Chapter 5: Security

Jyh-Cheng Chen and Tao Zhang

IP-Based Next-Generation Wireless Networks
Published by John Wiley & Sons, Inc.
January 2004

Outline

5.1 Introduction

5.2 Internet Security

5.3 Security in Wireless Networks

5.4 Security in IS-41

5.5 Security in GSM

5.6 Security in GPRS

5.7 Security in 3GPP

5.8 Security in 3GPP2

3

5.1 Introduction

5.1.1 Different Facets of Security

5.1.2 Security Attacks

5.1.3 Cryptography

5.1.4 Public-Key Infrastructure (PKI)

4

5.1.1 Different Facets of Security

◆ Authentication: validate authentic identity
◆ Authorization: access control
◆ Integrity: protection from unauthorized change
◆ Confidentiality or Privacy: keep information private such that only authorized users can understand it
◆ Availability: outsider cannot block legitimate access
◆ Non-repudiation: supply undeniable evidence to prove the message transmission and network access

5

5.1.2 Security Attacks

◆ Passive attacks: eavesdrop the transmission or monitor and analyze the network traffic

◆ Active attacks: modification of information, interruption of information transmission, and fabrication of messages
  - Denial-of-service (DoS)
  - Masquerade
  - Man-in-the-middle
  - Replay

6

5.1.3 Cryptography

5.1.3.1 Encryption

5.1.3.2 Message Authentication

7

5.1.3.1 Encryption

◆ Transforming of letters or characters without changing its information content
◆ Enciphering (encryption)
  ▪ plaintext (cleartext) -> ciphertext
◆ Deciphering (decryption)
  ▪ ciphertext -> plaintext (cleartext)
◆ Can be used to achieve the information confidentiality

8

4

Two Categories

◆ Secret-key algorithm
  - Symmetric: same secret-key is used for both encryption and decryption
  - DES: Data Encryption Standard
  - AES: Advanced Encryption Standard
◆ Public-key algorithm
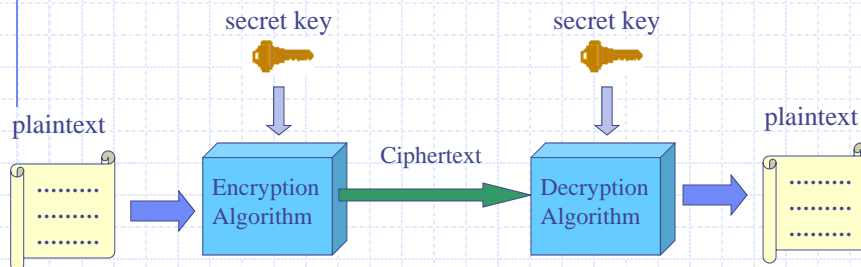 - Asymmetric: different keys are used for encryption and decryption
  - RSA

9

Transposition Ciphering

◆ Rearrange the characters in the plaintext to produce the ciphertext
◆ Permutation
i = 1, 2, 3, 4, 5, 6, 7 ->
f(i) = 2, 4, 1, 6, 5, 3, 7
◆ m = IP-Based Next-Generation Wireless Networks
f(m) = -IsPaBeNdt xe-nGaeretniioW ree lssNwektros

10

Substitution Ciphering

◆ Substitute characters in the plaintext with other characters to produce the ciphertext

◆ Caesar cipher: shift alphabet

A B C D E F G H I J K L M N ...

D E F G H I J K L M N O P Q ...

◆ m = THIS IS A PLAINTEXT

g(m) = WKLV LV D SODLQWHAW

11

Fig. **5.1** Secret-key encryption and decryption

secret key   secret key

plaintext   plaintext

Ciphertext

....   Encryption   Decryption   ....
....   Algorithm   Algorithm   ....
....

12

6

DES (Data Encryption Standard)

◆ Divide original message into blocks of 64 bits
◆ Each block is permuted
◆ Encrypt each block of plaintext using a 64-bit key
  ▪ 1 bit in each byte is for parity check
    ◆ Actual key length: 56 bits
  ▪ 16 identical iteration that combines substitution and transposition ciphers
◆ Inverse original permutation
◆ Triple DES

13

AES (Advanced Encryption Standard)

◆ By NIST (National Institute of Standards and Technology)
◆ AES-128
◆ AES-192
◆ AES-256

14

Public-Key Algorithm

◆ Public key
- Publicly available to anyone

◆ Secret (private) key
- Only users themselves know their own private keys.

Fig. **5.2** Public-key encryption and decryption

public key   secret key

plaintext   plaintext

Ciphertext

Encryption Algorithm   Decryption Algorithm
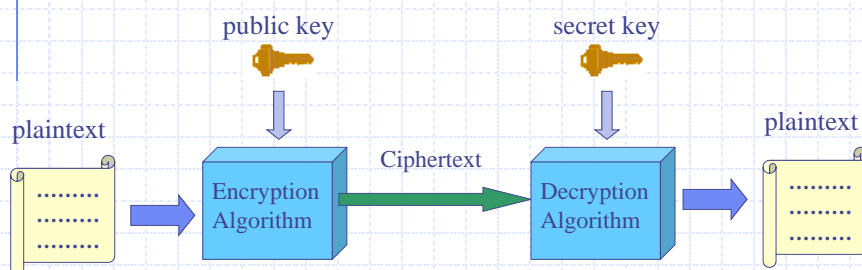
RSA

- ◆ It is extremely difficult to factor the product of two large prime numbers.
- ◆ A secret key can be generated by two selected large prime numbers.
- ◆ The product of the two large prime numbers will be used as the public key.
- ◆ Knowing the public key does not allow one to easily derive the associated private key.

17

5.1.3.2 Message Authentication

- ◆ A methodology to assure data integrity and to authenticate the data origin
- ◆ Message Authentication Code (MAC)
- ◆ One-way hash function
  - ■ A one-way hash function takes an arbitrarily long input message and produces a fixed-length, pseudorandom output called a hash.
  - ■ Knowing a hash, it is computationally difficult to find the message that produced that hash.
  - ■ It is almost impossible to find different messages that will generate the same hash.

18

Fig. 5.3 Message authentication code (MAC)

19
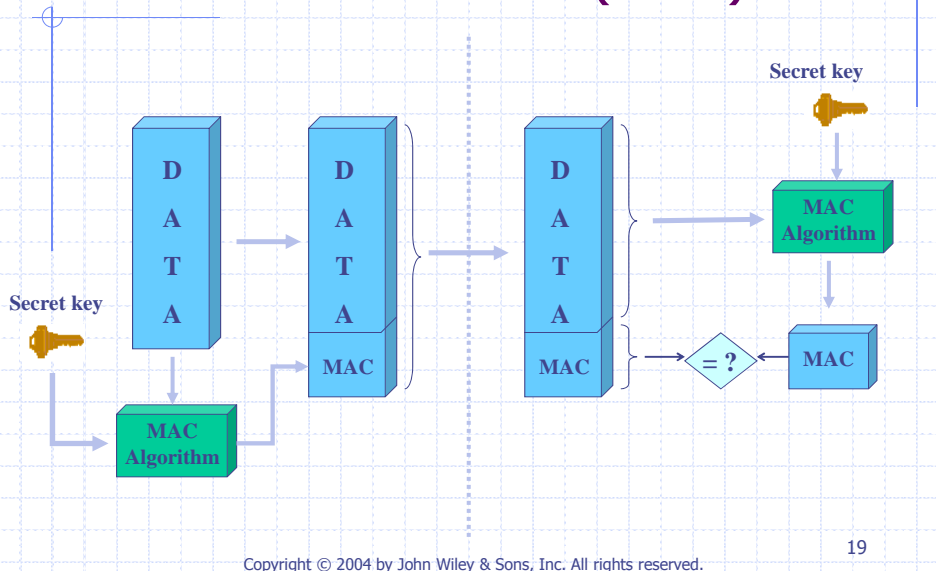
Hash Function

◆ Unkeyed hash: there is no secret key between the communicating parties
  - Message Digest 5 (MD5)
  - Secure Hash Algorithm (SHA-1)

◆ Keyed hash
  - HMAC

20

MD5 and SHA

◆ Message Digest 5 (MD5)
  - Produce an output of 128-bit *fingerprint* or *message digest*
  - The sender sends the original message and the message digest together to the destination.
  - The destination computes its own message digest from the received message.
  - Any change to the original message during transmission will result in a different message digest.

◆ Secure Hash Algorithm (SHA-1) generates a 160-bit message digest

21

Digital Signature

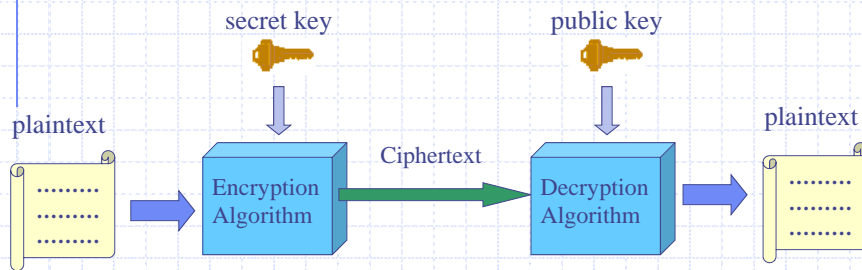◆ Public-key algorithms can be used for integrity and message authentication as well.

◆ Digital Signature Standard (DSS)
  - Specify algorithms for computing digital signatures that can be used by a receiver to verify the identity of the signatory and the integrity of the data

22

Fig. 5.4 Integrity and authentication by public-key

secret key   public key

plaintext   Ciphertext   plaintext

Encryption Algorithm → Decryption Algorithm

23

5.1.4 Public-Key Infrastructure (PKI)

◆ How can we assure that a public key is not forged?
◆ PKI: establish digital identities that can be trusted
  ■ A trusted third party is known as a certification authority (CA).
  ■ One can present a public key to the CA in a secure manner.
  ■ The CA then issues a *digital certificate* or *public-key certificate (PKC)* that contains the user's public key to the user.
  ■ The certificate is signed digitally by the CA.
◆ X.509 Certificate: standardized by the ITU

24

Fig. 5.5 Format of ITU X.509 certificate

Version
Certificate serial number
Signature algorithm identifier
Issuer name
Validity period
Subject name
Subject public-key information
Issuer unique identifier
Subject unique identifier
Extensions
Signature

25

5.2 Internet Security

5.2.1 IP Security (IPsec)

5.2.2 Authentication, Authorization, and Accounting (AAA)

26

5.2.1 IP Security (IPsec)

5.2.1.1 Security Protocols
5.2.1.2 Authentication and Encryption Algorithms
5.2.1.3 Security Associations
5.2.1.4 Key Management
5.2.1.5 Implementation
5.2.1.6 Authentication Header (AH)
5.2.1.7 Encapsulating Security Payload (ESP)
5.2.1.8 Traffic Processing
5.2.1.9 IPsec Applications

27

IPsec

- ◆ IPsec is a suite of protocols for protecting IP datagrams and upper layer protocols
- ◆ Defined by IETF
  - Optional for IPv4
  - Mandatory for IPv6

28

Fig. 5.6 Family of IPsec protocols

```
                    ┌─────────────────────────────────┐
                    │  IP Security Architecture RFC 2401 │
                    └─────────────────────────────────┘
        ┌─────────────────────┬─────────────────────────┐
┌──────────────────┐  ┌──────────────────┐  ┌──────────────────┐
│ Authentication   │  │ Encapsulating    │  │ IPsec ISAKMP DOI │
│ Header           │  │ Security         │  │ RFC 2407         │
│ (AH) RFC 2402    │  │ Payload (ESP)    │  └──────────────────┘
└──────────────────┘  │ RFC 2406         │  ┌──────────────────┐
                      └──────────────────┘  │ ISAKMP           │
                                            │ RFC 2408         │
┌──────────────┐ ┌──────────────┐ ┌──────────────┐ └──────────────────┘
│ HMAC-MD5-96  │ │ HMAC-SHA-1-96│ │ NULL         │ ┌──────────────────┐
│ RFC 2403     │ │ RFC 2404     │ │ Encryption   │ │ Internet Key     │
└──────────────┘ └──────────────┘ │ Algorithm    │ │ Exchange         │
                                  │ RFC 2410     │ │ RFC 2409         │
                                  └──────────────┘ └──────────────────┘
┌──────────────┐ ┌──────────────┐ ┌──────────────┐ ┌──────────────────┐
│ HMAC-        │ │ DES-CBC (with│ │ CBC-mode     │ │ OAKLEY           │
│ RIPEMD-160-96│ │ explicit IV) │ │ Cipher       │ │ RFC 2412         │
│ RFC 2857     │ │ RFC 2405     │ │ Algorithm    │ └──────────────────┘
└──────────────┘ └──────────────┘ │ RFC 2451     │
                                  └──────────────┘
```

29

5.2.1.1 Security Protocols

◆ AH (Authentication Header)
- support data integrity and authentication of the IP packets

◆ ESP (Encapsulating Security Payload)
- provides confidentiality services

30

Operation

◆ Transport
- security is applied to higher-level protocols to protect the payload

◆ Tunnel
- security is applied to the encapsulated IP packet to protect the entire packet

31

5.2.1.2 Authentication and Encryption Algorithms

◆ IPsec specifies various options for cryptography algorithm.
- HMAC-MD5-96, HMAC-SHA-1-96, NULL encryption algorithm, HMAC-RIPEMD-160-96, DES-CBC, and CBC-Mode cipher algorithms, and others

◆ To be compliant with ESP
- DES-CBC, HMAC-MD5-96, HMAC-SHA-1-96, NULL encryption algorithm, and NULL authentication algorithm must be implemented
- Encryption algorithm and authentication algorithm cannot be both NULL.

◆ To be compliant with AH
- HMAC-MD5-96 and HMAC-SHA-1-96 are mandatory

32

5.2.1.3 Security Associations

◆ A set of information maintained by the two nodes that defines:
- Which security services will be supported
- How these security services will be provided
- For example, it identifies:
  - Security mechanisms (e.g., cryptography algorithms, key management mechanisms) will be used to support the security services
  - Parameter values (e.g., security keys) needed by the security mechanisms
  - How long these parameter values (e.g., the keys) will be valid

33

Security Association Database (SAD)

◆ Because the information maintained in a SA generally is too big to fit into IP header, the SAs are maintained in SAD.

◆ Each SA is identified uniquely by a triplet:
- Security protocol identifier: AH or ESP
- Destination IP address: the IP address of the other node with which the SA is established
- Security Parameter Index (SPI): a 32-bit value that uniquely identifies one SA among different SAs terminating at the same destination

34

Security Policy Database (SPD)

◆ SA enforces *Security Policies* that define how communicating parties will communicate by IPsec.

◆ Security policies are stored on Security Policy Database (SPD), which specifies the policies that determine the disposition of all inbound or outbound, IPsec or non-IPsec IP traffic.

◆ Each packet is either applied IPsec, be allowed to bypass IPsec, or discarded.

35

5.2.1.4 Key Management

◆ Both manual and automated SA and key management are mandated in IPsec.

◆ Diffie-Hellman (DH) algorithm is adopted by most automated key management protocols.

◆ OAKLEY

◆ SKEME

◆ Internet Security Association and Key Management Protocol (ISAKMP)

◆ Internet Key Exchange (IKE): the default automated key management protocol selected for use with IPsec

36

Diffie-Hellman (DH) Algorithm

- First agree on a large prime number p and a number a such that a is primitive mod p
1. Tao chooses a random secret x and calculates A as follows

   $A = a^x \bmod p$

   Tao then sends A to Jyh-Cheng
2. Jyh-Cheng chooses a random secret y and calculates B as follows

   $B = a^y \bmod p$

   Jyh-Cheng then sends B to Tao
3. Tao calculates $K = B^x \bmod p$
4. Jyh-Cheng calculates $K' = A^y \bmod p$
- $K = K' = a^{xy} \bmod p$
- It is computationally difficult to calculate the discrete logarithm to get x and y

37

5.2.1.5 Implementation

- IP stack integration
  - IPsec could be integrated into the network layer of the protocol to provide security services.
- Bump-in-the-stack (BITS)
  - IPsec is inserted as a thin layer between IP layer and link layer.
- Bump-in-the-wire (BITW)
  - This implementation assumes that IPsec is running on a separate device attached to the physical interface of a host or router.
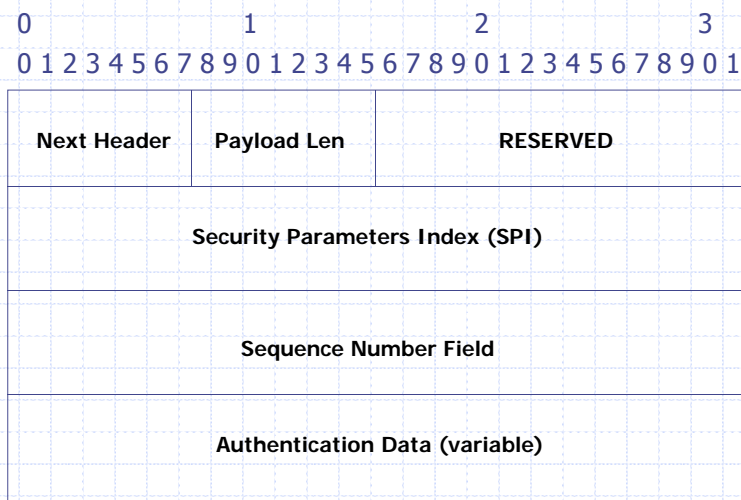
38

5.2.1.6 Authentication Header (AH)

- Provide data integrity and authentication of data origin
- Also optionally provides replay detection
- May be applied alone or in combination with the ESP to provide confidentiality service

39

Fig. 5.7 Header format of AH

0				1				2				3	

0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1

Next Header	Payload Len	RESERVED

Security Parameters Index (SPI)

Sequence Number Field

Authentication Data (variable)

40

20

Security Parameter Index (SPI)

◆ A 32-bit value that uniquely identifies one SA among different SAs terminating at the same destination

41

Sequence Number

◆ 32-bit

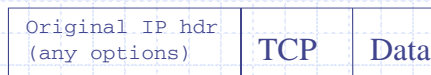◆ Incremented by 1 for each packet sent in order to protect against replay attacks

42

Authentication Data

◆ Integrity Check Value (ICV)
- Produced by MAC (Message Authentication Checksum) by an algorithm specified by the SA
  - Secret key between two parties
  - HMAC: produced by a *hash* function
- Variable length but must be an integral number of 32-bit words
- Computed over
  - immutable IP header fields
  - AH header
  - upper-level protocol data (assumed to be immutable)

43

Fig. 5.8 AH in IPv4 in transport mode

IPv4 – BEFORE APPLYING AH

Original IP hdr (any options)	TCP	Data

IPv4 – AFTER APPLYING AH

Original IP hdr (any options)	AH	TCP	Data

```
|<-----------authenticated ----------->|
       except for mutable fields
```

44

Fig. 5.9 AH in IPv6 in transport mode

IPv6 – BEFORE APPLYING AH

Original IP hdr	ext hdrs if present	TCP	Data

IPv6 – AFTER APPLYING AH

Original IP hdr	hop-by-hop, dest*, routing, fragment.	AH	Dest opt*	TCP	Data

|<--------- authenticated except for mutable fields ------------->|

* = if present, could be before AH, after AH, or both

45

Fig. 5.10 AH in tunnel mode

IPv4 – BEFORE APPLYING AH

New IP hdr (any options)	Original IP hdr (any options)	TCP	Data

IPv4 – AFTER APPLYING AH

New IP hdr (any options)	AH	Original IP hdr (any options)	TCP	Data

|<--------------authenticated except for mutable fields in the new IP header--------------->|

IPv6 – BEFORE APPLYING AH

New IP hdr	ext hdrs if present	orig IP hdr	ext hdrs if present	TCP	Data

IPv6 – AFTER APPLYING AH

New IP hdr	ext hdrs if present	AH	orig IP hdr	ext hdrs if present	TCP	Data

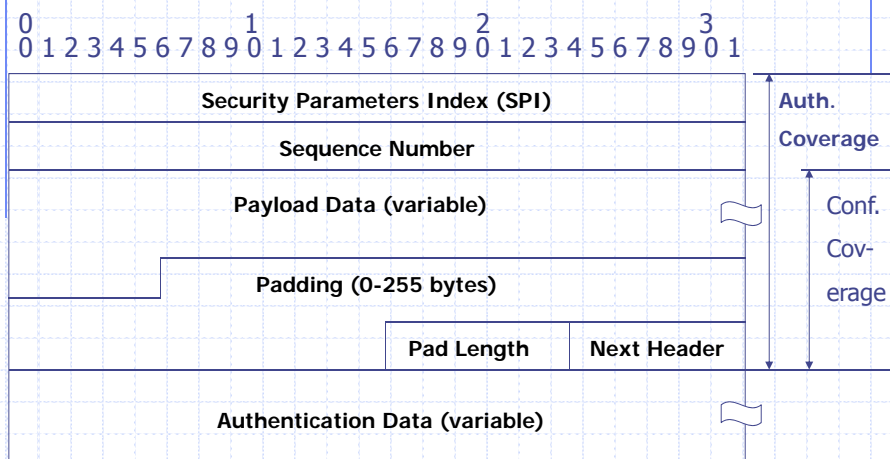|<------- authenticated except for mutable fields in the new IP header------->|

46

23

5.2.1.7 Encapsulating Security Payload (ESP)

- ◆ Provide confidentiality (encryption) and authentication
  - the authentication service includes data integrity and data origin authentication
- ◆ Also support replay detection
- ◆ Does not protect IP header unless it is encapsulated in the tunnel mode
- ◆ Either confidentiality or authentication must be selected

47

Fig. 5.11 ESP packet format

```
 0                   1                   2                   3
 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
```

Security Parameters Index (SPI)	Auth.
Sequence Number	Coverage
Payload Data (variable)	Conf. Cov- erage
Padding (0-255 bytes)	
Pad Length	Next Header	
Authentication Data (variable)	

48

ESP Header

◆ SPI

◆ Sequence Number

49

ESP Trailer

◆ Padding

◆ Pad Length

- indicate the number of pad bytes immediately preceding it

◆ Next Header

- an 8-bit field that identifies the type of data contained in the *Payload Data* field

50

25

Padding

◆ Some encryption algorithms require the plaintext to be a multiple of some number of bytes

◆ *Pad Length* and *Next Header* fields must be right aligned within a 4-byte word

◆ May be used to conceal the actual length of the payload

51

Authentication Data

◆ A variable-length field containing an Integrity Check Value (ICV)

52

Fig. 5.12 ESP in IPv4 in transport mode

IPv4 – BEFORE APPLYING ESP

Original IP hdr (any options)	TCP	Data

IPv4 – AFTER APPLYING ESP

Original IP hdr (any options)	ESP header	TCP	Data	ESP Trailer	ESP Auth

```
                       |<---encrypted-->|
                   |<---authenticated---->|
```

53

Fig. 5.13 ESP in IPv6 in transport mode

IPv6 – BEFORE APPLYING ESP

Original IP hdr	ext hdrs if present	TCP	Data

IPv6 – AFTER APPLYING ESP

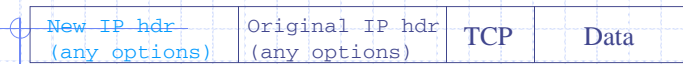| Orig IP hdr	hop-by-hop, dest*, routing, fragment.	ESP	Dest Opt*	TCP	Data	ESP Trailer	ESP Auth

```
                          |<----encrypted--->|
                      |<---authenticated---->|
```
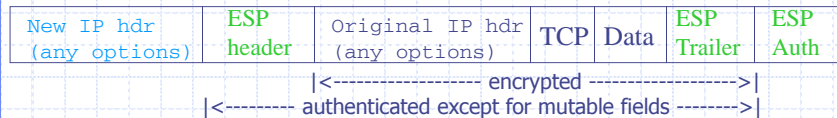
* = if present, could be before ESP, after ESP, or both

54

27

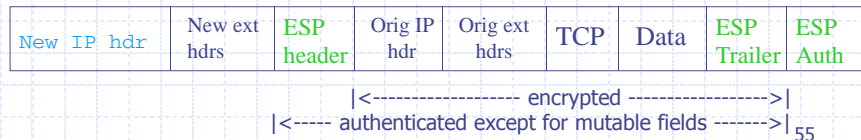## Fig. 5.14 ESP in tunnel mode

IPv4 – BEFORE APPLYING ESP

New IP hdr (any options)	Original IP hdr (any options)	TCP	Data

IPv4 – AFTER APPLYING ESP

New IP hdr (any options)	ESP header	Original IP hdr (any options)	TCP	Data	ESP Trailer	ESP Auth

```
                          |<------------------- encrypted ------------------->|
                          |<--------- authenticated except for mutable fields -------->|
```

IPv6 – BEFORE APPLYING ESP

New IP hdr	ext hdrs if present	Orig IP hdr	ext hdrs if present	TCP	Data

IPv6 – AFTER APPLYING ESP

New IP hdr	New ext hdrs	ESP header	Orig IP hdr	Orig ext hdrs	TCP	Data	ESP Trailer	ESP Auth

```
                          |<------------------- encrypted ------------------>|
                          |<----- authenticated except for mutable fields ------->|  55
```

5.2.1.8 Traffic Processing

- ◆ When a node wants to send a packet to another node, this outbound packet will be compared against the SPD to determine what processing is required for the packet.
- ◆ If IPsec processing is required, the packet is mapped into an existing SA or SA bundle in the SAD.
- ◆ If there is no SA that is currently available, a new SA or SA bundle is created for the packet.
  - To create a new SA or SA bundle, the communicating nodes may need to use IKE to establish IKE SA (SA bundle) first.
  - After the IKE SA is authenticated, IPsec SA is created under the protection of IKE SA.
- ◆ Once IPsec SA is established, either AH or ESP (or both) can be used in either transport mode or tunnel mode to protect the packets.
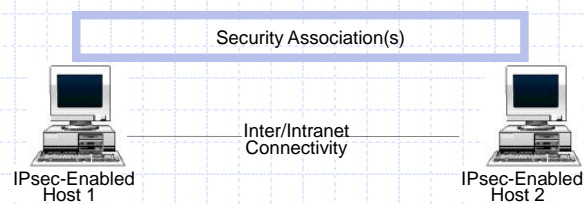
56

5.2.1.9 IPsec Applications

◆ End-to-end security
◆ VPN (virtual private network) with IPsec
◆ End-to-end with VPN security
◆ Secured remote access
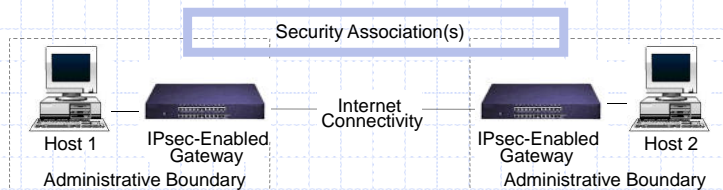
57

Fig. 5.15 End-to-end security

Security Association(s)

Inter/Intranet
Connectivity

IPsec-Enabled
Host 1

IPsec-Enabled
Host 2

Modes of operation:

Transport

| 1 | IP1 | AH | upper |

| 2 | IP1 | ESP | upper |

| 3 | IP1 | AH | ESP | upper |

Tunnel

| 1 | IP2 | AH | IP1 | upper |

| 2 | IP2 | ESP | IP1 | upper |

58

29

Fig. **5.16** VPN (virtual private network) with IPsec

Security Association(s)

Host 1 IPsec-Enabled Gateway   Internet Connectivity   IPsec-Enabled Gateway Host 2

Administrative Boundary   Administrative Boundary

Modes of Operation:

Tunnel

1   IP2 AH IP1 upper

2   IP2 ESP IP1 upper

59

Fig. **5.17** End-to-end with VPN security

Security Association(s)

Security Association(s)

IPsec-Enabled Host 1   IPsec-Enabled Gateway   Internet Connectivity   IPsec-Enabled Gateway   IPsec-Enabled Host 2

Administrative Boundary   Administrative Boundary
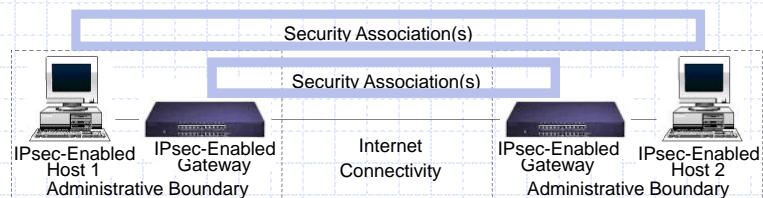
60

Fig. 5.18 Secured remote access

Transport Mode SA

Tunnel Mode SA

IPsec-Enabled
Host 1

Internet
(e.g. dialup PPP)

IPsec-Enabled
Gateway

IPsec-Enabled
Host 2

Administrative Boundary
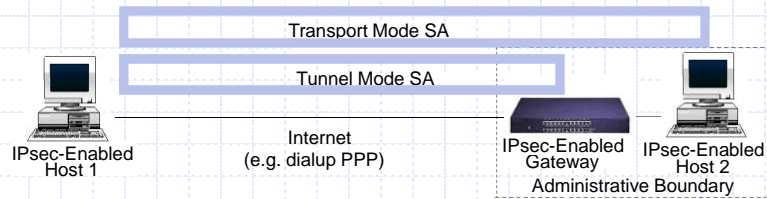
61

5.2.2 Authentication, Authorization, and Accounting (AAA)

5.2.2.1 Diameter

5.2.2.2 Diameter with Mobile IPv4 Application

62

AAA

- ◆ Remote Authentication Dial In User Service (RADIUS)
- ◆ SNMP
- ◆ COPS
- ◆ Diameter

63

5.2.2.1 Diameter

- ◆ Provide a base protocol to support AAA
- ◆ Typically not used alone unless used only for accounting
- ◆ Peer-to-peer protocol
  - A peer could be a client, agent, or server
- ◆ A agent could be a relay, proxy, redirect, or translation agent

64

Attribute Value Pair (AVP)

◆ Messages exchanged between peers
◆ Contain a header and a protocol-specific data
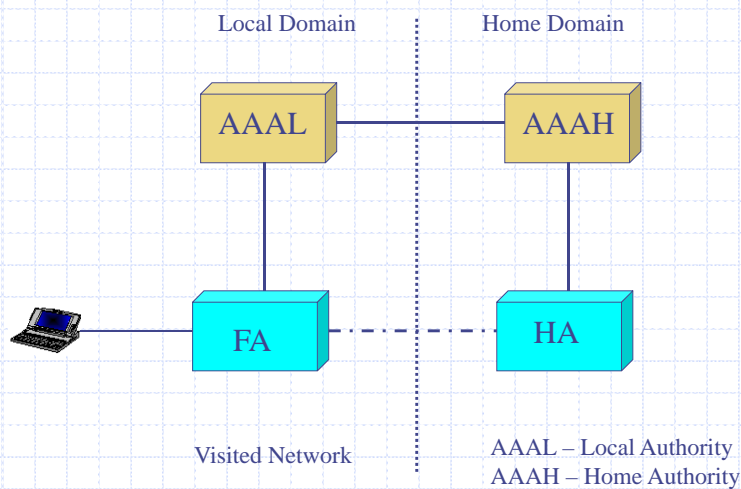◆ New Diameter applications can reuse existing AVPs and/or create new AVPs

65

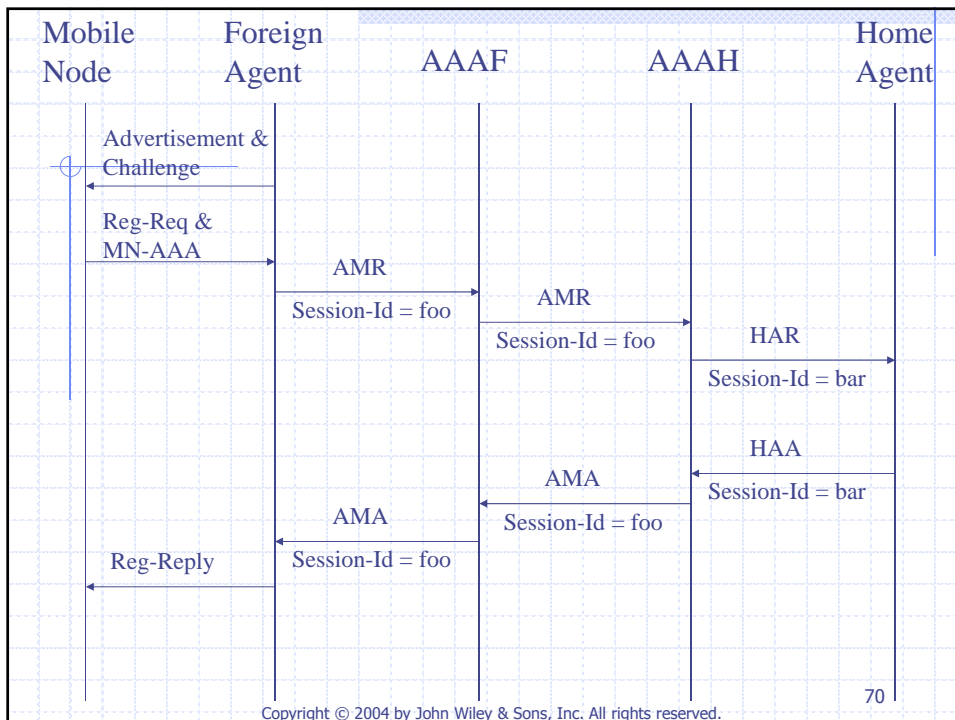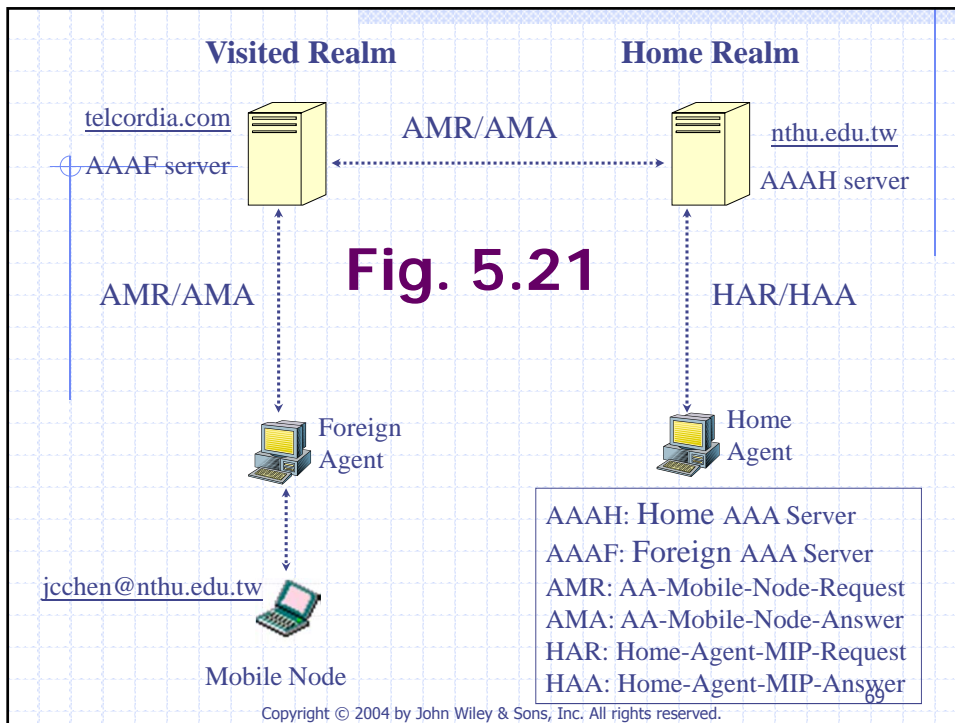# Fig. 5.19 Typical flows in Diameter

66

33
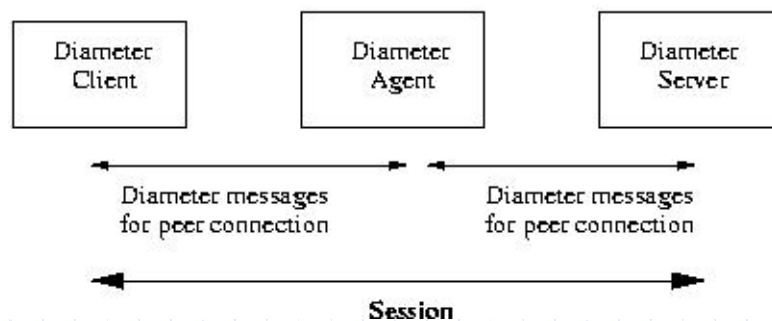
5.2.2.2 Diameter with Mobile IPv4 Application

◆ Allow Diameter to be used to authenticate, authorize and collect accounting information for Mobile IPv4 services

67

Fig. **5.20** Mobile IP with AAA

Local Domain   Home Domain

AAAL   AAAH

FA   HA

Visited Network   AAAL – Local Authority
AAAH – Home Authority

68

34

Visited Realm   Home Realm

telcordia.com   AMR/AMA   nthu.edu.tw

AAAF server   AAAH server

Fig. 5.21

AMR/AMA   HAR/HAA

Foreign
Agent

Home
Agent

jcchen@nthu.edu.tw

AAAH: Home AAA Server
AAAF: Foreign AAA Server
AMR: AA-Mobile-Node-Request
AMA: AA-Mobile-Node-Answer
HAR: Home-Agent-MIP-Request
HAA: Home-Agent-MIP-Answer

Mobile Node

69

| Mobile Node | Foreign Agent | AAAF | AAAH | Home Agent |

Advertisement & Challenge

Reg-Req & MN-AAA

AMR
Session-Id = foo

AMR
Session-Id = foo

HAR
Session-Id = bar

HAA
Session-Id = bar

AMA
Session-Id = foo

AMA
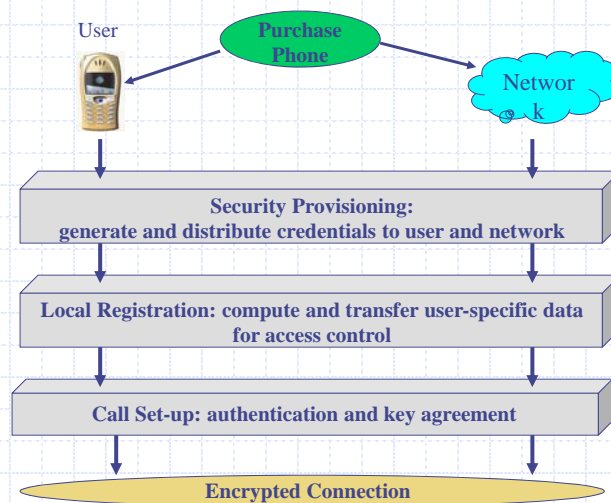Session-Id = foo

Reg-Reply

70

5.3 Security in Wireless Networks

◆ Security provisioning
◆ Local registration
◆ Authentication and key agreement (AKA)

71

Fig. **5.23** Generic security model in cellular systems

User

Purchase Phone

Network

Security Provisioning:
generate and distribute credentials to user and network

Local Registration: compute and transfer user-specific data for access control

Call Set-up: authentication and key agreement
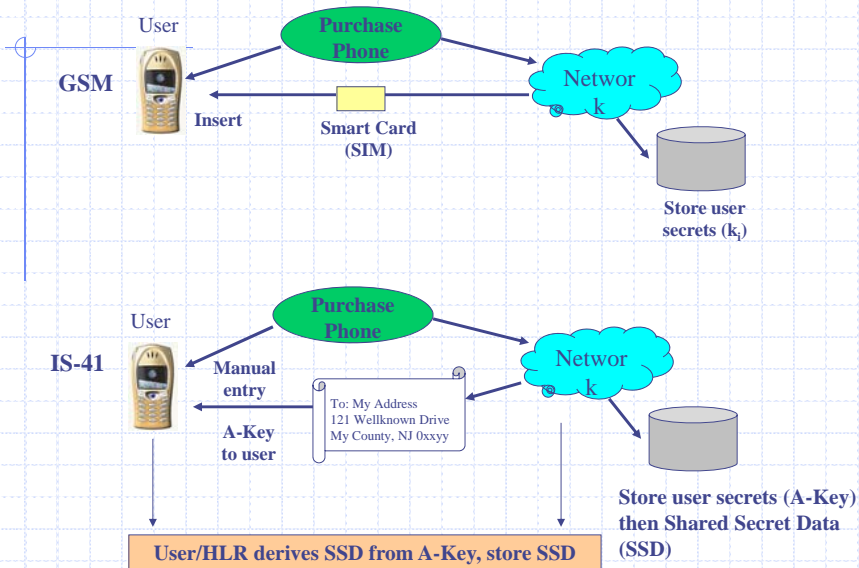
Encrypted Connection

72

Security Provisioning

◆ In GSM
- A secret key called K_i shared between the network operator and the user

◆ In IS-41
- A secret key called *Authentication Key (A-key)* shared by the user and the network provider

73

Fig. 5.24 Key generation and distribution
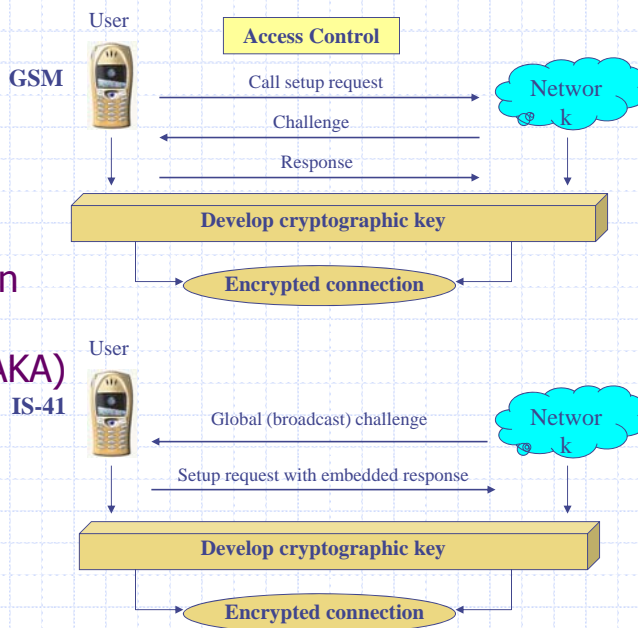
74

Authentication and Key Agreement (AKA)

◆ For GSM
   - Once the network receives a request for call setup, it challenges the user and expects a correct response from the user.

◆ For IS-41
   - Similar to GSM
   - IS-41 uses a global challenge that is broadcast periodically by the network

75

Fig. 5.25 Authentication and key agreement (AKA)

GSM — User — Access Control — Call setup request — Network — Challenge — Response — Develop cryptographic key — Encrypted connection

IS-41 — User — Global (broadcast) challenge — Network — Setup request with embedded response — Develop cryptographic key — Encrypted connection

76

5.4 Security in IS-41

5.4.1 Secret Keys

5.4.2 Authentication

5.4.3 Privacy

77

IS-41 Security

◆ Independent of the air interface

◆ Subscribers don't involve in the process

◆ Authentication Center (AC) is the primary functional entity

◆ Based on CAVE (Cellular Authentication and Voice Encryption) algorithm

78

Events for Authentication

- Registration
- Call origination
- Call termination

79

5.4.1 Secret Keys

- Authentication Key (A-key)
- Shared Secret Data (SSD)

80

40

Authentication Key (A-key)

- 64-bit *permanent* secret number used by MS and AC
- Installing A-key in the MS is not standardized
  - Program A-key manually: TIA/EIA TSB50
  - Over-the-air A-key programming: IS-725
- A-key is never transmitted over the air or passed between systems

81

Shared Secret Data (SSD)

- A 128-bit temporary secret key calculated in both MS and AC
- Can be shared with the serving system (VLR, etc.)
- Two parts
  - SSD-A: for authentication
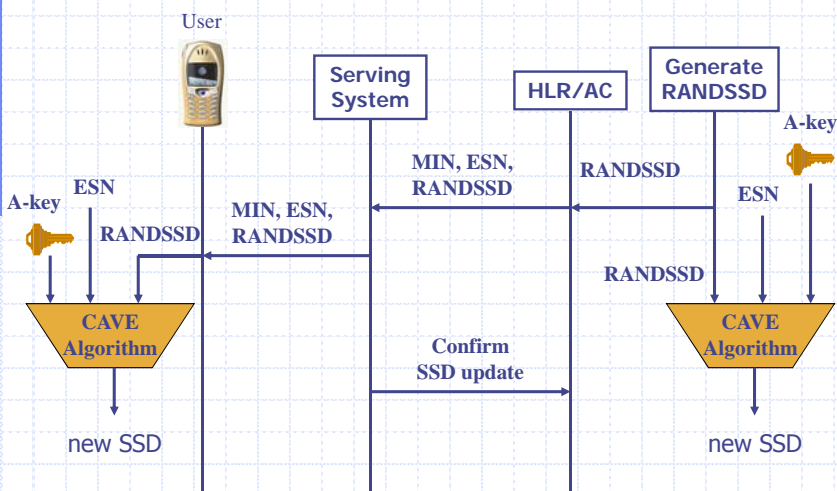 - SSD-B: for confidentiality

82

Generation of SSD

- ◆ Using CAVE algorithm
- ◆ Generate SSD random number (RANDSSD)
- ◆ Propagate to HLR/AC
  - ▪ Retrieve ESN (Electronic Serial Number) and MIN (Mobile ID)
- ◆ Propagate to the MS
- ◆ Generate SSD based on A-key, ESN, and RANDSSD
  - ▪ both MS and network

83

Fig. **5.26** Generation of shared secret data (SSD)

84

Fig. 5.27

User

Radio Interface

Serving System

HLR/AC

ESN, A-KEY

SSD Update Order (RANDSSD)

RANDSSD

RANDSSD

RANDSSD

ESN, A-KEY

CAVE Algorithm

CAVE Algorithm

RANDBS

BS Challenge Order (RANDBS)

RANDBS

RANDBS SSDnew

SSDnew

CAVE Algorithm

CAVE Algorithm

AUTHBS

BS Challenge Response (AUTHBS)

AUTHBS

AUTHBS

Verify AUTHBS

SSD = SSDNEW

SSD Update Confirmation

SSD = SSDNEW

5
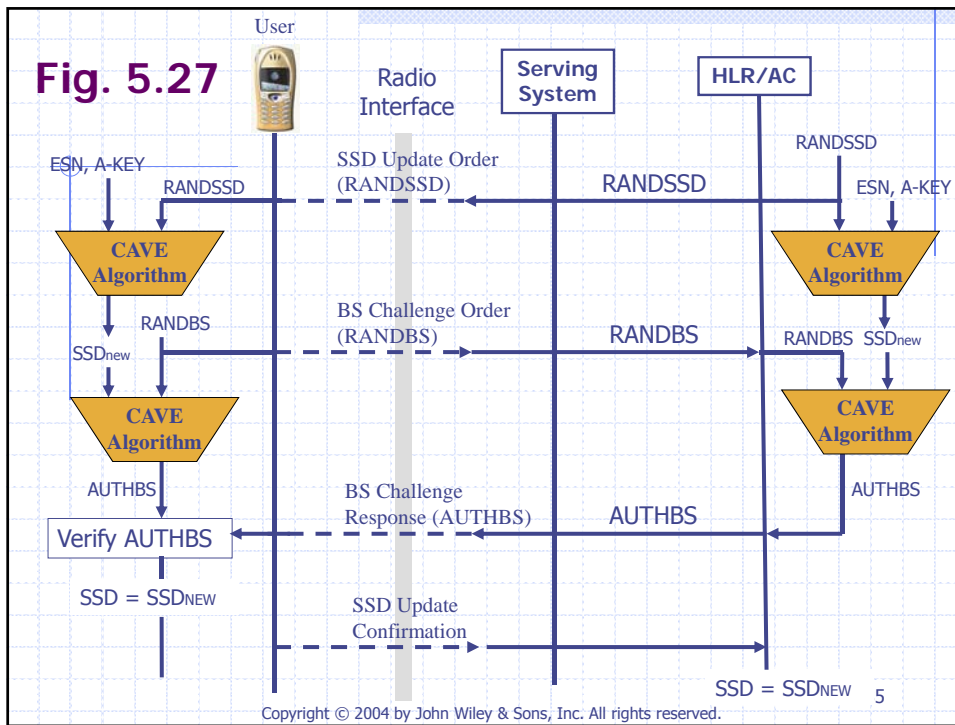
5.4.2 Authentication

◆ Global challenge
◆ Unique challenge

86

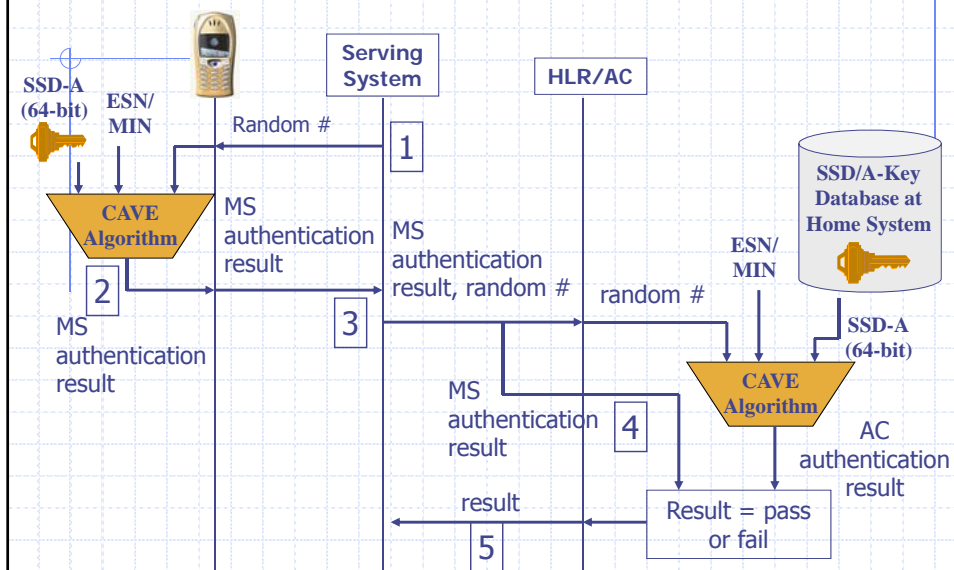# Global Challenge

♦ Serving system presents a challenge to all MSs using a particular radio control channel

  ■ Broadcast and update periodically

♦ AC verifies the response from an MS

87

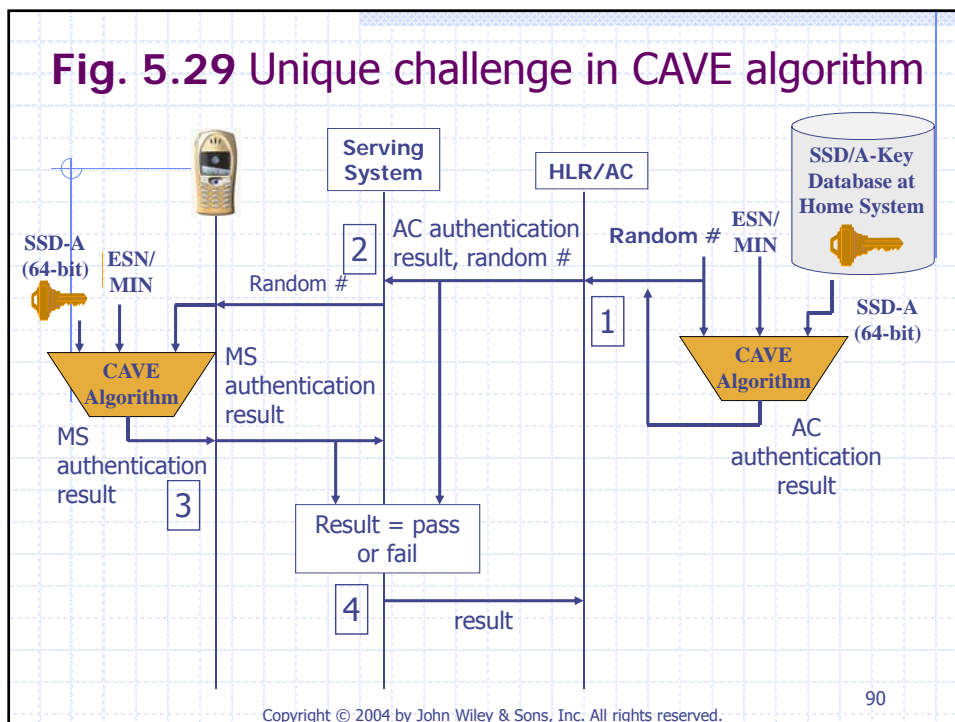**Fig. 5.28** Global challenge in CAVE algorithm

88

44

Unique Challenge

◆ AC directs the serving system to issue a challenge to a single MS which either is requesting service or is already engaged in a call

◆ MS and AC pass the calculation to the serving system

◆ The serving system verifies the authentication response

89

Fig. 5.29 Unique challenge in CAVE algorithm

90

45

5.4.3 Privacy

- ◆ Voice Privacy (VP)
    - ▪ VPMASK: generated using CAVE and SSD-B
- ◆ Signaling Message Encryption (SME)
    - ▪ Only certain fields of signaling messages are encrypted
    - ▪ SMEKEY: generated using CAVE and SSD-B
    - ▪ Cellular Message Encryption Algorithm (CMEA)
- ◆ Between MS and BS only

Weakness

- ◆ A 64-bit key may not be long enough
- ◆ Single cryptographic algorithm for authentication and privacy
- ◆ Does not provide for authentication of the network
- ◆ Critical key provisioning step required to get A-key to MS and AC
- ◆ Use of SSD and its periodic updating introduces complexity into the authentication process

5.5 Security in GSM

◆ Three algorithms

- A3: authentication
- A5: stream cipher algorithm
- A8: cipher key generation

93

Fig. 5.30 GSM algorithms

94

47
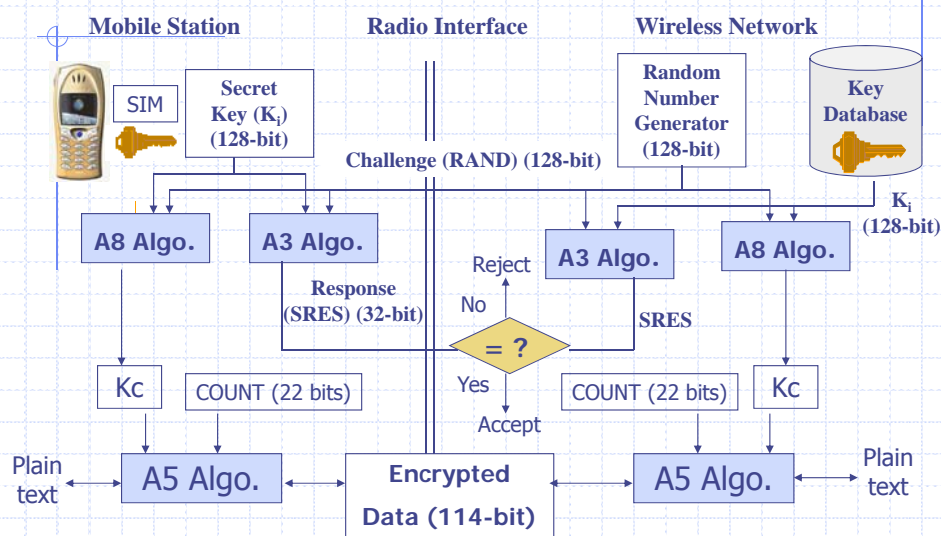
Weakness

- Does not provide for authentication of the network
- The home system trusts the visited system to handle cryptographic keying material, and to authenticate the MS
- Assume that the intersystem signaling links are secure
- A 64-bit key (Kc) may not long enough
- Lack of end-to-end encryption
- A number of attacks on the A5 algorithm have been reported

95

5.6 Security in GPRS

- Authentication: GSM authentication
- Confidentiality: GPRS Encryption Algorithm (GEA)
  - restricted to MS-SGSN encryption
  - installed in the MS and SGSN
  - ciphering for uplink and downlink are generated from different inputs

96

Fig. 5.31 GPRS encryption algorithm (GEA)

Input (32 bits) Direction (1 bit)

K_c (64 bits) → GEA

Output (≤1600 Octets)

Plain Text → ⊗ → Ciphered Text

Input (32 bits) Direction (1 bit)

K_c (64 bits) → GEA

Output (≤1600 Octets)

Ciphered Text → ⊗ → Plain Text
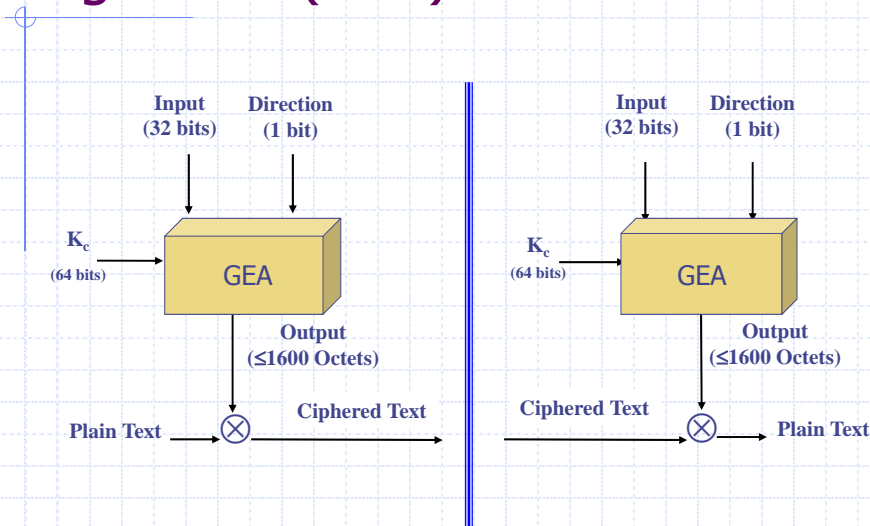
97

5.7 Security in 3GPP

5.7.1 Security Principles

5.7.2 Security Architecture

5.7.3 Network Access Security

5.7.4 Network Domain Security

5.7.5 Summary

98

5.7.1 Security Principles

◆ 3G security will build on the security of second generation systems. Security elements within GSM and other second generation systems that have proved to be **needed** and **robust** shall be adopted for 3G security.

◆ 3G security will improve on the security of second generation systems - 3G security will address and correct real and perceived weaknesses in second generation systems.

◆ 3G security will offer new security features and will secure new services offered by 3G.

99

Definitions

◆ **Confidentiality**: The property that information is not made available or disclosed to unauthorised individuals, entities or processes.

◆ **Data integrity**: The property that data has not been altered in an unauthorised manner.

◆ **Data origin authentication**: The corroboration that the source of data received is as claimed.

◆ **Entity authentication**: The provision of assurance of the claimed identity of an entity.

◆ **Key freshness**: A key is fresh if it can be guaranteed to be new, as opposed to an old key being reused through actions of either an adversary or authorised party.

100

Definitions (Cont.)

- **GSM Entity authentication and key agreement:** The entity Authentication and Key Agreement procedure to provide authentication of a SIM to a serving network domain and to generate the key Kc in accordance to the mechanisms specified in GSM 03.20.
- **User:** Within the context of this specification a user is either a UMTS subscriber or a GSM Subscriber or a physical person as defined in TR 21.905.
- **UMTS subscriber:** a Mobile Equipment with a UICC inserted and activated USIM-application.
- **GSM subscriber:** a Mobile Equipment with a SIM inserted or a Mobile Equipment with a UICC inserted and activated SIM-application.

101

Definitions (Cont.)

- **UMTS security context:** a state that is established between a user and a serving network domain as a result of the execution of UMTS AKA. At both ends "UMTS security context data" is stored, that consists at least of the UMTS cipher/integrity keys CK and IK and the key set identifier KSI. One is still in a UMTS security context, if the keys CK/IK are converted into Kc to work with a GSM BSS.
- **GSM security context:** a state that is established between a user and a serving network domain usually as a result of the execution of GSM AKA. At both ends "GSM security context data" is stored, that consists at least of the GSM cipher key Kc and the cipher key sequence number CKSN.
- **Quintet**, **UMTS authentication vector:** temporary authentication and key agreement data that enables an VLR/SGSN to engage in UMTS AKA with a particular user. A quintet consists of five elements: a) a network challenge RAND, b) an expected user response XRES, c) a cipher key CK, d) an integrity key IK and e) a network authentication token AUTN.

102

Definitions (Cont.)

◆ **Authentication vector**: either a quintet or a triplet.
◆ **Temporary authentication data:** either UMTS or GSM security context data or UMTS or GSM authentication vectors.
◆ **R98-:** Refers to a network node or ME that conforms to R97 or R98 specifications.
◆ **R99+:** Refers to a network node or ME that conforms to R99 or later specifications.
◆ **R99+ ME capable of UMTS AKA**: either a R99+ UMTS only ME, a R99+ GSM/UMTS ME, or a R99+ GSM only ME that does support USIM-ME interface.
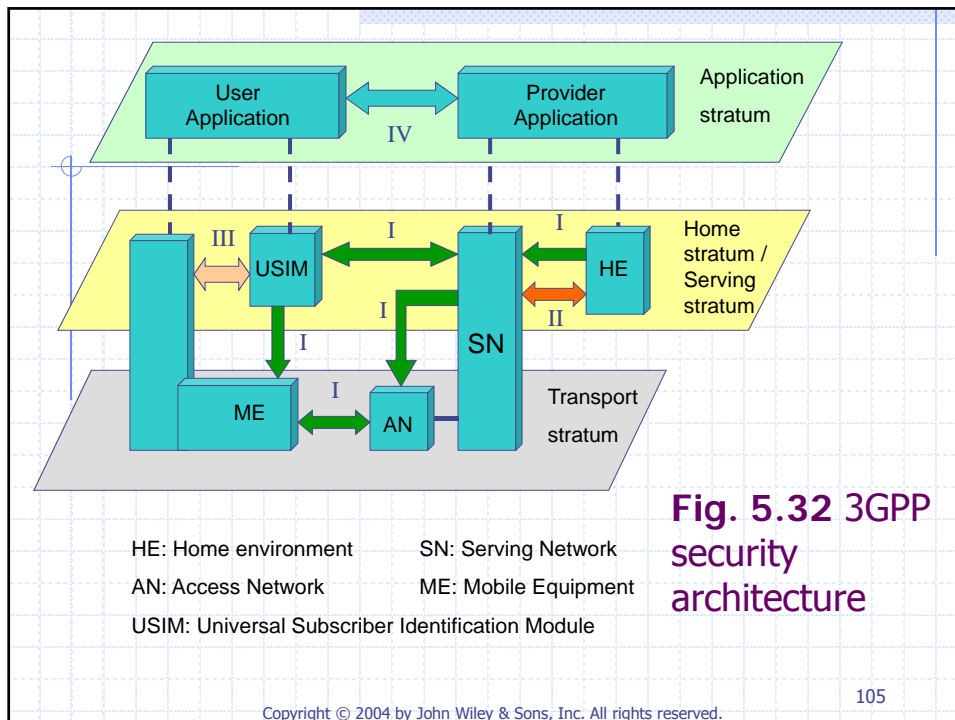◆ **R99+ ME not capable of UMTS AKA:** a R99+ GSM only ME that does not support USIM-ME interface.

103

5.7.2 Security Architecture

◆ **Network access security (I)**: the set of security features that provide users with secure access to 3G services, and which in particular protect against attacks on the (radio) access link;
◆ **Network domain security (II):** the set of security features that enable nodes in the provider domain to securely exchange signalling data, and protect against attacks on the wireline network;
◆ **User domain security (III):** the set of security features that secure access to mobile stations;
◆ **Application domain security (IV):** the set of security features that enable applications in the user and in the provider domain to securely exchange messages;
◆ **Visibility and configurability of security (V):** the set of features that enables the user to inform himself whether a security feature is in operation or not and whether the use and provision of services should depend on the security feature.

104

Fig. 5.32 3GPP security architecture

HE: Home environment   SN: Serving Network

AN: Access Network   ME: Mobile Equipment

USIM: Universal Subscriber Identification Module

105

Visibility

◆ Indication of access network encryption: the property that the user is informed whether the confidentiality of user data is protected on the radio access link, in particular when non-ciphered calls are set-up.

◆ Indication of the level of security: the property that the user is informed on the level of security that is provided by the visited network, in particular when a user is handed over or roams into a network with lower security level (3G -> 2G).

106

Configurability

◆ Enabling/disabling user-USIM authentication: the user should be able to control the operation of user-USIM authentication, e.g., for some events, services or use.

◆ Accepting/rejecting incoming non-ciphered calls: the user should be able to control whether the user accepts or rejects incoming non-ciphered calls;

◆ Setting up or not setting-up non-ciphered calls: the user should be able to control whether the user sets up connections when ciphering is not enabled by the network;

◆ Accepting/rejecting the use of certain ciphering algorithms: the user should be able to control which ciphering algorithms are acceptable for use.
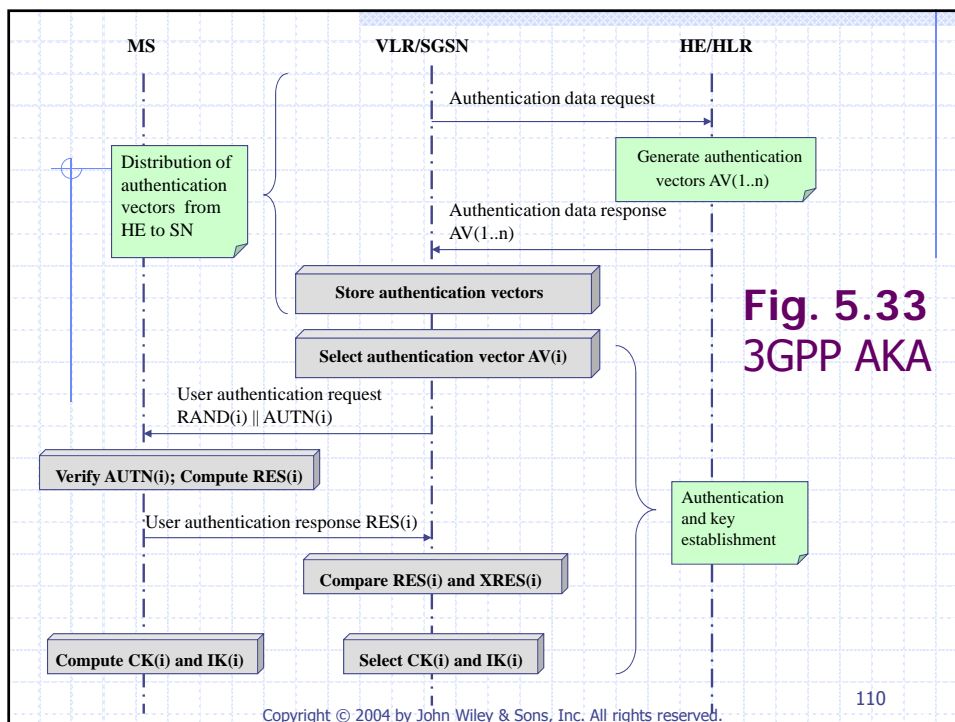
107

5.7.3 Network Access Security

5.7.3.1 Authentication and Key Agreement (AKA)

5.7.3.2 UMTS Encryption Algorithm (UEA)

5.7.3.3 UMTS Integrity Algorithm (UIA)

108

5.7.3.1 Authentication and Key Agreement (AKA)

- ◆ Main purpose
  - Mutual authentication
  - Establish a new pair of cipher and integrity keys
- ◆ Secret key K: shared between and available only to the USIM and the AuC in the user's HE
- ◆ SQN_{HE}: an individual counter for each user kept in HE
- ◆ SQN_{MS}: the highest sequence number the USIM has accepted
- ◆ Achieve maximum compatibility with the current GSM security architecture

109

| MS | VLR/SGSN | HE/HLR |

Authentication data request

Distribution of authentication vectors from HE to SN

Generate authentication vectors AV(1..n)

Authentication data response AV(1..n)

Store authentication vectors

Select authentication vector AV(i)

Fig. 5.33 3GPP AKA

User authentication request RAND(i) ‖ AUTN(i)

Verify AUTN(i); Compute RES(i)

Authentication and key establishment

User authentication response RES(i)

Compare RES(i) and XRES(i)

Compute CK(i) and IK(i)   **Select CK(i) and IK(i)**

110

55

Authentication Vector (AV)

- ◆ Ordered based on sequence number
- ◆ Consists of the following components
  - ■ a random number RAND
  - ■ an expected response XRES
  - ■ a cipher key CK
  - ■ an integrity key IK
  - ■ an authentication token AUTN
- ◆ Each authentication vector is good for one AKA between the VLR/SGSN and the USIM

111

Fig. **5.34** Generation of authentication vectors

| Generate SQN |
| Generate RAND |

SQN

RAND

AMF

Master Key (K) (128-bit)

| f1: MAC algorithm | f2: authenti-cation algo. | f3: cipher key generator | f4: integrity key generator | f5: anonymity key generator |

| MAC | XRES | CK | IK | AK |

AUTN := SQN $\oplus$ AK || AMF || MAC

AV := RAND || XRES || CK || IK || AUTN

112

56
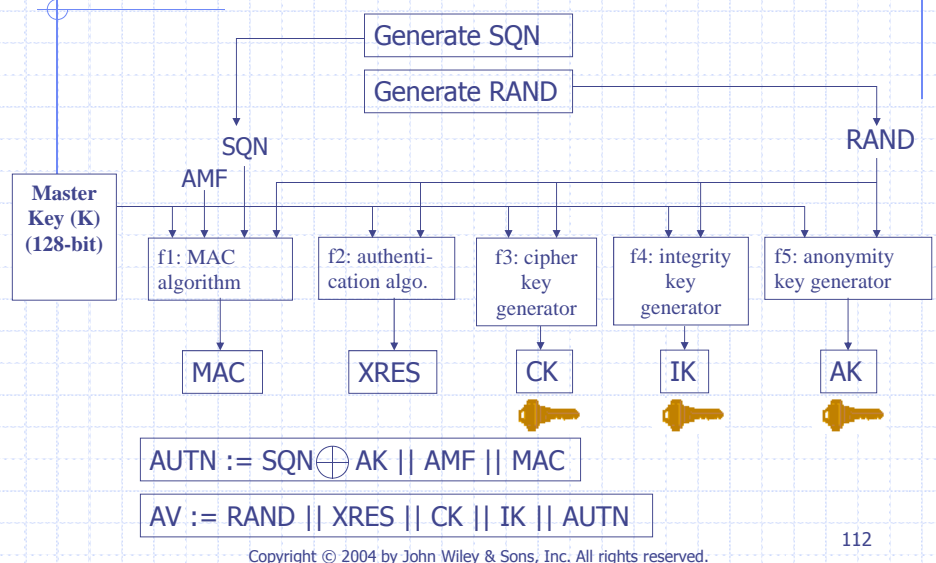
Anonymity Key (AK)

- AK is used to conceal the sequence number (SQN)
  - SQN may expose the identity and location of the user
- $f5 \equiv 0$, i.e. AK = 0 if no concealment is needed
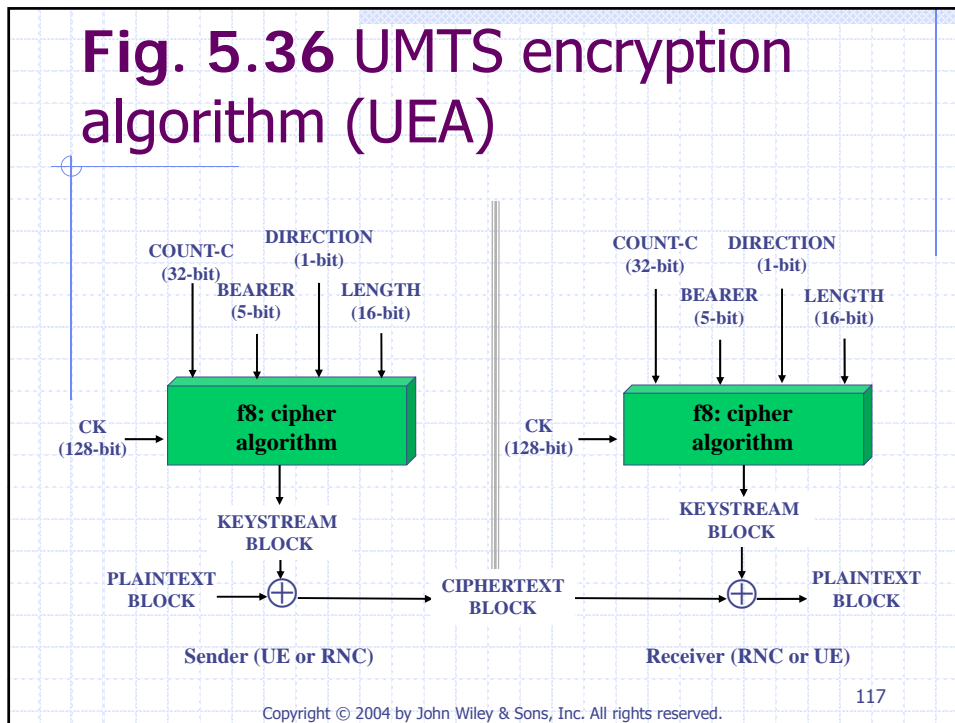
113

Fig. 5.35 Authentication process in USIM

114

57
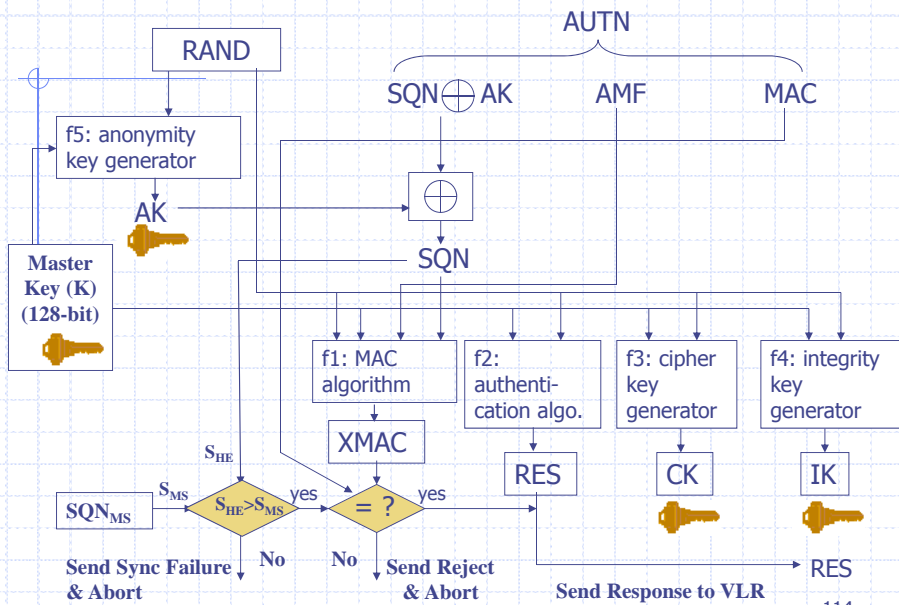
Key Length

- K: 128 bits
- RAND: 128 bits
- SQN: 48 bits
- AK: 48 bits
- AMF: 16 bits
- MAC: 64 bits
- CK: 128 bits
- IK: 128 bits
- RES: 32-128 bits

115

5.7.3.2 UMTS Encryption Algorithm (UEA)

- Access Link Data Confidentiality
- For data and some signaling traffic
- Applied on dedicated channels between ME and RNC

116

Fig. 5.36 UMTS encryption algorithm (UEA)

COUNT-C (32-bit)   DIRECTION (1-bit)
BEARER (5-bit)   LENGTH (16-bit)

CK (128-bit) → **f8: cipher algorithm**

KEYSTREAM BLOCK

PLAINTEXT BLOCK → ⊕ → CIPHERTEXT BLOCK → ⊕ → PLAINTEXT BLOCK

Sender (UE or RNC)   Receiver (RNC or UE)

117

5.7.3.3 UMTS Integrity Algorithm (UIA)

◆ Access Link Data Integrity
◆ Shall be implemented in the ME and in the RNC
◆ Most control signaling messages between ME and RNC are integrity protected
◆ Integrity protection should be applied at the RRC layer

118

Fig. 5.37 UMTS integrity algorithm (UIA)

COUNT-I (32-bit) DIRECTION (1-bit) MESSAGE FRESH (32-bit)

IK (128-bit) → **f9: integrity algorithm**

MAC-I

Sender (UE or RNC)

COUNT-I (32-bit) DIRECTION (1-bit) MESSAGE FRESH (32-bit)

IK (128-bit) → **f9: integrity algorithm**

XMAC-I

Receiver (RNC or UE)
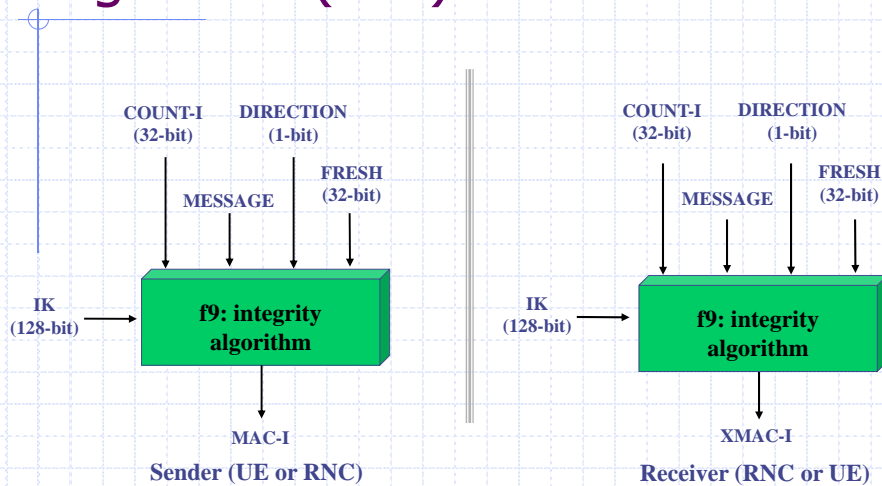
119

FRESH

- At connection set-up the RNC generates a random value FRESH and sends it to the user.
- The value FRESH is subsequently used by both the network and the user throughout the duration of a single connection.
- This mechanism protects the network against replay of signalling messages by the user.
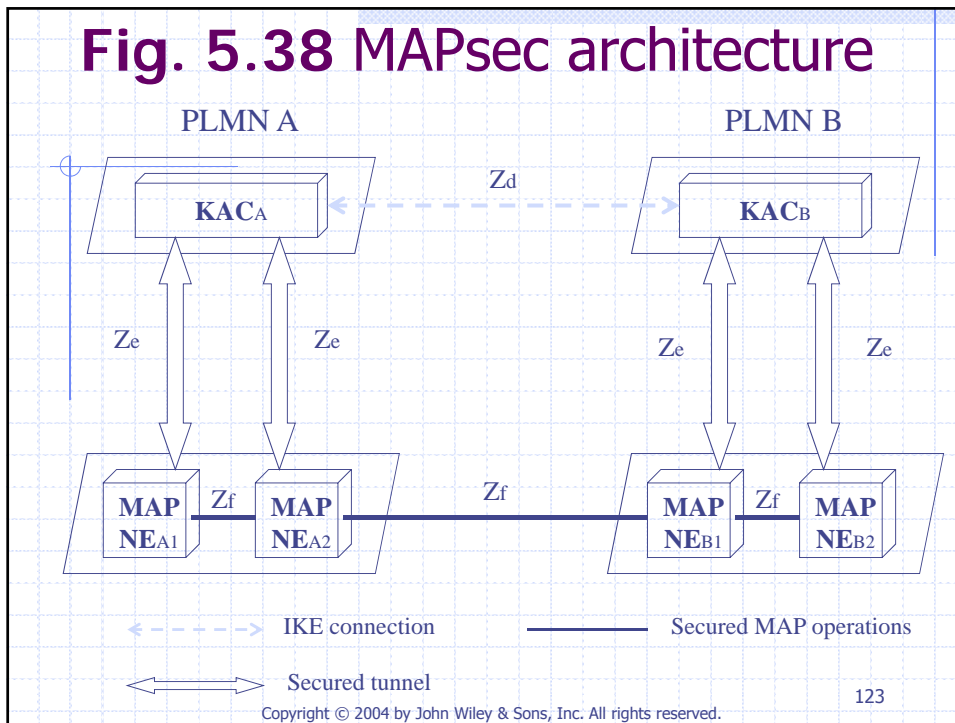
120

5.7.4 Network Domain Security

- IP network layer security
  - IPsec
- MAP application layer security
  - MAPsec

121

5.7.4.1 MAP Security (MAPsec)

- Protect the core network SS7 signalling protocols
- Confidentiality, integrity, authentication and anti-replay protection have been identified as necessary

122

Fig. 5.38 MAPsec architecture

PLMN A

PLMN B

Z_d

KAC$_A$

KAC$_B$

Z_e Z_e

Z_e Z_e

MAP NE$_{A1}$ Z_f MAP NE$_{A2}$ Z_f MAP NE$_{B1}$ Z_f MAP NE$_{B2}$

IKE connection   Secured MAP operations

Secured tunnel

123

Protection Modes

◆ Protection Mode 0: no protection
◆ Protection Mode 1: integrity, authenticity
◆ Protection Mode 2: confidentiality, integrity, and authenticity

124

Message Format

- ◆ Protection Mode 0:
  - *Security header = SPI || Original component Id*
- ◆ Protection Mode 1 and 2:
  - *Security header = SPI || Original component Id || TVP || NE-Id || Prop*

125

Fig. **5.39** Protection mode 1 in MAPsec

Security Header	payload	MAC-M

|<------------------- authenticated ----------------->|

126
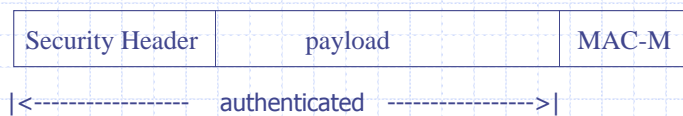
Fig. 5.40 Protection mode 2 in MAPsec

Security Header	payload	MAC-M

|<--------- encrypted -------->|

|<------------------ authenticated ----------------->|

127

Release 99+ HLR/AuC

Quintets

Release 99+ VLR/SGSN

CK,IK

UTRAN

RAND,AUTN,RES

R99+ ME capable of UMTS AKA

CK,IK

USIM

Fig. 5.41 3GPP network access security

128

Slide 1 (diagram)

Release 99+ HLR/AuC		CK,IK → Kc RES → SRES

Quintets   Triplets

Release 99+ VLR/SGSN CK,IK → Kc CK,IK → Kc RES → SRES **Release 98 – VLR/SGSN** — SGSN /VLR

CK,IK   [Kc]   [Kc]   [Kc]

UTRAN   **GSM BSS**   RNC/ BSS

RAND,AUTN,RES RAND,AUTN,RES RAND,[AUTN],SRES RAND,SRES

R99+ ME capable of UMTS AKA **R99+ ME not capable of UMTS AKA or R98. ME** **ME** ME

CK,IK,Kc CK,IK,Kc Kc Kc

CK,IK → Kc	CK,IK → Kc	CK,IK → Kc RES → SRES	CK,IK → Kc RES → SRES

USIM

◄— UMTS security context —►◄— GSM security context —►

129

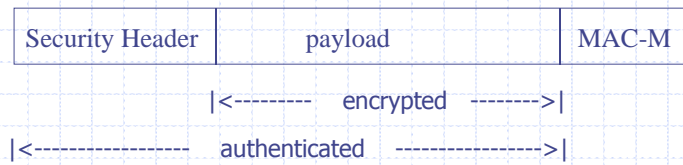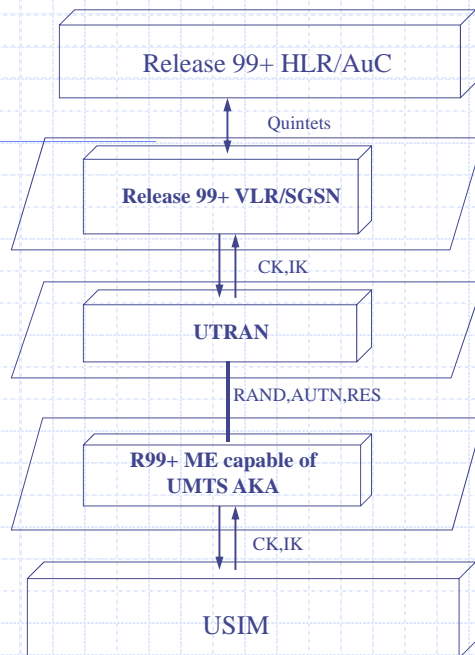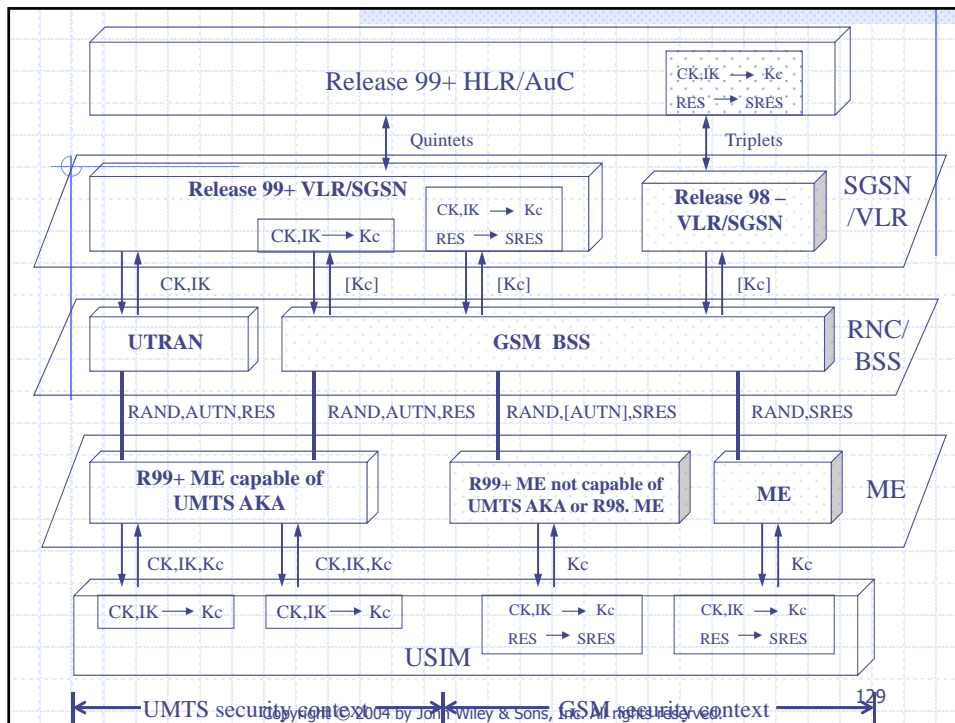## Security in IMS

- ◆ SIP is chosen as the signaling protocol for creating and terminating Multimedia sessions
- ◆ IMS security deals with
  - How the SIP signaling is protected between the subscriber and the IMS
  - How the subscriber is authenticated
  - How the subscriber authenticates the IMS

130

Lawful Interception

◆ The lawful interception provides means for an authorized person to access sensitive information and monitor other users.

◆ It however should be compliance with the national or regional laws and technical regulations.

131

5.8 Security in 3GPP2

5.8.1 Network Access Security
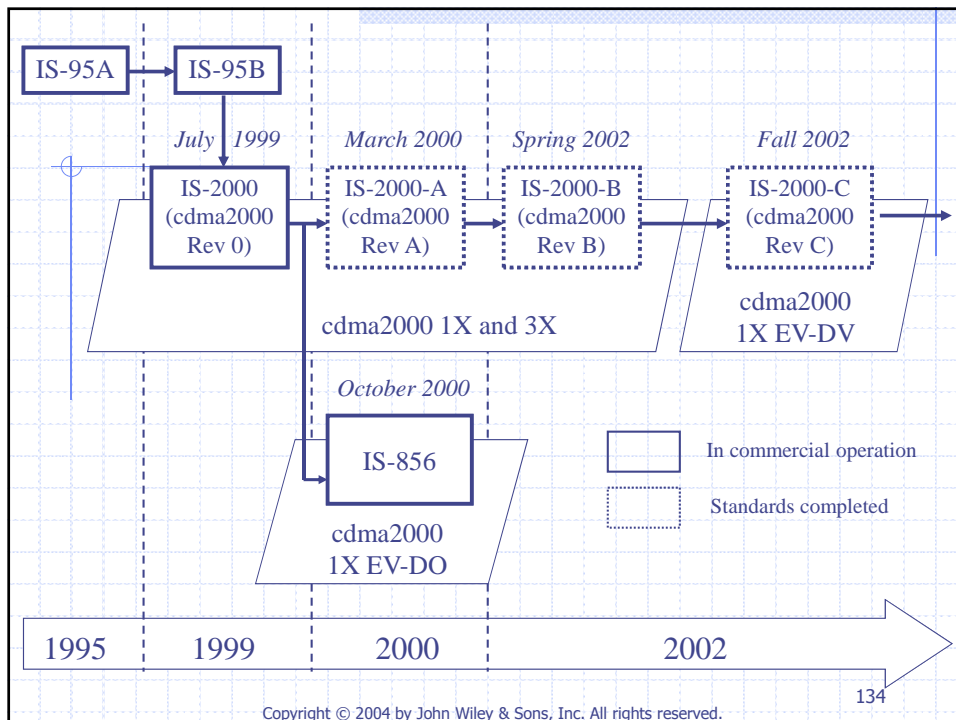
5.8.2 Network Domain Security

132

3GPP2 Security

◆ Network Access Security
  - AKA
  - Privacy
  - Integrity
◆ Network Domain Security
  - IPsec
  - AAA

133

| IS-95A | → | IS-95B |

July 1999

IS-2000
(cdma2000
Rev 0)

March 2000

IS-2000-A
(cdma2000
Rev A)

Spring 2002

IS-2000-B
(cdma2000
Rev B)

Fall 2002

IS-2000-C
(cdma2000
Rev C)

cdma2000 1X and 3X

cdma2000
1X EV-DV

October 2000

IS-856

cdma2000
1X EV-DO

In commercial operation

Standards completed

| 1995 | 1999 | 2000 | 2002 |

134

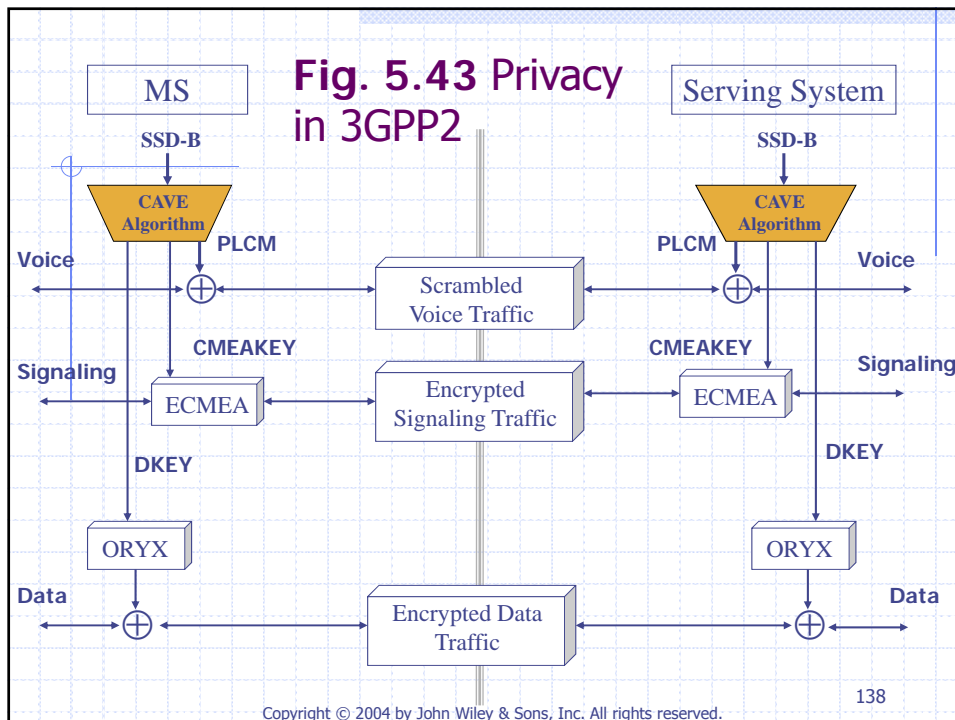# 5.8.1.1 Authentication and Key Agreement (AKA)

- ◆ cdma2000 1x and 3x (Rev B and earlier): IS-41 CAVE
- ◆ Enhanced Subscriber Authentication (ESA): 1x EV-DV (Rev C)
  - ▪ Similar to 3GPP AKA
- ◆ cdma2000 1x EV-DO: PPP Challenge Handshake Authentication Protocol (CHAP)

135

Enhanced Subscriber Authentication (ESA)

- ◆ ESA Requirements
  - ▪ The *root authentication key* should be known only to the MS and the Authentication Center (AC) in the home network.
  - ▪ The ESA should employ 128-bit authentication key and support mutual authentication.
  - ▪ The ESA should be backward compatible with CAVE.
  - ▪ The ESA should be able to negotiate the cryptographic algorithms.
  - ▪ The ESA algorithm should be published openly and commercially available, and should have been scrutinized thoroughly.
- ◆ TR-45 has adopted 3GPP AKA as the basis

136

5.8.1.2 Privacy

- ◆ cdma2000 1x and 3x (Rev 0 and Rev A): IS-41 CAVE
- ◆ Enhanced Subscriber Privacy (ESP): Rev B and later
  - ▪ 128-bit Rijndael AES
- ◆ cdma2000 1x EV-DO: AES

Fig. 5.43 Privacy in 3GPP2

MS		Serving System

SSD-B

CAVE Algorithm

PLCM

Voice

Scrambled Voice Traffic

CMEAKEY

Signaling

ECMEA

Encrypted Signaling Traffic

DKEY

ORYX

Data

Encrypted Data Traffic

SSD-B

CAVE Algorithm

PLCM

Voice

CMEAKEY

Signaling

ECMEA

DKEY

ORYX

Data

Enhanced Subscriber Privacy (ESP)

- Keys for ESP may be based on the root authentication key but should be cryptographically decoupled from the keys used for authentication.
- The privacy key in MS can be modified under control of the home system.
- Keys for ESP are changed with each new security association.
- Privacy keys for each call are established at the time when a mobile is authenticated.
- Privacy keys for control channel are established after a mobile is authenticated successfully.

139

5.8.1.3 Integrity

- cdma2000 1x and 3x (Rev B and earlier): no integrity service
- cdma2000 1x EV-DV (Rev C):
  - Similar to 3GPP UIA
- cdma2000 1x EV-DO: no integrity service

140

5.8.2 Network Domain Security

- ◆ For both Simple IP and Mobile IP access mechanisms, IP network authentication of the mobile station is via a static security association between the mobile station and the home IP network.
- ◆ For Mobile IP, the service provider network shall use the Foreign Agent Challenge to authenticate and authorize the mobile station.
- ◆ For Simple IP the service provider network may use CHAP or PAP to authenticate and authorize the mobile station;
  - if the mobile station does not support CHAP or PAP, there is no IP network authentication.

141

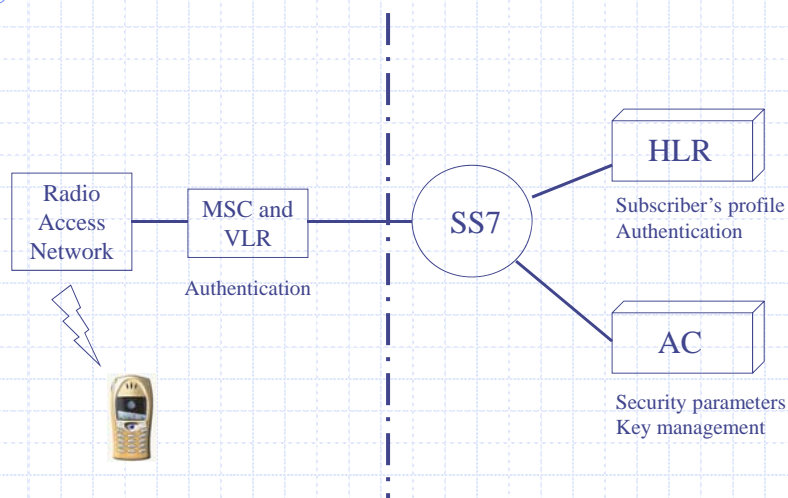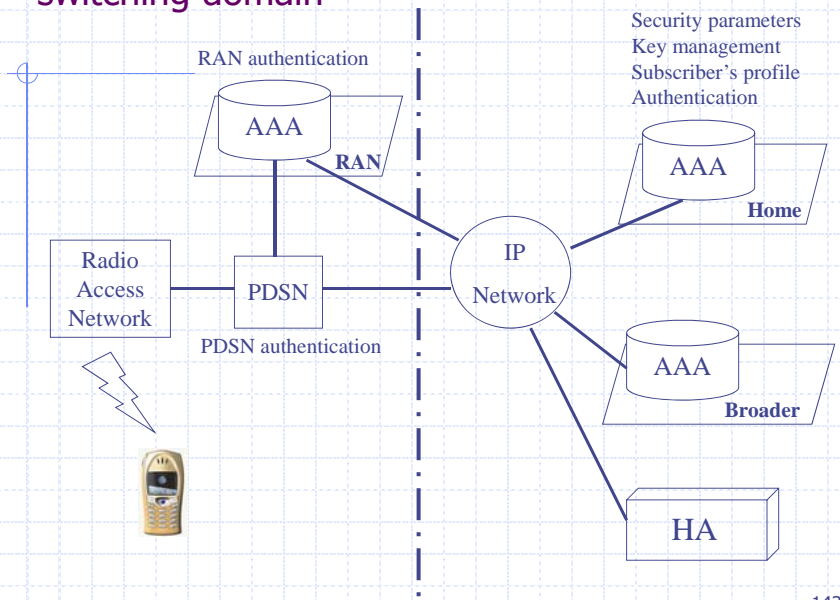# Fig. 5.44 Security architecture for circuit-switching domain

142

Fig. 5.45 Security architecture for packet-switching domain

Security parameters
Key management
Subscriber's profile
Authentication

RAN authentication

AAA
RAN

AAA
Home

Radio Access Network

PDSN

IP Network

AAA
Broader

PDSN authentication

HA

143

PPP Session Authentication

◆ The PDSN should support CHAP and PAP.

◆ The PDSN should also support a configuration option to allow an MS to receive Simple IP service without CHAP or PAP.

144

PDSN

- ◆ The PDSN should support IPsec and IKE.
- ◆ A SA between the PDSN in a visited network and the mobile's Mobile IP HA may be established using X.509-based certificates.
- ◆ Alternatively, a shared secret for IKE may be statically configured or dynamically provisioned by the mobile's Home AAA server.
- ◆ IPsec ESP is preferred over AH
  - To insure backward compatibility, AH should also be implemented.
- ◆ The PDSN should act as a AAA client for the AAA server.

145

Authentication, Authorization and Accounting (AAA)

- ◆ May support both the IP domain and the legacy circuit-switching domain.
- ◆ Provide IP based Authentication, Authorization, and Accounting
- ◆ Maintains security associations with peer AAA entities to support intra- and/or inter-administrative domain AAA functions

146

Fig. 5.46

147

74