Mobile Security
Fall 2015

Patrick Tague

#3: Brief History of Telecom Security

Class #3

And now...

A brief history of telecom security

Basics of Telecom Security

- Different players in the mobile ecosystem have different security concerns

- Security concerns and techniques have evolved along with the infrastructure

- Let's go through that evolution, starting with some of the basic concerns that different players may have

Users' Security Goals

- No user/entity should be able to bill calls on another user's behalf
- Stolen mobile devices shouldn't be able to make calls
- The network shouldn't record calls, only enough info to perform billing functions
- No records of digital service usage should be made
- Voice eavesdropping should be impossible
- A mobile user's location should be private until disclosed (except in emergencies)
- A device's user should not be identifiable until disclosed
- …

Providers' Security Goals

- Communication service billing should be correctly managed
- All types of fraud should be prevented and mechanisms should be updated as necessary
- Correct naming and addressing of devices must be implemented; routing functions must be secure
- Providers should be able to add services / functions and provide desired security for them
- …

Government Security Goals

- Location information must be provided to emergency services
- Robust infrastructure should be available in emergencies
- Communication and information must be accessible to law enforcement
- Useful measures must be in place for monitoring and protection of essential assets and infrastructures
- …

Let's walk through some history to see how these goals were (not) met

Early Cell Systems - "1G"

- Most well known system is AMPS (advanced mobile phone system)
  - AMPS was introduced in 1978 (FCC-approved and first used in 1983)
  - First use of the hexagonal cell structure (W. R. Young @ Bell Labs)

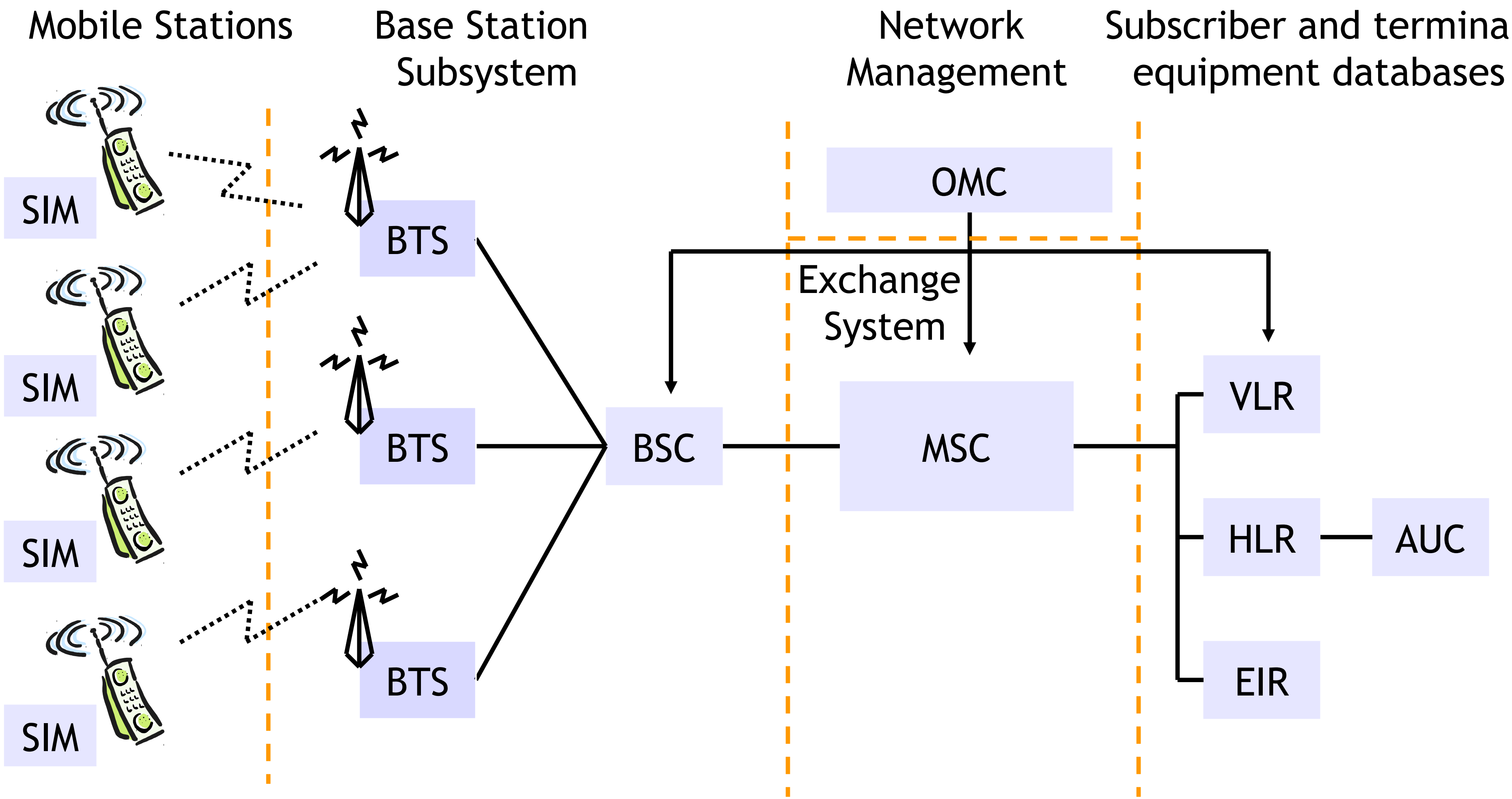
1G Security

- Security provided by AMPS
  - User/device authentication and call authorization in AMPS is very simple:
    - Device provides the 10-digit telephone number (MIN: mobile identity number) and the 32-bit serial number (ESN: electronic serial number = 8-bit manufacturer code + 6-bit unused + 18-bit mfg-assigned serial number)
    - If MIN/ESN matches (in home or visiting register), connection is made
  - No encryption is provided
  - See any vulnerabilities?

From 1G to 2G

- Primary difference between 1G and 2G is the switch from analog to digital
  - Better mechanisms for authentication / authorization were also mandated, due to weakness of MIN/ESN matching protocol
  - Digital also means voice can be encrypted for over-the-air transmission

2G GSM/CDMA Architecture

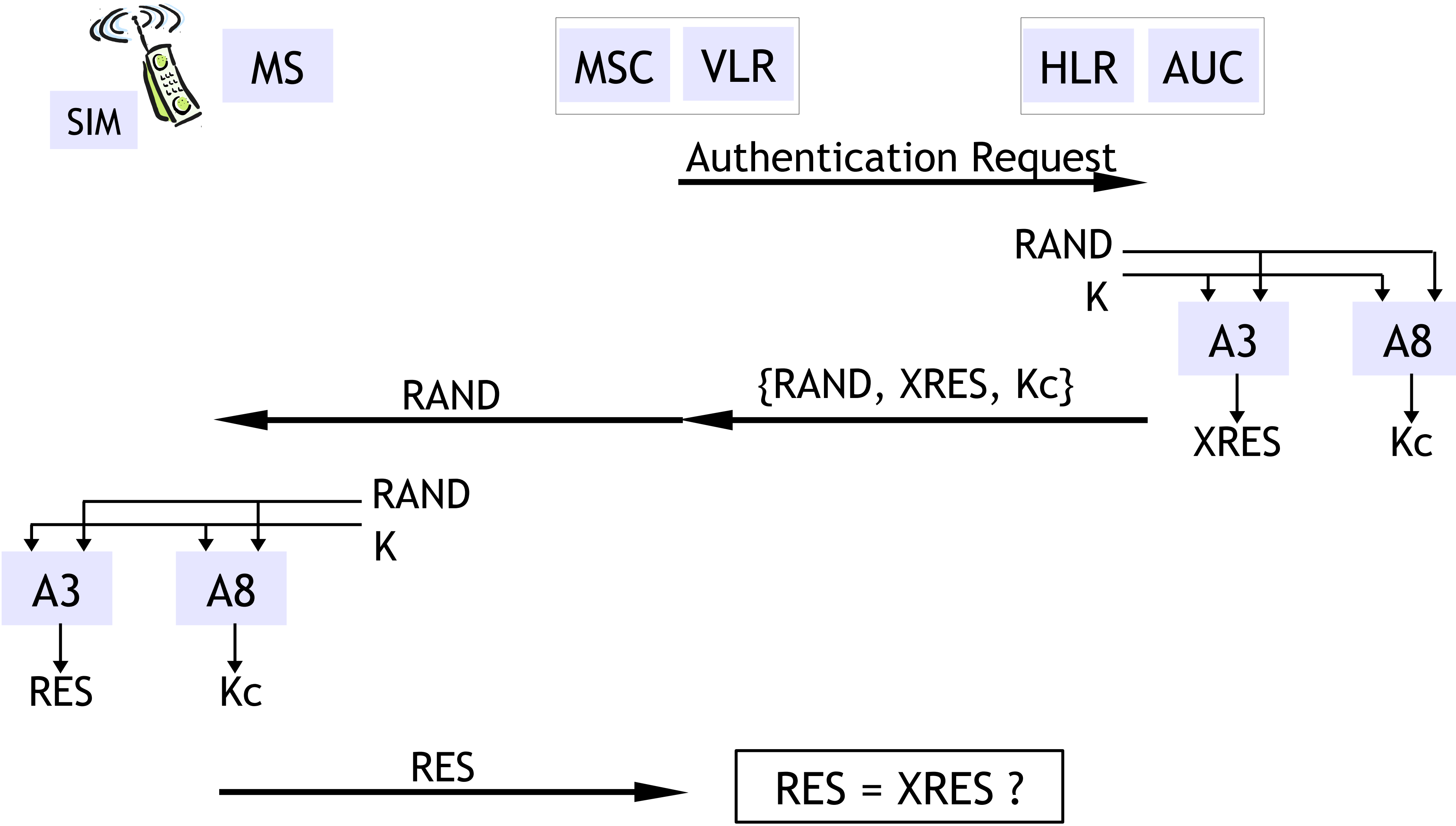


adapted from [M. Stepanov; http://www.gsm-security.net/]

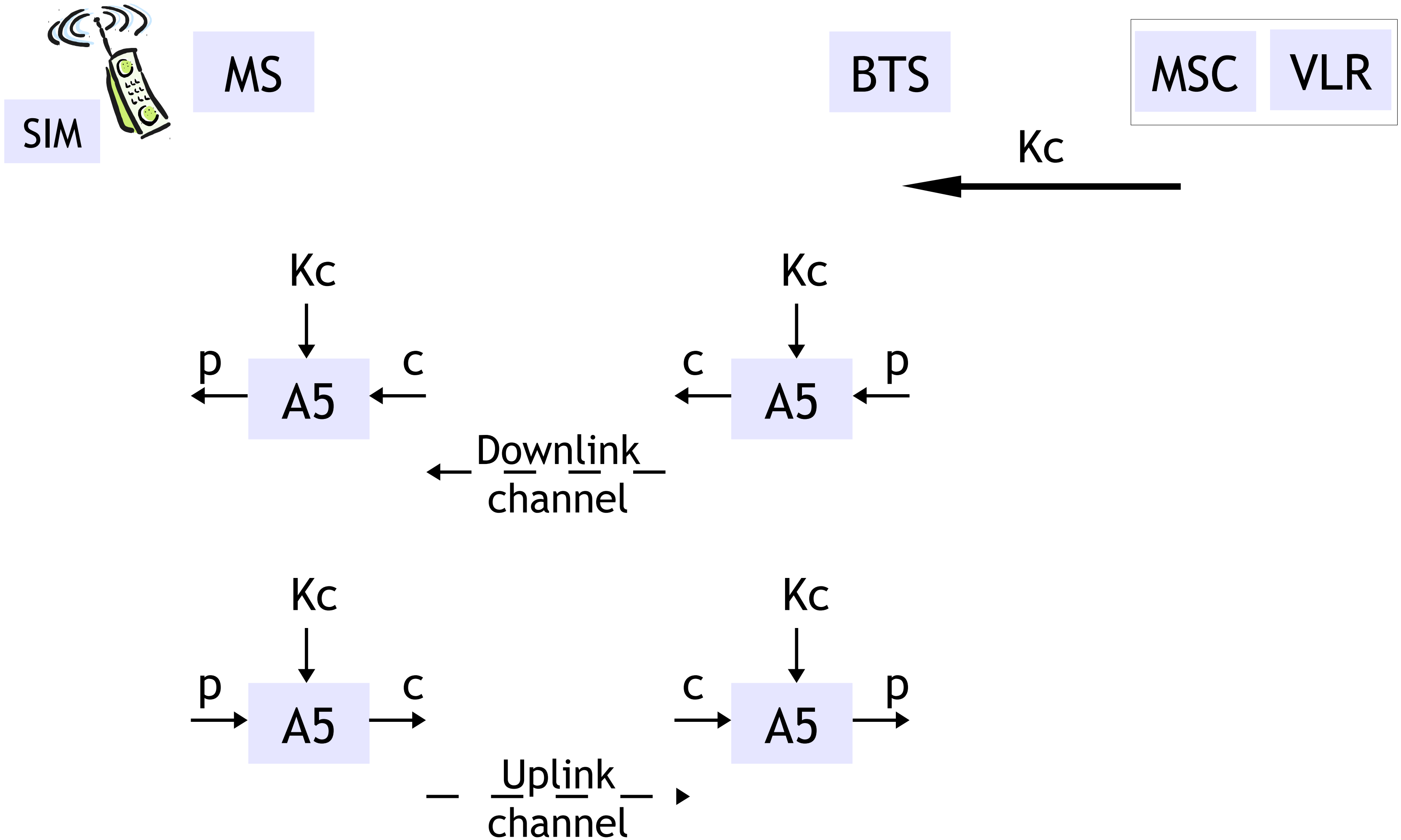
2G GSM Security

- Secure access
  - User authentication for billing and fraud prevention
  - Uses a challenge/response protocol based on a subscriber-specific authentication key (at HLR)
- Control and data signal confidentiality
  - Protect voice, data, and control (e.g., dialed telephone numbers) from eavesdropping via radio link encryption (key establishment is part of auth)
- Anonymity
  - Uses temporary identifiers instead of subscriber ID (IMSI) to prevent tracking users or identifying calls

Auth. & Key Agreement

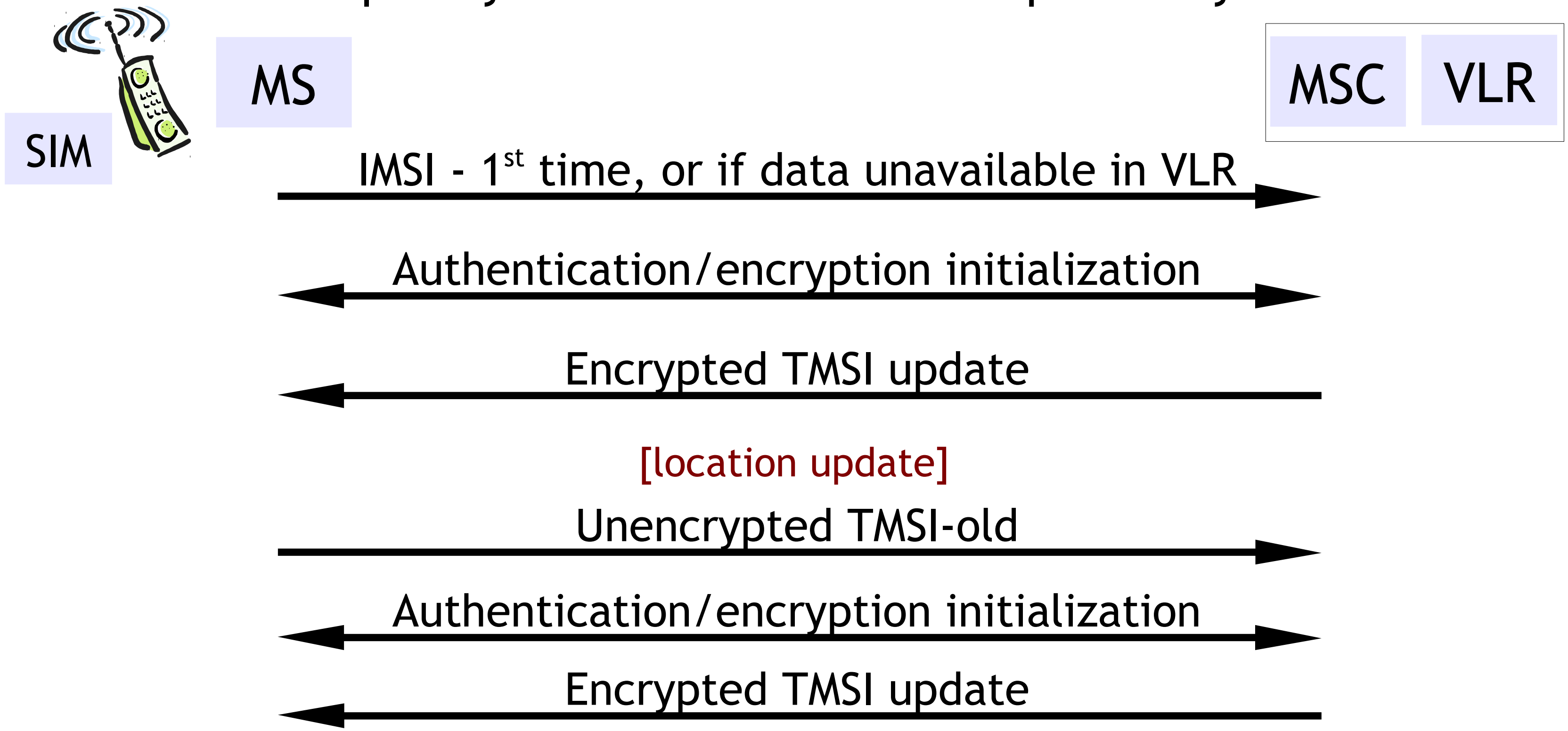


Radio Link Encryption



Temporary ID Management

- User and device identity:
  - IMEI: Int'l Mobile Equipment ID - device
  - IMSI: Int'l Mobile Subscriber ID - user
  - TMSI: Temporary Mobile Subscriber ID – pseudonym



Algorithm Implementations

- A3 and A8 are implemented on the SIM, operator-dependent
  - Most use COMP128 algorithm

- A5 is efficiently implemented in hardware
  - Design was never published (security through obscurity...), but it leaked to R. Anderson and B. Schneier
  - Variants A5/1 (strong), A5/2 (weak), A5/3 (similar to KASUMI used in 3G), and A5/4 (also based on KASUMI)

Attacks on GSM Security

- April 1998
  - Smartcard Developer Association and UC-Berkeley researchers crack COMP128 and recover K in hours
  - Discovered Kc is only 54 bits (instead of 64)
- Aug 1999
  - A5/2 was cracked using a single PC within seconds
- December 1999
  - Biryukov, Shamir, and Wagner publish break of A5/1 - 2 minutes of intercepted call and 1 second attack

Attacks on GSM Security

- May 2002
  - IBM Research group extracts COMP128 keys using side-channel attack

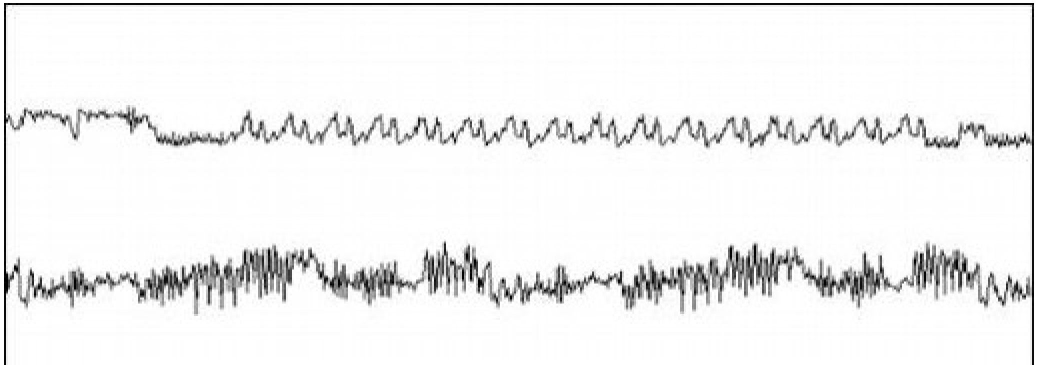


image from [M. Stepanov; http://www.gsm-security.net/]

- More details:
  - M. Stepanov, http://www.gsm-security.net/
  - G. Greenman, http://www.gsm-security.net/
  - Traynor et al., *Security for Telecommunications Networks*

More GSM Attacks

- In-network attacks
  - Transmissions are only encrypted MS → BTS
    - Any attacker between BTS-MSC (such as an eavesdropper on a microwave back-haul) or inside the operator's network has read/modify data access
  - Signaling network (SS7) is completely unsecured
  - Access to HLR → retrieve all K keys
- Over-air attack
  - Repeated MS queries for RES values can be used to recover K via cryptanalysis – potential attack by a rogue base station

Later Developments

- GPRS security
  - Same authentication and key agreement architecture
  - Encryption extends further into network core
  - Updated encryption algorithms

- SIM security toolkit
  - Establish secure channel from SIM to a network server
  - Extends GSM security to sensitive applications
    - E-commerce applications
    - Secure remote SIM/MS management

3G Evolution

- 3G: mixed switching, MMS, location services
  - UMTS, TD-CDMA, WCDMA, CDMA-3xRTT, TD-SCDMA
- 3.5G: increased download speeds
  - HSDPA (high speed downlink packet access)
- 3.75G: increased upload, multimedia
  - HSUPA (" uplink ") → HSPA
  - Multimedia broadcast → mobile TV
- 3.9G: ~2x UL/DL rates
  - HSPA+
  - Often marketed as 4G…

Example: VZW's 3G Network

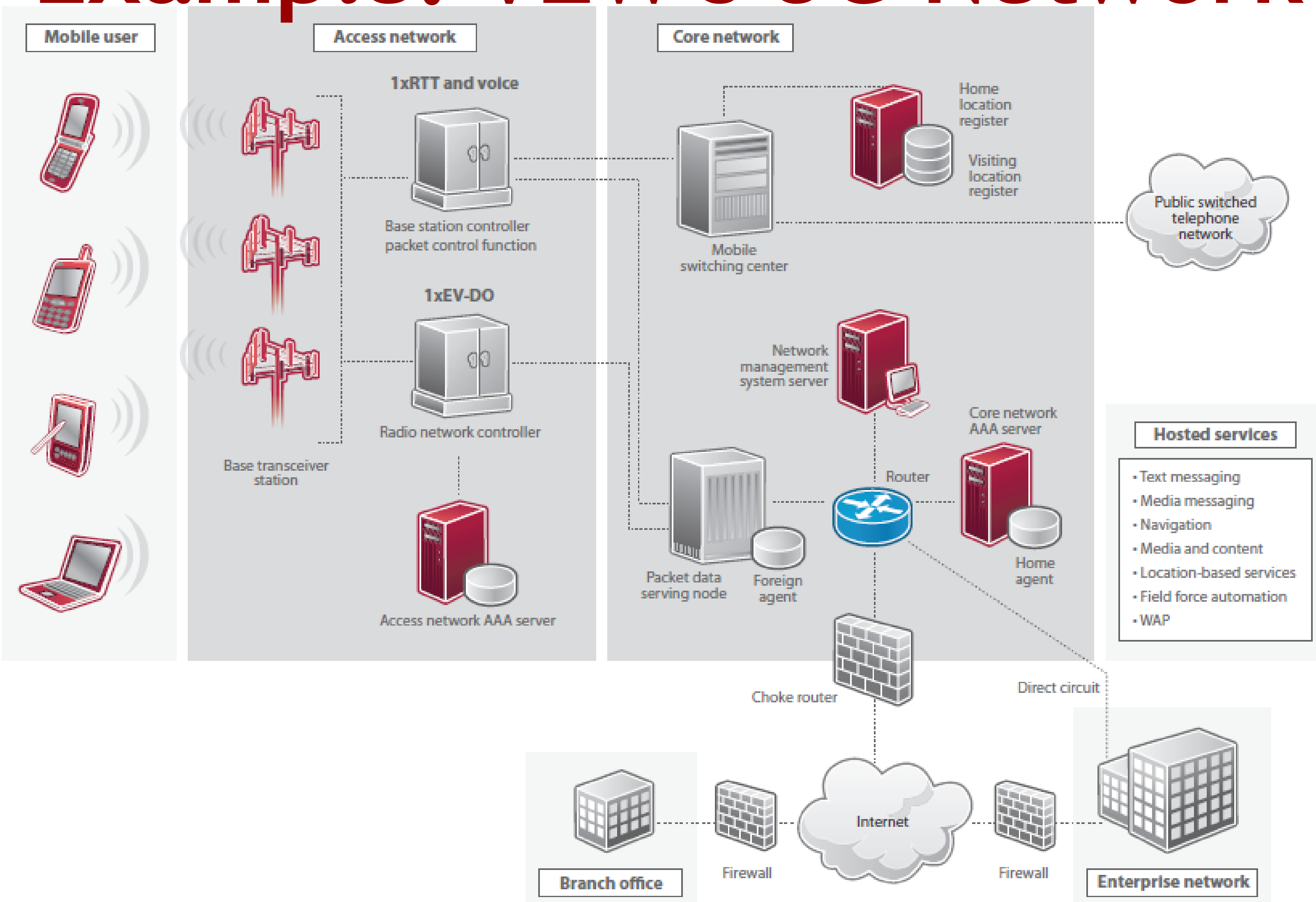
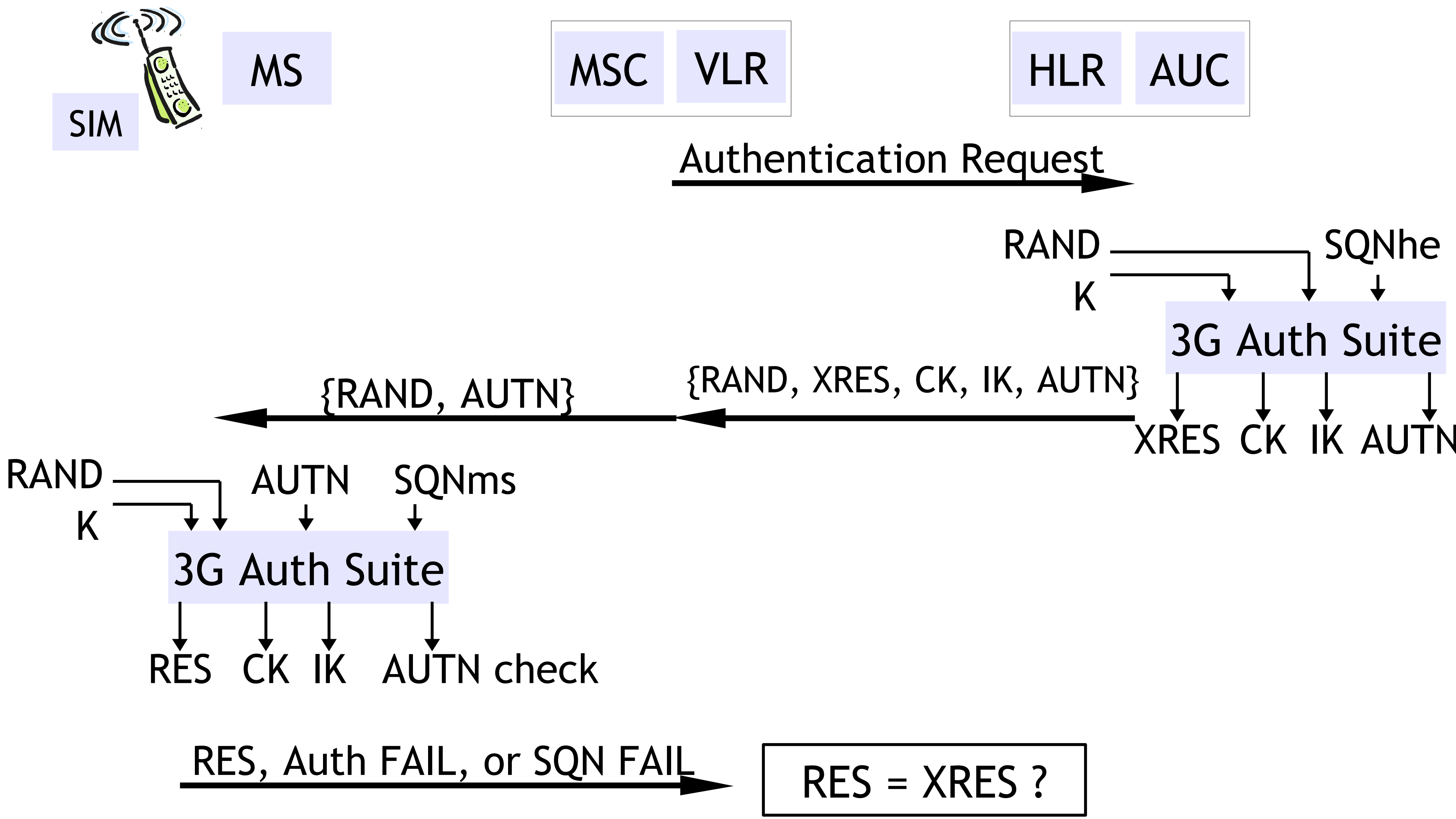


image from [VZW "CDMA Network Security" whitepaper]

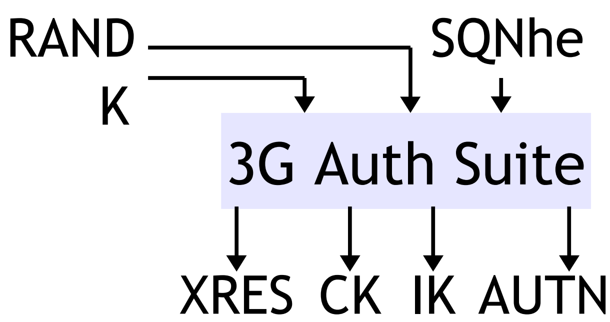
Re-Design in 3G

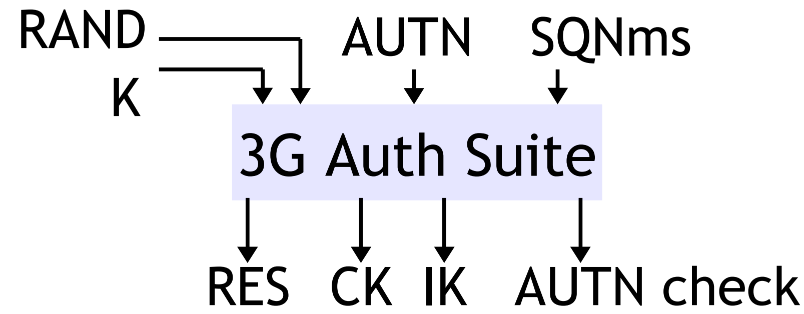
- 3G security model builds on GSM
- Protection against active attacks
  - Integrity mechanisms to protect critical signaling
  - Enhanced (mutual) authentication w/ key freshness
- Enhanced encryption
  - Stronger (public) algorithm, longer keys
  - Encryption deeper into the network
- Core security – signaling protection
- Potential for secure global roaming (3GPP auth)

Enhanced Auth. & Keying



Enhanced Auth. & Keying





3G Auth Suite = { F1 , F2 , F3 , F4 , F5 , ...}

$XMAC = F1_K(RAND \mid SQN \mid AMF)$

$XRES = F2_K(RAND)$

$CK = F3_K(RAND)$

$IK = F4_K(RAND)$

$AK = F5_K(RAND)$

AUTN = SQN [xor AK] | AMF | XMAC

SQN > SQNhe

$MAC = F1_K(RAND \mid SQN \mid AMF)$

$RES = F2_K(RAND)$

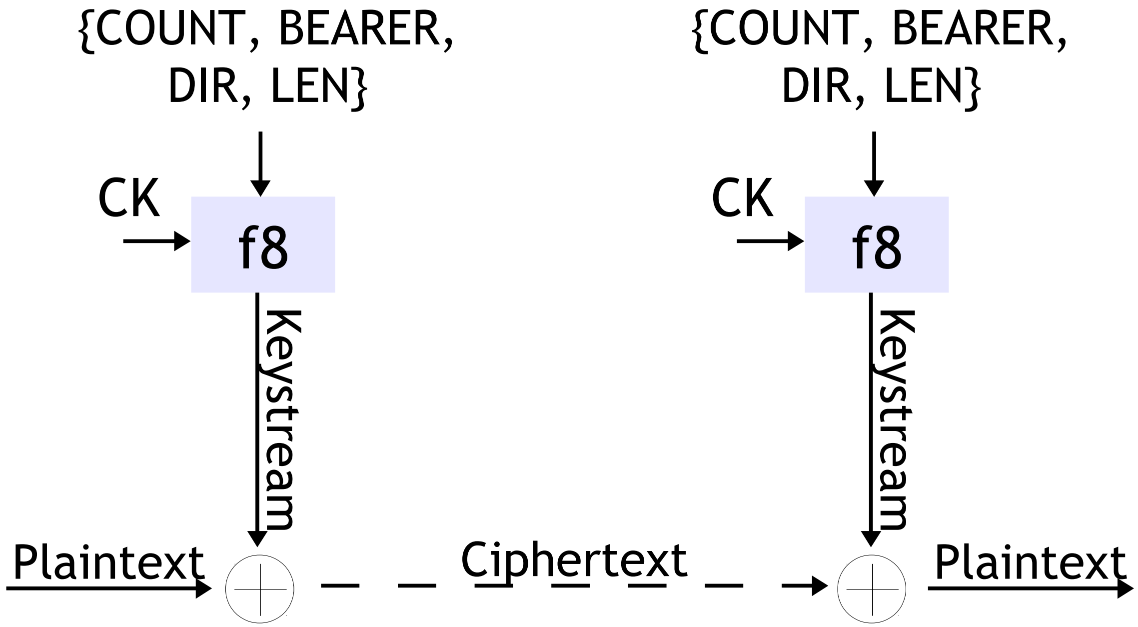
$CK = F3_K(RAND)$

$IK = F4_K(RAND)$

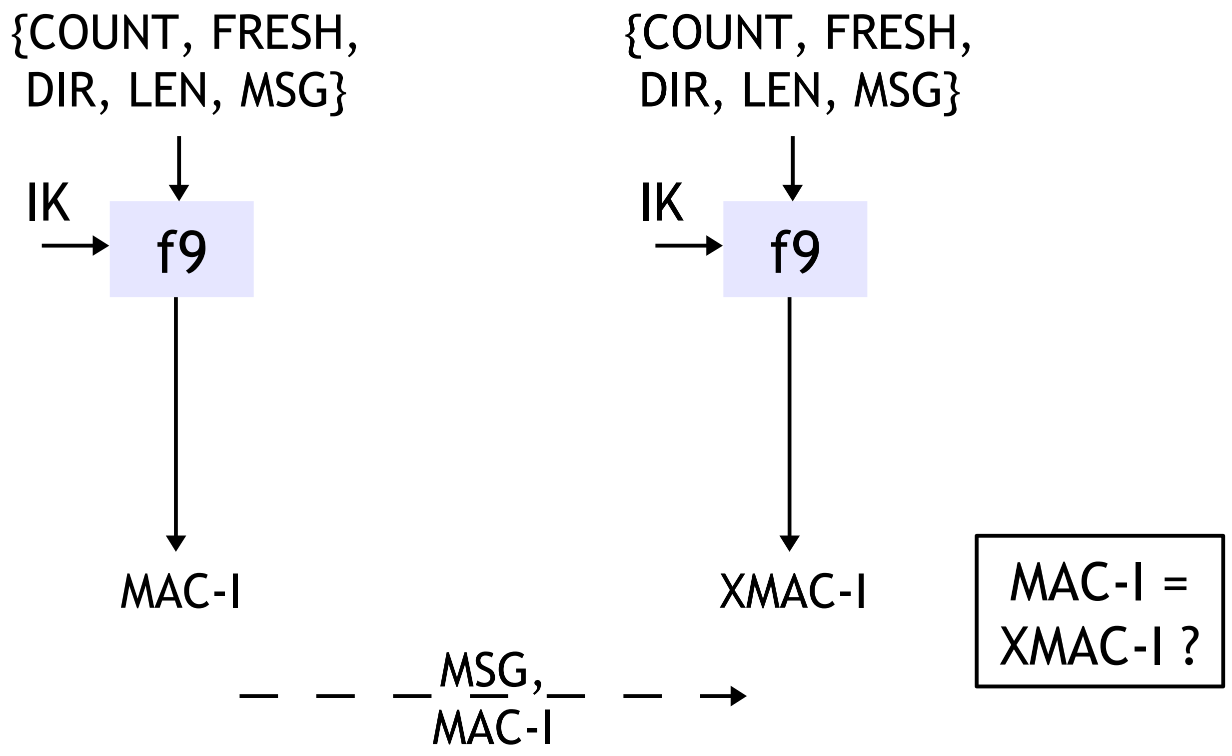
$AK = F5_K(RAND)$

XMAC = MAC ?
SQN > SQNms ?

Enhanced Confidentiality



Enhanced Integrity



Algorithm Implementation

- KASUMI
  - Based on MISTY block cipher (Mitsubishi)
  - Two operational modes
    - f8 for encryption
    - f9 for integrity
  - Externally reviewed (positively)
  - Published
  - Broken
    - Dunkelman, Keller, and Shamir – January 2010
    - Interestingly, MISTY isn't affected by this technique...

Sept 10:
Telecom System Security Issues

Sept 15:
Tutorial 1: Android Tips & Tricks