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

General information

- Exam
  - For those who want one???

- Prerequisite: some knowledge of
  - Cellular Phones itself
  - How cellular networks work
  - How operating systems work
  - Little bit of undergraduate math for cryptography

- Additional contact persons:
  - Collin Mulliner (SECT)

Collin Mulliner gets interviewed at Black Hat USA 2009

What is this course about?

- Wireless Security?
  - Not at all!
- Focus here:
  - Telecommunication Security:
    - Security of Cell phones
    - Security of Cellular network architectures
- Protection and defense mechanisms for securing critical **infrastructure**

Topics

- Basics of cellular network architecture
- Cryptographic pitfalls (but not a cryptography class!)
- The role of correct software
- The role of DOS
- The role of SMS, MMS, …
- Bluetooth, etc.

- Practical focus
  - This is not a pure academic-style course
  - You'll see real security holes
  - A lot of (in)security is about doing the unexpected
  - „Think sideways"

How to think about *IN*security

- Bad guys don't follow rules
- Need to understand what sort of attacks are possible to compromise a system
  - Prerequisite to understand what to protect in a system!
- This is not the same as actually launching them!
  - Taking a security class is not an excuse for hacking
  - Hacking is any form of unauthorized access, including exceeding authorized permissions
  - The fact that a file or computer is not properly protected is no excuse for unauthorized access
  - There is a new law in Germany for Hackers! Italy?

Reading

- Computer Security: Art and Science
  Matt Bishop
  Addison-Wesley Professional 2002

- GSM - Architecture, Protocols and Services
  Jorg Eberspacher, Christian Bettstetter, and Christian Hartmann
  Wiley & Sons 2009

- Security and Telecommunications Networks
  Patrick Traynor, Patrick McDaniel, and Thomas F. La Porta
  Springer, Berlin 2007

- Mobile Communications
  Jochen Schiller
  Addison Wesley 2003

Reading

- Security and Cooperation in Wireless Networks
  Levente Buttyan and Jean-Pierre Hubaux
  Cambridge University Press 2007

- Wireless Communications And Networks
  STALLINGS WILLIAM
  Prentice Hall India 2004

- Wireless Communications: Principles and Practice
  Theodore S. Rappaport
  Prentice Hall India 2002

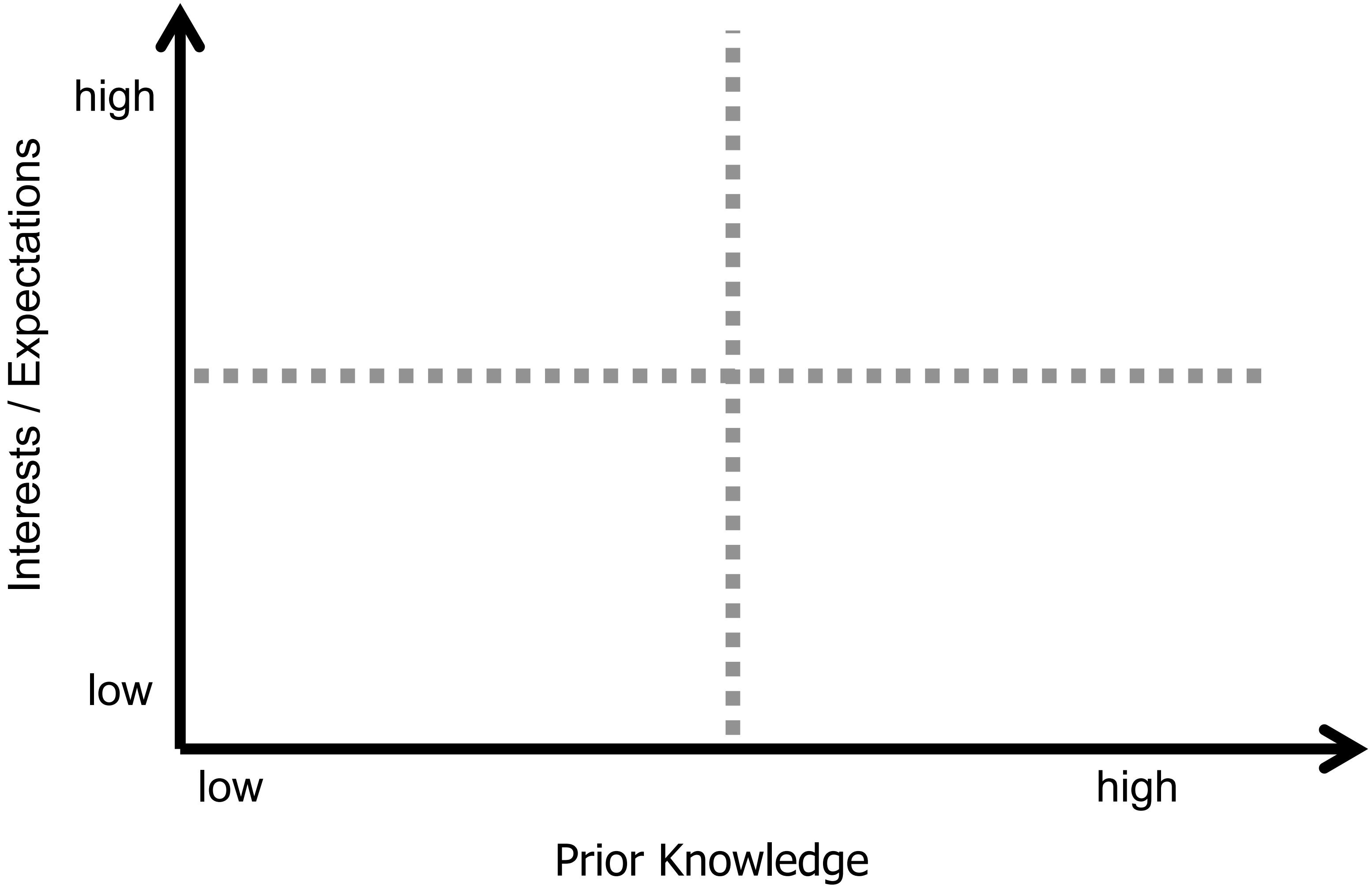
- Computer Security: Principles and Practice
  William Stallings and Lawrence Brown
  Pearson Education 2008

- BUILDING A SECURE COMPUTER *SYSTEM*
  Morrie Gasser
  Van Nostrand Reinhold 1988
  http://nucia.unomaha.edu/dspace/documents/gasserbook.pdf

Reading online

- Universal Software Radio Peripheral
  http://en.wikipedia.org/wiki/Universal_Software_Radio_Peripheral#References
- OpenBSC
  http://bs11-abis.gnumonks.org/trac/wiki/OpenBSC
- OpenBTS (GNU Radio)
  http://gnuradio.org/trac/wiki/OpenBTS
- ... (see Web)
- **Research papers** (see course slides)

Self-Assesment



Ethics Statement

- This course considers topics involving personal and public privacy and security. As part of this investigation we will cover technologies whose abuse may infringe on the rights of others. As an instructor, I rely on the ethical use of these technologies. Unethical use may include circumvention of existing security or privacy measurements for any purpose, or the dissemination, promotion, or exploitation of vulnerabilities of these services. Exceptions to these guidelines may occur in the process of reporting vulnerabilities through public and authoritative channels. Any activity outside the letter or spirit of these guidelines will be reported to the proper authorities and may result in dismissal from the class.
- When in doubt, please contact the instructor for advice. Do not undertake any action which could be perceived as technology misuse anywhere and/or under any circumstances unless you have received explicit permission from Professor Jean-Pierre Seifert.

Cell Phone Security

Cell Phone Security

- A cellular phone is only one part of a much larger system
  - Other parts of the system at next lecture
  - Historically, both network and devices were closed (starting to open)
  - Provided some level of protection
- 17.5% of American homes have only wireless telephones in year 2008.
  - What about Europe?
  - Myself I only have one single phone – a cell phone
- What happens to the network and devices when interfaces open?
- What happens when we start relying on cell phones for general computing needs?

Cellphone OS Security vs. OS Security

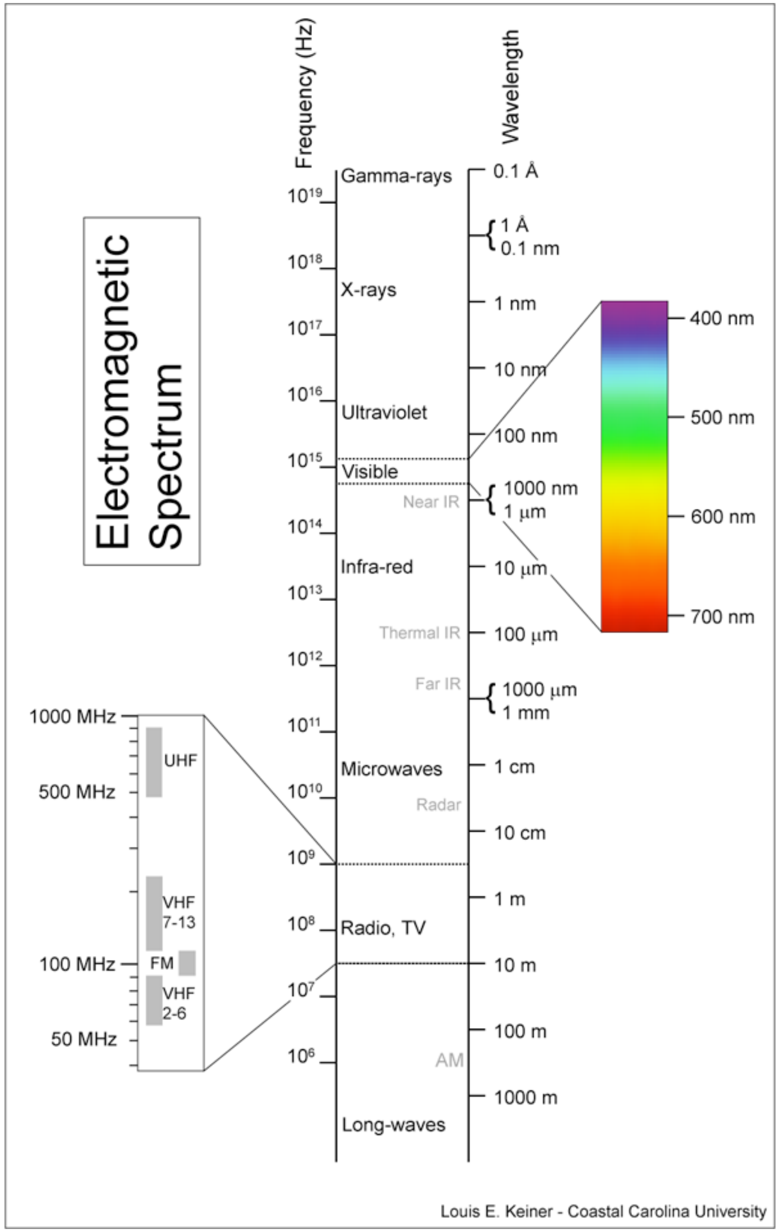
- *Why is cellphone OS security different than ordinary OS security?*
- Connected to critical infrastructure - warnings of phone botnets
- Connected to people - attacks can cross into the physical world
- Multiple Stakeholders - there is a lot of money at risk
  - provider, mfg, enterprise, 3rd-party app developer, end user, etc.
  - Who has control?
  - Who is the adversary?
- Specific usage scenarios
  - Always with you
  - Only want to carry *one*
    (for business *and* personal)

Radio Spectrum

- Electromagnetic Radiation: energy waves that travel through a vacuum
  - all forms of light (visible and not), radio waves, X-Rays, etc
  - Higher frequency = more energy

- Cellular phones share the Ultra High Frequency (UHF) band (300-3000 MHz) along with TV, microwave ovens, WiFi, Bluetooth, etc.
  - Typically at 800-900 MHz or 1700-2100 MHz

- ... a scarce resource



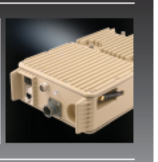
Louis E. Keiner - Coastal Carolina University

Spectrum Frequency Chart

QRC Specializes in Active & Passive Survey Tools for Cellular Systems.

QRC has Products for Phone Forensics, Base Station Location, Mobile Location (DF), & Cellular Surveys.

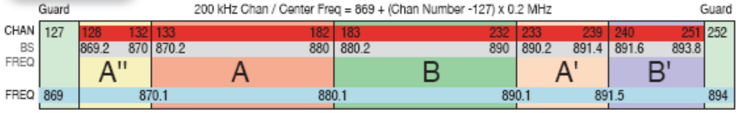
Our Tools Cover CDMA, WCDMA, GSM, & iDEN Protocols.



Specializing in Mobile Communication Information

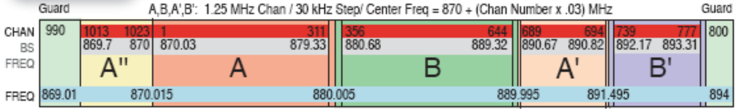
GSM 850

200 kHz Chan / Center Freq = 869 + (Chan Number -127) x 0.2 MHz



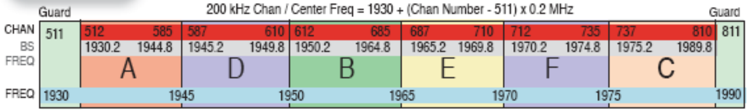
CDMA 850

A'': 1.25 MHz Chan / 30 kHz Step/ Center Freq = 870 + (Chan Number -1023) x .03 MHz
A,B,A',B': 1.25 MHz Chan / 30 kHz Step/ Center Freq = 870 + (Chan Number x .03) MHz



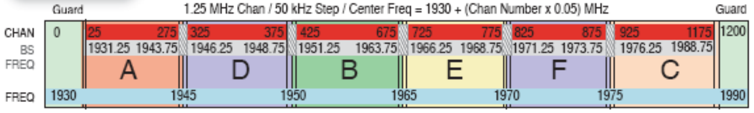
GSM 1900

200 kHz Chan / Center Freq = 1930 + (Chan Number - 511) x 0.2 MHz



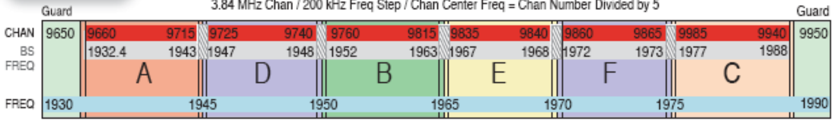
CDMA 1900

1.25 MHz Chan / 50 kHz Step / Center Freq = 1930 + (Chan Number x 0.05) MHz



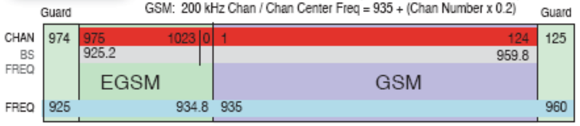
WCDMA 1900

3.84 MHz Chan / 200 kHz Freq Step / Chan Center Freq = Chan Number Divided by 5



GSM 900

EGSM: 200 kHz Chan / Chan Center Freq = 925 + (Chan Number - 974) x 0.2 MHz
GSM: 200 kHz Chan / Chan Center Freq = 935 + (Chan Number x 0.2)

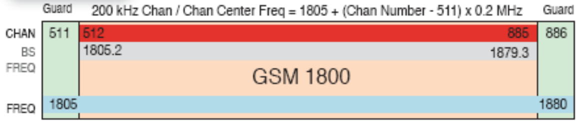


LEGEND:

- 🟥 Valid Center Channels
- ⬜ Valid Center Frequencies
- 🟦 Full Spectrum Block
- ▨ Conditionally Valid

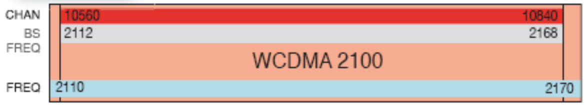
GSM 1800

200 kHz Chan / Chan Center Freq = 1805 + (Chan Number - 511) x 0.2 MHz

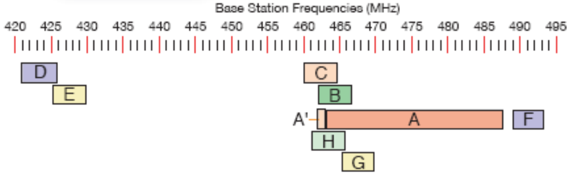


WCDMA 2100

3.84 MHz Chan / 200 kHz Freq Step / Chan Number = Center Freq Divided by 5



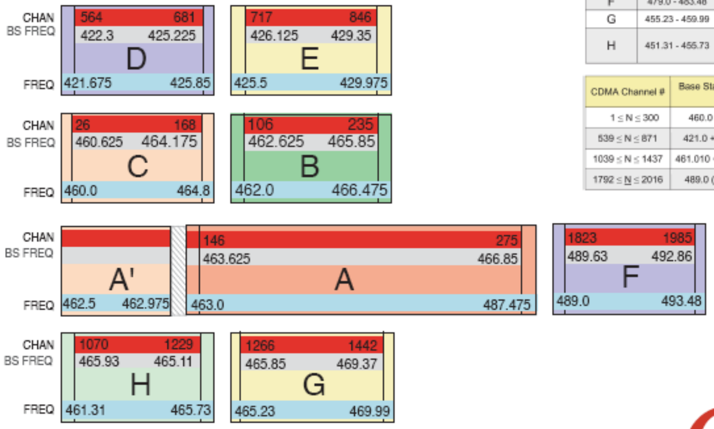
CDMA 450



Band Subclass	Mobile Station (MHz)	Base Station Frequencies (MHz)	Countries
A (Preferred Band Subclass)	452.5 - 457.475	462.5 - 467.475	Argentina, Bulgaria, China (Daging), Denmark, Estonia, Finland, Iceland, Indonesia, Latvia, Lithuania, Moldova, Norway, Poland, Portugal, Peru, Romania, Russia, Spain, Sweden, Tunisia, Ukraine
B	452.0 - 456.475	462.0 - 466.475	Malaysia
C	450.0 - 454.8	460.0 - 464.8	France
D	411.675 - 415.85	421.675 - 425.85	Croatia, Slovenia
E	415.5 - 419.975	425.5 - 429.975	Turkey
F	479.0 - 483.48	489.0 - 493.48	Thailand
G	455.23 - 459.99	465.23 - 469.99	Hungary
H	451.31 - 455.73	461.31 - 465.73	Austria, Belgium, Czech Republic, Netherlands, Slovakia,

CDMA Channel #	Base Station Center Frequency (MHz)	Mobile Center Frequency (MHz)
1 ≤ N ≤ 300	460.0 + (Chan # - 1) * .025	Base Freq – 10 MHz
539 ≤ N ≤ 871	421.0 + (Chan # - 512) * .025	Base Freq – 10 MHz
1039 ≤ N ≤ 1437	461.010 + (Chan # - 1024) * .020	Base Freq – 10 MHz
1792 ≤ N ≤ 2016	489.0 (Chan # - 1792) * .020	Base Freq – 10 MHz

Note: Not to Scale



LEGEND for CDMA 450:

- 🟥 Valid CDMA Channels
- ⬜ CDMA Center Frequencies
- 🟦 Full Spectrum Block
- ▨ Conditionally Valid

QRC TECHNOLOGIES

2680 Jefferson Davis Highway
Stafford, VA 22554
Voice: 540.446.2270

www.qrctech.com

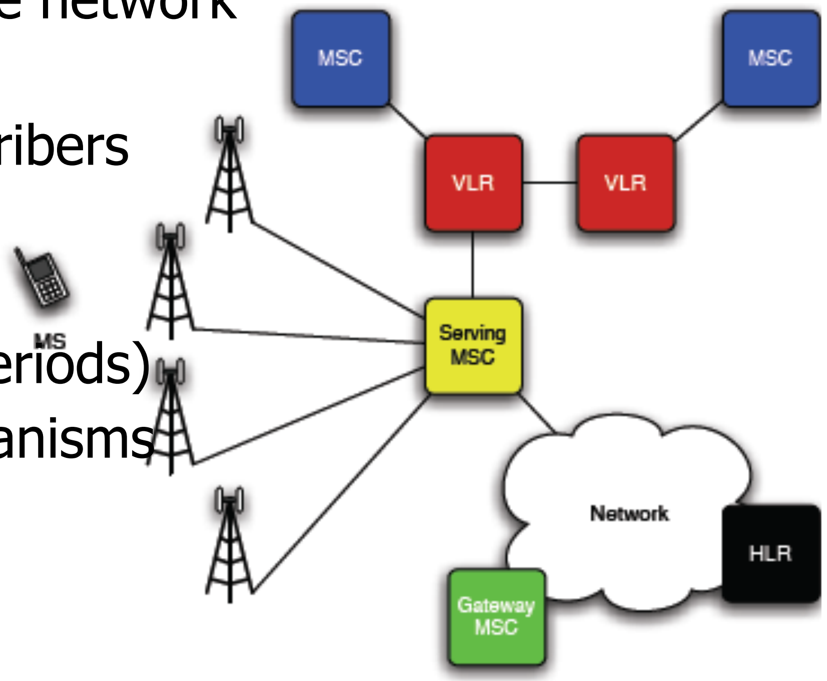
Spectrum Auctions

- Before the auctions licenses determined by hearings and lotteries
- Congress passed the Omnibus Budget Reconciliation Act of 1993
- In 1994, the Federal Communications Commission (FCC) conducted its first auctions for spectrum
  - Simultaneous Multiple-Round (SMR) auction - no preset number of rounds
  - Package Bidding: SMR, but bids can be on groups of licenses
  - Application process itself is multistage including various public notices
  - Current auctions are web browser based (all electronic)
- Spectrum auctions raised significant revenue during the tech bubble
- US 2008: 700 MHz spectrum - UHF channels 52 through 69
  - Google requested wholesale lease and open devices, guaranteed $4.6 billion
  - Split into five blocks (A-E): total $19.592 billion

Cellular Networks

- Cellular networks are complex systems made up of many components and defined by thousands of pages of standards documents
  - 3GPP aka GSM, and 3GPP2 aka CDMA ... leads to alphabet soup

- There are many concerns (most of them are non-security)
  - Interconnectivity with “landline” phone network
  - Efficient radio spectrum deployment
  - Maximizing number of active of subscribers
  - Low latency call-setup and in-call
  - Mobility and roaming (which tower?)
  - Handset power consumption (sleep periods)
  - Customer databases and billing mechanisms
  - and many more ...



Cellular Network *In*security

- Classical cellular network vulnerabilities
  - Weak crypto in GSM, eavesdropping, jamming, …
- Transition from "voice-only" opened interfaces resulted in:
  - Vulnerabilities with SMS [Enck, Mulliner, et.]
  - Exploiting teardown mechanisms [Traynor, et al., 2007]
  - Exploiting setup mechanisms [Traynor, et al., 2007]
  - …
- These attacks result from details in the network design
  - We will spend some time during the class looking at the design
- Conflicting system design philosophies ...

Stakeholders

- A cellphone stakeholder is an entity with valued interests in proper phone functioning and something to loose from malfeasance.
  - Variety of stakeholders, and each has its own goals and concerns

- A stakeholder can be identified by its presence on a phone
  1. Provides a means of communication with the outside world
  2 .Uses the handset to deliver information
     (e.g., news, music, etc)
  3. Provides software or hardware to facilitate 1 and 2
  4. An end user of the phone

- *What are examples of things that could go wrong?*

Cellular Network Providers

- Cell network providers are called Mobile Network Operators (MNO)
  - Licenses radio spectrum from the government (acquired through auctions)
  - Deploys base stations, chooses which technology (GSM, UMTS vs. CDMA)

- Some providers are really Mobile Virtual Network Operators (MVNO)
  - MVNO’s lease access from an MNO in that area (Example: Virgin Mobile)

- An MNO can act as a MVNO in regions where it is not allocated radio spectrum (Example: Alltel)

- Provider‘s economic model is service based
  - Subsidize handsets with the expectation of return

- Who is your cellular provider?
  - Verizon, AT&T, T-Mobile, Sprint-Nextel, Vodafone, O2, etc.

Provider Concerns

- Network providers are concerned about service fidelity and customer subscription fees

- Handset abuse can effect network fidelity (indirect profit loss)
  - Packets that attack back-end components
  - Packets that degrade service
  - Network scanning (reconnaissance for later attack)
  - Radio frequency jamming (or protocol abuse)

- Other abuse directly effects profit
  - SIM network locking (subsidized phone costs)
  - Phone to laptop "tethering" (and not paying for it)
  - "free" alternatives to value added services (e.g., VoIP, MMS)

Handset/OS Manufacturers

- Cellular phone handsets consist of many parts (hardware and software) that are designed and manufactured by different corporations

- We are concerned mostly with the handset and OS manufacturers

- Handset manufacturers design how the physical phone looks and feels
  - Combine chips (ICs) and peripherals (e.g., radio, camera, keyboard)
  - Often write low-level firmware (e.g., radio, bootloader) and device drivers
  - Handset manufacturers sometimes change the OS user interface (e.g., HTC)

- OS Manufacturers design user “experience” and many things never seen
  - The OS often includes a base set of applications for the user
  - Frequently, an SDK is provided for third-party application development

Handset/OS Manufacturers Concerns

- Handset and OS manufacturers have similar high-level concerns, and frequently, compromise of one leads to the compromise of the other
  - Access to rewrite radio and bootloader firmware from the OS
  - Access to rewrite the OS image from the bootloader
- Both have guarantees to the network providers
  - SIM network locking, prevent laptop tethering
- Both have guarantees to applications and users
  - DRM (hardware-based?), preventing malware access, battery consumption, etc.
- Both are concerned about protection circumvention
  - firmware replacement, tamperproof platform

Operating System Zoo

- Android
- Apple iPhone OS
- BlackBerry OS
- Symbian OS
- Windows Mobile OS
- LiMo Foundation
- Palm WEB OS
- Openmoko
- Garnet OS (formerly Palm OS)
- Access Linux Platform (ACCESS acquired Palm)
- BREW (Binary Runtime Environment for Wireless)

Operating Systems

- Android

  Android is an mobile phone operating system created by the Open Handset Alliance, which is visibly let by Google. While Android runs on top of a Linux kernel, the programming environment is anything but, defining a middleware API based on Java. The first Android-based phone is the T-Mobile G1, released October 2008; however, more expected to follow in early 2009. The source code for Android is publicly available, as is an SDK including an emulator based on QEMU.

- Apple iPhone OS

  The Apple iPhone OS is a mobile version of Mac OS X also based on Darwin. It debuted on the first generation iPhone and iPod Touch, but had limited application capacity. Version 2.0 of iPhone OS, released along with the 3G iPhone, added the capacity of the Apple AppStore, though which developers distribute there applications. The iPhone is the canonical smartphone used for comparison purposes, and its AppStore has revolutionized mobile phone software. Due to application limitations, the "iPhone Dev Team" has released methods of "jailbreaking" the iPhone.

Operating Systems

- BlackBerry OS

  BlackBerry OS is a proprietary operating system seen exclusively on Research In Motion's (RIM) BlackBerry handsets, known simply as "BlackBerries". With a long history as the mobile device for business professionals, BlackBerry devices are known primarily for email; however, an application SDK is available with an applications store about to appear.

- Symbian OS

  Symbian OS is one of the most widespread operating systems for smartphones. It has also been the target of most mobile phone malware, despite its maturing security architecture. An SDK exists for third-party development. Students researching Symbian OS are required to note significant changes in the application and security architectures as the operating system matured.

Operating Systems

- Windows Mobile OS

  Microsoft Windows Mobile the latest iteration of Windows CE, which was originally called PocketPC 2000. Windows Mobile is an increasingly common platform for smartphones. An SDK exists for third-party development.

- LiMo Foundation

  The Linux Mobile (LiMo) Foundation is an alliance founded in January 2007 by a number of handset developers and telecommunications providers. Their goal is to create an open hardware-independent Linux-based operating system for mobile devices. LiMo has replaced previous standards groups such as LiPS (Linux Phone Standards) Forum.

Operating Systems

- Openmoko

  The Openmoko project consists of more than just the operating system, including open hardware specifications. While Openmoko handsets have been known to run Android, students researching Openmoko will consider the Openmoko operating system. The OS is opensource and a QEMU emulator exists.

- Garnet OS (formerly Palm OS)

  Garnet OS is the new name for Palm OS after ACCESS acquired Palm, Inc. Palm OS has a long history in the PDA market and has been ported to support mobile phones. Students researching Garnet OS do not need to worry about Palm OS Cobalt, which is a Linux-based Palm OS that was introduced but eventually terminated.

Operating Systems

- Access Linux Platform (ACCESS acquired Palm)

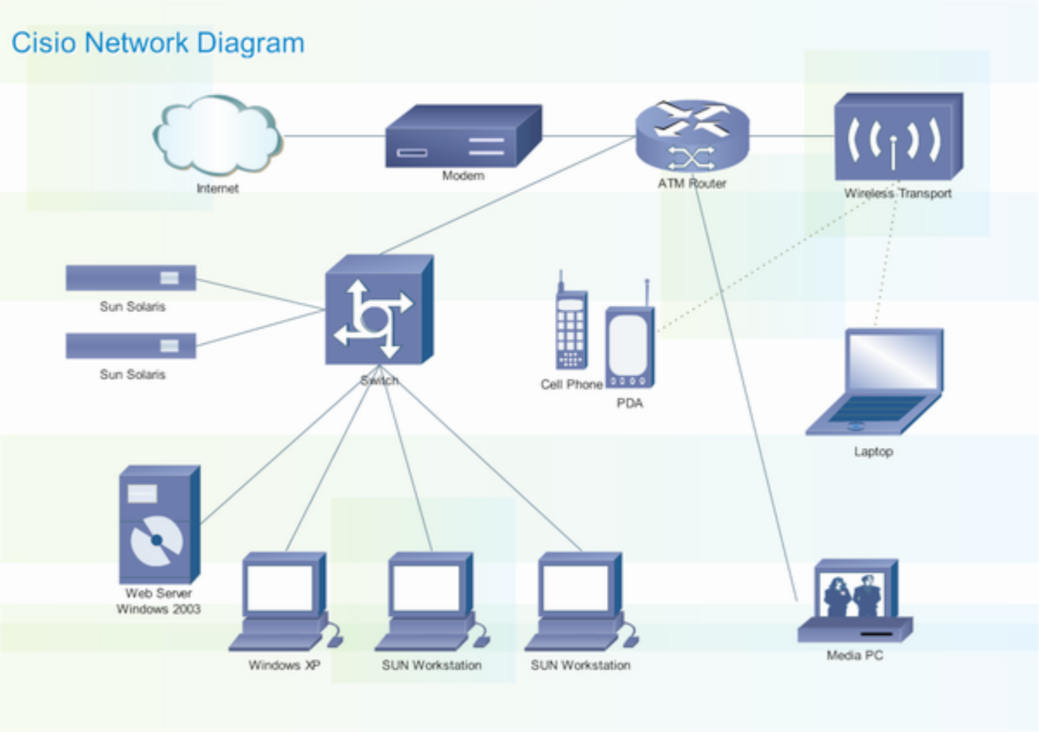
  The Access Linux Platform (APL) is the newest operating system offering from Palm after being acquired by ACCESS. Students researching APL will focus on how native applications operate, as well as it contains applications running in the Garnet VM. Note, the Access Linux Platform is expected to become LiMo compatible, but is still a distinct platform with its own APIs and software stack.

- BREW (Binary Runtime Environment for Wireless)

  BREW is an mobile phone operating system developed by QUALCOMM. BREW is distinct from Java ME, and students researching BREW are required to contrast BREW and Java ME from both an application and security perspective.

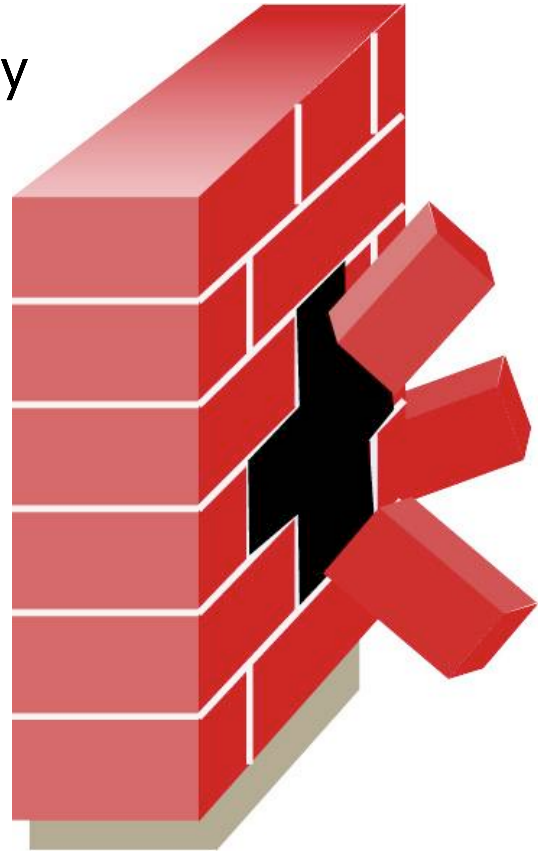
Enterprises

- Enterprises are indirectly affected by the security of a cellular phone
- Traditionally, enterprises maintain administration of all employee desktops and laptops ... the enterprise owns those devices
- Enterprises frequently do not own cellular phone handsets
  - This makes them harder to administer
- Cellular phones are being used to access corporate email, calendars, inventory ... potential access to trade secrets
- Cellular phones are begin connected to enterprise networks (WiFi)



Enterprise Concerns

- Enterprises are concerned about information and network access
  - Camera phones are already band from many classified environments
- Access to corporate email is often a primary use (e.g., BlackBerry)
  - Enterprise may design specific applications (e.g., inventory)
- Allowing cellphones to access WiFi may break policy
  - Circumvent Firewalls and VPN policies (traffic relay)
  - Spread malware or scan networks
- Large enterprises sometimes work with providers to install corporate software policies on phones
  - Need to ensure correctness
  - Must not be circumventable



Application Developers

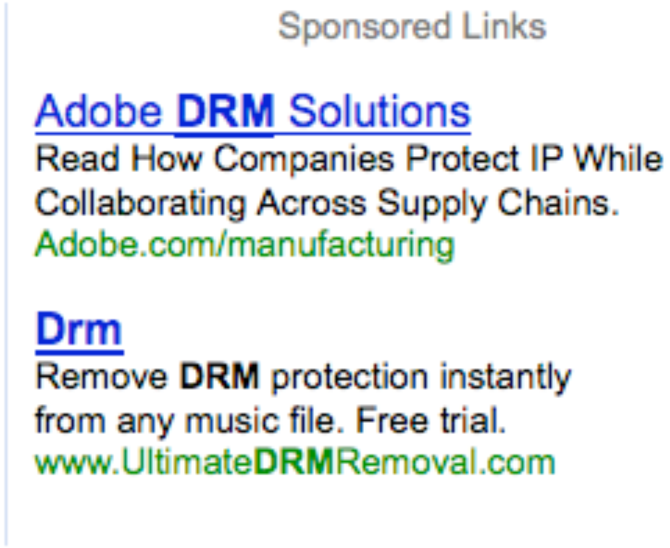
- A wide variety of software currently exists for cellular phones
  - AppStore categories: games, entertainment, utilities, social networking, music, productivity, lifestyle, reference, travel, sports, navigation, healthcare & fitness, news, photography, finance, business, education, weather, books, medical
- Significant time and effort to create applications ... just like PC software
  - Applications have varying costs (free apps often have advertisements)
  - Some applications provide access to larger services (e.g., Facebook)
  - Other applications enhance products (e.g., lighting control)

Application Developers

- Third-party app developers concerned with service fidelity and DRM
  - A cellular phone application may have exclusive access to a web-service
  - Account details, including passwords, are stored on the phone
  - Pandora iPhone app has unique "device number"

- Users should not be able to turn off or discard advertisements

- Software and media piracy is a significant concern
  - Unlicensed copies of software
  - Unregistered users in multiplayer games
  - Recording streaming audio



Sponsored Links

Adobe DRM Solutions
Read How Companies Protect IP While Collaborating Across Supply Chains.
Adobe.com/manufacturing

Drm
Remove **DRM** protection instantly from any music file. Free trial.
www.Ultimate**DRM**Removal.com

End Users

- End users have the most dynamic set of concerns depending on values (cellular phones are purchased for a variety of reasons).

- Most phones and service plans are purchased for *at least* voice functionality (however, SMS is becoming more popular, and so is Web usage)

- The percentage of people depending on cellphones increases daily
  - Purpose: emergency, accessibility, gossip, entertainment, business

- The same handset is frequently used for both business and personal
  - The handset market is based on "features per square/cubic inch"
  - Device consolidation, access convenience, and cost are all reasons why users only want to carry one handset.

End User Concerns

- Cellphones follow users everywhere, which allows attackers to cross into the physical world

- End users are at personal risk
  - Data integrity: ransom-ware, etc.
  - Identity theft: passwords, every field every entered
  - M-commerce: Bank account access
  - Privacy ...

- Potential Privacy concerns:
  - Invasive hardware - microphone, camera, etc
  - Personal information - contacts, SMS messages
  - Eavesdropping - voice conversations are intimate
  - Location tracking - on phone, in network
  - Targeted advertising - value added services

Controlling Security Policy

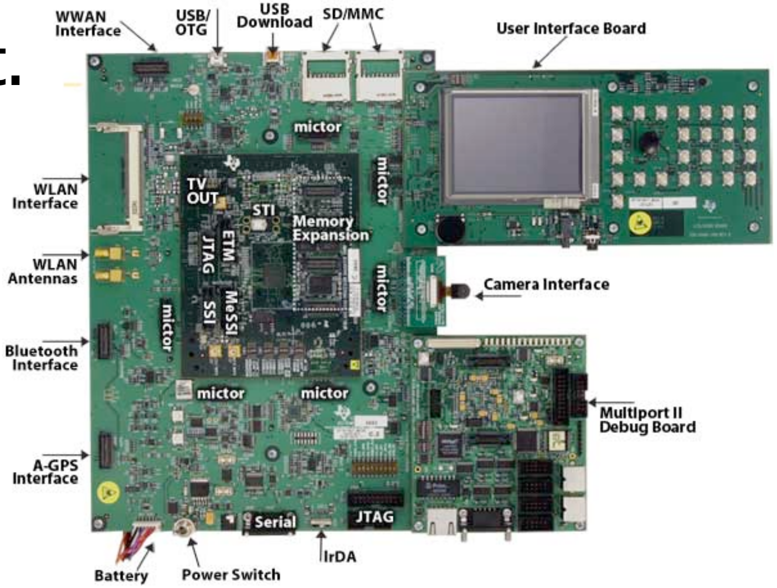
- Which stakeholder should control a phone's security policy?
  - Who controls it now?

- Answer: follow the money
  - Providers want to keep users from unlocking the phone
  - Users see providers as a privacy risk
  - Third-party apps want DRM protection
  - Some users want to circumvent DRM

- Tension: stakeholders can be adversaries of each other
  - Some advanced cellphone OS architectures propose allowing all stakeholders to influence phone policy, but gives precedence

Basic Phone Architecture = Embedded System

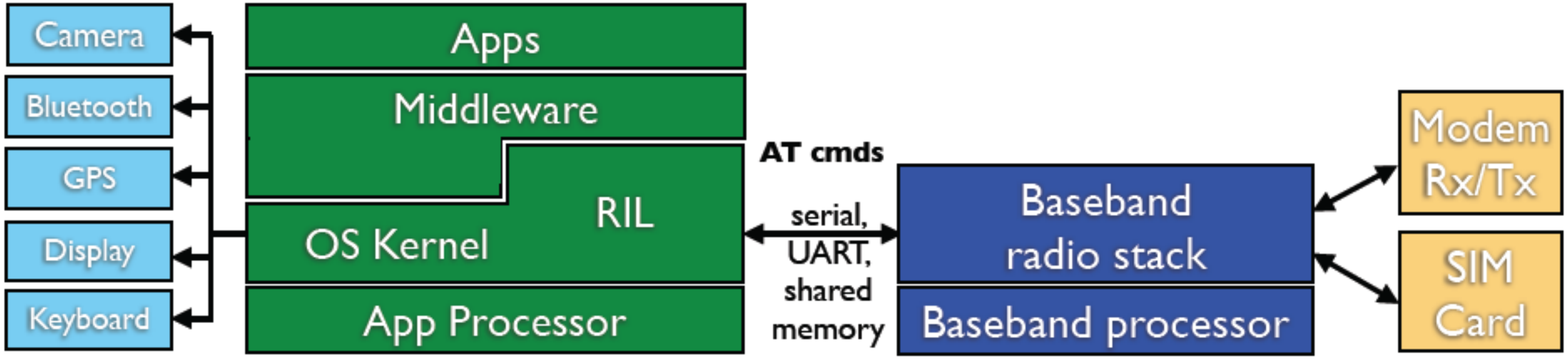
- Embedded systems consist of many small components put together to comprise the system. Frequenly contain many microcontrollers and "mini-OSes".
- Embedded systems design is a trade-off between performance, size, and cost.
  - Performance comes in many flavors, e.g., processing and power consumption
  - Frequently, performance is sacrificed for smaller and cheaper devices
  - Small variations in price are significant at large volumes



- Smartphones are upper scale embedded devices, but they are still embedded systems, and subject to many such constraints

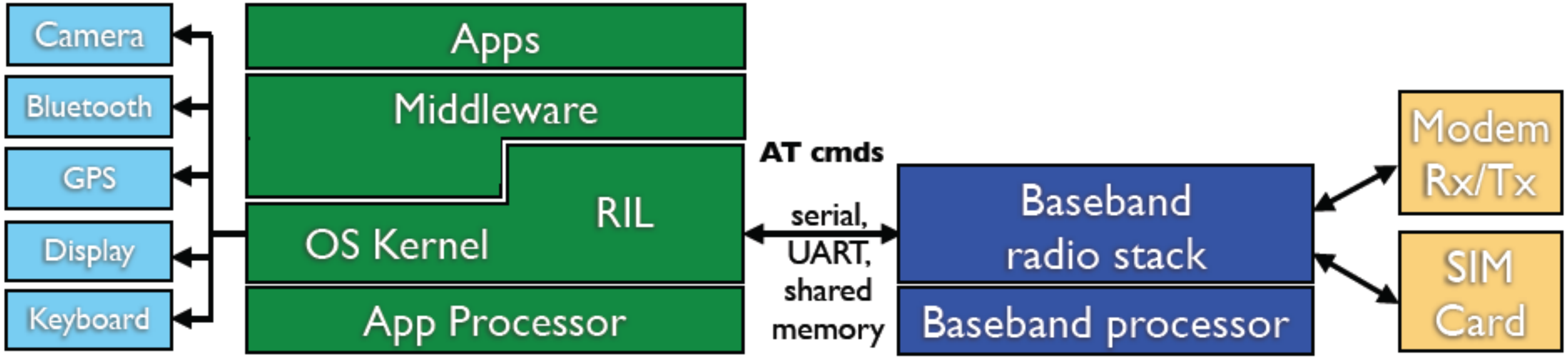
Basic Phone Architecture

- 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



Basic Phone Architecture

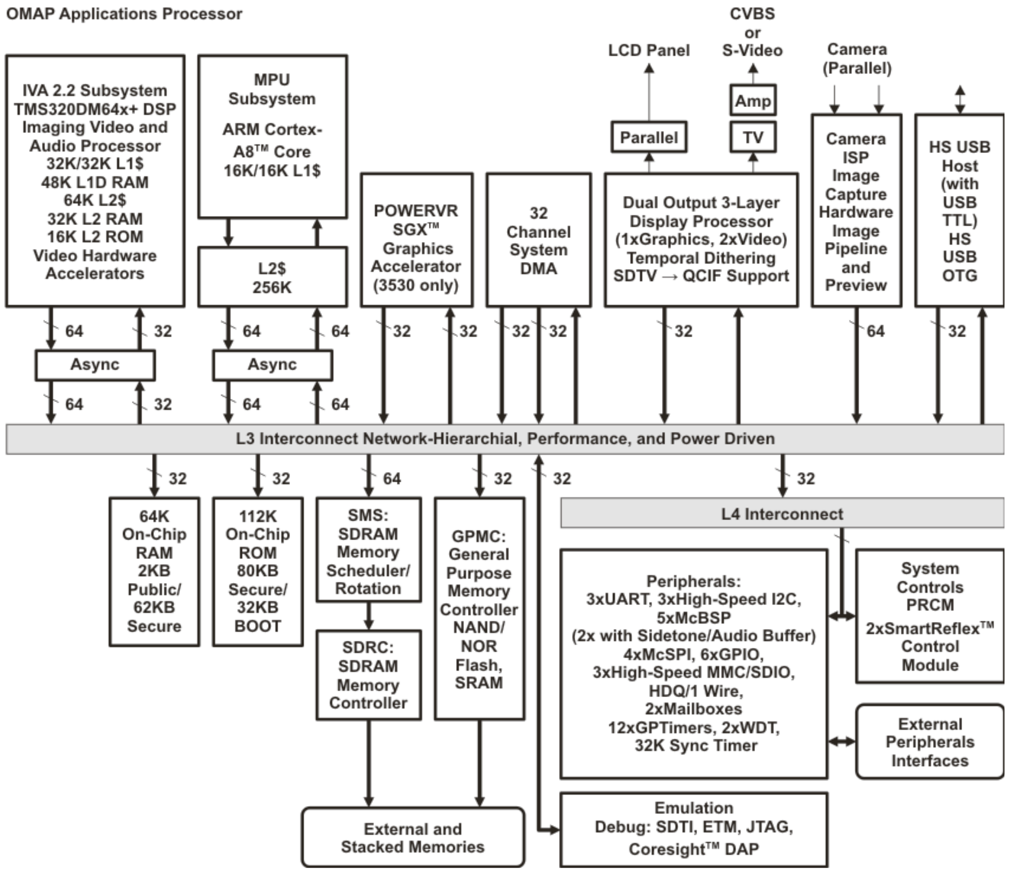
- *The hardware and software configuration dictates what sorts of policy are possible.*
- Each phone has implementation specific details, but some general trends
- Application processor and Baseband processors (sometimes single chip)
  - Separate firmwares and execution environments
- Example Chips (SoC) -- often bundle hardware features like GPS, bluetooth, etc.
  - Qualcomm Mobile Station Modem (MSM 7x, e.g., MSM 7201a) - single chip
  - TI Open Multimedia Application Platform (OMAP 1xxxx, OMAP 3xxxx) - only app
  - Broadcom baseband processors (e.g., ML2011)
  - Marvell (PXA series)



Peripherals

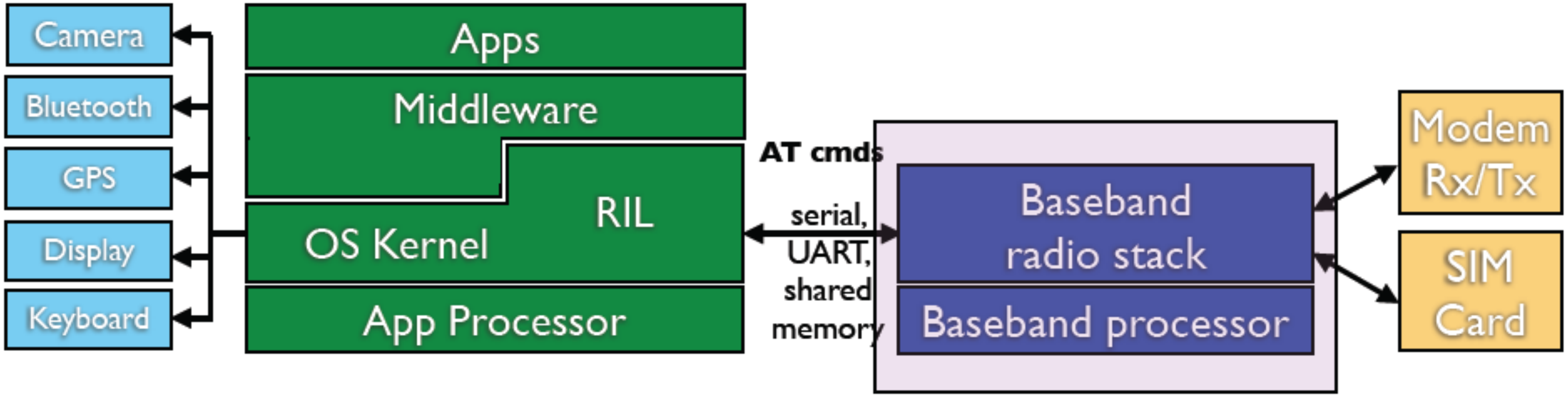
- Consumers choose devices based on functionality. Frequently, this includes hardware peripherals
- Standard peripherals: display, keyboard (or touchscreen), microphone, speaker (w/ headset), camera (more pixels is better)
- Emerging standard peripherals: GPS, accelerometer, compass, video acceleration, graphics acceleration, FM radio

Functional Block Diagram for TI OMAP3530


OMAP Applications Processor
LCD Panel
CVBS or S-Video
Camera (Parallel)
Amp
Parallel
TV
IVA 2.2 Subsystem TMS320DM64x+ DSP Imaging Video and Audio Processor 32K/32K L1$ 48K L1D RAM 64K L2$ 32K L2 RAM 16K L2 ROM Video Hardware Accelerators
MPU Subsystem
ARM Cortex-A8™ Core 16K/16K L1$
L2$ 256K
POWERVR SGX™ Graphics Accelerator (3530 only)
32 Channel System DMA
Dual Output 3-Layer Display Processor (1xGraphics, 2xVideo) Temporal Dithering SDTV → QCIF Support
Camera ISP Image Capture Hardware Image Pipeline and Preview
HS USB Host (with USB TTL) HS USB OTG
64
32
Async
64
64
32
64
64
32
32
32
32
32
64
32
L3 Interconnect Network-Hierarchial, Performance, and Power Driven
32
32
64
32
32
32
L4 Interconnect
64K On-Chip RAM 2KB Public/ 62KB Secure
112K On-Chip ROM 80KB Secure/ 32KB BOOT
SMS: SDRAM Memory Scheduler/ Rotation
SDRC: SDRAM Memory Controller
GPMC: General Purpose Memory Controller NAND/ NOR Flash, SRAM
Peripherals: 3xUART, 3xHigh-Speed I2C, 5xMcBSP (2x with Sidetone/Audio Buffer) 4xMcSPI, 6xGPIO, 3xHigh-Speed MMC/SDIO, HDQ/1 Wire, 2xMailboxes 12xGPTimers, 2xWDT, 32K Sync Timer
System Controls PRCM 2xSmartReflex™ Control Module
External Peripherals Interfaces
External and Stacked Memories
Emulation Debug: SDTI, ETM, JTAG, Coresight™ DAP

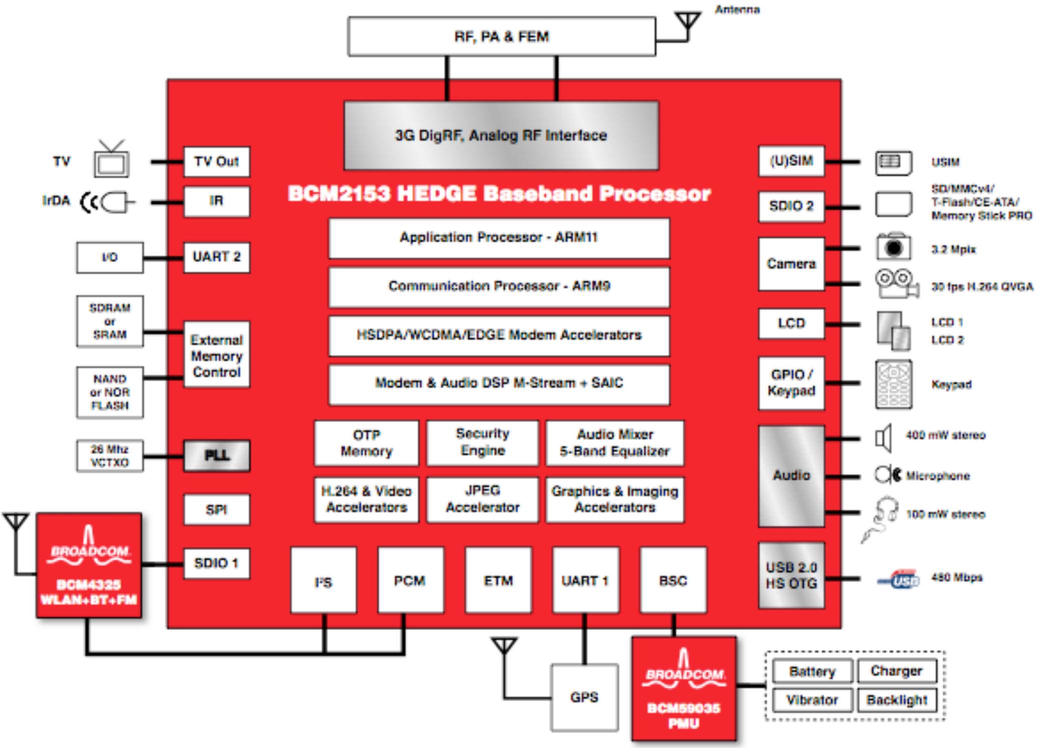
Baseband OS

- The baseband OS is responsible for controlling the radio
- The "radio firmware" ... receives buzz in the hacking community
- Facilitates network registration, authentication, mobility
- Often, in-call audio (mic, speaker) bypasses the Application OS



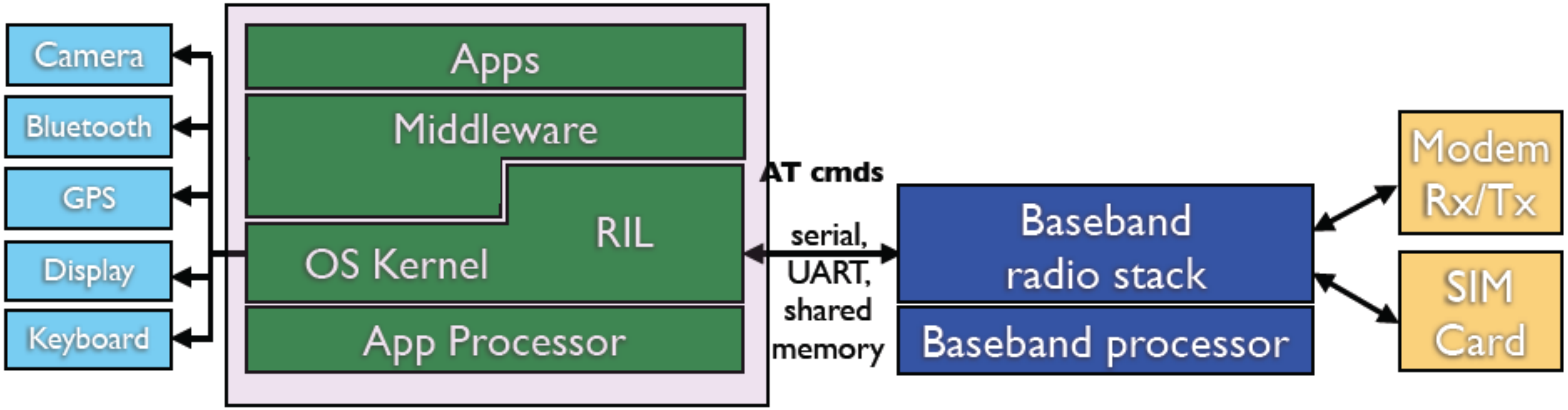
Baseband OS = Modem Processor

- Voice and data communications processing is intensive. For realtime and security reasons, a separate baseband processor and OS exist (no need for RTOS or preemption for App OS).
- More and more frequently, the broadband (aka modem or communications) processor is located on the same silicon chip as the application and peripheral logic.
- Separate ARM core (DSP extensions) and sometimes modem accelerators.

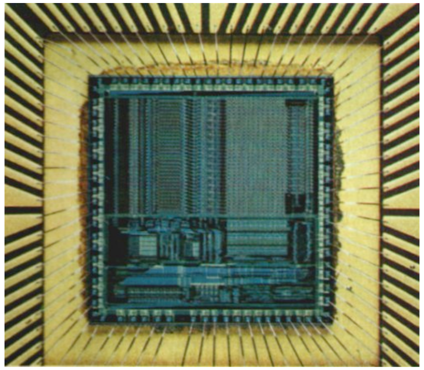


Application OS

- This is the part *you* interact with -- functionality users care about
- New phones support full featured operating systems based on Linux, Mac OS X, and Windows
- Traditionally dialer, PIM, etc., but not much more elaborate
  - Many alternatives: Windows Mobile, BlackBerry OS, Symbian OS, iPhone OS, Android, etc.
  - Commonly a middleware of some sort (e.g., J2ME, .NET, etc)
  - Features and application model varies greatly between OSes



Application Processor



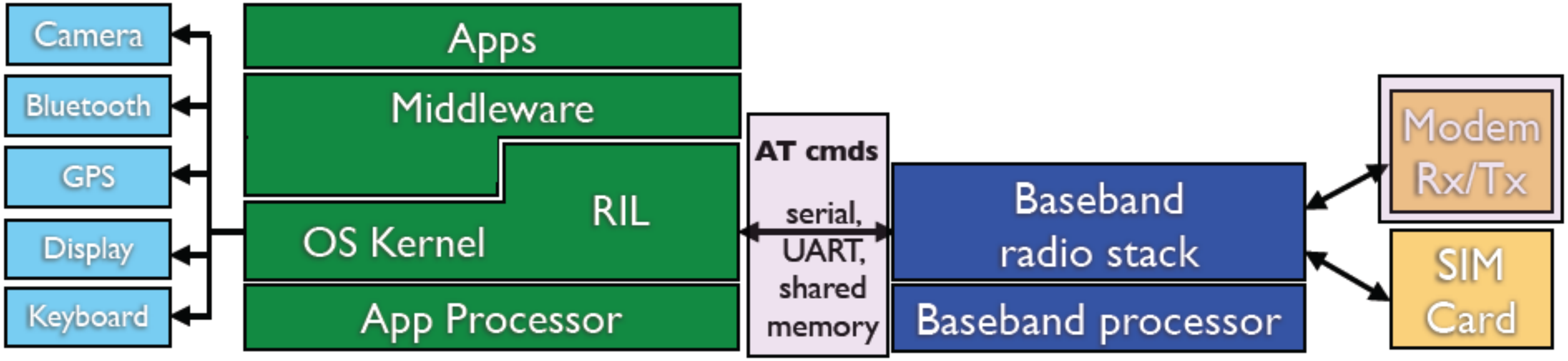
- Almost all mobile phones use an ARM-based processor
  - ARM based processors are very common in embedded systems. For example, Game Boy Advance, Nintendo DS, and iPod use an ARMv4T processor.
  - Many smartphones use ARMv5 or ARMv6 architectures.
  - Naming is a big mess: Family vs. Architecture vs. core.
- Example, iPhone uses ARM11 family, ARMv6KZ architecture, and ARM1176JZ(F)-S core (which has SIMD, Jazelle DBZ, and TrustZone ...)
- ARM Ltd. doesn’t actually sell hardware chips
  - Licenses Intellectual Property (IP) to merchant foundries for chip (SoC) designs
- Long history of low transistor count: ARM2 was 30,000 transistors when Motorola 68000 was around 70,000 (6 year older design)

OS Comunication

- App OS has indirect access to the cellular radio

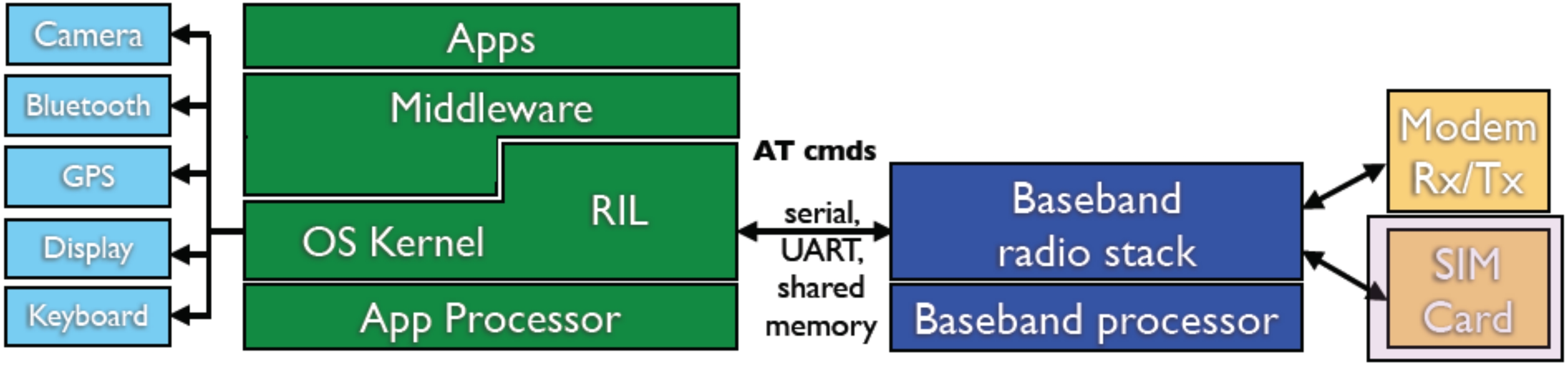
- Radio Interface Layer (RIL) communicates with baseband firmware
  - Modem-like interface (AT Commands - 3GPP TS 27.007)
  - Universal Asynchronous Receiver/Transmitter (UART) or shared memory
  - Commonly split into userspace and kernelspace components

- Control and data mode switching depends on hardware
  - e.g., one or two UART channels



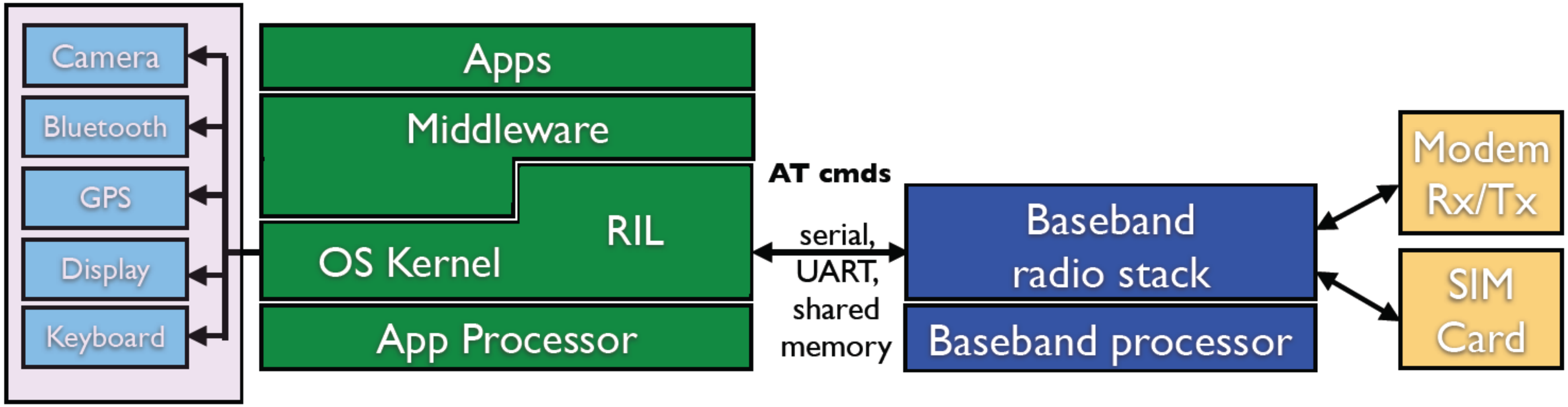
SIM Card

- Not all providers use SIM cards. Part of the 3GPP GSM standard
- Stores IMSI, authentication tokens, address book -- swap between handsets
  - Crypto operations for authentication are performed on-chip
  - Also contains a provider identifier ... used to “lock” a subsidize phone
  - Black-market for SIM network unlocking phones (revisit this later)
- Application OS accesses the SIM using AT commands



Hardware Features

- Hardware Features
- Cellular phones are marketed based on their hardware features ... beyond keyboard and display
- Cameras and Bluetooth have been standard on phones for a while
- Emerging standard hardware features (part of SoC, e.g, MSM, OMAP):
  - GPS (A-GPS), accelerometer, compass
  - Video processing chips



Resources of Interest

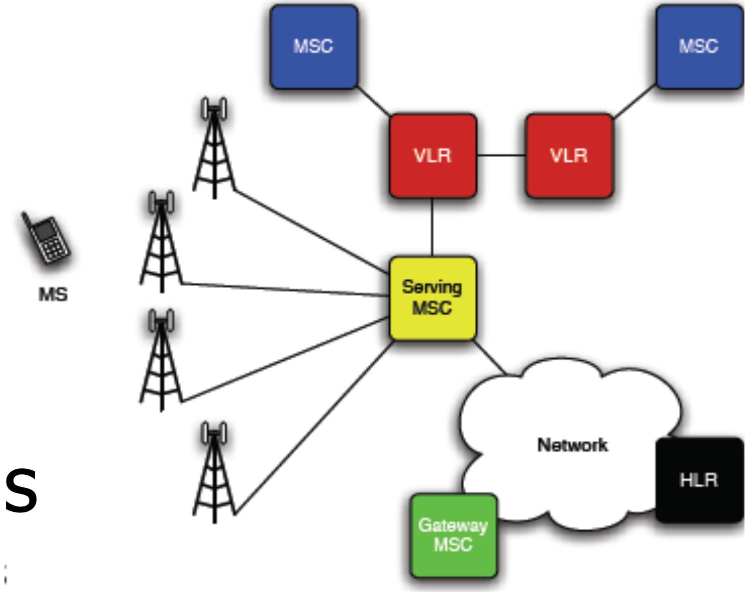
- What resources might an adversary wish to abuse?
  - Think of "resource" in its most general sense
- Hardware (availability and consumption)
  - CPU, memory, battery, storage, storage fabric
- Networking (abuse and scanning)
  - RIL, bluetooth, WiFi, NFC
  - Calling premium numbers
- Privacy
  - microphone, camera, RIL, GPS, accelerometer, compass?
  - Contacts, SMS, Email, etc
- Application specific data
- What else?

Fresh Start?

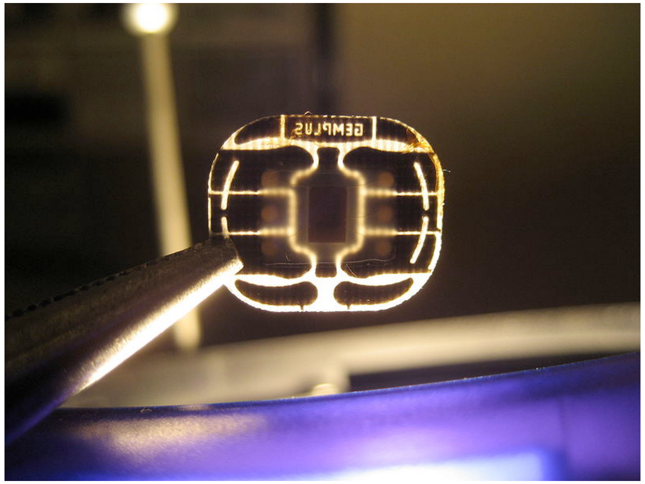
- What would you do if you could start fresh?
- How do you handle the deluge of applications?
  - Isolate everything?
- What about hardware/resource access?
  - Controlled communication?
  - Context for mediation?
  - Policy specification?
- Who controls it?
- These are the same problems as desktop and server OSes
- Need to take advantage of Cellphone-specific properties
  - Small screen. Limited input mechanisms.
  - One user? Do friends borrow it?
  - Always connected.
  - Look at the purpose of running applications

Upcoming Lectures

- Telco Network Background

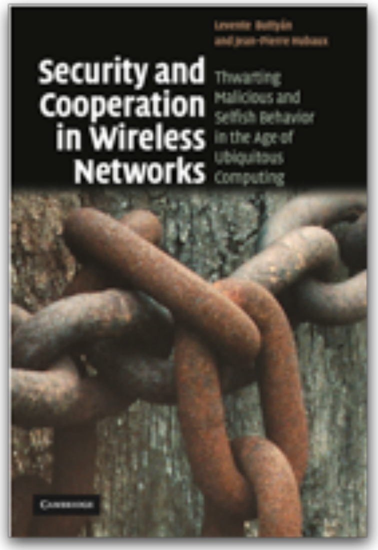


- SIM cards



Next Time

- Overview of how the cellular network operates


Levente Buttyán
and Jean-Pierre Hubaux
Security and Cooperation in Wireless Networks
Thwarting Malicious and Selfish Behavior in the Age of Ubiquitous Computing
Cambridge

- Online Resources:
  - 3GPP and 3GPP2 websites
  - http://secowinet.epfl.ch/

- Please study for next time the cited literature on how the cellular network operates!!!