Wireless Communications Security Issues, Solutions and Challenges

Michel Barbeau

Carleton UNIVERSITY
Canada's Capital University

Outline

- Availability
- Privacy
- Integrity
- Legitimate participants
- Absence of misbehavior

Carleton UNIVERSITY
Canada's Capital University

Security Requirements

- Availability
  - no jamming, adaptability to unforeseen topologies
- Privacy
  - nondisclosure of cell phone communications and 802.11 frames
- Integrity
  - data is not intercepted and tampered
- Legitimate participants
  - no cell phone cloning and 802.11 frame spoofing
- Absence of misbehavior
  - fairness, greedy user detection

Carleton UNIVERSITY
Canada's Capital University

Availability

- Jamming
- Inability to deal with unforeseen topologies

Carleton UNIVERSITY
Canada's Capital University

Jamming

- Shannon's model:

$$C = W \log\left(1 + \frac{S}{N}\right)$$

Carleton UNIVERSITY
Canada's Capital University

How to Deal With Jamming?

- Increase the bandwidth
  - Frequency Hopping/Direct Sequence Spread Spectrum
    - 801.11(b) : 2.4 - 2.4835 Giga Hertz
    - 801.11a: 5.15- 5.35 Giga Hertz; 5.725- 5.825 Giga Hertz
  - Ultra Wide Band
    - Bandwidth greater than 25% if center frequency
- Increase the power
  - GPS III, planned for 2010 [Ashley, Next-Generation GPS, Scientific American, September 2003.]

Carleton UNIVERSITY
Canada's Capital University

Inability to Deal With Unforeseen Topologies

Images by: J.&G. Naudet (9/11/2001)

Carleton UNIVERSITY
Canada's Capital University

Privacy

- Cellular phone eavesdropping
- Overview of privacy techniques in 2G and 3G of cellular mobile radiophones
  - Refs.:
    - V. Niemi and K. Nyberg, UMTS Security, Wiley, 2003.
    - M.Y. Rhee, CDMA Cellular Mobile Communications and Network Security, Prentice Hall PTR,1998.
  - GSM, UMTS
- Challenges
- Future
  - Reconfigurable security
  - Chaotic communication
  - Quantum cryptography

Carleton UNIVERSITY
Canada's Capital University

Cellular Phone Eavesdropping

- Inexpensive equipment for intercepting analog communications is easy to obtain in Canada.
- In US, the regulations authorize selling scanners to the general public only is cellular frequencies are blocked. However, there are several workarounds
  - Web sites publish modifications to restore reception of cellular frequencies by scanners.
  - Frequency converters can translate cellular frequencies within the coverage of a receiver.
  - With receivers using non quadrature mixing, the image frequency technique can be used.
- Digital communications can also be intercepted with the appropriate equipment!

Carleton UNIVERSITY
Canada's Capital University

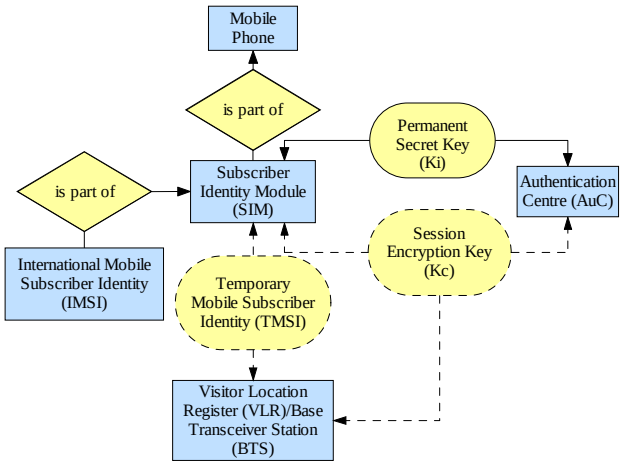
Generations of Cellular Mobile Radiophones*

- 1G
  - Advanced Mobile Phone System (AMPS): 1980s, Frequency Modulation (FM), Frequency Division Multiple Access (FDMA), handover between cells, limited roaming between networks
- 2G
  - Global System for Mobile communications (GSM): 1990s, digital-coding of voice, Time Division Multiple Access (TDMA), Subscriber Identity Module (SIM), data communications
- 3G
  - 3G Partnership Project (3GPP), Universal Mobile Telecommunications System (UMTS): 1998-, Wideband Code Division Multiple Access (WCDMA), uses GSM network model, global roaming; 2 Mbps data
- 4G
  - All-IP-based, 100 Mbps data

* List of cited technologies is not exhaustive.

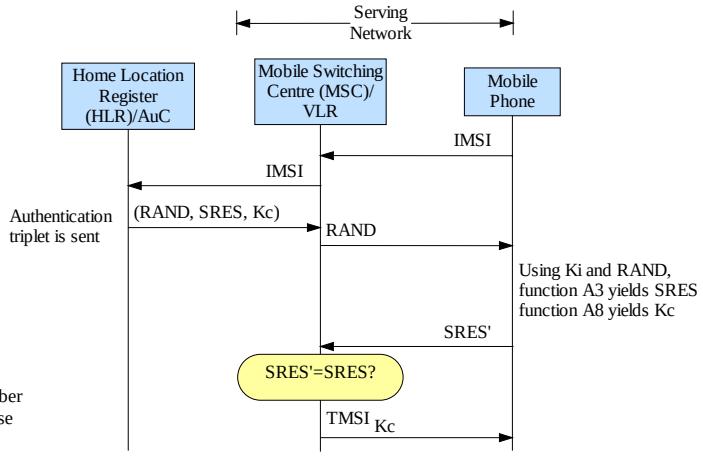
Carleton UNIVERSITY
Canada's Capital University

Security Associations in GSM



Carleton UNIVERSITY
Canada's Capital University

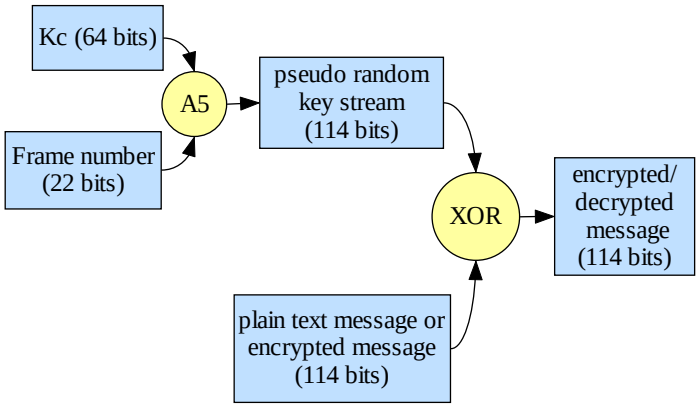
Authentication in GSM



RAND Random Number
SRES Signed Response

Carleton UNIVERSITY
Canada's Capital University

Encryption/Decryption in GSM



Carleton UNIVERSITY
Canada's Capital University

Stream Cipher Weakness

$$Encrypted(M_1) \oplus Encrypted(M_2) = M_1 \oplus M_2$$

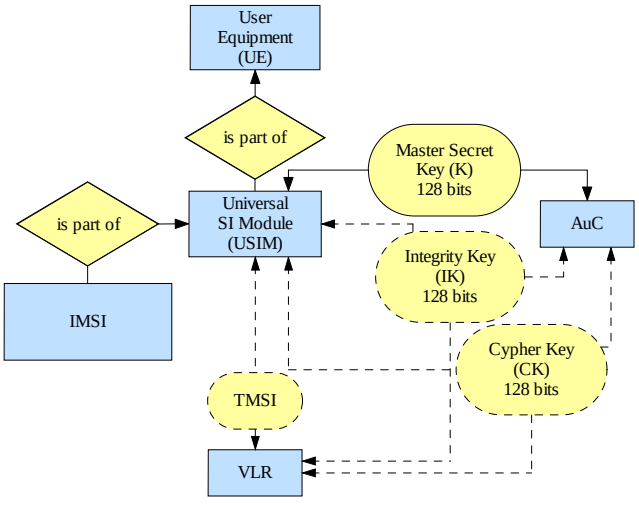
Carleton UNIVERSITY
Canada's Capital University

Security Holes in GSM [Niemi & Nyberg '03]

- Active attack
  - Attacker masquerades a legitimate base station/cell phone
- Encryption keys
  - Plain text session key inter-network forwarding
  - Brute force attack
- Some encryption algorithms are kept secret
  - Haven't go through an analysis/peer review

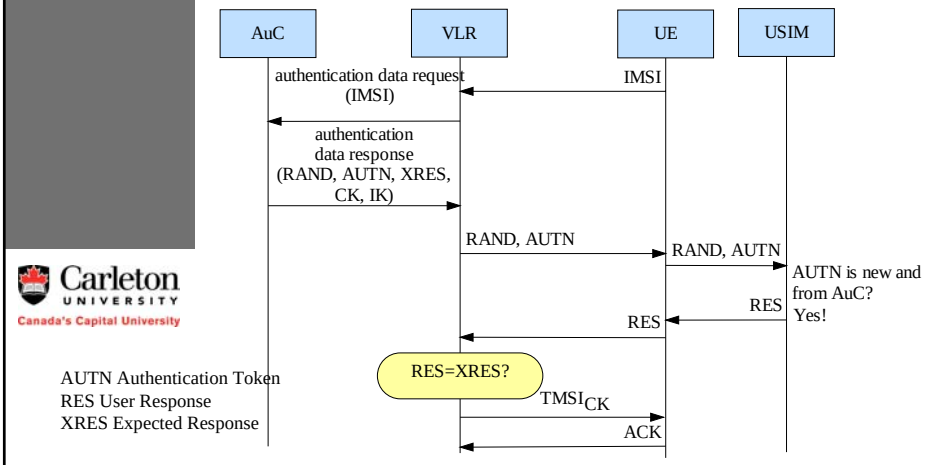
Carleton UNIVERSITY
Canada's Capital University

Security Associations in UMTS

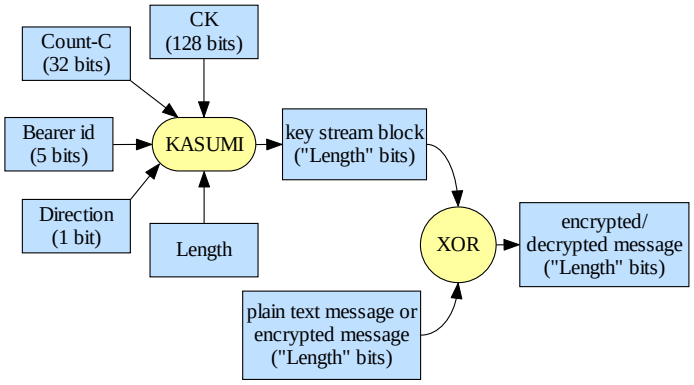


Carleton UNIVERSITY
Canada's Capital University

Mutual Authentication and Key Agreement in UMTS

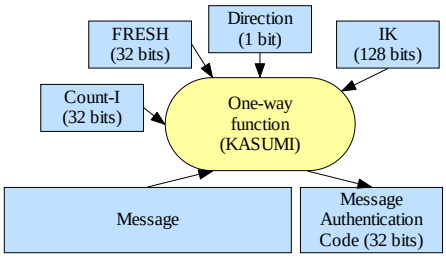


Encryption/Decryption in UMTS



COUNT-C: Frame number plus Hyper frame number, incremented when the frame number wraps around
Direction: up/down-link

Integrity in UMTS



COUNT-I: similar to COUNT-C, replay protection
FRESH: start value of COUNT-I

Challenge: Co-existence of analog technology and digital technology

- The digital technology as higher potential for being secure than analog technology. For example, the Cellular Digital Packet Data (CDPD) uses data encryption and provides privacy.
- Most of the cellular phones are hybrid technology, both analog and digital. The reason for that is that digital communications require a relatively stronger signal, for intelligibility, than analog communications, all other things being equal (such as bandwidth of a voice channel). A cell phone will hence operate in digital over relatively short distances.
- In order to enable long rang communications, cell phones fall back in the analog mode when the signal gets to weak for digital communications. Because of that, digital systems inherit of all the security vulnerabilities of analog systems.
- Co-existence of legacy analog technology and digital technology is a challenge for system security design.

Challenge: Introduction of new defense method in existing systems

- Attack methods evolve
- Defence methods evolve
- New defense methods are difficult to introduce in existing systems

Carleton UNIVERSITY
Canada's Capital University

Reconfigurable security

Reference

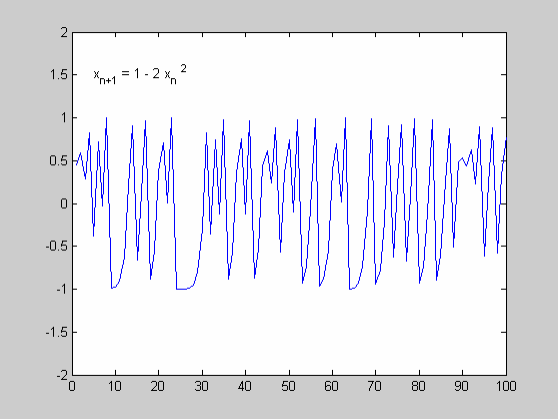
- Al- Mohtadi at al., A lightweight reconfigurable security mechanism for 3G/4G mobile devices, IEEE Wireless Communications, April 2002.

Definition

- Security mechanisms are reconfigured dynamically according to capabilities, processing power, and needs
- Loading/configuration/unloading of software components implementing security services

Carleton UNIVERSITY
Canada's Capital University

Chaotic Communication (1)



Chaotic Communication (2)

Background

- Abel and Schwarz, Chaos Communications—Principles, Schemes, and System Analysis, Proceedings of the IEEE, 2002.
- Itoh, Spread Spectrum Communication via Chaos, World Scientific Publishing Company, International Journal of Bifurcation and Chaos, 1999.

Theoretical Attacks

- Guojie, Zhengjin, and Ruiling, Chosen Ciphertext Attack on Chaos Communication Based on Chaotic Synchronization, IEEE Transactions on Circuits and Systems, 2003.
- Ogorzatek and Dedieu, Some Tools for Attacking Secure Communication Systems Employing Chaotic Carriers, IEEE, 1998.

Theoretically Broken Chaotic Communication (cont'd)

- Chaotic masking
  - Low amplitude modulating signal, high amplitude chaotic carrier
- Chaotic switching
  - Two waveforms representing binary values zero and one
  - Has a differential version
- Chaotic modulation
  - Chaotic carrier influenced by an non invertible function, according to the information

Carleton UNIVERSITY
Canada's Capital University

Quantum Cryptography

- Wiesner, "Quantum Money", 1960 (unpublished)
  - Polarity of photons (angle of vibration) can be verified, but not measured
- Bennett, Brassard, and Ekert, Quantum Cryptography, Scientific American, October 1992.
- Hughes et al., Quantum cryptography for secure satellite communications, Aerospace Conference Proceedings, 2000.
  - 0.5 km free-space link
- Kurtsiefer et al., Long Distance Free Space Quantum Cryptography, SPIE, 2002.
  - 23.4 km free-space link (try to achieve 1000 km)
- First Quantum Cryptography Network Unveiled, NewScientist.com news service, June 2004.
  - Quantum Net: six servers, 10 km links, software-controlled optical switches

Carleton UNIVERSITY
Canada's Capital University