

etaCOM 1996
Emerging Technologies &
Applications in Communications

Wireless Security Implementation

Çetin Kaya Koç
Oregon State University
Koc@ece.orst.edu

May 10, 1996

1

Contents

- Fundamentals of Network Security
- Cryptographic Techniques and Tools
- Threats to Wireless Communication
- Security Services and Requirements
- GSM Security Implementation

2

Network Security

In a typical network environment, there are three aspects information of security:

- *Security Attacks*: Actions which compromise the security of information
- *Security Mechanisms*: Methods to detect, prevent, or recover from security attacks
- *Security Services*: A service which employs one or more security mechanisms to enhance the security of the network

3

Security Services

- *Confidentiality*: Stored or transmitted information is accessible only by authorized parties
- *Authentication*: Identity of the origin of the message is correctly identified
- *Integrity*: Stored or transmitted information and system assets are modified only by authorized parties

4

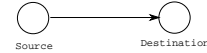
Security Services

- *Nonrepudiation*: Sender or receiver cannot deny the transmission
- *Access Control*: Information resources are controlled
- *Availability*: Network resources are available to authorized parties

5

Security Attacks

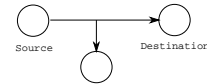
One categorization of the security attacks is to consider the effect of the attack on the normal flow of information:



- *Interruption*: An asset of the system is destroyed or has become unavailable. This is an attack on **availability**.



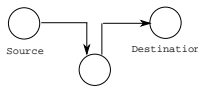
- *Interception*: An unauthorized part gains access to the system assets. This is an attack on **confidentiality**.



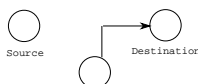
6

Security Attacks

- *Modification*: An unauthorized party gains access and modifies an assets. This is an attack on **integrity**.



- *Fabrication*: An unauthorized party inserts counterfeit objects into the system This is an attack on **authenticity**.



7

Passive and Active Attacks

Another useful categorization is in terms of *passive* and *active* attacks

Passive Attacks: Attacks to **confidentiality**

- *Access to message content*: Sensitive or confidential information is accessed by an unauthorized party.
- *Traffic analysis*: The unauthorized party determines the location and identity of the communicating entities, obtains the length and frequency of the message. This information can be used to guess the nature of communication.

8

Active Attacks

- *Masquerade* (Attack to **authenticity**)
An entity pretends to be another entity.
The purpose is to obtain extra privileges
- *Replay* (Attack to **integrity**)
Passive capture of data and its subsequent transmission to produce an unauthorized effect

9

Active Attacks

- *Modification* (Attack to **integrity**)
Legitimate data is altered, delayed, or re-ordered to produce an unauthorized effect
- *Denial of service* (Attack to **availability**)
Attacking a specific target, e.g., suppressing all messages directed to a particular destination

10

Security Mechanisms

In order to detect, prevent, or recover from these security attacks, we use security mechanisms

There is no single mechanism which will provide all the services or perform all the functions mentioned

A variety of mechanisms are used to detect and prevent certain attacks, and to provide certain functions and services

However, most security mechanisms use methods and tools from **cryptography**

11

Cryptography

The art/science of designing and breaking ciphers

Traditionally, cryptography was used by the military and diplomatic services for secure communication

Public-key cryptography offers techniques for authenticating data and exchanging keys over an insecure network

Cryptographic techniques provide the methods and tools required to establish the security services of a network

12

Tools from Cryptography

- Key-agreement protocols
- Secret-key cryptosystems
 - Encryption algorithms
- Public-key cryptosystems
 - Encryption and signature algorithms
- Digital signatures
- Authentication protocols
- Message authentication codes
- Proofs of knowledge protocols
- Message digest functions

13

Security using Cryptography

- Protection against interception:
 - Encryption, secret-key cryptographic algorithms provide confidentiality
- Protection against modification:
 - Signatures provide authentication of data and user identity
- Access control also protects against interception and modification

14

Cryptographic Protocols

Actions involving two or more parties which use cryptographic techniques

Protocols usually involve basic cryptographic algorithms

Protocols may contain components other than algorithms

Protocols may provide more complicated security services than algorithms

15

Security Services by Cryptography

- Confidentiality
 - Provided by secret-key and public-key cryptographic algorithms
- Authentication
 - Data origin authentication by message authentication codes, digital signatures, and hash functions
 - Entity authentication by protocols
- Key Management
 - Key establishment and key backup services

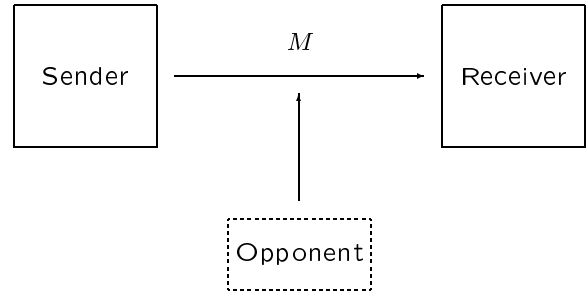
16

Security and Cryptography

- Cryptography is the basis for security services
- Security services are implemented with algorithms and protocols
- Protocols rely on algorithms
- Algorithms require secret keys which are handled by key management architecture
- Key management architecture relies on security services

17

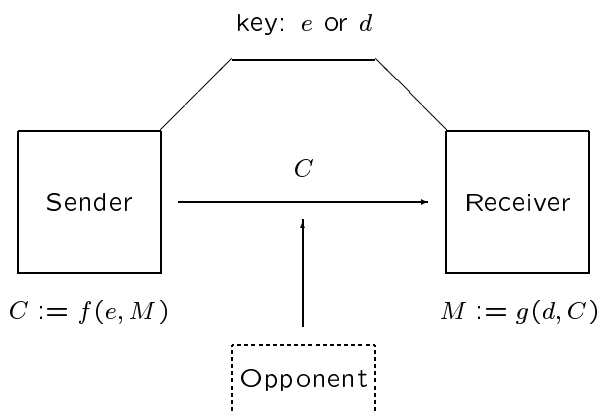
Cryptographic Techniques and Tools



Objective: Secure communication over an insecure channel

18

Secret-Key Cryptography



Exchange the key over a **secure** channel

19

Secret-Key Cryptography

- Functions $f(e, -)$ and $g(d, -)$ are inverses of one another
- Encryption and decryptions processes are **symmetric**:

Either $f = g$ and $e \neq d$

$C := f(e, M)$ and $M := f(d, C)$

d is **easily** deduced from e

e is **easily** deduced from d

Or $f \neq g$ and $e = d$

$C := f(e, M)$ and $M := g(e, C)$

g is **easily** deduced from f

f is **easily** deduced from g

20

Data Encryption Standard

DES was designed by a group at IBM TJ Watson Research Center at the request of the US NIST for the protection of sensitive unclassified data

DES has become a US federal standard in 1976 to be reviewed every 5 years

It was reaffirmed in 1987

In 1992, after some controversy, it was recertified for another 5 years

21

Data Encryption Standard

DES is a block cipher operating on a 64-bit plaintext to produce a 64-bit ciphertext with a key size of 56 bits

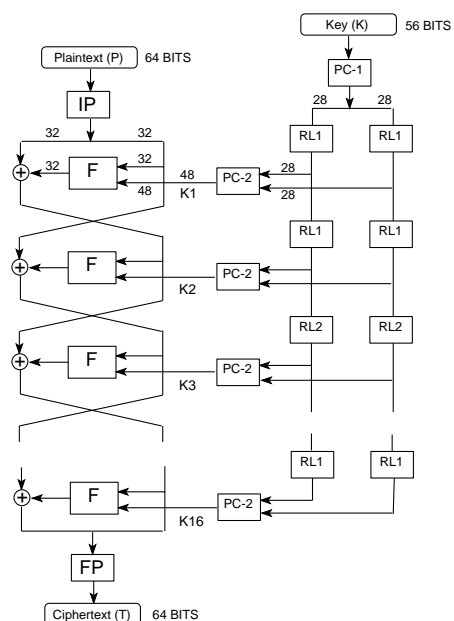
The fundamental building block is a substitution followed by a permutation on the text, based on the key

This is called a round function

DES has 16 rounds

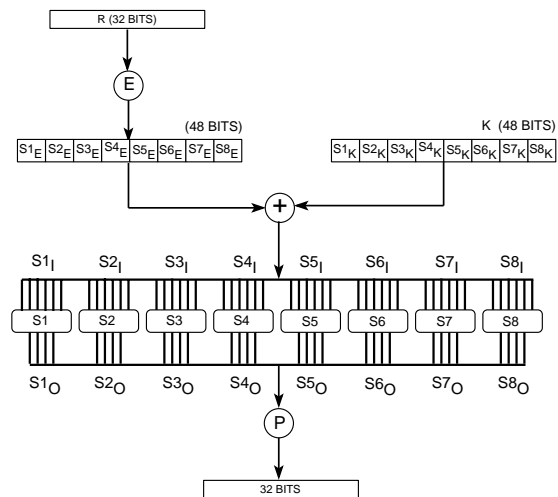
22

Outline of DES



23

Round Function of DES



24

Public-Key Cryptography

Problems with secret-key cryptography:

- requires establishment of a secure channel for key exchange
- two parties cannot start communication if they never met

Alternative: Public-Key Cryptography (PKC)

- requires establishment of a public-key directory in which everyone publishes their encryption keys
- two parties can start communication even if they never met
- provides ability to sign digital data

25

Key Exchange

- Parties S and R agree on a large prime number p

This is accomplished in public

- S selects $a \in GF(p)$ and computes a^{-1} such that $a \cdot a^{-1} = 1 \pmod{p-1}$

S keeps these integers secret

- R selects $b \in GF(p)$ and computes b^{-1} such that $b \cdot b^{-1} = 1 \pmod{p-1}$

R keeps these integers secret

26

Key Exchange

- Suppose S wants to pass the key x to R
- S computes $x^a \in GF(p)$ and sends it to R
- R computes $(x^a)^b = x^{ab} \in GF(p)$ and sends it to S
- S computes $(x^{ab})^{a^{-1}} = x^b \in GF(p)$ and sends it to R
- R Computes $(x^b)^{b^{-1}} = x \in GF(p)$

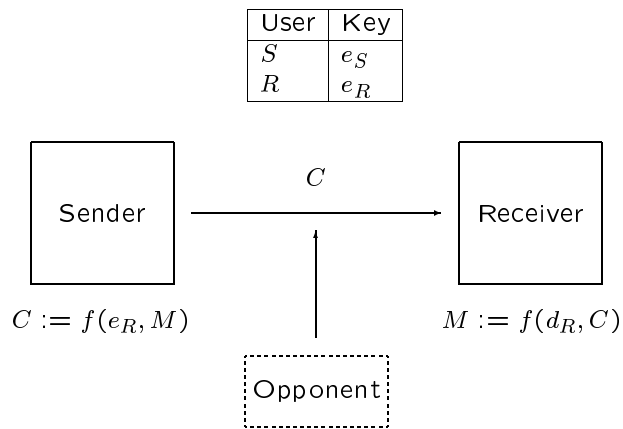
27

Key Exchange

- Opponent knows the field $GF(p)$ and sees x^a, x^{ab}, x^b
- Computing α from x^α in the field $GF(p)$ is discrete analogue of taking logarithms
- Discrete logarithm problem is known to be very hard

28

Public-Key Directory



29

Public-Key Cryptography

- Functions $f(e_R, \cdot)$ and $f(d_R, \cdot)$ are inverses of one another
- Encryption and decryptions processes are asymmetric:
 - $e_R \neq d_R$
 - $C := f(e_R, M)$ and $M := f(d_R, C)$
 - e_R is public; known to everyone
 - d_R is private; known only to User R
 - e_R is easily deduced from d_R
 - d_R is NOT easily deduced from e_R

30

Public-Key Cryptography

A public-key cryptography system is based on a function $f(x)$ such that

Given x , computing $y = f(x)$ is EASY

Given $y = f(x)$, computing x is HARD

$$x \begin{array}{c} \xrightarrow{\text{easy}} \\ \xleftarrow{\text{hard}} \end{array} f(x)$$

We call $f(x)$ a one-way function

In order to decide what is hard:

We can use the theory of complexity

Often the test of time determines

31

Public-Key Cryptography

Example: *Discrete Logarithm*

Given x , a , and p , computing $y \equiv x^a \pmod{p}$ is EASY

However, given y , x , and p , computing a is HARD

Example: *Factoring*

Given x and y , computing $n = xy$ is EASY

However, given n , computing the factors x and y is HARD

32

Public-Key Cryptography

One additional structure about the function $y = f(x)$ is needed to design a public-key cryptosystem

Given y and some special information about $f(x)$, computing x is EASY

Given y without this special information, computing x is HARD

We call $f(x)$ a one-way trapdoor function

Special information is trapdoor information

33

RSA Algorithm

RSA algorithm was invented in 1977

p and q be two distinct large random primes

The modulus n is the product of these two primes: $n = pq$

Euler's totient function of n is given by

$$\phi(n) = (p-1)(q-1)$$

Now, select a number $1 < e < \phi(n)$ such that

$$\gcd(e, \phi(n)) = 1$$

and compute d with

$$d = e^{-1} \pmod{\phi(n)}$$

using extended Euclid's algorithm

34

RSA Algorithm

Here, e is the public exponent and d is the private exponent

Usually one selects a small public exponent, about 16–32 bits

The modulus n and the public exponent e are published

The value of d and the prime numbers p and q are kept secret

Encryption is performed by computing

$$C = M^e \pmod{n}$$

where M is the plaintext such that $0 \leq M < n$

Decryption is performed by computing

$$M = C^d \pmod{n}$$

35

RSA Signatures

The user *signs* the digital data H by computing

$$S = H^d \pmod{n}$$

The signature is *verified* by computing

$$H' = S^e \pmod{n}$$

and the checking if $H' = H$

Only the user can sign since he knows d

Anyone can verify since e and n are published

Large chunks can be signed by computing digest of the data using a hash function, and then signing this digest value

Since the digest algorithm is public, the verification is easily performed

36

Digital Signatures

Cryptographic message enhancement which

- identifies signer
- authenticates message
- anyone can verify
- only signer can sign

37

Digital Signature Algorithm (DSA)

NIST digital signature standard, FIPS 186

Parameters:

p is a prime

q is a prime dividing $p - 1$

g is an integer such that the set

$$\{g^x \bmod p \mid 0 \leq x \leq q - 1\}$$

contains q distinct integers

x (private key) is an integer

y (public key) is an integer such that

$$y = g^x \bmod p$$

38

Digital Signature Algorithm (DSA)

Signing:

m is message

k is a random integer

(r, s) is the signature such that

$$r = (g^k \bmod p) \bmod q$$

$$s = (m + xr)k^{-1} \bmod q$$

Verification:

First compute $w = s^{-1} \bmod q$

Then compute r' such that

$$r' = (g^{mw}y^{rw} \bmod p) \bmod q$$

Is $r' = r$?

39

Authentication Protocols

Two parties are about to begin communication, and they want to be sure they are talking to one another

This is called entity authentication or identification

Assurance of the identity of communicating parties

Example: Login protocol

A and B share a secret key K

A sends K to B to prove identity

40

Authentication Protocols

Goal: Other parties should not gain information to impersonate later on

General design approaches:

- Message authentication codes
- Encryption with redundancy
- Digital signatures
- Proofs of knowledge

41

Message Authentication Codes

A message authentication code (MAC) is a function which is used to ensure that two communicating parties share a common key

Suppose A and B share the key K

A wants to send a message M to B

A appends C to M , which is computed as

$$C = \text{MAC}(K, M)$$

42

Message Authentication Codes

B receives (M, C) , and verifies

$$C = \text{MAC}(K, M)$$

B is assured that message was not altered

B is assured that message is from A

MAC function is similar to encryption, however, it need not be reversible

43

Timestamp Authentication

A sends B a timestamp T and a message authentication code M computed with a secret key K

$$M = \text{MAC}(K, T)$$

B receives (T, M) , and verifies $M = \text{MAC}(K, T)$

B checks that timestamp is current

Since time stamp changes with each run, old messages are not useful (prevents replay)

If B's name is included in the input to MAC, an opponent cannot send the message back to A, pretending to be B

$$M = \text{MAC}(K, T, B)$$

44

Timestamps and Signatures

A signs the timestamp with his private key

$$S = \text{SIGN}_A(T)$$

and sends T and S to B

If B's name is included in the signature

$$S = \text{SIGN}_A(T, B)$$

then an opponent cannot send this message to someone else to pretend that he is A

45

Random Numbers and Authentication

B sends a random number R to A

A computes a MAC using R and the key K

$$M = \text{MAC}(K, R)$$

Assuming R is random, old messages are not useful to an opponent

B's name can be included in MAC as well

$$M = \text{MAC}(K, R, B)$$

This prevents reflection attack

A can also include another random number R' to strengthen the protocol

$$M = \text{MAC}(K, R, B, R')$$

and send R' to B. This prevents an opponent to forge R s to extract information about K

46

Random Numbers and Signatures

B sends a random number R to A

A signs it using his private key

$$S = \text{SIGN}(R)$$

To prevent reflection attack, we include B's name

$$S = \text{SIGN}_A(R, B)$$

This protocol is also strengthened by including B's name and another random number R'

$$S = \text{SIGN}_A(R, R', B)$$

47

Proofs of Knowledge

These are theoretical constructions by which a prover can demonstrate knowledge of secret information

For user authentication, the user demonstrates the knowledge of private key

A sends a random commitment R_A

B sends a random challenge R_B

A computes a function $f_A(R_A, R_B)$ with his private key

B verifies using A's public key

This process may be repeated several times

48

Proofs of Knowledge

The function f_A should have certain properties:

- For a given R_A , it should be difficult to compute $f_A(R_A, R_B)$ for two or more R_B s without the knowledge of the private key

A correct reply proves that A knows the private with high probability

- In general, it need not be difficult to compute $f_A(R_A, R_B)$ for one R_B

Thus, f_A need not be as strong as a digital signature scheme

49

Comparing Authentication Methods

Protocols based on MACs or encryption are generally the most efficient in terms of message size and computation time, but parties must share a secret key

Protocols based on digital signatures are less efficient, but parties need only know one another's public key

Protocols based on timestamps require synchronization

Protocols based on random numbers require more messages

Protocols based on proofs of knowledge are faster than those based on digital signatures, but require more messages

50

Threats to Wireless Communication

Two aspects of wireless communication do not provide the same level of protection as a fixed network:

- Radio path
- Access to mobile services

51

Threats to Wireless Communication

Radio path: Interception of data on the air interface is a threat

- Loss of confidentiality of user data
- Loss of confidentiality of user signalling information
- Loss of confidentiality of user identity information

Access to mobile services: Illegitimate access to services needs to be prevented

The illegitimate use is in terms of masquerading or impersonating a subscriber while using system services

52

Wireless Security Services

In order to protect network providers and subscribers from these attacks, the following security features must be provided:

- Subscriber identity confidentiality
- Subscriber identity authentication
- User data confidentiality
- Signalling information confidentiality

53

Wireless Security Services

A typical wireless communication system (such as GSM) provides three basic security services:

- Confidentiality of the user identity
- Authentication of the user identity
- Confidentiality of the user data

54

GSM Security Implementation

- GSM Architecture
- GSM Security Services
 - Temporary identities for confidentiality of the user identity
 - Use of SIM in authentication of the user identity
 - Encryption for confidentiality of the user data

55

GSM Architecture

Mobile Station (MS)

Mobile Equipment plus SIM card

Subscriber Identity Module (SIM)

Provides an identity to ME

A smart card with a CPU and memory
Subscriber parameters are stored in SIM
PIN protects SIM against unauthorized use
PUK (personal unblocking key) protects
against subsequent wrong PIN entries

56

GSM Architecture

Subscriber Identity Module (SIM)

SIM has EEPROM and ROM

ROM contains the algorithms A3 and A8

EEPROM contains IMSI and K_i

	typical	maximum
ROM	4–6 KByte	16 KByte
RAM	126–160 Byte	256 Byte
EEPROM	2–3 KByte	8 KByte

57

GSM Architecture

Home Location Register (HLR)

HLR stores the identity and user data of all subscribers belonging to the area

These are IMSI, K_i , supplementary service permissions, and some temporary data

Temporary data: address of the current VLR in which the user is registered, call forwarding information, transient parameters of authentication and encryption

58

GSM Architecture

Visitor Location Register (VLR)

VLR contains relevant data of all mobile stations currently registered in a serving area

The permanent data is found in HLR

The temporary data differs slightly, for example, it contains TMSI

Even if the mobile station is in its own area, it is registered in VLR in addition to HLR

59

GSM Architecture

Authentication Center (AuC)

All authentication algorithms and parameters are stored in AuC

AuC provides HLR or VLR the parameters required to authenticate the user identity

AuC knows which algorithms and parameters to use for a specific user

SIM card assigned to user contains the same algorithms and parameters as the ones in AuC

60

User Identity Confidentiality

Before the user makes a call or go on standby to receive calls, his identity needs to be known to the network

IMSI (International Mobile Subscriber Identity) uniquely identifies the subscriber

Rather than sending IMSI, a temporary identity called TMSI is sent in most instances

TMSI: Temporary Mobile Subscriber Identity

61

User Identity Confidentiality

The reason for sending TMSI in place of IMSI is to deny an intruder

- To gain information on the resources the user is using
- To prevent the tracing of the location of the user
- To make it difficult to match the user and the transmitted data

IMSI is sent only when necessary, for example, when the user uses his SIM for the first time or there is data loss at VLR

62

User Identity Confidentiality

When SIM is used for the first time, MS reads the default TMSI stored in the card

MS sends the default TMSI to VLR

Since VLR does not know this TMSI, it requests IMSI from MS

MS sends IMSI to VLR

VLR then assigns a new TMSI to this user

63

User Identity Confidentiality

VLR sends the new TMSI to MS in encrypted form

The encryption algorithm is A5

The encryption key K_c

MS decrypts the message and obtains TMSI

From now, MS uses only TMSI to identify itself

64

User Identity Confidentiality

TMSI is only 5 digits, it is unique within that location area where MS moves

LAI (Location Area Identification) and TMSI uniquely identify the user

VLR stores LAI and TMSI for each user in its area

A new TMSI is to be assigned at each location update procedure

If the system does not malfunction, IMSI is never used again

The new VLR always obtains IMSI from the old VLR by using the old TMSI and LAI which was sent by the mobile station

65

User Identity Authentication

Authentication is verification of the claimed identity

The reason for subscriber identity authentication is to protect the network against unauthorized use, and thus, to ensure correct billing, and to prevent masquerading attacks

The method is a challenge/response protocol using unpredictable numbers

SIM contains a secret subscriber specific authentication key K_i which is 128 bits

An authentication algorithm called A3 is used both by SIM and the network

A3 is a MAC; it is unpublished

66

User Identity Authentication

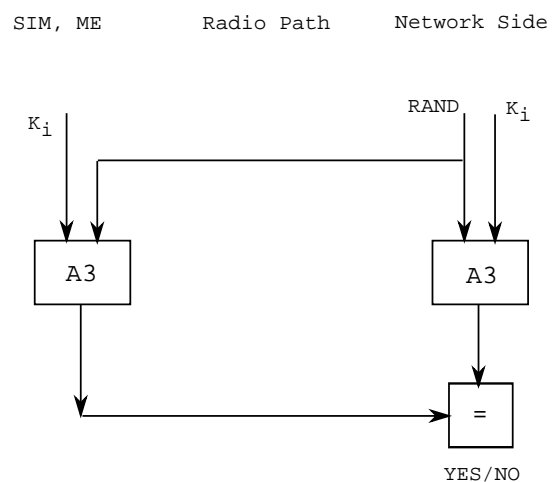
General Procedure:

Verification is performed by VLR where MS is currently registered

Network knows TMSI and thus IMSI
 Network retrieves K_i from IMSI
 Network generates a random number RAND
 Network sends RAND to MS as a challenge
 SIM contains K_i
 SIM computes SRES using K_i and RAND
 MS sends SRES to network
 If two values are equal, identity is authentic

67

User Identity Authentication



K_i is 128 bits
 RAND is 128 bits
 SRES is 32 bits

68

Why Not PKC?

The use of PKC would allow the local verification of the response without any secret information given to VLR

Authentication by means of PKC is now nearly standardized

However, PKC is not used in both GSM and DECT (Digital European Cordless Telephone) systems

Reason: Time constraints of the authentication process and the amount of data to be handled; PKC is slower and requires more data

The air interface does not support the transmission of the required amount of data

69

Key Management

The key parameters are: K_i (128 bits), RAND (128 bits), SRES (32 bits), K_c (64 bits)

Verification is performed by VLR where MS is currently registered

Computation is performed by HLR/AuC of the subscriber

The triplet RAND, SRES, K_c is called an authenticating triplet

70

Key Management

VLR obtains 5 triplets from HLR/AuC, and stores them

Each triplet is used only once, and discarded after being used

When the user moves to a different VLR, the new VLR requests IMSI from the old VLR by sending the old TMSI and LAI

The old VLR transfers IMSI and any unused triplets to the new VLR

This speeds up the authentication procedures

71

Key Management

The authentication key K_i and IMSI are allocated during the subscription time

K_i is stored at Authentication Center (AuC)

Authentication algorithm A3 and cipher key K_c are implemented in AuC

Key management is a major issue: the number of subscribers of GSM are expected to reach 20 million in the year 2000

72

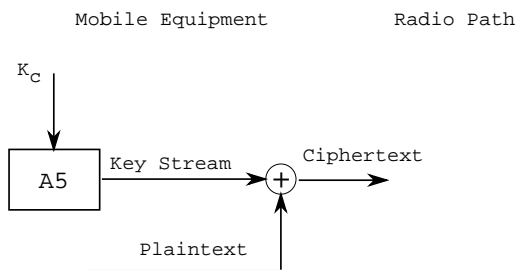
User Data Confidentiality

An encryption algorithm named A5 is used

This algorithm is unpublished and it can be implemented using about 3,000 transistors

It is contained in a dedicated piece of silicon in Mobile Equipment and Base Station

Activation is controlled by Base Station by a Start Cipher command



73

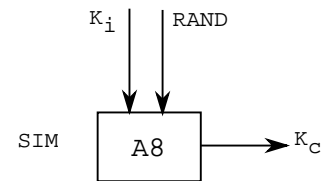
User Data Confidentiality

The plaintext is broken into blocks of 114 bits

The key K_c is derived in the SIM during the authentication process using the network specific algorithm A8

A8 is a key generator algorithm; its specifics are to be defined by network providers

The challenge number RAND (128 bits) and the authentication key K_i (128 bits) are used to generate K_c which is 64 bits



74

Key Generation

The method of generating and storing several million user authentication keys and handling of requests are very important from the security and smooth operation of the network

The functionality of AuC is not specified in GSM

It is left to the network providers

However, it is specified that A3 and A8 will be implemented in AuC

75

Key Generation

There are basically two approaches in generating user authentication keys:

Random Numbers:

We select K_i at random from all possible 128-bit binary numbers

However, there is no natural link between K_i and user information (IMSI)

Thus, AuC needs to store K_i and user information in a data bank

Keys need to be stored in encrypted form in order to protect against unauthorized reading

A backup in a physically different location may also be necessary

76

Key Generation

Algorithmic Method:

We select K_i using user data information as an input to an encryption algorithm controlled by a master key MK

A good choice would DES algorithm

$$K_i = \text{DES}(MK_1, UD) \parallel \text{DES}(MK_2, UD)$$

where UD is user data and MK_1 and MK_2 are master keys

Master keys need to be updated often for increased security

A variation is to append a random string (salt) to the user data UD and save this random number

77

Abbreviations

A3 Algorithm 3. Authentication algorithm used for authenticating the subscriber

A5 Algorithm 5. Secret-key cryptographic algorithm used for encrypting/decrypting data

A8 Algorithm 8. Key generator used to generate K_c

AuC Authentication Center. Used to store keys K_i . A3 and A8 are implemented in AuC

DECT Digital European Cordless Telephone

ETSI European Telecommunications Standards Institute

GSM Global System for Mobile Communications

HLR Home Location Register. A register in the HPLMN of the subscriber where all information related to the location and the subscription are permanently stored

HPLMN Home PLMN. The network in which a subscriber is registered

IMSI International Mobile Subscriber Identity. The identity which uniquely identifies the subscriber in all GSM networks. It is used for routing in GSM (not to be confused with the subscriber's mobile telephone number)

K_c The encryption (cipher) key. Used in A5 to generate keystream

K_i The subscriber authentication key. Used in A3 and A8

78

Abbreviations

LAI Location Area Identification. Information indicating the location of a cell or a set of cells

ME Mobile Equipment. The MS without the SIM

MS Mobile Station. The equipment used to access GSM

PIN Personal Identification Number. Used by the SIM for the verification of the identity of the user.

PLMN Public Land Mobile Network. A network providing communication possibilities for mobile users

PUK Personal Unblocking Key. Used to unblock the GSM application which occurred as a result of three consecutive wrong PIN entries

RAND A random (unpredictable) large number. Used as a challenge in the authentication process

SIM Subscriber Identity Module. The subscriber card containing security, subscription, and network related information

SMG Special Mobile Group. The new name of the ETSI technical committee which was formerly called Groupe Spécial Mobile

SRES Signed Response. Used by the network to verify the identity of the SIM in the authentication process

TMSI Temporary Mobile Subscriber Identity. The temporary identity issued by a VLR to provide subscriber identity confidentiality

VLR Visitor Location Register. The register where the user is (temporarily) registered while in a location controlled by this register

79

References

H. Beker and F. Piper. *Cipher Systems*, John Wiley & Sons, 1982.

ETSI Technical Specification GSM 02.09, Security Aspects.

ETSI Technical Specification GSM 03.20, Security-Related Network Functions.

J. M. Kaplan. *Smart Cards*, International Thomson Computer Press, 1996.

S. M. Redl, M. K. Weber, and M. W. Oliphant. *An Introduction to GSM*, Artech House, 1995.

R. Steele. *Mobile Radio Communications*, IEEE Press, 1992.

W. Stallings. *Network and Internetwork Security*. Prentice-Hall, 1995

D. R. Stinson. *Cryptography: Theory and Practice*, CRC Press, 1995.

M. Walker. Security in Mobile and Cordless Telecommunications. *CompEuro 1992 Proceedings*, pages 493–496, IEEE Computer Society Press, 1992.

K. Vedder. Security aspects of mobile communication. *Computer Security and Industrial Cryptography*, B. Preneel, R. Govaerts, and J. Vandewalle (editors), pages 192–210, Springer-Verlag 1991.

80