

Wireless Technologies and Security

Elke De Mulder
Roel Peeters



March 11, 2009

Mobile Data and Wireless Security - LSEC

1

WHY WIRELESS?

The benefits

- Convenient
- Flexible
- Mobility
- Easy to use

Some applications

- Moving equipment while maintaining connectivity
- Share data and applications in a network without any cables
- Using services like wireless email, web browsing from everywhere
- Wireless printing, presenting
- Internet of Things : The 4A Vision
 - Any Time
 - Any Place
 - Connectivity for Anyone
 - Any Thing



March 11, 2009

Mobile Data and Wireless Security - LSEC



Personal Digital Assistant

March 11, 2009

Mobile Data and Wireless Security - LSEC

3
Extension of Zone-H.org

Wireless Technologies and Protocols

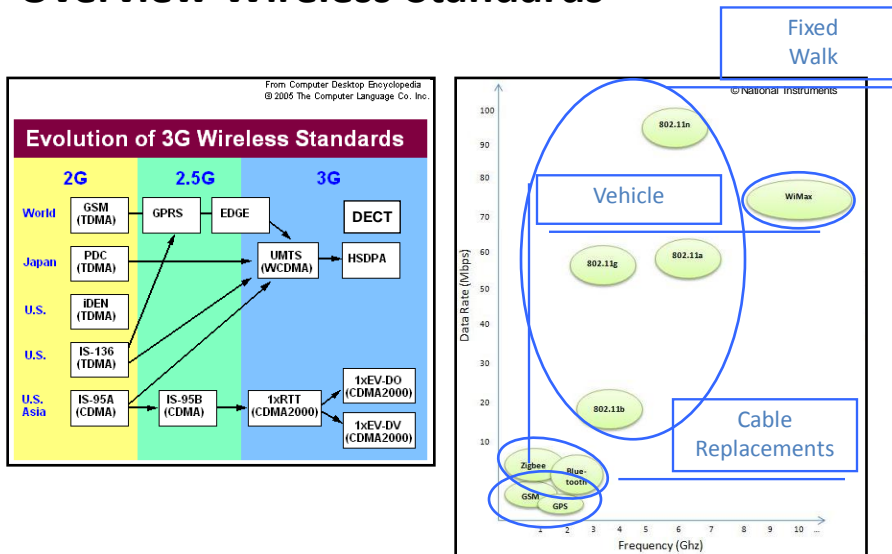
- WiFi ————— Wi-Fi (802.11) is a suite of specifications for wireless Ethernet
- GSM ————— GSM (Global System for Mobile communications) is the most popular standard for mobile phones in the world
- Bluetooth ——— Bluetooth is a specification for “short” distance wireless communication between two devices
- EDGE ————— EDGE (Enhanced Data rate for GSM Evolution) is a specification for data transfer on GSM networks.
- GPRS ————— GPRS (General Packet Radio Service) is a specification for data transfer on TDMA and GSM networks
- WiMAX ————— WiMAX stands for Worldwide Interoperability for Microwave Access. WiMAX is a broadband wireless ultra wideband and is a unique type of wireless technology that uses orthogonal frequency division multiple access (OFDMA) for data transfer
- UWB ————— Ultra wideband is a unique type of wireless technology that uses orthogonal frequency division multiple access (OFDMA) for data transfer
- DECT ————— DECT is a suite of transmission standards for digital cordless telephones and other low power devices
- 3G / UMTS ——— Universal Mobile Telecommunications System (UMTS) is one of the third generation (3G) cell phone technologies
- ZIGBEE ————— ZigBee is a wireless headsets connecting with cell phones via short-range radio.

March 11, 2009

Mobile Data and Wireless Security - LSEC

4

Overview Wireless Standards



March 11, 2009

Mobile Data and Wireless Security - LSEC

5

Impact of ICT



- Personal Computer
 - 1 billion PCs
- Internet
 - 1.3 billion people access the Internet
- Mobile phone
 - 3.95 billion mobile subscribers
 - There are more mobile phones than fixed phones
 - 70% of developing world's population lives within the footprint of a mobile phone service
- Bluetooth
 - 2 billion devices

(world population: 6.7 billion people)

March 11, 2009

Mobile Data and Wireless Security - LSEC

6

Insecure ICT

CSI Computer Crime & Security survey

- Virus: 50%
- Laptop theft: 42%
- Unauthorized access: 29%
- Denial-of-Service attacks: 21%
- Malicious bot: 20%
- Theft/loss of customer data: 17%
- Abuse of wireless network: 14%
- Password sniffing: 9%
- Theft/loss of proprietary info: 9%
- ...



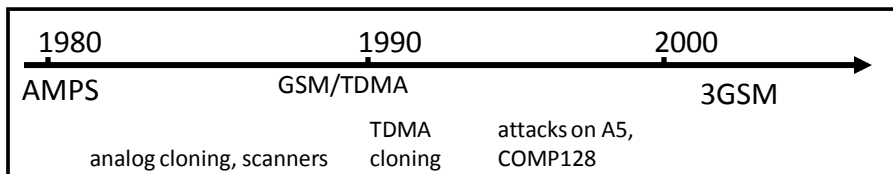
March 11, 2009

Mobile Data and Wireless Security - LSEC

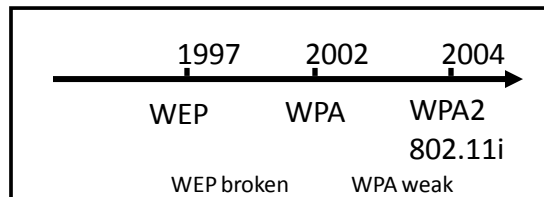
7

A little bit of history

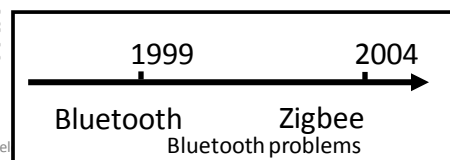
mobile phones technologies



WLAN



PAN



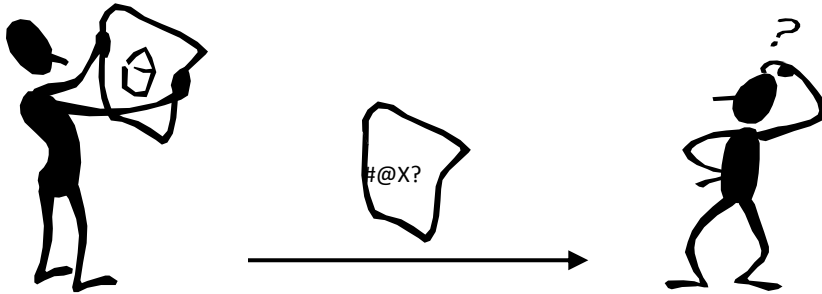
March 11, 2009

Mobile Data and Wireless Security - LSEC

Goals of Information Security

Confidentiality

ensuring that information is accessible only to those authorized to have access



March 11, 2009

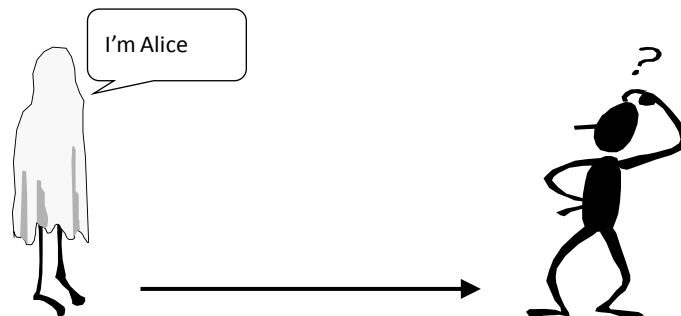
Mobile Data and Wireless Security - LSEC

9

Goals of Information Security

Entity authentication

is the act of establishing or confirming something or someone as *authentic*



March 11, 2009

Mobile Data and Wireless Security - LSEC

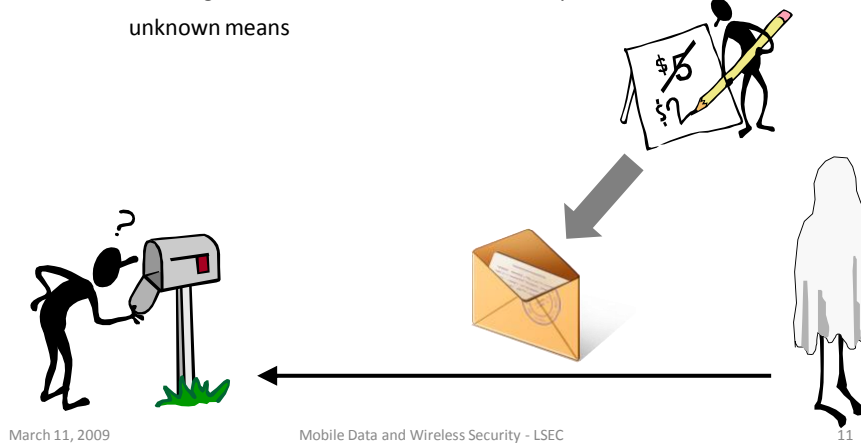
10

Goals of Information Security

Data authentication

Integrity

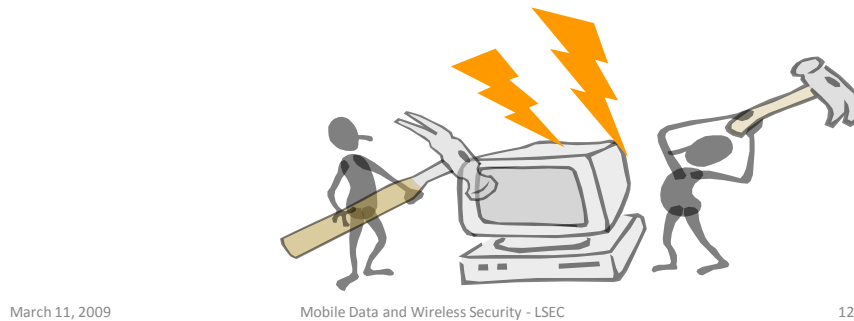
ensuring information has not been altered by unauthorized or unknown means



Goals of Information Security

Availability

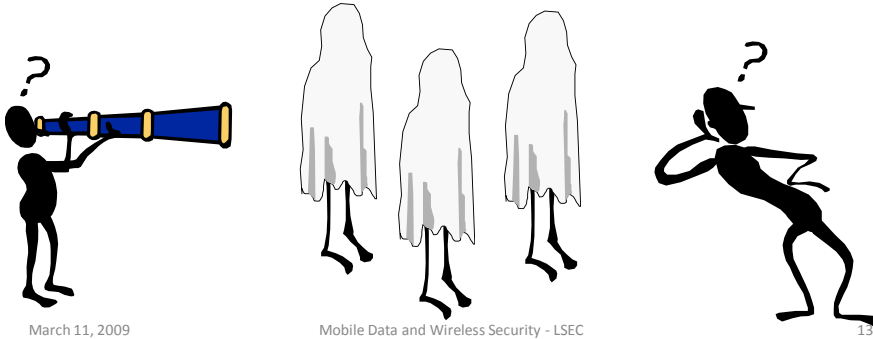
allowing legitimate users access to confidential information after they have been properly authenticated



Goals of Information Security

Privacy

is the ability of an individual or group to seclude themselves or information about themselves and thereby reveal themselves selectively



Risks

Particular security risks associated with mobile and wireless systems:

- Intrusion
 - No physical connection required
- Leeching
 - Bandwidth use
- Exploitation
 - Misuse of infrastructure
 - Also against third parties

Common wireless insecurity reasons


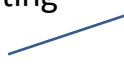


- architectural errors
 - wrong trust assumptions
 - default = no security
- protocol errors
 - unilateral entity authentication
 - weak entity authentication mechanism
 - downgrade attack
- modes of operation errors
 - no authenticated encryption
 - wrong use of crypto
- cryptographic errors
 - weak crypto
- implementation errors

March 11, 2009

Mobile Data and Wireless Security - LSEC

15

Passive attacks

- Eavesdropping
 - Fingerprinting  Devices can be identified by looking at their electromagnetic fingerprint
 - Listening  Detect if somebody is home by checking if the wireless network is switched on
 - Scanning  Check broadcast message from all kinds of devices to detect unsecured networks
- Traffic Analysis
 - Location privacy  Analyze data to locate people

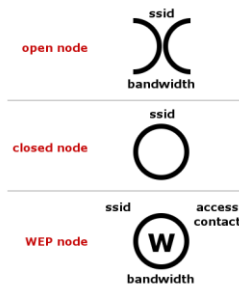
March 11, 2009

Mobile Data and Wireless Security - LSEC

16

Detecting wireless networks

- War driving
 - Identify, locate and categorize wireless networks by driving around with a car
- War walkers
 - Same principle but healthier
- War chalking
 - Symbols representing wireless networks and their associated security levels
- War flying
 - From inside a private plane

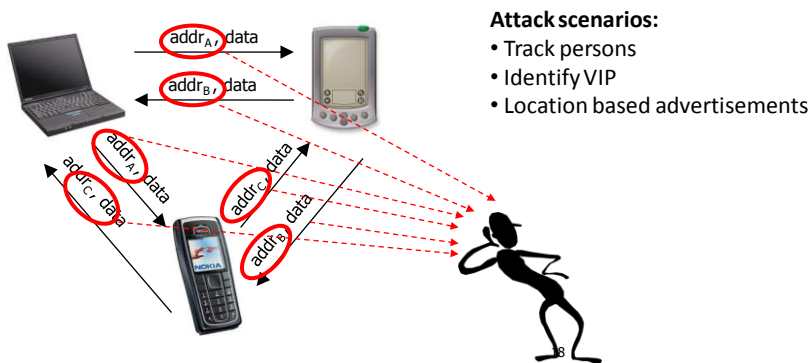


March 11, 2009

Mobile Data and Wireless Security - LSEC

Traffic Analysis

Location Privacy



Attack scenarios:

- Track persons
- Identify VIP
- Location based advertisements

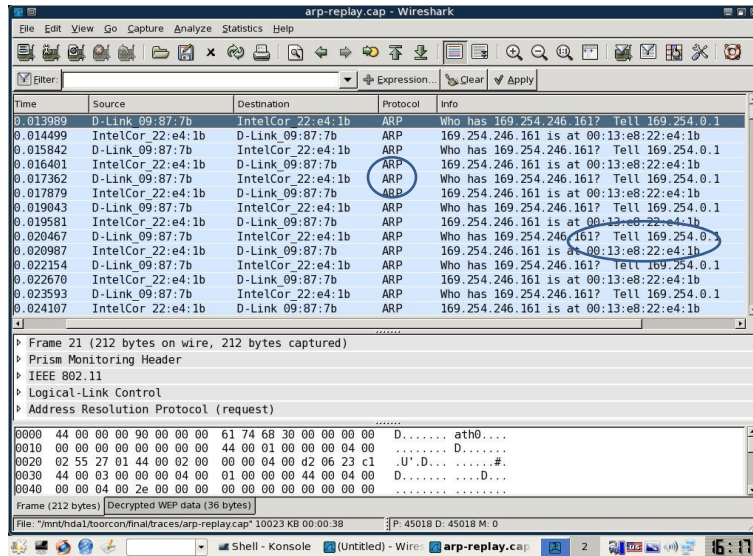
Data is often encrypted, the address is not...

March 11, 2009

Mobile Data and Wireless Security - LSEC

18

Sniffing wireless network

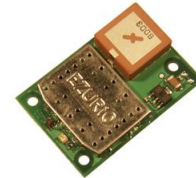


March 11, 2009

Mobile Data and Wireless Security - LSEC

19

Wireless boundless



- Coverage does not stop at the borders of the building ...
- Often underestimated



March 11, 2009

Mobile Data and Wireless Security - LSEC

20

Active Attacks

- Spoofing
 - Impersonating an authorized client to gain access to a protected resource
- Rogue Access Points
- Denial Of Service attacks
 - Rendering a network device or entire network unable to communicate
- Malicious code
 - Can infect and corrupt network devices
- Social Engineering
 - Using the weakness of humans and corporate policies to obtain access
- Message modification
 - Change messages

March 11, 2009

Mobile Data and Wireless Security - LSEC

21

Denial of Service (DoS)

- Radio jamming attacks: GSM BLOCKERS



range: 10-20 m
 COST: 99 euro
 1 AA battery = 4 h

- Battery exhaustion : sleep deprivation attack
- Blacklist flooding
- WIRELESS LAN:
 - Requests for authentication at such a frequency as to disrupt legitimate traffic
 - Requests for deauthentication of legitimate users. These requests may not be refused according to the current 802.11 standard
 - Mimics the behavior of an access point and convinces unsuspecting clients to communicate with it
 - Repeatedly transmits RTS/CTS frames to silence the network

March 11, 2009

Mobile Data and Wireless Security - LSEC

22

A closer look at some protocols

- GSM
- UMTS
- DECT

March 11, 2009

Mobile Data and Wireless Security - LSEC

23

GSM

- 1982 CEPT: Groupe Speciale Mobile
- 1989 ETSI: GSM
- 1991 First live demonstrations
- GSM Association (www.gsm.org) Q4/2008
 - 860 operators on air (includes 3G)
 - 214 countries and areas
 - close to 2.7 billion subscribers
- Evolution towards 3GPP/3GSM:
 - first services: Q4/2001 in Japan and Q3/2003 in Europe
 - over 200 UMTS operators on air in Jan 2008 in 42 countries
 - 131 million subscribers in Q2/2007 (354 million for CDMA2000 1X)

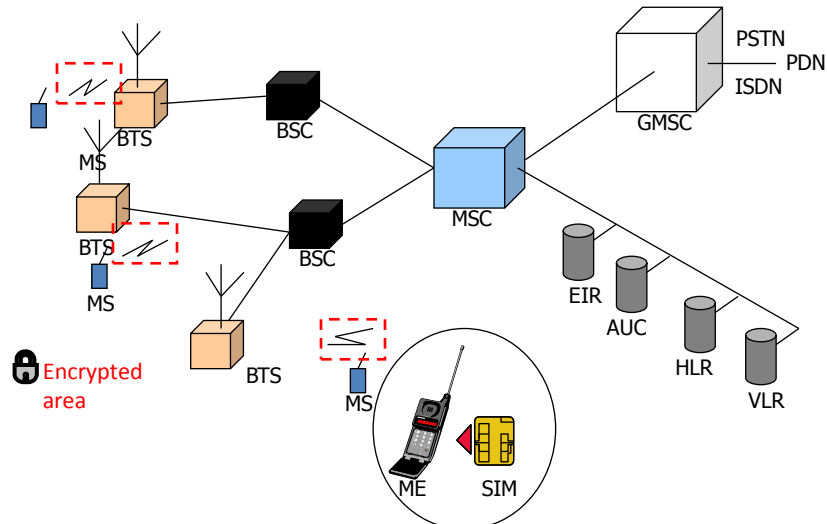


March 11, 2009

Mobile Data and Wireless Security - LSEC

24

GSM Architecture



March 11, 2009

Mobile Data and Wireless Security - LSEC

25

Security threats

- Interception of data on the air interface
 - data confidentiality
 - anonymity of user
- Illegitimate access to a mobile service
 - billing
 - masquerading
- Security services:
 - subscriber identity confidentiality
 - subscriber identity authentication
 - user data confidentiality
 - signaling information confidentiality

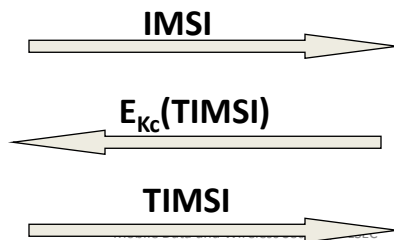
March 11, 2009

Mobile Data and Wireless Security - LSEC

26

Temporary identities

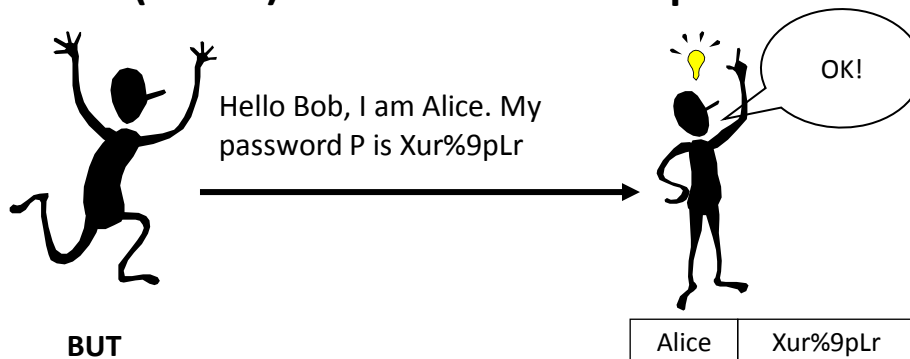
- IMSI (15 digits) is used only for first call, or in exceptional circumstances
- replaced by TIMSI (5 digits)
 - assigned by VLR, stored with IMSI and location info
 - sent encrypted to MS
 - replaced at each location update procedure
- TIMSI is forwarded to new VLR



March 11, 2009

27

1G (AMPS) identification with passwords



BUT

- Eve can guess the password
- Eve can listen to the channel and learn Alice's password
- Bob needs to know Alice's secret
- Bob needs to store Alice's secret in a secure way

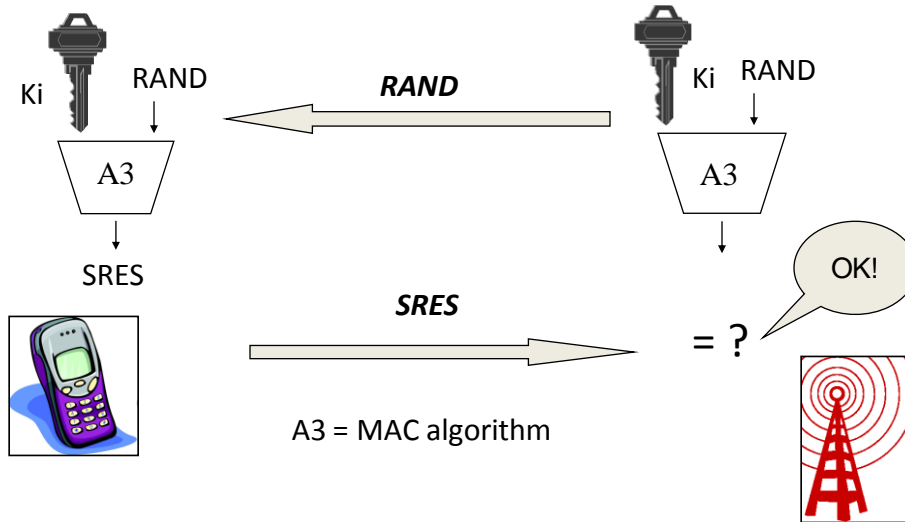
March 11, 2009

Mobile Data and Wireless Security - LSEC

28

Entity authentication in GSM

challenge response



March 11, 2009

Mobile Data and Wireless Security - LSEC

29

Entity Authentication in GSM (2)

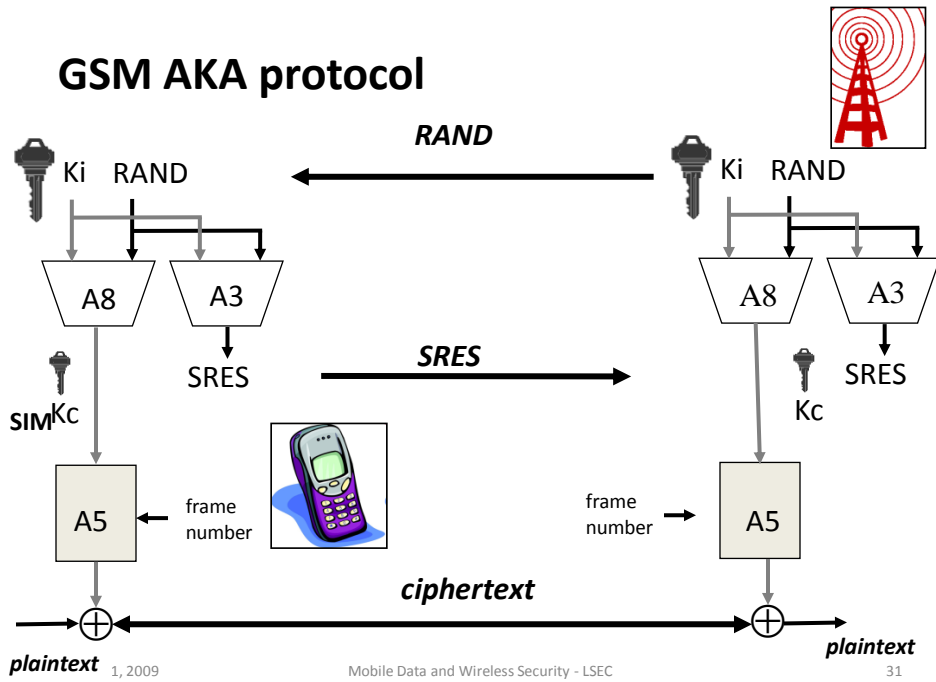
- + Eve cannot guess the secret key K_i (128 bits)
- + Eavesdropping the channel does not help Eve: next time Bob will ask a different question (different challenge $RAND$)
- Bob needs to know Alice's secret, and needs to store it securely
- Eve can just wait till the end of the call setup and then.....
 - how to address this problem?
AKA, Authentication and Key Agreement

March 11, 2009

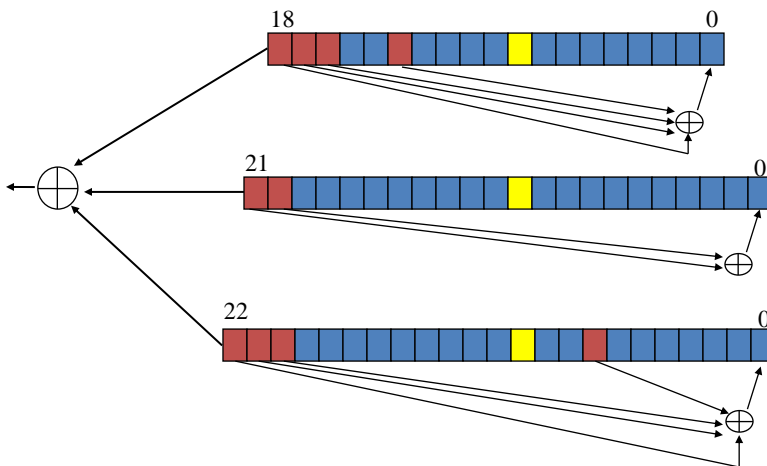
Mobile Data and Wireless Security - LSEC

30

GSM AKA protocol



A5/1: stream cipher (GSM)



Clock control: registers agreeing with majority are clocked (2 or 3)

The GSM encryption ciphers

- **A5/1: clock controlled LFSR**
 - exhaustive key search: 2^{54} rather than 2^{64}
 - search 2 registers: 2^{45} steps
 - [BD00] 2 minutes of plaintext, 2^{40} steps
 - [BWS00] 2 minutes of plaintext: 1 second
 - [BWS00] 2 seconds of plaintext: 1 minute
 - [BB05] 3-4 minutes of **ciphertext only**: 10 minutes
- **A5/2: clock controlled LFSR**
 - Deliberately weak
 - 2^{16} steps, known plaintexts for 2 separate frames (6 sec. apart); this requires 10 milliseconds [BGW99]
 - a few seconds with ciphertext only [BB03]
- **A5/0**
 - No encryption
- **A5/3 (2003)**
 - block cipher similar to KASUMI

March 11, 2009

Mobile Data and Wireless Security - LSEC

33

Limitations of GSM Security, 1

- Problems with GSM security stem by and large from design limitations on what is protected rather than on defects in the security mechanisms themselves
 - only provides **access security** - communications and signalling in the fixed network portion are not protected
 - does not address **active attacks**, whereby network elements may be impersonated
 - designed to be only as secure as the fixed networks to which they connect
 - lawful interception only considered as an after thought

March 11, 2009

Mobile Data and Wireless Security - LSEC

34

Limitations of GSM Security, 2

- Failure to acknowledge limitations
 - encryption needed to guard against radio channel hijack
 - the terminal is an unsecured environment - so trust in the terminal identity is misplaced
 - order of encryption and channel coding
- Inadequate flexibility to upgrade and improve security functions over time
- Lack of visibility that the security is being applied
 - no indication to the user that encryption is on
 - no explicit confirmation to the home network that authentication is properly used when customers roam

March 11, 2009

Mobile Data and Wireless Security - LSEC

35

Limitations of GSM Security, 3

- Lack of confidence in cryptographic algorithms
 - lack of openness in design and publication of A5/1
 - misplaced belief by regulators in the effectiveness of controls on the export or (in some countries) the use of cryptography
 - key length too short, but some implementation faults make increase of encryption key length difficult
 - need to replace A5/1, but poor design of support for simultaneous use of more than one encryption algorithm, is making replacement difficult
 - ill advised use of COMP 128 (A3)

March 11, 2009

Mobile Data and Wireless Security - LSEC

36

Specific GSM Security Problems

- Encryption terminated too soon
 - user traffic and signalling in clear on microwave links
- Clear transmission of cipher keys & authentication values within and between networks
 - signalling system vulnerable to interception and impersonation
- Confidence in strength of algorithms
 - failure to choose best authentication algorithms
 - improvements in cryptanalysis of A5/1
- Use of false base stations

March 11, 2009

Mobile Data and Wireless Security - LSEC

37

False Base Stations

- Used as *IMSI Catcher* for law enforcement
- Used to intercept mobile originated calls
 - encryption controlled by network and user unaware if it is not on
- Dynamic cloning risk in networks where encryption is not used



March 11, 2009

Mobile Data and Wireless Security - LSEC

38

Principles for 3G Security

- Build on the security of GSM
 - adopt the security features from GSM that have proved to be needed and robust
 - try to ensure compatibility with GSM in order to ease inter-working and handover
- Correct the problems with GSM by addressing its real and perceived security weaknesses
- Add new security features
 - as are necessary to secure new services offered by 3G
 - to take account of changes in network architecture

March 11, 2009

Mobile Data and Wireless Security - LSEC

39

Building on GSM Security

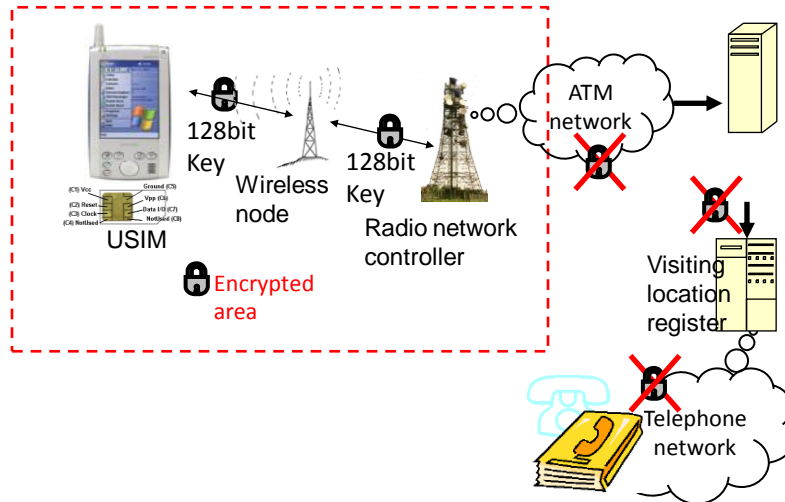
- Remain compatible with GSM network architecture
- User authentication & radio interface encryption
- SIM used as security module
 - removable hardware
 - terminal independent
 - management of all customer parameters
- Operates without user assistance
- Requires minimal trust in serving network
- Extend encryption to Base Station Controller (but unencrypted in the rest of the network)

March 11, 2009

Mobile Data and Wireless Security - LSEC

40

Extended encryption of UMTS



March 11, 2009

Mobile Data and Wireless Security - LSEC

41

Choice of algorithms

- Mobile phone: KASUMI in hardware for encryption and MAC calculation (standard for all operators)
- USIM card: operator specific algorithm for f1 through f5
 - example is MILENAGE, based on Rijndael/AES
 - operators inclined to design their own algorithms

March 11, 2009

Mobile Data and Wireless Security - LSEC

42

Kasumi

- Simpler key schedule than MISTY
- Additional functions to *complicate* cryptanalysis without affecting provable security aspects
- Changes to improve statistical properties
- Minor changes to speed up or simplify hardware
 - goal: < 10.000 gates / 2 Mbit/s
- Stream ciphering f8 uses Kasumi in a form of output feedback, but with:
 - BLKCNT added to prevent cycling
 - initial extra encryption added to protect against chosen plaintext attack and collisions
- Integrity f9 uses Kasumi to form CBC MAC with:
 - non-standard addition of 2nd feedforward

March 11, 2009

Mobile Data and Wireless Security - LSEC

43

Other Aspects of 3GPP Security

- Options in AKA for sequence management
- Re-authentication during a connection and periodic in-call
- Failure procedures
- Interoperation with GSM
- AKA+ and interoperation with 3GPP2 standards
- Formal analysis of AKA
- User identity confidentiality and enhanced user identity confidentiality (R00)
- User configurability and visibility of security features
- User-USIM, USIM-terminal & USIM - network (SAT)
- Terminal (identity) security
- Lawful interception
- Fraud information gathering
- Network wide encryption (R00)
- Location services security
- Access to user profiles
- Mobile IP security (R00+)
- Provision of a standard authentication and key generation algorithm for operators who do not wish to produce their own

March 11, 2009

Mobile Data and Wireless Security - LSEC

44

DECT

(Digital Enhanced Cordless Telecommunications)

- 2007 : > 117 million base unit
> 166 million handset units

["Worldwide Consumer Cordless Telephone Analysis", MZA]

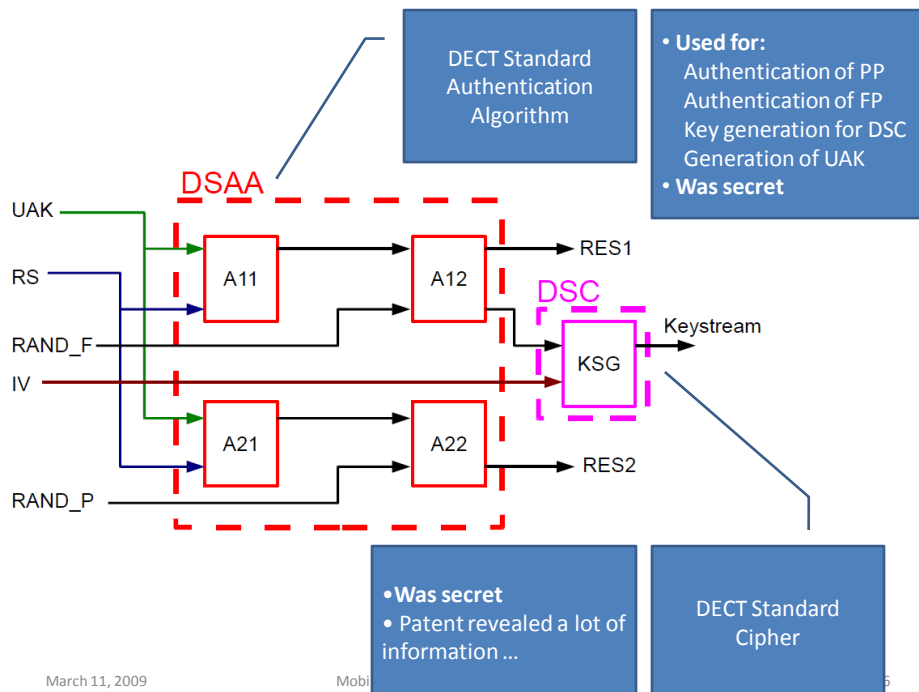
- Security and cryptography
 - Security mechanisms defined in ETSI EN 300 175-7 (freely available)
 - Algorithms only available under NDA



March 11, 2009

Mobile Data and Wireless Security - LSEC

45



March 11, 2009

Mobi

5

Attacks summary

- Eavesdropping: most phones do not encrypt
- Impersonation attacks for base stations (FPs),
- no knowledge of secret algorithms necessary
- UAK recovery: offline/online decryption of all
- encrypted phone calls, impersonation FP/PP

March 11, 2009

Mobile Data and Wireless Security - LSEC

47

Credits

- Bart Preneel, for his slides on mobile security
- Part on GSM: Klaus Vedder, Security Aspects of Mobile Communications, LNCS 741, Springer-Verlag, 1993.
- Part on 3GPP is based on: Mike Walker, On the security of 3GPP networks, invited talk at Eurocrypt 2000, May 2000, Bruges, Belgium.

March 11, 2009

Mobile Data and Wireless Security - LSEC

48

References to 3GPP Security www.3gpp.org

Principles, objectives and requirements

- TS 33.120 Security principles and objectives
- TS 21.133 Security threats and requirements

Architecture, mechanisms and algorithms

- [TS 33.102 Security architecture](#)
- TS 33.103 Integration guidelines
- TS 33.105 Cryptographic algorithm requirements
- TS 22.022 Personalisation of mobile equipment

Lawful interception

- TS 33.106 Lawful interception requirements
- TS 33.107 Lawful interception architecture and functions

Technical reports

- [TR 33.900 A guide to 3G security](#)
- TR 33.901 Criteria for cryptographic algorithm design process
- TR 33.902 Formal analysis of the 3G authentication protocol
- TR 33.908 General report on the design, specification and evaluation of 3GPP standard confidentiality and integrity algorithms

Algorithm specifications

- Specification of the 3GPP confidentiality and integrity algorithms
 - Document 1: f8 & f9
 - [Document 2: KASUMI](#)
 - Document 3: implementors' test data
 - Document 4: design conformance test data

March 11, 2009

Mobile Data and Wireless Security - LSEC

49

References - WLAN (1)

- W.A. Arbaugh, N. Shankar, Y. Wan, Your 802.11 Wireless Network has No Clothes, March 30, 2001.
- N. Borisov, I. Goldberg and D. Wagner, Intercepting Mobile Communications: The Insecurity of 802.11, Proc. of the Seventh Annual International Conference on Mobile Computing and Networking, July 16-21, 2001.
- R. Cowell, War Dialling and War Driving: An Overview, <http://www.sans.org/infosecFAQ/wireless/war.htm>
- EE Times, Sucker punch to WLAN security, Electronic Engineering Times, August 6, 2001.
- S. Fluhrer, I. Mantin and Adi Shamir, Weaknesses in the Key Scheduling Algorithm of RC4, SAC 01.
- IEEE 802 Standards, <http://standards.ieee.org/getieee802>

March 11, 2009

Mobile Data and Wireless Security - LSEC

50

References - WLAN (2)

- Practically Networked,
[http://www.practicallynetworked.com/tools/wireless articles security.htm](http://www.practicallynetworked.com/tools/wireless%20articles%20security.htm)
- A. Stubblefield, J. Ioannidis and A.D. Rubin, Using the Fluhrer, Mantin and Shamir Attack to Break WEP, AT&T Labs Technical Report TD-4ZCPZZ.
- Bellare, Meritt, Limitations of the Kerberos Authentication system, USENIX 1991.
- T. Wu, A Real-World Analysis of Kerberos Password Security, 1998
<http://theory.stanford.edu/~tjw/krbpass.html>
- J. Hill, An Analysis of the RADIUS Authentication Protocol
<http://www.untruth.org/~josh/security/radius>
- W. Arbaugh, A. Mishra, An Initial Security Analysis of the IEEE 802.1X Standard, Feb 2002.

March 11, 2009

Mobile Data and Wireless Security - LSEC

51

References - Bluetooth

- <http://www.bluetooth.com>
- IEEE 802.15, the Wireless Personal Area Network Working Group,
<http://www.ieee802.org/15/>
- V. Bagini, J. Golic, G. Morgari, Linear cryptanalysis of Bluetooth stream cipher, Eurocrypt 2002, LNCS 2332, Springer-Verlag, 2002, pp. 238-255.
- H. Lamm, G. Falauto, J. Estrada, J. Gadiyaram, Security attacks against Bluetooth wireless networks, Proc. 2001 IEEE Workshop on Information Assurance and Security, June 2001, pp. 265-272.
- War Nibbling: Bluetooth Insecurity - @Stake, October 2003
- Y. Lu, W. Meier, S. Vaudenay, The Conditional Correlation Attack: A Practical Attack on Bluetooth Encryption, Crypto 2005

March 11, 2009

Mobile Data and Wireless Security - LSEC

52