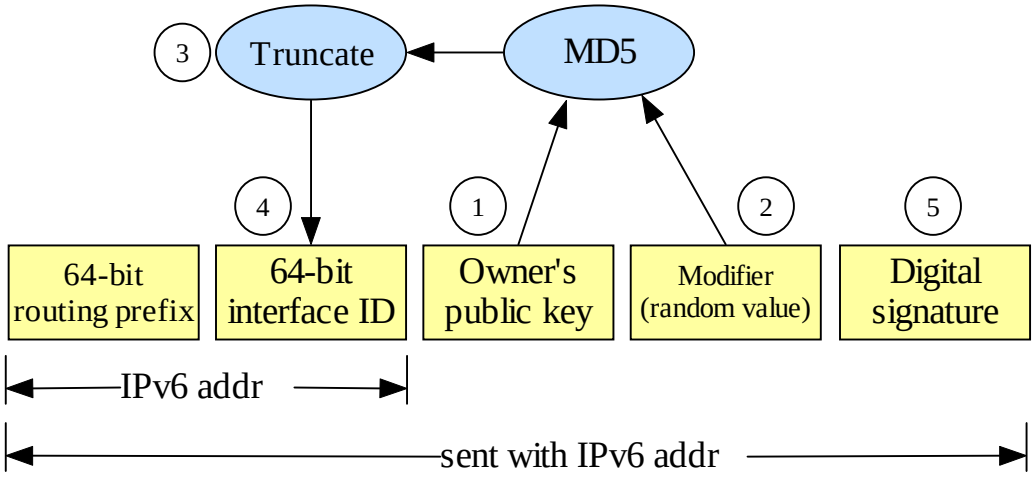


1) Authentication does not solve the problem!

2) MN1 is not authorized to specify new routing information for MN2's home address.

An MN must be able to prove ownership of the addresses it uses!

Cryptographically Generated Addresses Defined [Aura 2003]



1) A public and private key pair is generated according to a selected public key encryption algorithm (e.g. RSA).

2) Contributes to *statistical uniqueness* to the address.

3) Keep rightmost 64 bits of MD5's output.

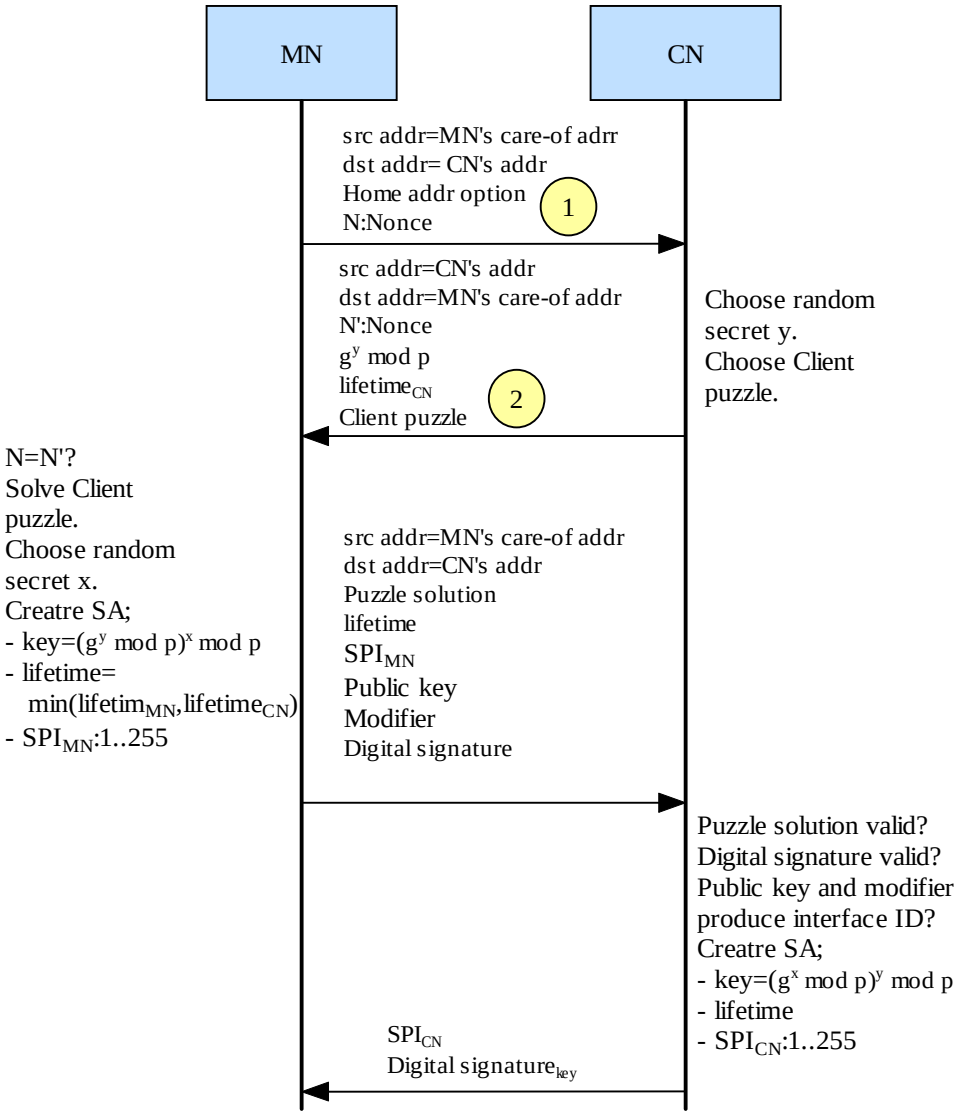
4) Before usage, collision detection must be performed.

5) Digital signature:

- Generation: E_{RSA}(MD5(message), private key)
- Verification: D_{RSA}(MD5(message), public key)

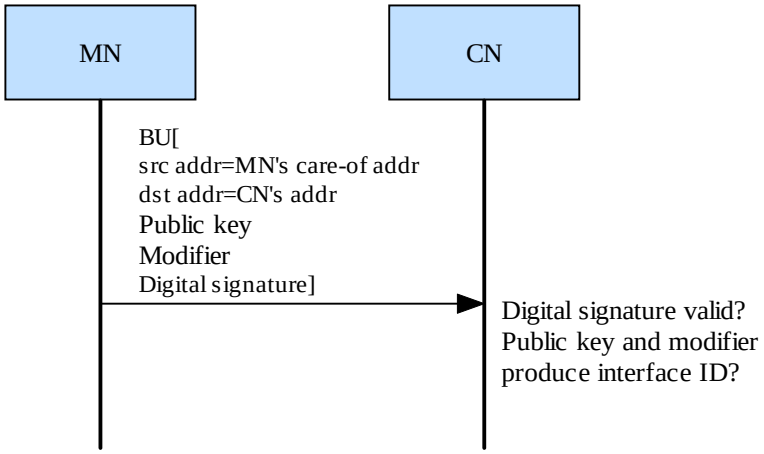
Montenegro and Castelluccia's Proposal

- Traffic redirection operations are accepted solely from entities that can prove ownership of their addresses (e.g., home addr and care-of addr).
- Unavailability of a public key infrastructure or a key distribution centre is assumed.
- The principal auto creates private key and a public key
- Separate authorization protocol for binding updates:
  - Sets up a security association (session key, lifetime, SPI)
- The ESP of IPSec is used to secure binding updates/acknowledgements



1) Nonce (random value) is used to eliminate non fresh messages [Aura et al 2001].
2) Client puzzle prevents denial of service attacks.

Montenegro and Castelluccia's proposal (cont'd)



Firewall traversal

References

Definition of the difficulty

- C.E. Perkins, Mobile IP - Design Principles and Practices, Addison-Wesley Wireless Communications Series, 1998 (Section 7.2)

Solutions

- M. Leech, Username/Password Authentication for SOCKS V5, The Internet Society, Request for Comments: 1929, 1996.
- M. Leech, M. Ganis, Y. Lee, R. Kuris, D. Koblas, and L. Jones, SOCKS Protocol Version 5, The Internet Society, Request for Comments: 1928, March 1996.
- V. Gupta and G. Montenegro, Sun's SKIP Firewall Traversal for Mobile IP, The Internet Society, Request for Comments: 2356, 1998.

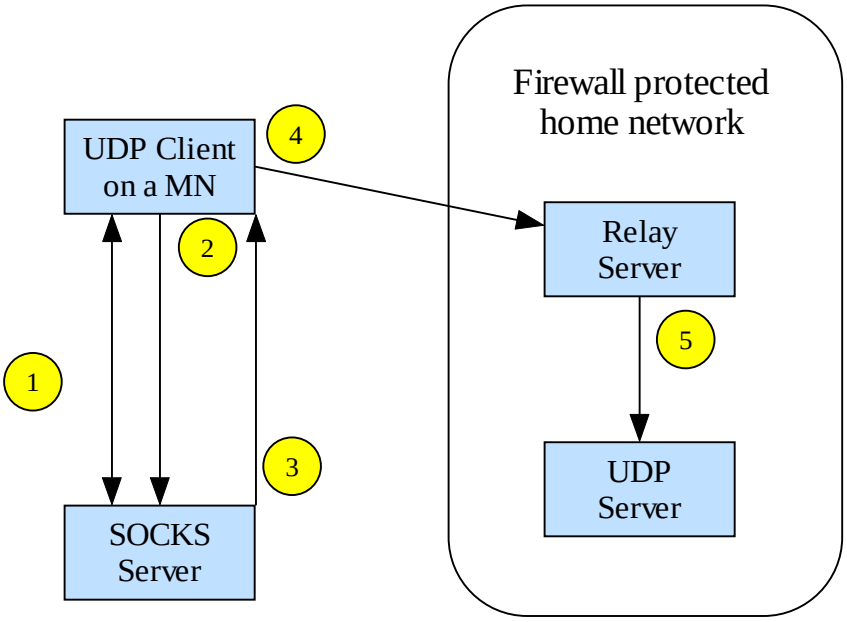
The Firewall Traversal Problem

- MNs send packets using their home address as source address. As a defense against masquerading, firewalls discard incoming packets with internal source addresses.
- Packets may be admitted in private network only if they are either authenticated or destined to the firewall (i.e. not destined to a private node).
- Impossibility for a MN to reach CNs of the home network!

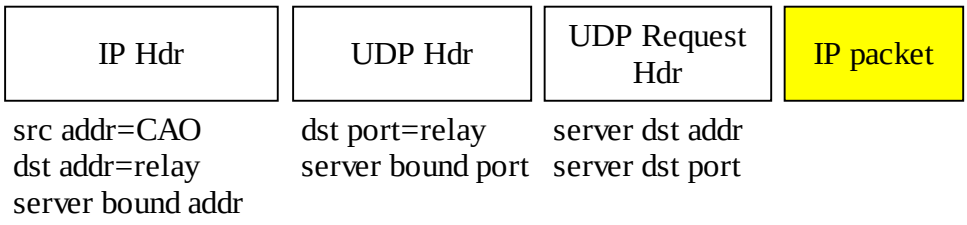
Solutions

1. Reverse tunneling: FA (or MN) to HA, care-of address is used as source address, leads to quadrilateral routing!
2. SOCKS5
3. SKIP

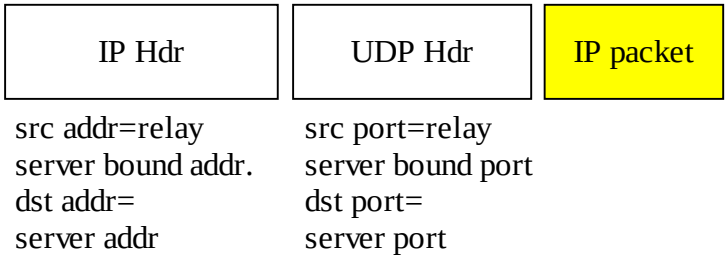
SOCKS5: A Proxying Approach!



1. Authentication phase (RFC 1928, username and pw based)
2. Transmission of an request with UDP Server addr. and UDP Server port.
3. Transmission of a reply with relay server bound addr. and relay server bound port
4. Packet transmission



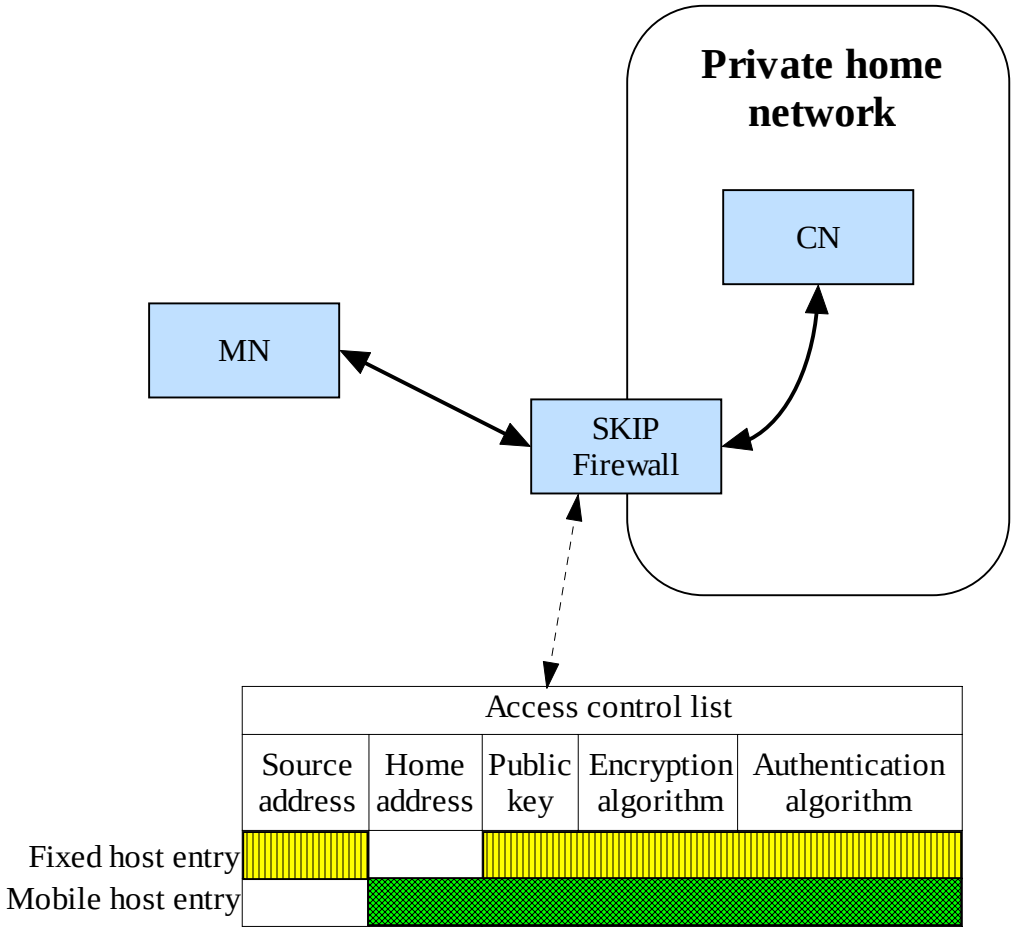
5. Relay



Disadvantages: Several setup ctrl messages are required, encapsulation overhead, setup has to be reapplied each time the location (CAO) of the MN changes.

Simple Key-Management Internet Protocol (SKIP): An IP Security Based Approach!

- Uses IPSec (Authentication Header (AH) and Encapsulating Security Payload (ESP)) and public keys



Complementary Topics

Ad-hoc network security

S. Capkun, L. Buttyan and J.-P. Hubaux, Self-Organized Public-Key Management for Mobile Ad Hoc Networks, IEEE Transactions on Mobile Computing, Vol. 2, No. 1, 2003, pp. 52-64.

H. Deng, W. Li and D.P. Agrawal, Routing Security in Wireless Ad Hoc Networks, IEEE Communications Magazine, October 2002, pp. 70-75.

Y.-C. Hu, A. Perrig and D.B. Johnson, Ariadne: A Secure On-Demand Routing Protocol for Ad Hoc Networks, MobiCom'02, 2002.

M. Just, E. Kranakis and T. Wan, Resisting Malicious Packet Dropping in Wireless Ad-Hoc Networks Using Distributed Probing, In: Proceedings of 2nd Annual Conference on Adhoc Networks and Wireless (ADHOCNOW'03), Montreal, Canada, Oct 09-10, 2003.

Identity malleability

J. Hall, M. Barbeau and E. Kranakis, Detection of Transient in Radio Frequency Fingerprinting Using Phase Characteristics of Signals, In: L. Hesselink (Ed.), Proceedings of the 3rd IASTED International Conference on Wireless and Optical Communications (WOC), ACTA Press, Banff, Alberta, 2003, pp. 13-18.

Intrusion detection

P. Kyasanur and N.H. Vaidya, Detection and Handling of MAC Layer Misbehavior in Wireless Networks, Technical Report, CSL, UIUC, August 2002.

Y. Zhang and W. Lee, Intrusion Detection in Wireless Adhoc Networks, In Mobile Computing and Networking, pages 275--283, 2000.

Cryptography

A. Menezes, P. van Oorschot, and S. Vanstone, Handbook of Applied Cryptography, CRC Press, 1996.

Acronyms

AH	Authentication Header
AP	Access Point
BSS	Basic Service Set
BU	Binding Update
CA	Certification Authority
CN	Correspondent Node
CRL	Certificate Revocation List
DS	Distribution System
DSA	Digital Signature Algorithm
DSS	Digital Signature Standard
ESP	Encapsulating Security Payload
FA	Foreign Agent
HA	Home Agent
ICV	Integrity Check Value
IV	Initialization Vector
LD	Location Directory
MAC	Media Access Control
MD5	Message Digest version 5
MIC	Message Integrity Code
MN	Mobile Node
MSDU	MAC Service Data Unit
PK	Public Key
PKI	Public Key Infrastructure
RSA	Rivest Shamir Adelmann
SHA	Secure Hash Algorithm
SA	Security Association
WLAN	Wireless Local Area Network
WEP	Wired Equivalent Privacy