Mobile Security
14-829 – Fall 2013

Patrick Tague

Class #3 – Telecom Security from 1G to 4G

Carnegie Mellon University
Silicon Valley

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)
  - Analog mobile phone system introduced in 1978 (FCC-approved and first used in 1983)
  - First use of the hexagonal cell structure (W. R. Young @ Bell Labs)

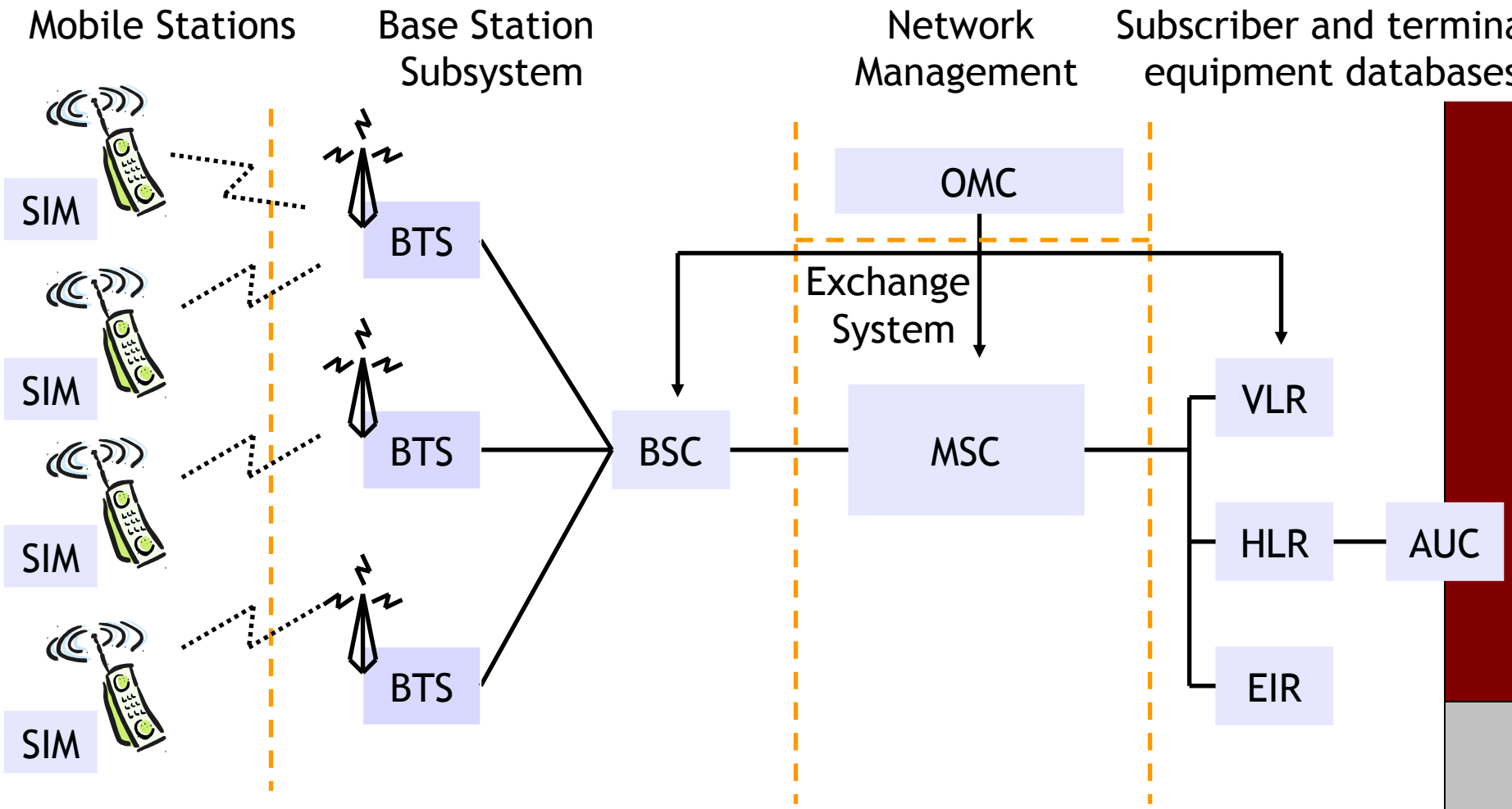
1G Security

- 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 Evolution

- 2G (digital PCS)
  - GSM – global system for mobile communication
  - CDMA Cellular (IS-95A)
- 2.5G (IP-based)
  - GPRS (general packet radio service): adds IP-overlay over GSM circuits, provides packet data service, uses additional support node as Internet gateway
  - CDMA2000: wider-band, higher capacity CDMA
- 2.75G (IP-based)
  - EDGE (enhanced data rates for GSM evolution): modifies physical layer, no other changes

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

SIM

MS

MSC VLR

HLR AUC

Authentication Request

RAND

K

A3 A8

XRES Kc

{RAND, XRES, Kc}

RAND

RAND

K

A3 A8

RES Kc

RES

RES = XRES ?

Radio Link Encryption

SIM

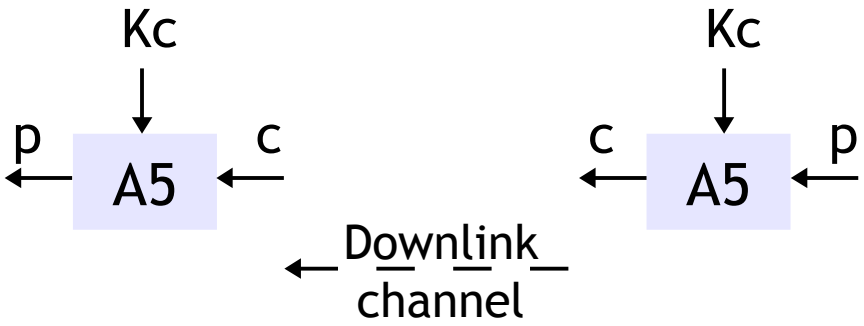
MS

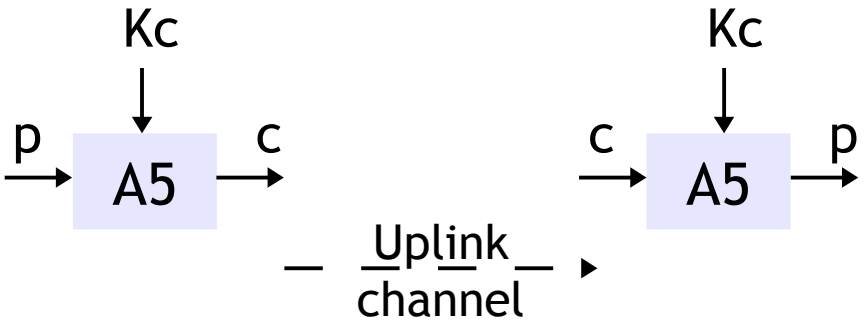
BTS

MSC

VLR

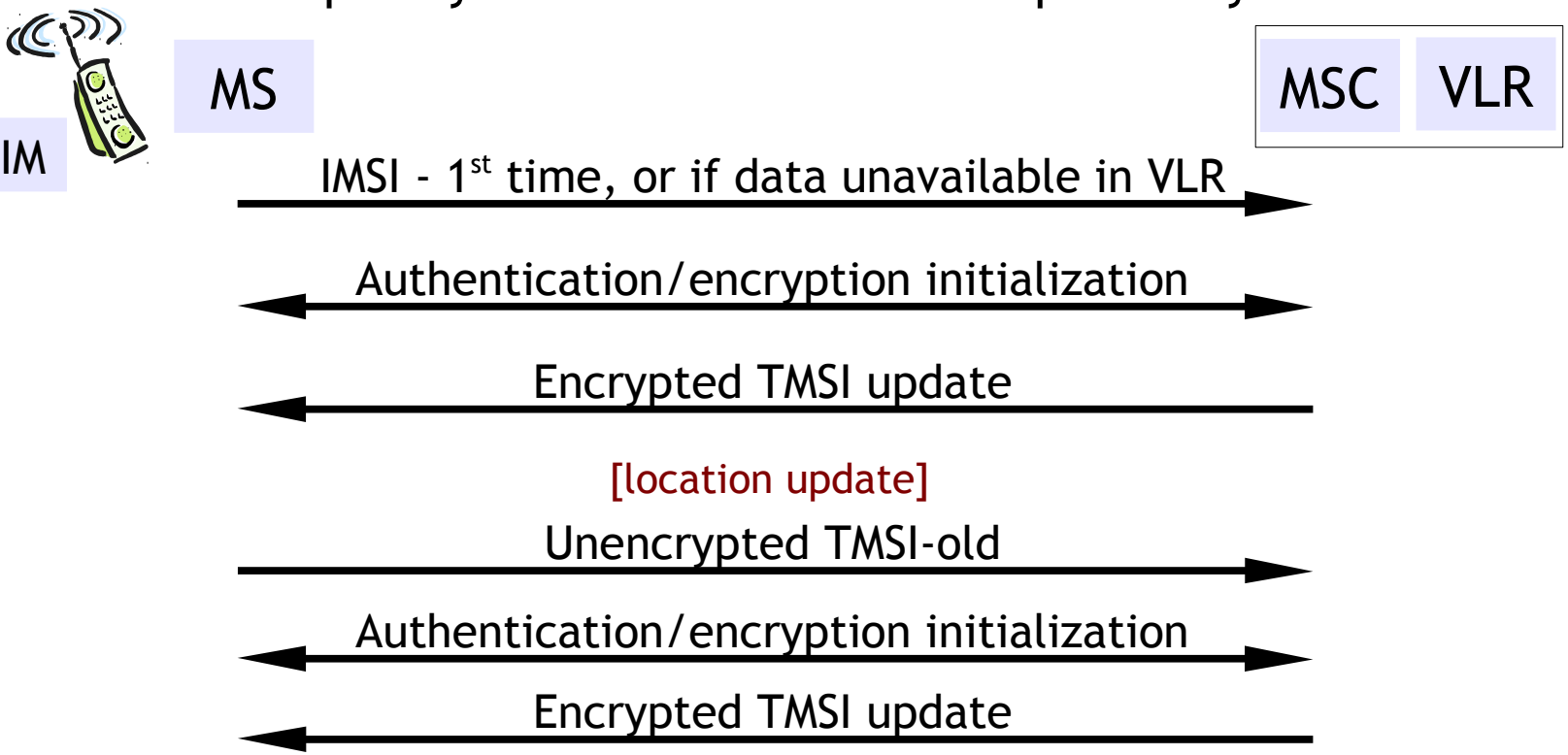
Kc





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

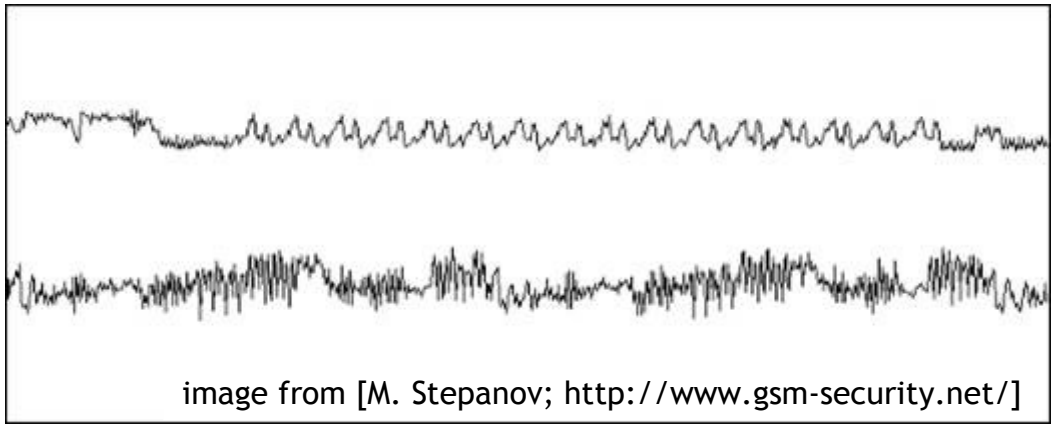


image from [M. Stepanov; http://www.gsm-security.net/]

- 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

What About CDMA Systems?

- Most of what we're covering for GSM systems has a direct analog in the CDMA world

- CDMA has some fundamentally different features than GSM, but that's a discussion for another day
  - Anyone remember the TDMA vs. CDMA debate?

From 2G to 3G

- GSM and CDMA technologies have started to converge in 3G, with UMTS basically representing this convergence
  - UMTS = universal mobile telecom system, comes in many different flavors
  - TD-CDMA combines TDMA and CDMA
  - WCDMA (similar to EDGE with CDMA)
  - CDMA2000-3xRTT (three times the channel usage as 1xRTT)

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+
  - Sometimes marketed as 4G… we'll get to that soon

Example: VZW's 3G Network

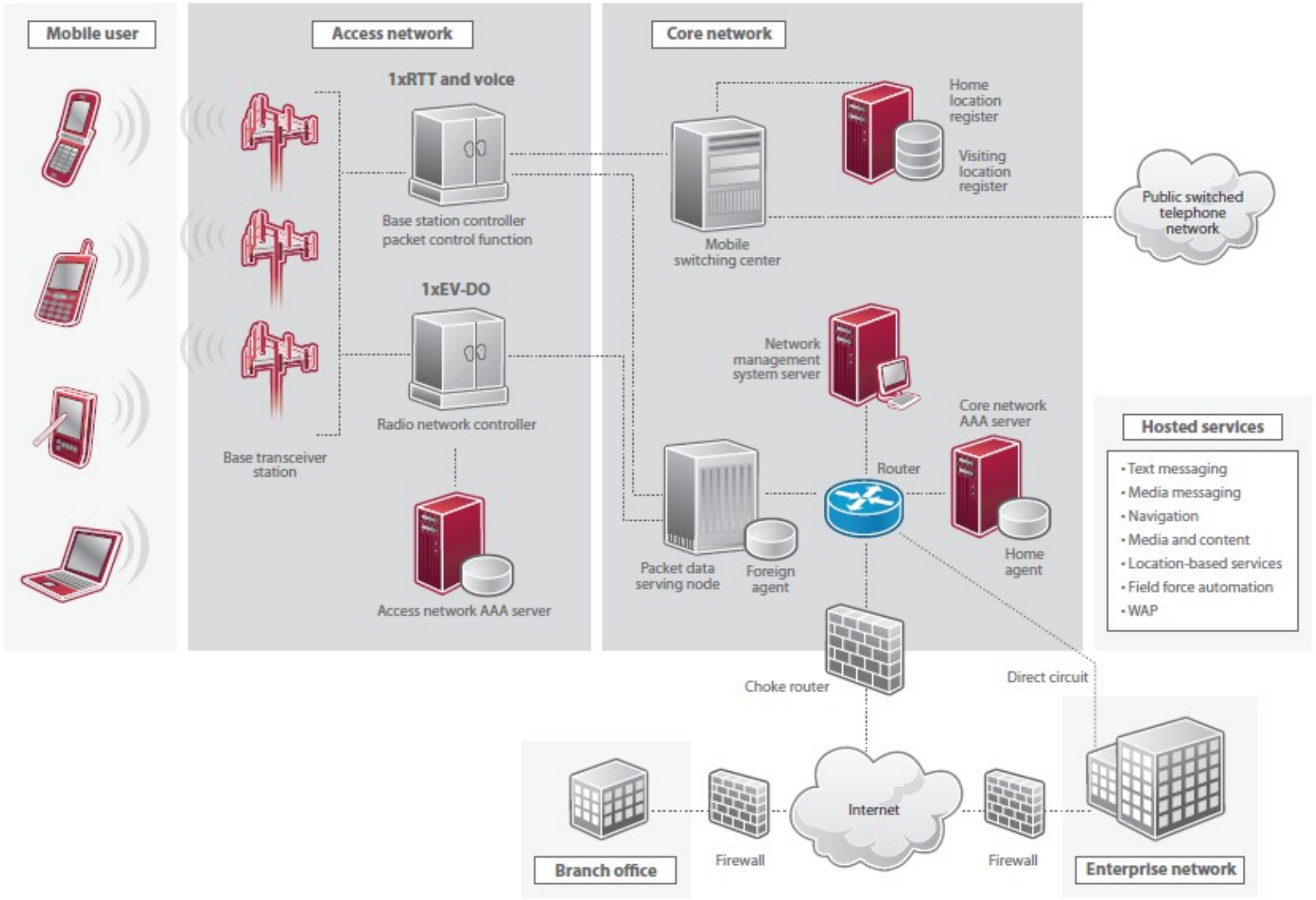


image from [VZW "CDMA Network Security" whitepaper]

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

SIM

MS

MSC VLR

HLR AUC

Authentication Request

RAND

K

SQNhe

3G Auth Suite

XRES CK IK AUTN

{RAND, XRES, CK, IK, AUTN}

{RAND, AUTN}

RAND

K

AUTN

SQNms

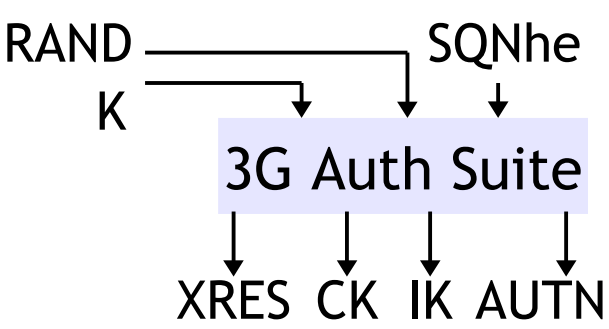
3G Auth Suite

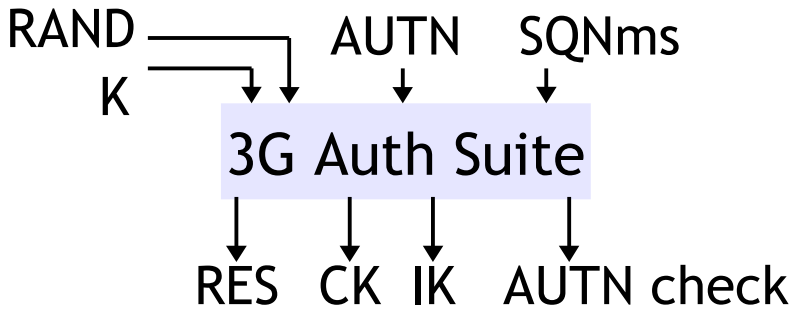
RES CK IK AUTN check

RES, Auth FAIL, or SQN FAIL

RES = XRES ?

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] $\mid AMF \mid XMAC$

$SQN > SQNhe$

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

$RES = F2_K(RAND)$

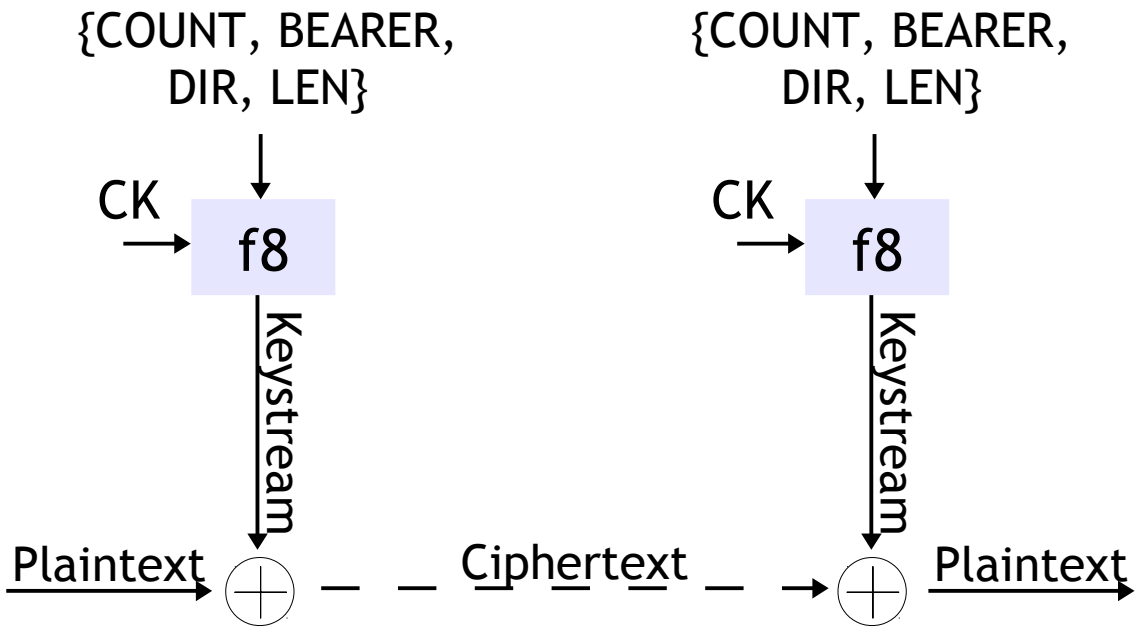
$CK = F3_K(RAND)$

$IK = F4_K(RAND)$

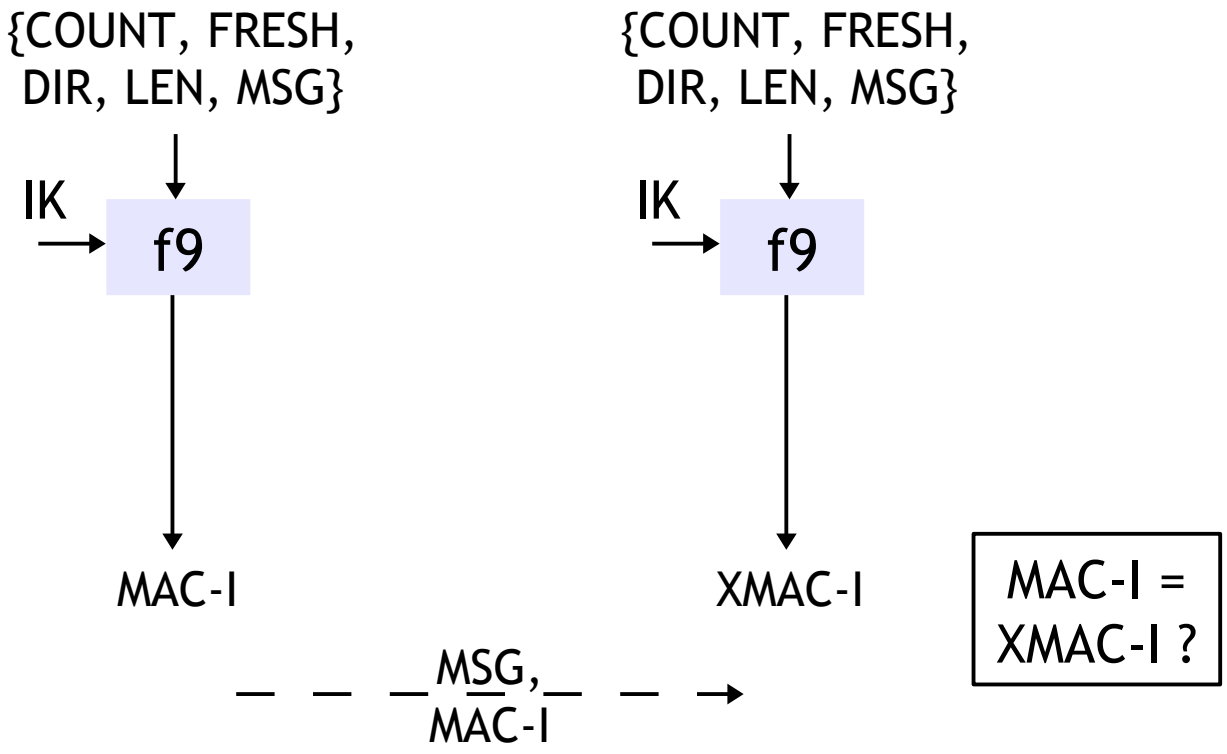
$AK = F5_K(RAND)$

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 authentication
  - Externally reviewed (positively)
  - Published
  - Broken
    - Dunkelman, Keller, and Shamir – January 2010
    - Interestingly, MISTY isn't affected by this technique...

From 3G to 4G

- 4G represents the next generation in cellular communication
  - Cellular broadband wireless access -or- “mobile broadband”

- MAGIC:
  - **M**obile multimedia
  - **A**nytime anywhere
  - **G**lobal mobility support
  - **I**ntegrated wireless solution
  - **C**ustomized personal service

4G vs. "4G"

- "4G is a combination of marketing speak and future tech" [Warren, Mashable 02/2011]
  - Current "4G" systems are actually 3.75G or 3.9G, but they'll be upgraded to real 4G in the future
- True 4G:
  - Will provide 10x speed of 3G with better coverage
  - WiMAX Release 2, LTE-Advanced
    - WiMAX and LTE are not really 4G, but "4G"
    - Verizon uses LTE, AT&T uses HSPA+ and LTE, T-Mobile uses HSPA+, Sprint uses WiMAX and LTE

What is 4G, Really?

- According to ITU-R standard, 4G delivers 1Gbps to stationary/slow devices and 100Mbps to (fast) mobile devices
  - *Eventually*, a replacement for cable/DSL/etc.
  - LTE and WiMAX currently peak at 100 and 144Mbps, but currently deliver ~10Mbps
  - T-Mobile's HSPA+ delivers ~20Mbps in some areas

- Several other improvements are included in the standard, but you can look them up for yourself

4G Security Issues

- All-IP network → all IP-based threats apply
- Verification of users
- Heterogeneous network access
  - User-preferred connection methods
  - Multiple available connections:
    - Attacker has more opportunity for exploit/attack
    - Device is exposed to attacks on each connection
      - Exploits based on driver code, comm protocols, transport / signaling, file-sharing, update, etc.
  - Complex management systems are required
- ?

"It is difficult to quantify the security risks of 4G when it has yet to be developed, however it is essential that developers find a definable way to find a balance between practical applications and the necessary security levels involved with the network."

- Kevin Rio, Krio Media blog

4G Authentication

- Authentication must be robust to DoS, resource consumption, unbilled service, etc. attacks
- User authentication may be desired over device or session (pre-)authentication from a management perspective
- Network authentication protects against MitM attacks and establishes end-to-end trust
- Some systems use weaker authentication (e.g., 802.11 only authorizes the interface/device, not the AP)
- How to allow integration into 4G systems with such different authentication goals?

Sept 9:
Telecom System Security; Some Interesting Threats

I'll be teaching from Pgh – let me know if you want to meet.