Security in Telecommunications

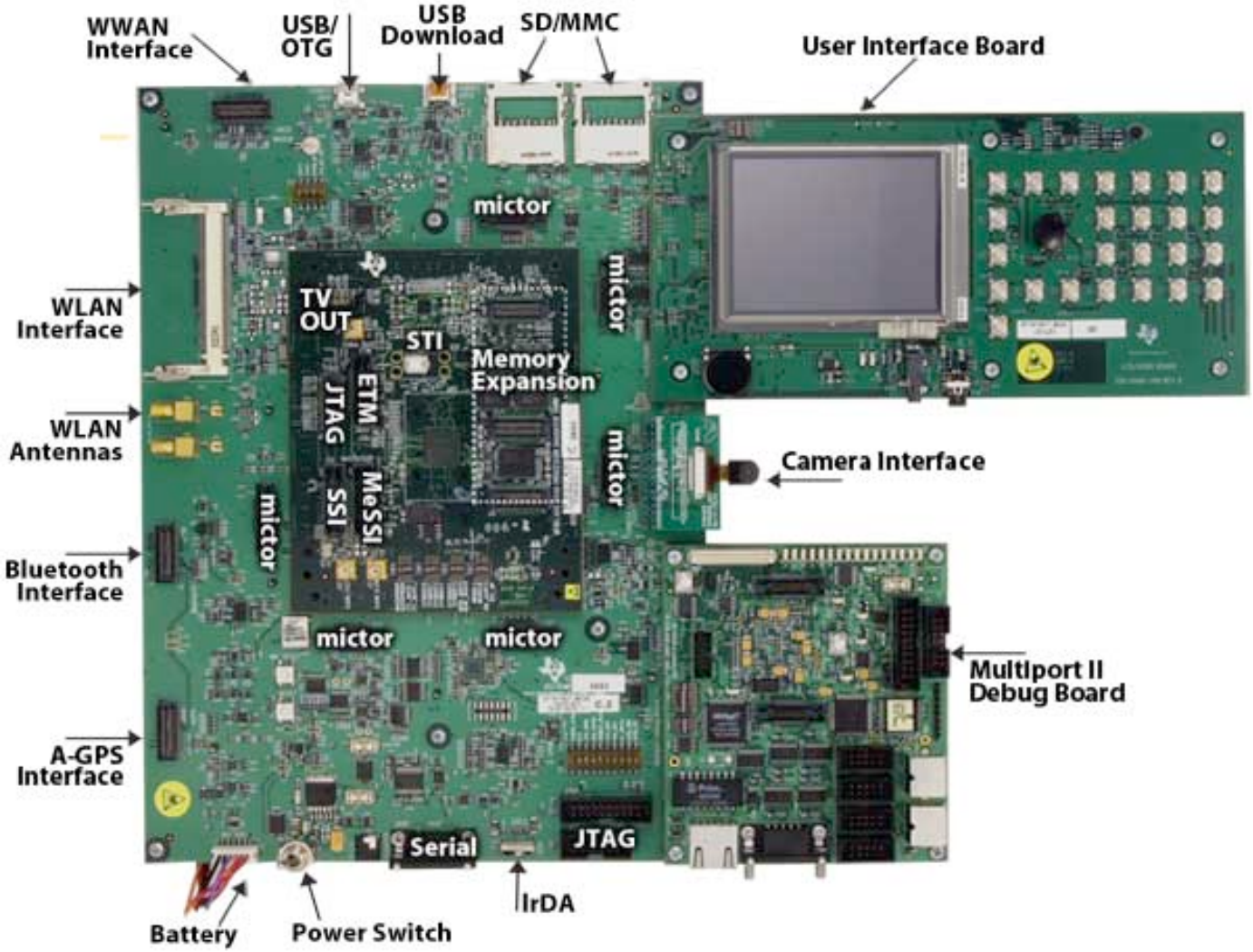
Prof. Dr. Jean-Pierre Seifert

jpseifert@sec.t-labs.tu-berlin.de

http://www.sec.t-labs.tu-berlin.de/

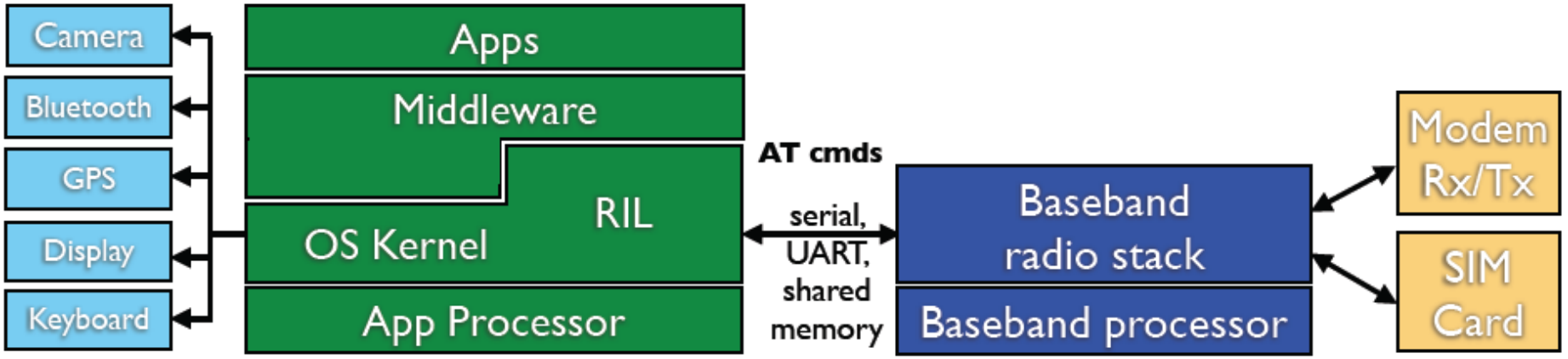
SECT Security IN TELECOMMUNICATIONS

Cellphone Hardware

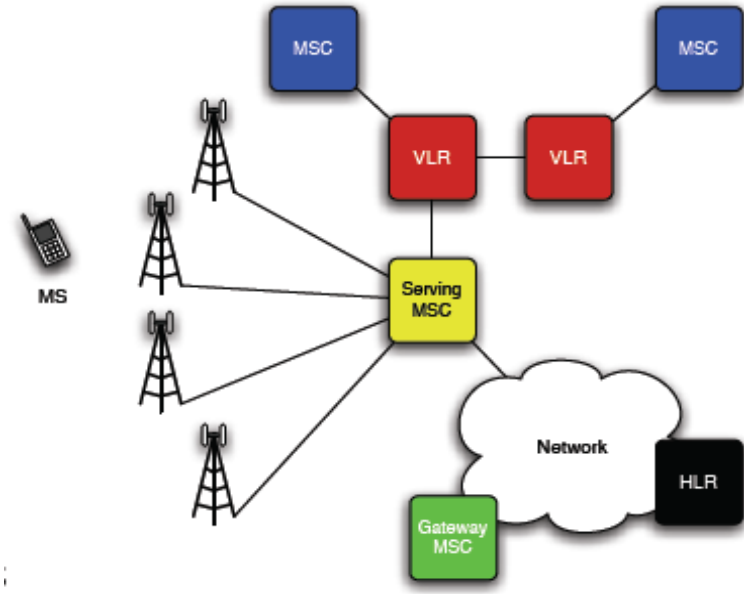


Handset Architecture

- Most mobile handsets comprise of two main processors (baseband and application) and peripheral-specific logic cores
- Commonly, a System-on-Chip (SoC) for the application processor and peripheral-specific logic. Sometimes the baseband processor is included on that SoC
  - SoC means more efficient data transfers and lower exposure to potential physical attackers



Cellular Networks Background



Cellular Networks

- Provide communications infrastructure for an estimated *2.6 billion* users daily.
  - The Internet connects roughly 1 billion.
- For many people, this is their only means of reaching the outside world.
- Portable and inexpensive nature of user equipment makes this technology accessible to most socioeconomic groups.

Aren't They The Same?

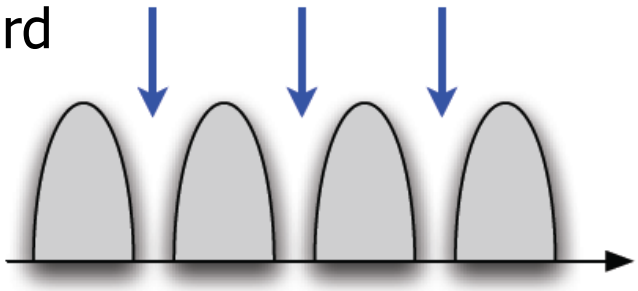
- Cellular networks and the Internet are built to support very different kinds of traffic.
  - Real-time vs. Best Effort
- The notions of control and authority are different.
  - Centralized vs. distributed
- The underlying networks are dissimilar.
  - Circuit vs. packet-switched

Network Characteristics

- Composed of wired backbone and wireless last-hop
- Inconsistent performance
  - Variable delay
  - High error rates
  - Lower bandwidth
- Potentially high mobility

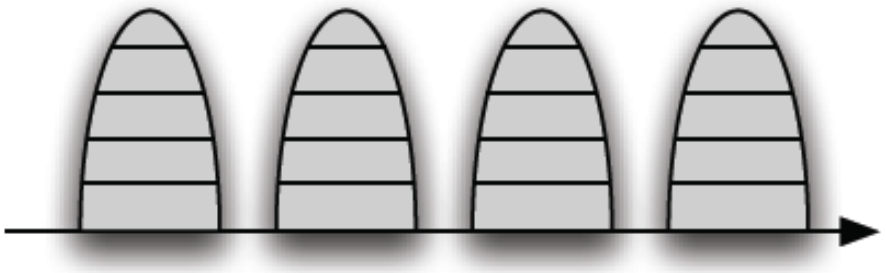
Access Basics - FDMA

- The most basic access technique is known as *Frequency Division Multiple Access* (FDMA).
- Each user in these systems receives their own dedicated frequency band (i.e., "carrier").
  - Requires one for uplink and another for downlink.
- To reduce interference, each carrier must be separated by *guard bands*.
  - Protects against interference
  - AMPS used 30 kHz carriers with 1 KHz guard



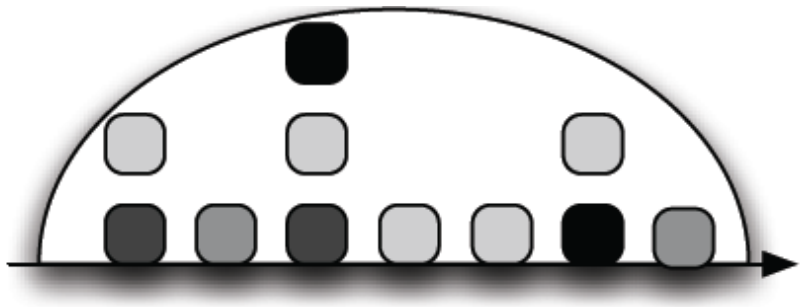
TDMA Access

- *Time-Division Multiple Access* (TDMA) systems greatly increase spectrum utilization.
- Each carrier is subdivided into timeslots, thereby increasing spectrum use by a factor of the divisor.
  - GSM has 8 timeslots service every 4.615 msec
- Requires tight time synchronization in order to work.
  - To protect against clock drift, we need to buffer our timeslots with guard-time.



CDMA Access

- *Code-Division Multiple Access* (CDMA) systems have users transmit simultaneously on the same frequency.
- The combined transmissions are viewed additively by the receiver.
- By applying a unique code, the receiver can mask-out the correct signal.
  - Picking these codes must be done carefully.
  - No fixed upper bound on concurrent devices!

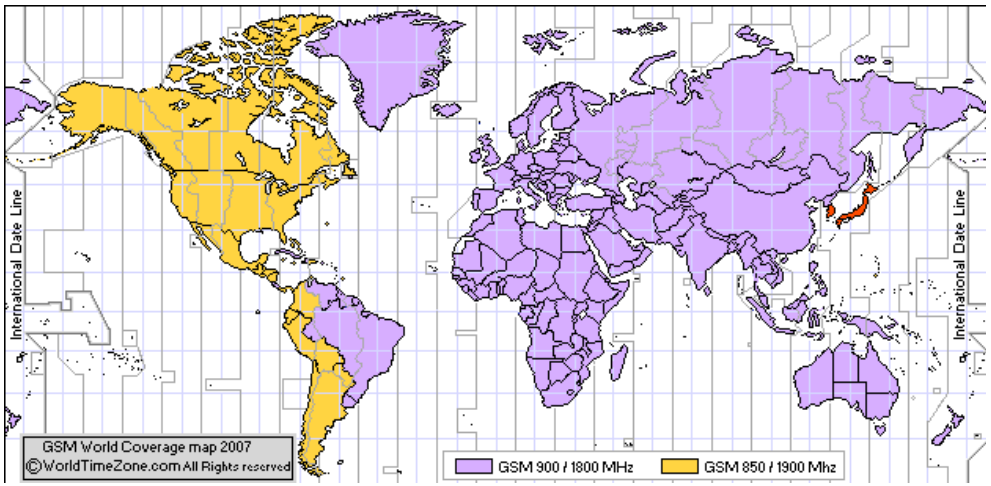


In the beginning... (1G)

- First commercial analog systems introduced in the early 1980's.
- Two competing standards arose:
  - The Advanced Mobile Phone System (AMPS)
  - Total Access Communication System (TACS)
- Both systems were FDMA-based, so supporting a large number of calls concurrently was difficult.
- Used for home security systems (e.g., ATD, GE Security)
  - FCC called end to AMPS in early 2008

The Advent of Digital (2G)

- Second Generation systems were introduced in the early 1990's.
- Three competing standards:
  - IS-136 and GSM (TDMA) - used by e.g., AT&T, T-Mobile, Europe
  - IS-95-A/cdmaOne (CDMA) - used by e.g., Verizon, Sprint
- 2G networks introduced dedicated control channels, which greatly increased the amount of information exchanged between devices and the network.
- IS-136 (known as TDMA) is very similar to GSM, but eventually phased out in the US; effort to support global roaming



Introducing Data (2.5G)

- Digital brings higher bandwidth, and the opportunity to deploy data services.

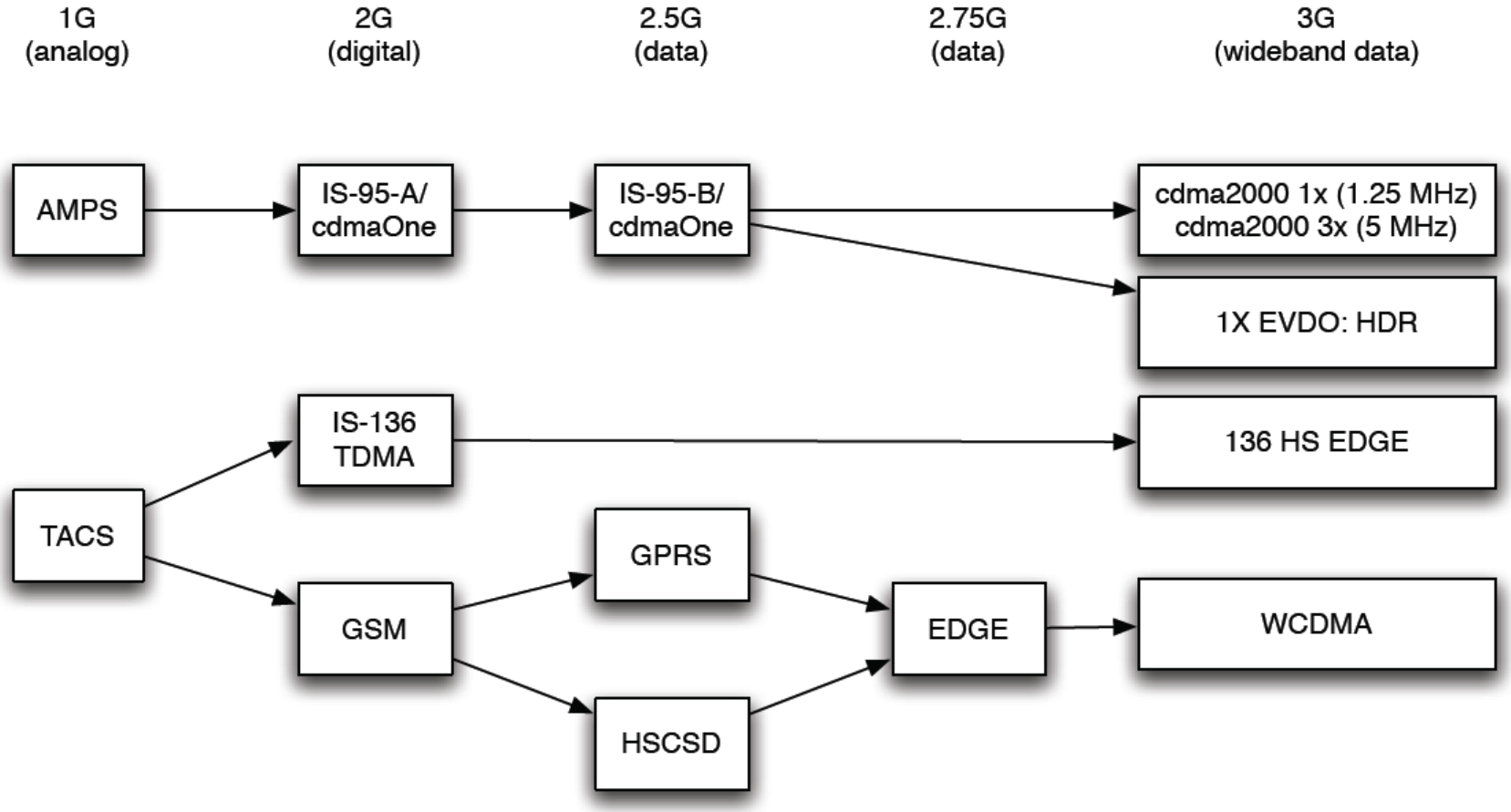
- Standards for data systems
  - High Speed Circuit Switched Data (HSCSD) – TDMA
    - Can use multiple time slots at the same time.
  - General Packet Radio Service (GPRS) – TDMA
    - More cost effective: charged by the megabyte instead of usage time.
    - Compatible with TCP/IP
  - IS-95-B/cdmaOne – CDMA

- 2.5G Data services have been met with varying success.
  - 2.75G provides significant improvements.
  - Enhanced Data rates for GSM Evolution (EDGE), aka EGPRS (still TDMA)

High Speed (3G)

- In theory, can provide rates of 10 Mbps downlink.
- Slow to roll out, 3G systems are only now becoming widespread.
  - In Pennsylvania, only a few major cities have coverage.
  - Nearly all of Central Europe
- Competing standards:
  - cdma2000/EV-DO (Evolution-Data Optimized aka Evolution-Data only)
  - W-CDMA/UMTS (Universal Mobile Telecommunications System) aka 3GSM
- High-Speed Packet Access (HSPA) sometimes referred to as HSDPA and HSUPA for downlink and uplink portions, respectively
  - AT&T uses 1900 MHz band, while T-Mobile uses 1700 MHz band
- Narrowband vs. Wideband CDMA
  - 1.25 MHz channels vs. 5 MHz channels

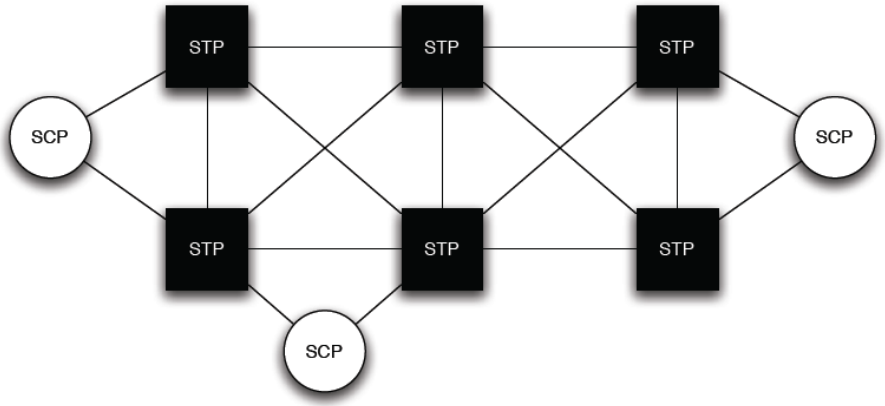
Evolution Summary



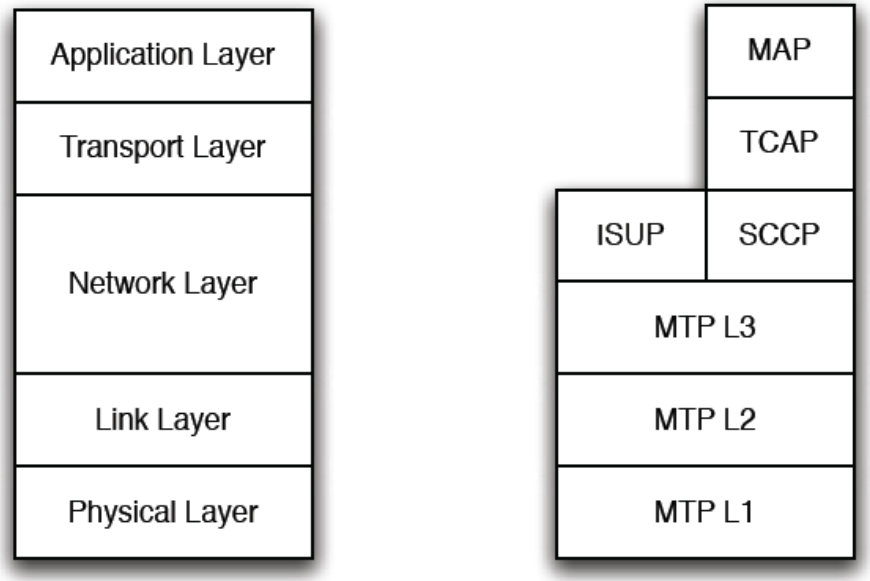
- 3rd Generation Partnership Project (3GPP) - GSM standards group
- 3rd Generation Partnership Project 2 (3GPP2) - IS-95 and CDMA standards

SS7 Network

- Powering all of these networks is the SS7 core.
  - 3G networks will eventually shift to the all-IP IMS core, but SS7 will never fully go away.
- These systems are very different from IP networks.
  - The requirements are different: real-time vs. best-effort services.
- Signaling Transfer Points (STP)
- Signaling Control Point (SCP)



Protocol Architecture



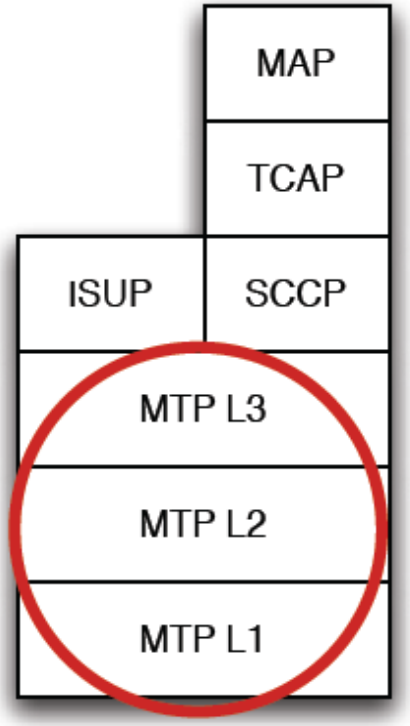
- All of the functionality one expects to find in the OSI/Internet protocol stack is available in SS7.

- Where those services are implemented may be different.

Message Transfer Part

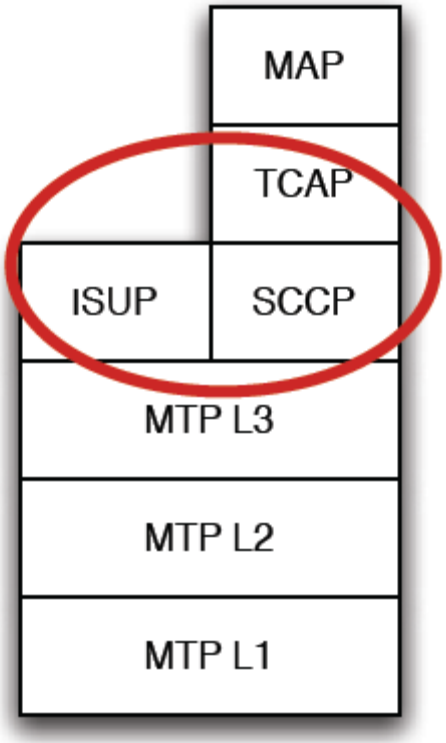
- Covers most of the functionality of the lowest three OSI/Internet protocol stack.

- Broken into three "levels".
  - MTP1: 56/64 KBps physical links. Up to four physical links can be combined between two nodes (1.544 Mbps)
  - MTP2: Link layer and reliable message delivery.
    - Go-Back-N (negative acknowledgments)
    - Alerts higher protocol layers of link failure
    - Explicit flow control mechanisms to help with congestion
  - MTP3: Network layer functionality.
    - Whenever possible, STP attempts to balance traffic sent across each link
    - Explicit flags can keep messages on the same link MTP L1



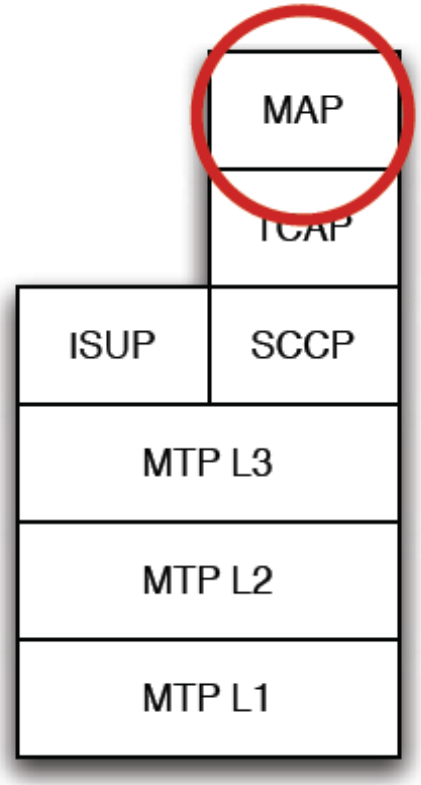
ISUP, SCCP, TCAP

- ISDN User Part (ISUP): Carries call routing information for resource reservation.
  - ISUP messages are routed hop-by-hop through the switches a call will pass
- Signaling Connection Control Part (SCCP): Carries routing information for specific functions (e.g., for 800 number processing; MTP3 can only address nodes)
  - Five "classes of service", e.g., connectionless vs. connection-oriented and flow control
  - MTP + SCCP referred to as the Network Services Part (NSP)
- Transaction Capabilities Application Part (TCAP): Interface to request the execution of remote procedures.
  - Intelligent Network (IN) functions such as toll free calling and automatic call blocking



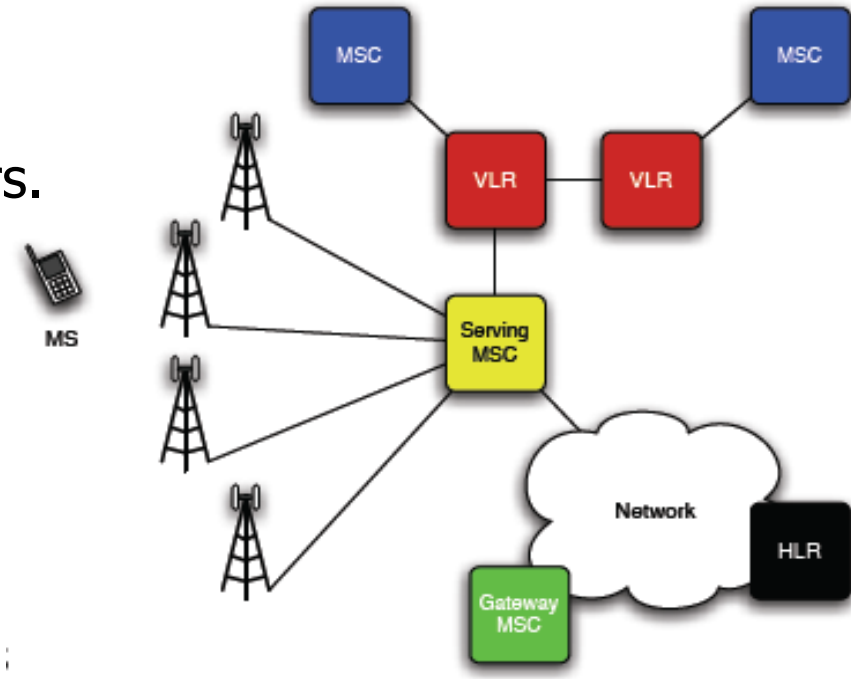
Mobile Application Part

- The application layer for SS7 networks.
- This supports services directly visible by the user:
  - Call handling
  - Text messaging
  - Location-based services
- Protected by MAPsec
  - Allows security associations between nodes as well as between networks (can use IKE to setup keys)
  - Defines different Protection Modes (PMs) defining if the association has confidentiality, integrity, or neither
  - The single deployment of MAPsec (performance issues)
  - Does not defend against propagation attacks (msg. format only)



Network Components (GSM)

- The GSM network consists of the following components
  (IS-95 networks have analogous counterparts)
- HLR stores records for all phones in the network.
- MSC/VLR connect wired and wireless components of the network and perform handoffs.
- BS communicate wirelessly with users.
- MS is a user's mobile device.



HLR

- The HLR maintains permanent copies of user profiles and is the authoritive lookup for determining where in the network a phone is (i.e., which MSC the phone is currently attached to)

- Authentication Center (AuC) - functionality subsumed in HLRs
  - International Mobile Subscriber Identity (IMSI) - identifies all users
  - Subscriber Identity Module (SIM) card - stores crypto keys (K_i) and performs operations on the phone side

- Device level authentication
  - Equipment Identity Register (EIR) - absorbed into HLR

- Includes a blacklist (e.g., for stolen phones)
  - International Mobile Equipment Identity (IMEI) - identifies a specific phone.

MSC and VLR

- The Mobile Switching Center (MSC) delivers circuit switched telephony traffic within the cellular network
  - Gateway MSC is the term given to an MSC bridging the cellular network and another network, e.g., Public Switched Telephone Network (PSTN) or another cellular network.
  - Serving MSC is the term given to an MSC currently serving an MS
  - The MSC also assists handoffs between base stations and billing

- The Visitor Location Register (VLR) caches information from the HLR for fast lookup by an MSC
  - A particular VLR may serve multiple MSC components (not always)
  - The VLR does not have K_i ; stores "triplets" from HLR (discussed shortly)

BSS

- The Base Station Subsystem (BSS) links wireless devices to the cellular network and consists of two subcomponents
  - Base Transceiver Station (BTS): the transmission radio (multiple directional antennas dividing the cell into sectors)
  - Base Station Controller (BSC): intelligence for radios (includes scheduling and encryption), controlling one or more BTSs

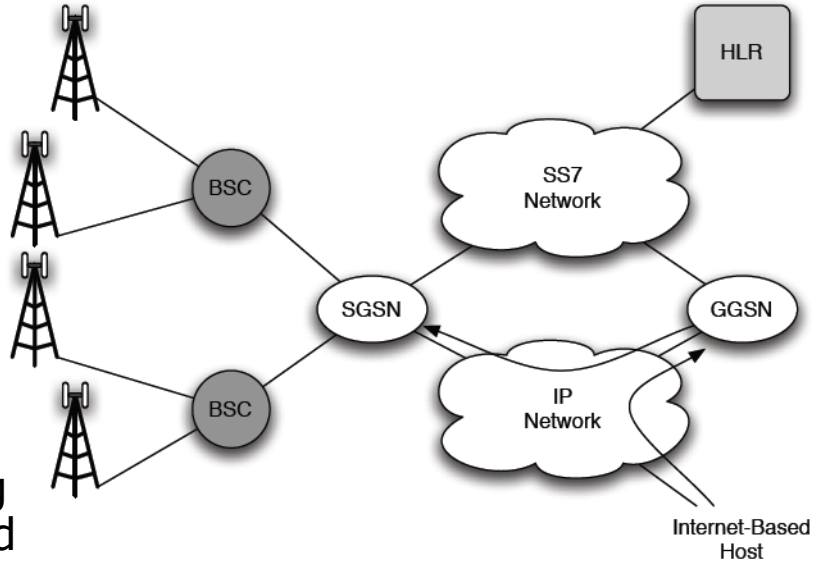
- The BSSs (commonly referred to as simply a "base stations") are often grouped into *Location Areas* (LAs) corresponding to geographic regions
  - Devices can move between BSSs in an LA without re-registering
  - Active devices must still participate in handoffs
    - Hard handoffs (current GSM) vs. Soft handoffs (two BSSs at once)

Data Network Elements

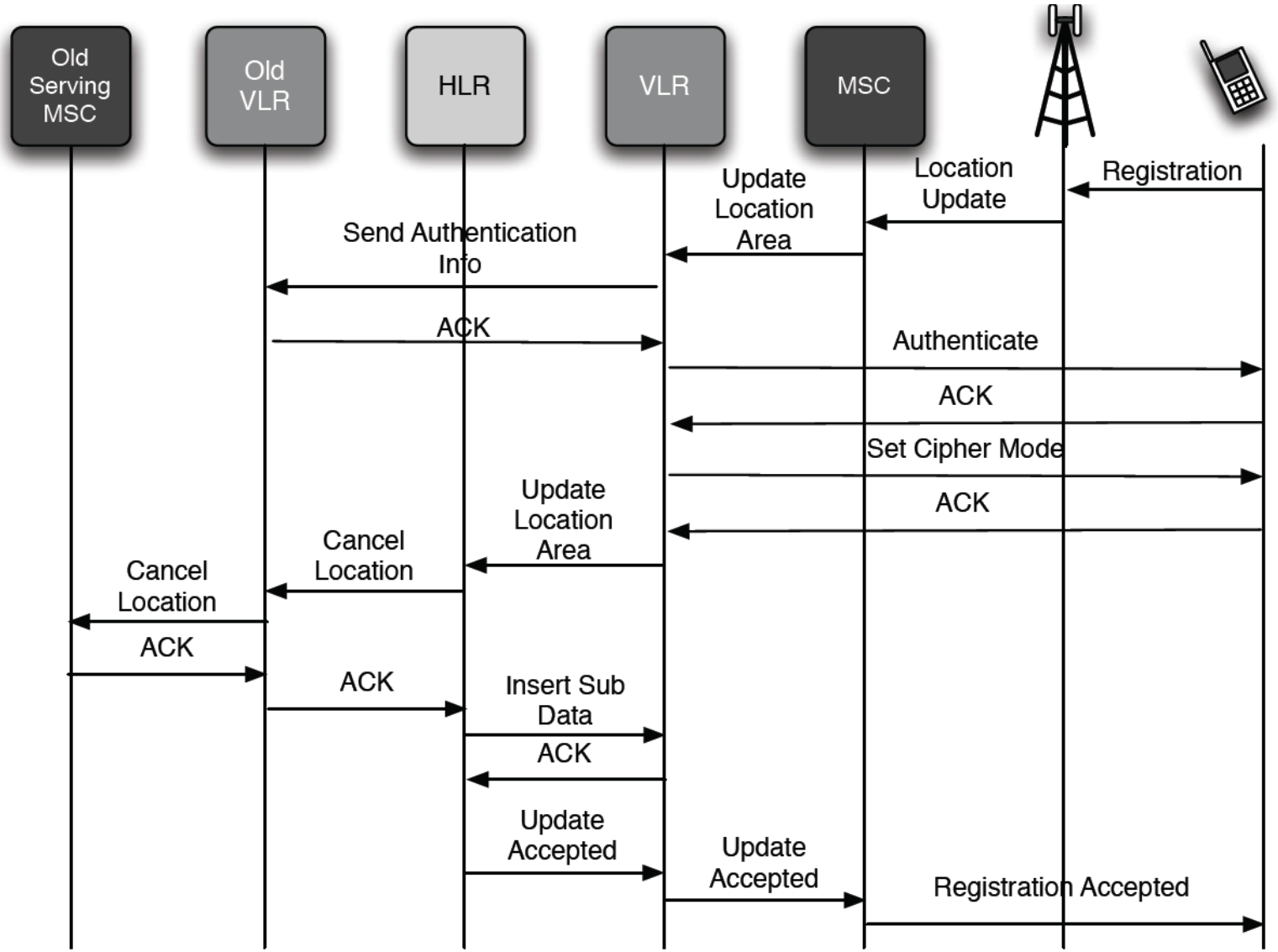
- GPRS and EDGE enabled cellular systems add additional components to provide packet-based data functionality

- GPRS Support Nodes (GSNs) are connected with higher bandwidth links (e.g. IP rather than SS7)

  - Gateway GSN (GGSN): bridges other networks such as the Internet with the cellular network.
    - Acts similar to DHCP server in assigning device addresses (knows the device and its SGSN)
    - GGSN also perform other operations, e.g., Quality of Service (QoS)
  - Serving GSN (SGSN): stores user profile information locally (to reduce signaling)

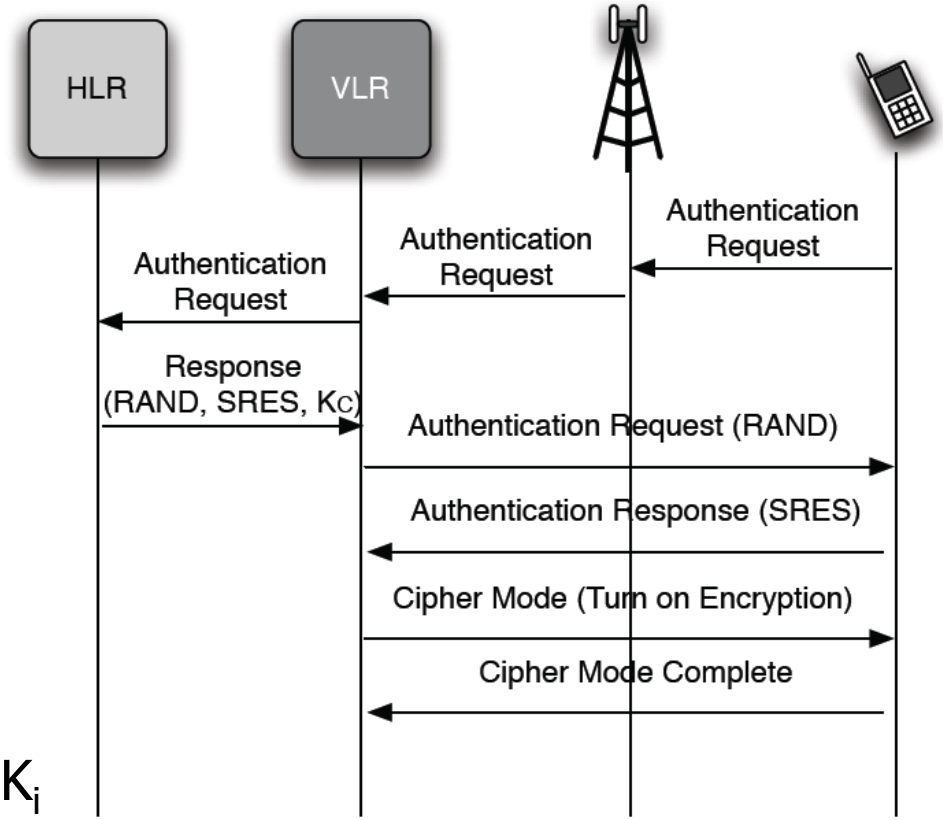


Phone Registration



Phone Authentication (GSM)

- GSM defines three algorithms (based on 128-bit key, K_i)
  - A3 - Authentication
  - A8 - Generates cipher key
  - A5 - Ciphering data
- VLR retrieves 5 triplets from HLR
  - RAND - random challenge
  - SRES - expected response
  - [SRES = A3(K_i, RAND), 32 bits]
  - K_c - corresponding cipher key
  - [K_c = A8(K_i, RAND), 64 bits]
- Only the HLR and SIM card know K_i

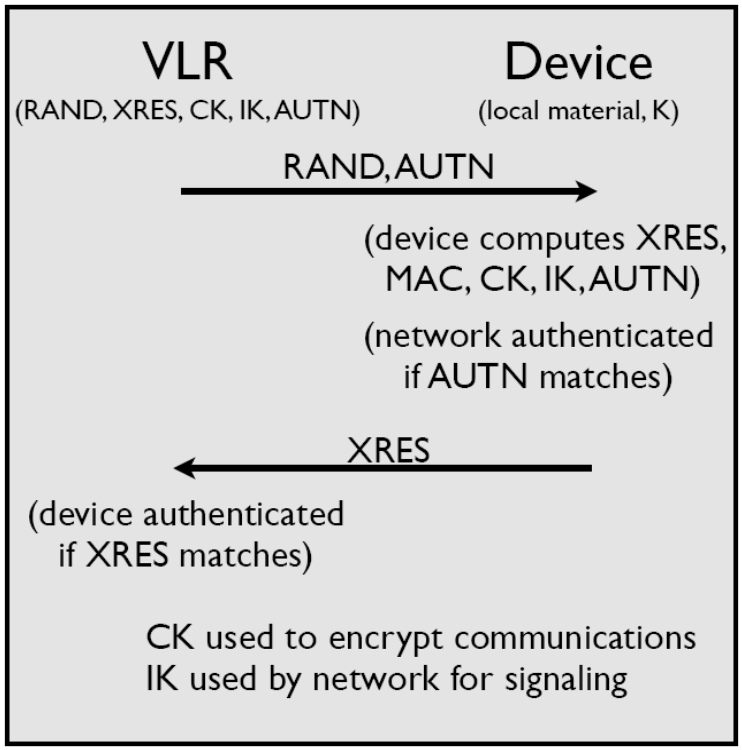


Phone Authentication (UMTS)

- GSM authentication has a number of weaknesses, including vulnerabilities in algorithms, one-way authentication, and plaintext backhaul (discussed later)

- UMTS addresses these issues
- 5 algorithms (F1-F5): use RAND, sequence #, shared key K
  - F1 - outputs a MAC
  - F2 - outputs signed response XRES
  - F3 - outputs a cipher key (CK)
  - F4 - outputs an integrity key (IK)
  - F5 - outputs an authentication key (AK)

- HLR sends VLR set of 5-tuples:RAND, XRES, CK, IK, AUTN (AUTN = authentication token from local material, AK, and MAC)

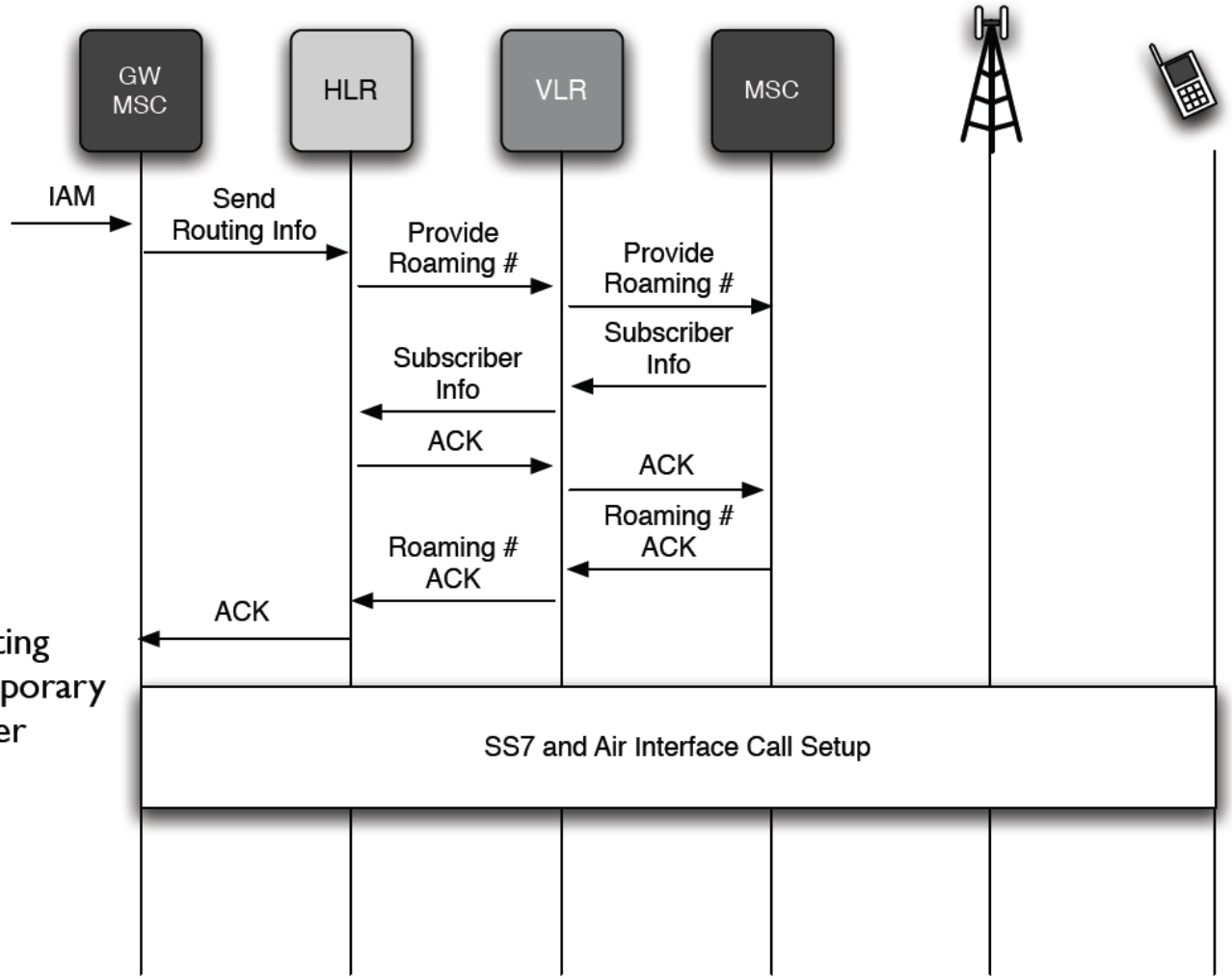


New Call Setup

From within or outside provider network, or PSTN

Initial Address Message (IAM)

Mobile Station Routing Number (MSRN) - temporary local phone number



GSM Feature Codes

- Dialpad can be used to send commands to the network (e.g., call forwarding). Support for codes is provider dependent.
- GSM Code Scheme:
  <type><code>#
  Types:
  - * - activate (*<code>*[dest]#)
  - ** - register and activate
  - *# - check status
  - # - unregister
  - ## - unregister and deactivate
- See http://www.geckobeach.com/cellular/secrets/gsmcodes.php for notes
- Forward Codes: (try *#21#) (be careful changing things)
  - 21 - all
  - 67 - if busy
  - 61 - if no answer
  - 62 - if unreachable
  - 002 - all 4
- Call Waiting: 43
  - Try disabling and enabling
- Masking caller ID: 31
  - #31#[phone number]
  - *#31# status (AT&T and TMobile won't set default)
  - *67[phone number] - landline

Other Fun Codes

- Minutes Used/Remaining
  - *646# (AT&T), #646# (T-Mobile)
  - Prepaid: *777# (AT&T), #999# (T-Mobile)
- Text Messages remaining
  - #674# (T-Mobile)
- Check your balance:
  - *225# (AT&T)
- Phone number of the phone:
  - #686# (T-Mobile)
- *#06# : shows your IMEI
- SMS notification: prefix with either 111 or *noti# depending on your carrier.
  - *noti# works from T-Mobile G1
- More listed online:
  - http://wiki.howardforums.com/index.php/AT%26T
  - http://wiki.howardforums.com/index.php/T-Mobile

Security Issues

- Such networks have long been viewed as secure because few had access to them or the necessary knowledge.
- However, attacks are not a new phenomenon.
  - Many different classes of attacks are well documented.
- We investigate a number of such attacks throughout the remainder of this lecture.

Caller-ID Spoofing

- Caller-ID spoofing has existed as long as Caller-ID (not specific to cellular networks) -- "Orange boxing"

- Caller ID can be easily spoofed (if you are willing to pay for it)
  - Star38.com (launched September 2004, stopped offering in 2005)
  - Others quickly joined: See http://www.calleridspoofing.info/ for a history
  - Commonly used for prank calls and telemarketers

- Legitimate uses include displaying a business number when calling from mobile phone

- Pending legislation in US congress to make Caller-ID spoofing illegal (separate bills passed in House and Senate, reintroduced Jan 2009)

Weak Crypto

- GSM networks use COMP128 for all operations.
  - Authentication (A3), session key gen (A8) and encryption (A5).

- COMP128 was a proprietary algorithm...
  - First break: Recover K_i by querying SIM 2^{19} times (6-8 hours)
    Solution: SIM manufacturers limit cards to 216 operations
  - The next break determined K_i in under a minute
  - A5/1 and A5/2 (weaker) similarly broken to retrieve K_c

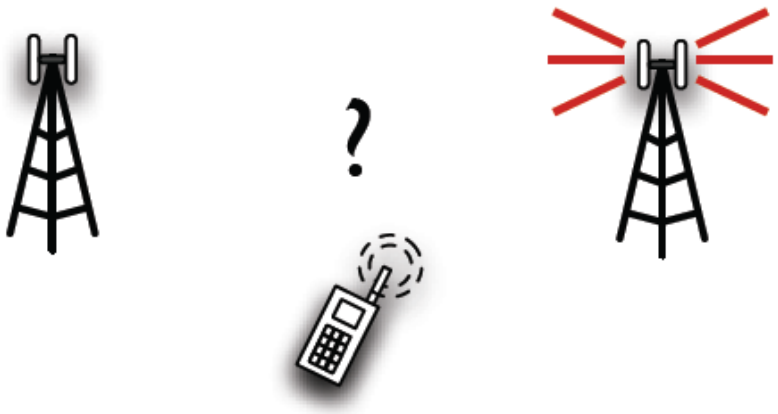
    - A5/2 within milliseconds

    - A5/1 passively in approximately 30 seconds (rainbow tables)

- Replaced by COMP128-2 and COMP128-3 (maybe)
  - Also proprietary.

One-Way Authentication

- In GSM systems, the network cryptographically authenticates the client.
- The client assumes that any device speaking to it is the network.
- Accordingly, it is relatively easy to perform a "Man in the Middle" attack against all GSM networks.



Core Vulnerabilities

- Messages sent within the network core are not authenticated.
  - MAPsec attempts to address this problem by providing integrity and/or confidentiality.
  - The only known deployment of MAPsec was online for two days before being shut off.
    - Serious performance degradation prevent its use.

- Telecommunications Act of 1996 allows an individual or group to connect to the SS7 infrastructure by paying a relatively small fee ($10,000 in 1999).
  - All providers are reliant on the weakest security link
  - ASN.1 vulnerability
  - Failure modes in AT&T network (1990)
  - Physical protection of deployed infrastructure

Eavesdropping

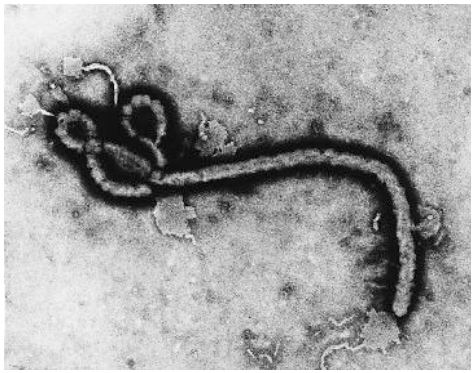
- Early analog systems were easy to eavesdrop upon.
  - Processing power, export rules and bandwidth worked against cryptography.
- GSM systems use weak crypto, so eavesdropping is still possible over the air.
- Nothing is encrypted through the network itself, so anyone with access can listen to any call.

Jamming

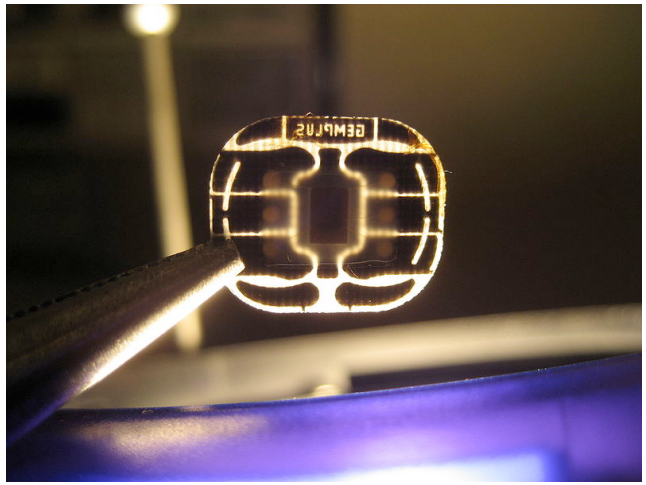
- Targeting the control channel is effective for even CDMA based networks
- The legality of cell phone jamming varies by country
  - USA: Illegal
  - France: Legal in certain circumstances
- Just because it is illegal in some countries does not mean it is not a threat.
  - You can buy hand-held jammers on the street in most major cities.
  - Do It Yourself instructions online (e.g., WaveBubble open source jammer)

Malware

- Known malware does not target the cellular infrastructure...
  - ...yet.
- The proliferation of laptop cellular cards is wreaking havoc on these networks.
  - Spyware "phoning home" is already taxing the network.
- Differences between the Internet and cellular networks make malware MORE dangerous in this setting.



SIM Cards

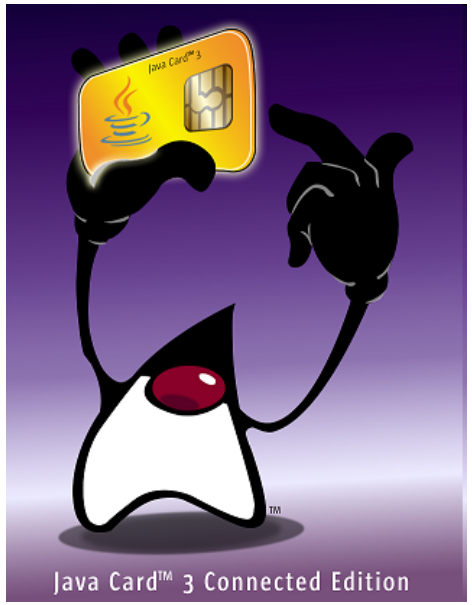


Disambiguation

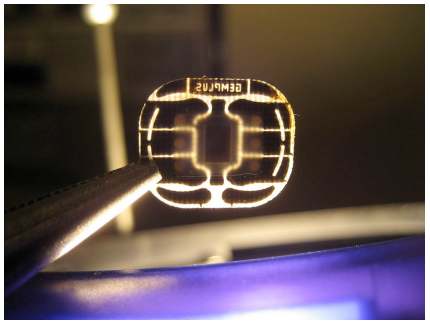
- What is a "SIM card"?
  - "Subscriber Identity Module"
  - In general terms, a SIM card is a smart card like device that identifies a user (account) in a *GSM* system and may be transferred between devices.
  - "SIM card" often refers to both hardware and software.
- Universal Integrated Circuit Card (UICC)
  - In UMTS system, runs USIM software (entire card is not the USIM)
  - Supports different software modules: ISIM (IMS), CSIM (CDMA)
  - R-UIM (Removable User Identity Module) - CDMA system
    - Sometimes used to refer to card containing CSIM, USIM, and SIM apps

Hardware/OS

- Hardware is typically a smartcard punchout (25x15 mm)
  - UICC contains CPU, ROM, RAM, EEPROM, and I/O circuits
  - W-SIM (Willcom) variation includes radio receiver/transmitter
- SIM operating systems are either proprietary or Java Card
- Java Card is commonly found on both SIMs and ATM cards
  - Uses a subset of the Java language
  - Optimized byte-code format
  - Applets are "firewalled" from one another



SIM Data (1)



- Integrated Circuit Card ID (ICC-ID) (aka SIM Serial Number - SSN)
  - Uniquely identifies a SIM card (hardware)
  - Conforms to ISO/IEC 7812 (19-20 digits)
- International Mobile Subscriber Identity Module (IMSI)
  - Uniquely identifies the mobile subscriber (15 digits, ITU E.212 standard)
  - MCC (3 digits), MNC (2 or 3 digits), MSIN (9 or 10 digits)
- Authentication Key (K_i)
  - Key shared with provider.
  - Never leaves the smartcard.
- GSM authentication algorithm performed on-chip.

SIM Data (2)

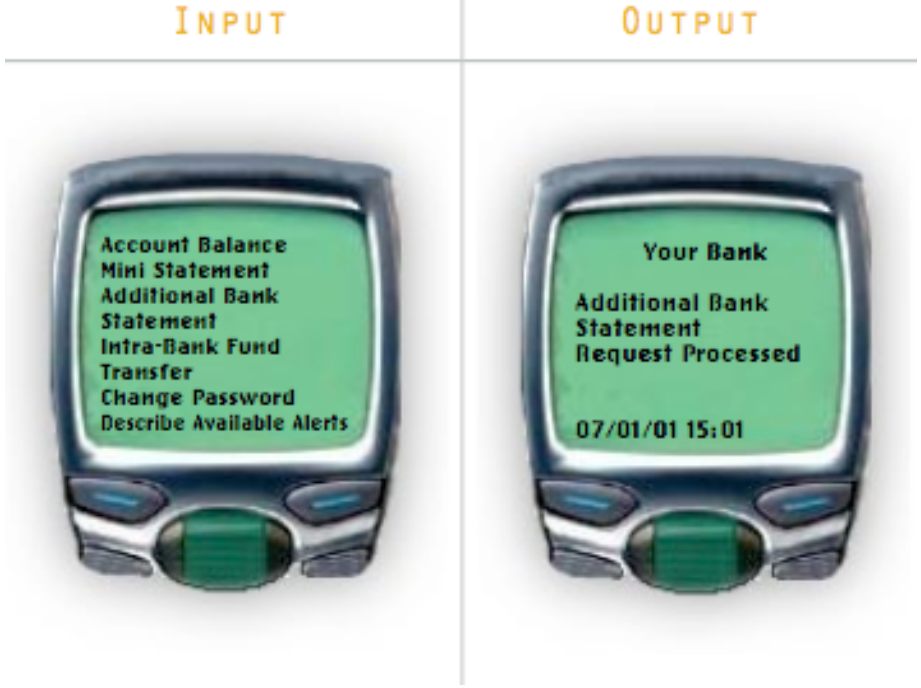
- Location Area Identity (LAI)
  - Stores the last known location area (saves time on power cycle)
- Address book and SMS messages
  - Higher capacity in more advanced cards
- And more ...
  - SMSC number
  - Service Provider Name (SPN)
  - Service Dialing Numbers (SDN)
  - value-added-services
  - See GSM/3GPP TS 11.11 for more details

SIM Application Toolkit

- Before smart phones became popular, the SIM Application Toolkit (STK) was a popular method of deploying applications on mobile phones. - Defined in GSM 11.14; GSM 03.48 is STK security
  - Allowed for mobile banking applications (and other value added services) to run off the SIM (no handset hardware/OS dependence)
  - Commonly written in Java (for JavaCard) using predefined commands (applications are menu driven)
  - Send data to remote application using SMS
  - OTA update method were eventually incorporated
- STK in UMTS defined as the USIM Application Toolkit (USAT) - 3GPP TS 31.111, security is 3GPP TS 23.048
  - Will new mobile phone OSes make STK and USAT obsolete?

STK Interface Commands

- Applications define menus, which are basically lists of questions for the user to answer. Depending on the provided answers, the application takes different actions.
- Example SIM Commands available in STK
  - SET UP MENU
  - GET INPUT
  - SELECT ITEM
  - PLAY TONE
  - SEND SHORT MESSAGE
  - SEND DTMF
  - TIMER MANAGEMENT



SIM Card Readers

- SIM cards can be connected to a PC for various purposes
- SIM card readers are cheap (~$10-20) or build yourself
  - Provide a serial (TTY) interface (DB9 or USB)
- Allows you to: backup contacts and SMS, see list of previously called numbers, probe keying data to extract K_i ...
- Frequently used for Forensics
  - See NIST "Guidelines on Cell Phone Forensics", Special Pub 800-101
  - Includes list of SIM tools

Restricting Access

- The SIM card restricts access using two PINs (4-8 digits)
  - PIN 1: If set, the PIN is required to make calls
  - PIN 2: Protects certain network settings
- What happens if you forget your PIN?
  - Commonly, three failed attempts locks the SIM
- Unlocking a locked SIM card
  - Personal Unblocking Code (PUC) or Personal Unblocking Key (PUK)
  - Commonly acquired from the network provider
  - Ten failed attempts often permanently locks the SIM

SIM Cloning

- SIM Cloning is the process of extracting Ki from one SIM card and writing it onto another.
  - It less frequently than before due to updates in crypto algorithms and authentication protocols, but is still possible in some cases.
  - Extracting K_i can take 4-8 hours and may damage the card
  - Many software and hardware cloners exist
- Why clone? - steal service, forensics, SIM/ network lock circumvention, *not* eavesdropping (but knowing K_i helps)
- Network can detect cloned SIMs; protections vary
  - Simultaneous calls cannot occur

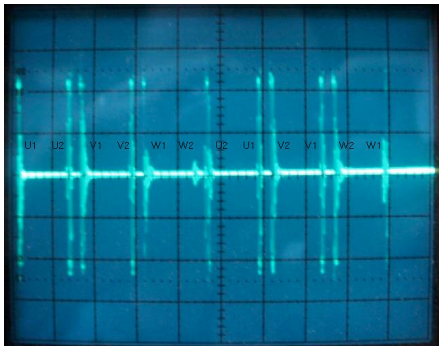
Power Analysis

- SIM cards are smart cards, therefore, they are also vulnerable to power analysis attacks (requires special equipment).
  - Hardware implementations cause power consumption of the chip to become a side-channel to determine the key used to perform some cryptographic algorithms.
  - See work by Kocher et al. (Differential Power Analysis)

- Simple Power Analysis (SPA) - visual examination of current (can be performed with standard digital oscilloscopes)

- Differential Power Analysis (DPA) - statistical analysis of power consumption (multiple cryptographic operations)

- Resulted in tamper resistant techniques to defend against power analysis



SIM/Network Locking

- Network providers often subsidize the handset cost. The phone can be "locked" to that provider, only allowing SIM cards from that provider.
  - "Unlocked" phones sell for significantly more (e.g., eBay)
- Network providers usually provide an unlock code after some time (often request a reason, e.g., traveling abroad).
- Third party unlocking has become a profitable business
  - "Box breaking" in the UK
  - Selling unlock codes
- Locking techniques:
  - Algorithm based on IMEI (early Nokia phones)
  - Random number embedded in device firmware

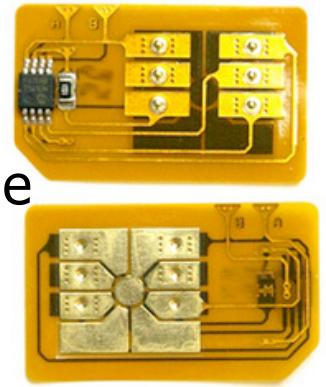
SIM Locking Laws

- Countries have different laws determining if a network provider is allowed to SIM/network lock a phone
  - Often no restrictions (e.g., US and UK)
  - Some countries prohibit it outright (Singapore, Finland GSM with 3G exception)
  - Others yet put time frame restrictions with requirements of providing systematic unlocking procedures (e.g., France)
- Originally, in US, DMCA restricted customers unlocking phones without provider consent
  - Exception in Nov 2006, expires after three years

> *"Computer programs in the form of firmware that enable wireless telephone handsets to connect to a wireless telephone communication network, when circumvention is accomplished for the sole purpose of lawfully connecting to a wireless telephone communication network."*

SIM Unlocking

- There is a great demand for unlocked phones (e.g., travel abroad, phone exclusively sold with another provider, etc)
- Most common technique is to purchase an unlock code online
  - Submit an IMEI, receive unlock code via email
  - Entering the wrong code more than 3-4 times causes hard lock. After which, special equipment is needed to unlock
- High profile phones (e.g., iPhone) have firmware hacks
- Mail-in services also exist
- Shim cards can "piggyback" and fake provider name
- SIM cloning (new card fools the phone)



References

- GSM Association, http://www.gsmworld.com
- M. Rahnema, "Overview of the GSM System and Protocol Architecture", IEEE Communication Magazine, April 1993
- L. Pesonen, "GSM Interception", November 1999
- J.Rao, P. Rohatgi, H. Scherzer, S. Tinguely, "Partitioning Attack: Or How to Rapidly Clone Some GSM Cards", IEEE Symposium on Security and Privacy, May 2002.
- P.Kocher, J. Jaffe, "Introduction to Differential Power Analysis and Related Attacks", Cryptography Research, 1998
- S. Babbage, "A Space/Time Trade-off in Exhaustive Search Attacks on Stream Ciphers", Europian Convention on Security and Detection, IEE Conference publication, No. 408, May 1999.
- A. Biryukov, A. Shamir, D. Wagner, "Real Time Cryptanalysis of A5/1 on a PC", Preproceedings of FSE '7, pp. 1-18, 2000
- ISAAC, University of California, Berkeley, "GSM Cloning", http://www.isaac.cs.berkeley.edu/iChansaac/gsm-faq.html
- S. Chan, "An Overview of Smart Card Security", http://home.hkstar.com/~alanchan/papers/smartCardSecurity/
- R. Anderson, M. Roe, A5, http://jya.com/crack-a5.htm, 1994.
- M. Briceno, I. Goldberg, D. Wagner, A pedagogical implementation of A5/1, http://www.scard.org, May 1999.
- Golic, Cryptanalysis of Alleged A5 Stream Cipher, proceedings of EUROCRYPT'97, LNCS 1233,pp.239{255, Springer-Verlag 1997.
- M. E. Hellman, A Cryptanalytic Time-Memory Trade-Off, IEEE Transactions on Information Theory, Vol. IT-26, N 4, pp. 401{406, July 1980.