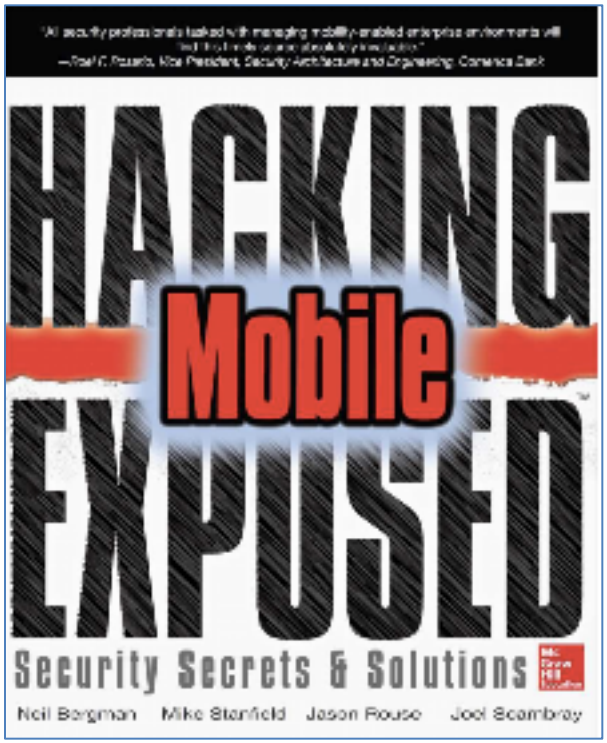
Ch 2: Hacking the Cellular Network



CNIT 128: Hacking Mobile Devices

Updated 1-14-16

Basics

GSM/CDMA

- We'll start with a standard carrier network using
  - Global System for Mobile (GSM), or
  - Code Division Multiple Access (CDMA)
- With these functions
  - Phone calls
  - Text messages via Short Message Service (SMS)
  - Multimedia Messaging Service (MMS)
  - Data connectivity via IP

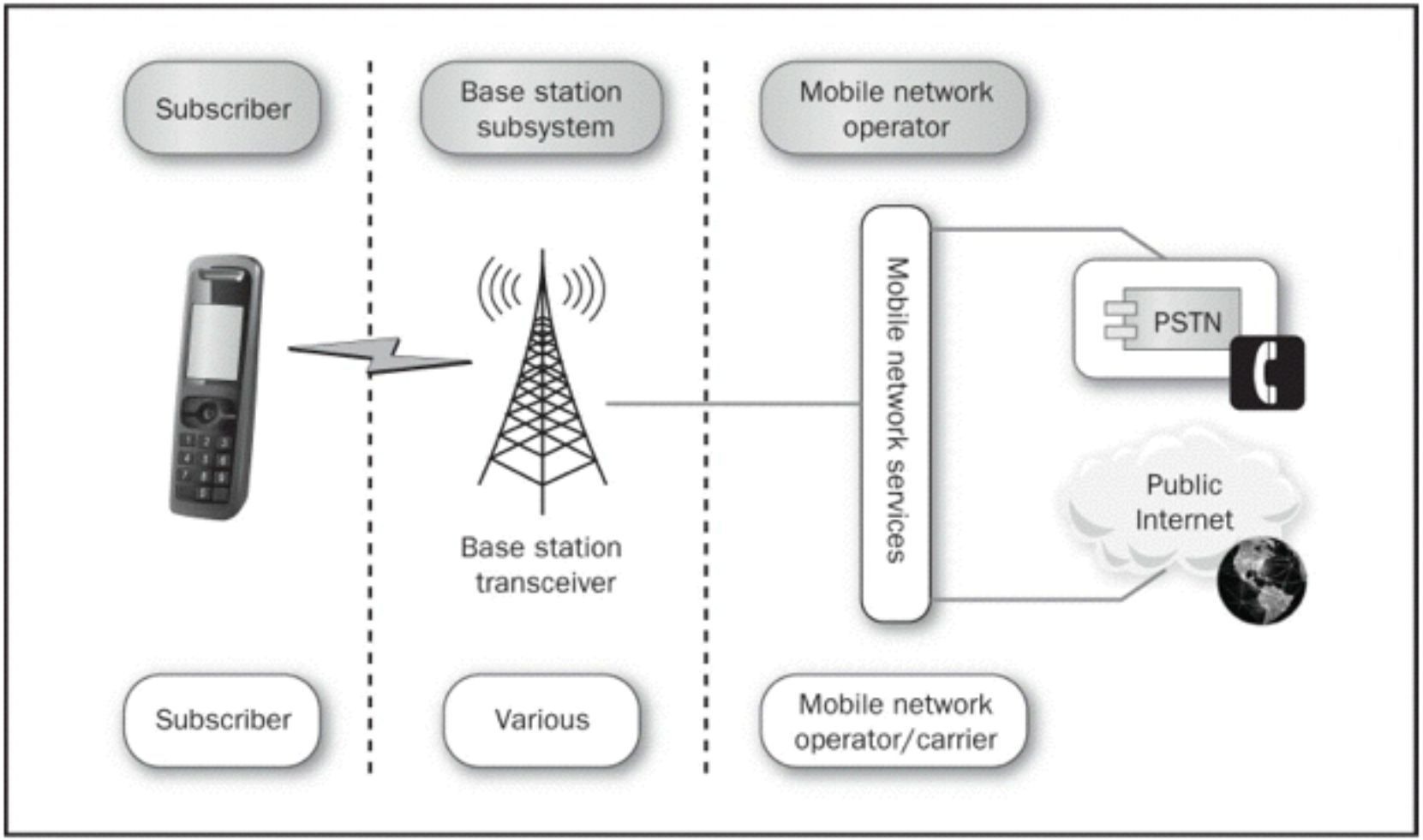


Figure 2-1 Simplified GSM/CDMA mobile network

Basic Cellular Network Functionality

Interoperability

- Different carriers and connection methods can connect to one another seamlessly
- A GSM phone can text or call a CDMA phone

Functions to Target

- All major cellular networks support
  - Voice calls
  - Voice mail (VM)
  - Short Message Service (SMS)
  - Location-based Services (LBS)
  - IP Connectivity
- Most also support
  - Binary configuration messages
  - Multimedia messages (MMS)
  - Faxing

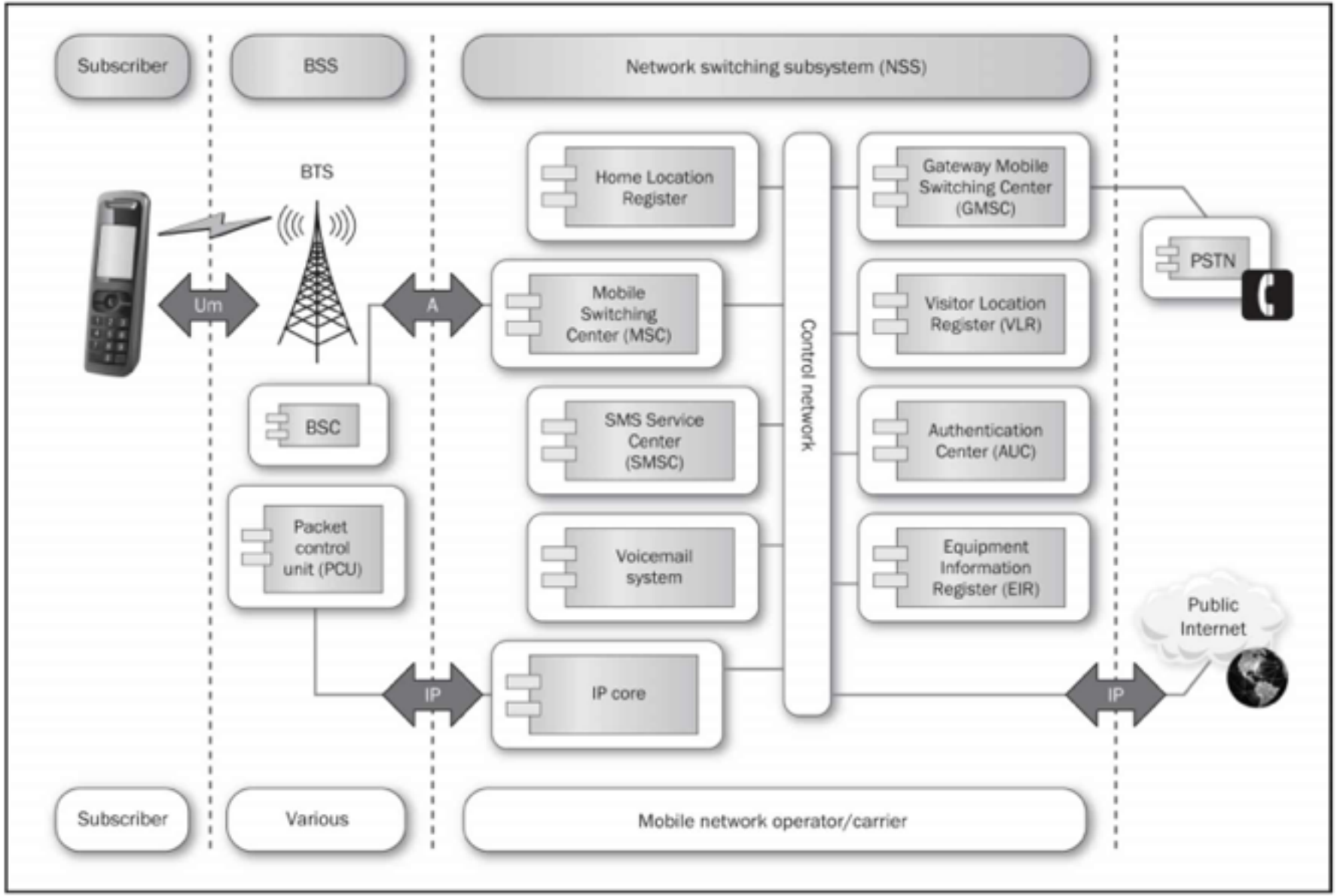


Figure 2-2 Service overview of a GSM cellular network

Players

- Customer is on the left
  - Known as Mobile Terminals (MTs) in GSM
- Connect to antennas
  - Called Base Transceiver Stations (BTS)
  - The connection from a mobile device to a BTS is called an **Um** (U-channel mobile)

Players

- Each BTS connects to a **base station**
  - A rack of equipment that takes the signals the antenna receives and converts them to digital packetized data
  - **Base station** has two components
    - **Base Station Controller (BSC)** for voice and control
    - **Packet Control Unit (PCU)** for forwarding IP packets and managing mobile IP

Players

- Base Station Subsystem (BSS)
  - Includes BTS, BSC, and PCU
  - Can be owned by people who are not part of a large carrier

Voice Calls

- Time Division Multiplexing (TDM)
  - Tried-and-true method for dividing radio capacity among many devices
- Time Division Multiple Access (TDMA)
  - Each device gets time slots
  - Very successful for slow and medium bit rates
  - Devices 1, 2, and 3 might get these time slots

Control Channels

- Traffic channels
  - Carry voice data
- Control channels
  - Manage association, usage, handoff, and disconnection
- Cell phone jammer
  - A loud, badly tuned, transmitter
  - Easy to build
  - Illegal

The Broadcast Control Channel: Learning About the Network

- When a device first turns on, it listens on standard frequencies
- First thing it hears will be BCCH (Broadcast Control Channel)
  - Allows the device to synchronize and understand which network it is attaching to
  - Features of the network the BTS (Base Transceiver Station) is serving

RACH (Random Access Channel)

- The mobile device then knows how to access the RACH
  - The first step in a GSM handshake
  - How the mobile asks for information
  - Mobile sends a channel request via the RACH
  - BTS tries to service the request

Standalone Dedicated Control Channel (SDDCH) & Access Granted Channel (AGCH)

- If the BTS has slots available, it assigns a control channel, called the **Standalone Dedicated Control Channel (SDDCH)** to the mobile device
- The BTS tells the mobile about this assignment via the **Access Granted Channel (AGCH)**
- Once the mobile has received a SDCCH, it's a member of the network and can request a **location update**

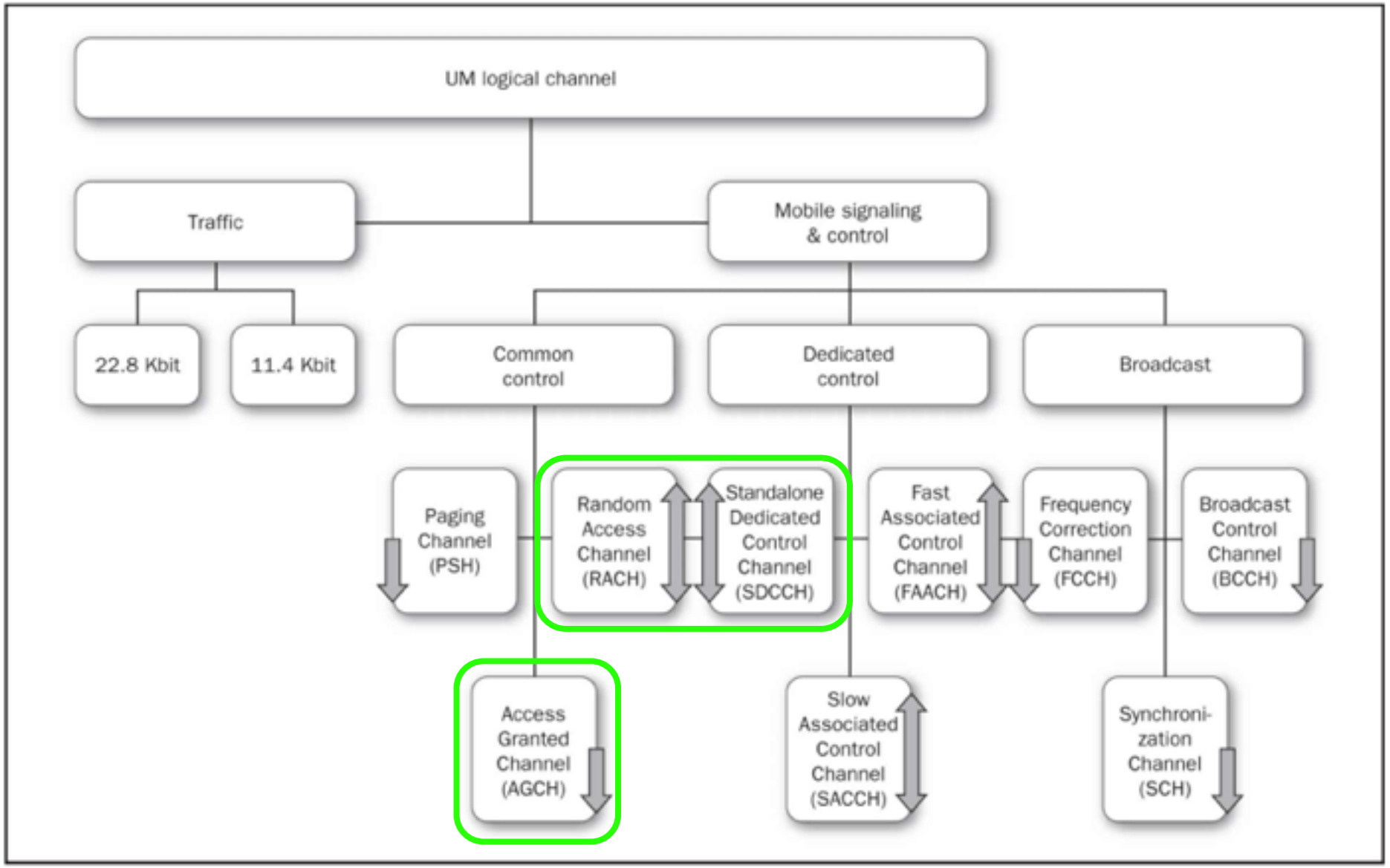


Figure 2-3 GSM logical control channel layout

Location Update

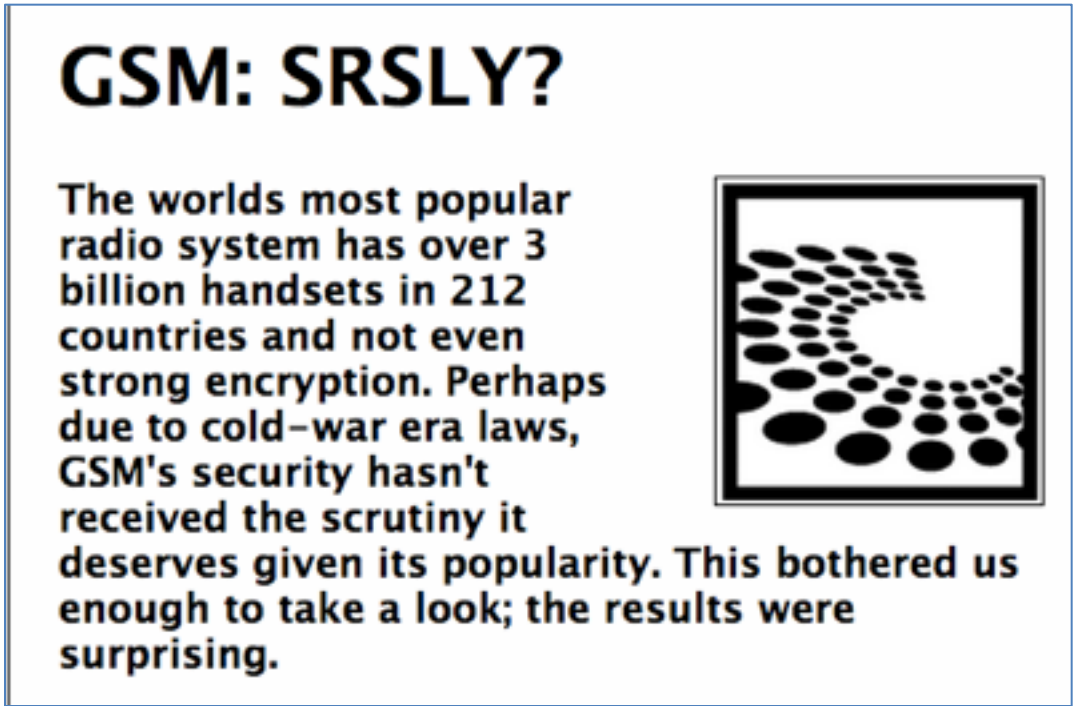
- Mobile device is telling the GSM network what area it's in
- Requires authentication with the network
- Informs the **Home Location Register (HLR)**
  - Database of subscriber information
- Of the mobile's geographic area
  - Hence, which Mobile Switching Center (MSC) a device is located within

Sleep

- Once a mobile device has performed a location update
- The BSC tells the mobile to go to sleep
  - By deallocating the SDCCH
- This maximizes reuse and capacity in dense cells

Authentication and A5/1, CAVE, and AKA

- A5/* ciphers are used in GSM networks
  - Crackable – see link Ch 2a
- CAVE and AKA are used in CDMA

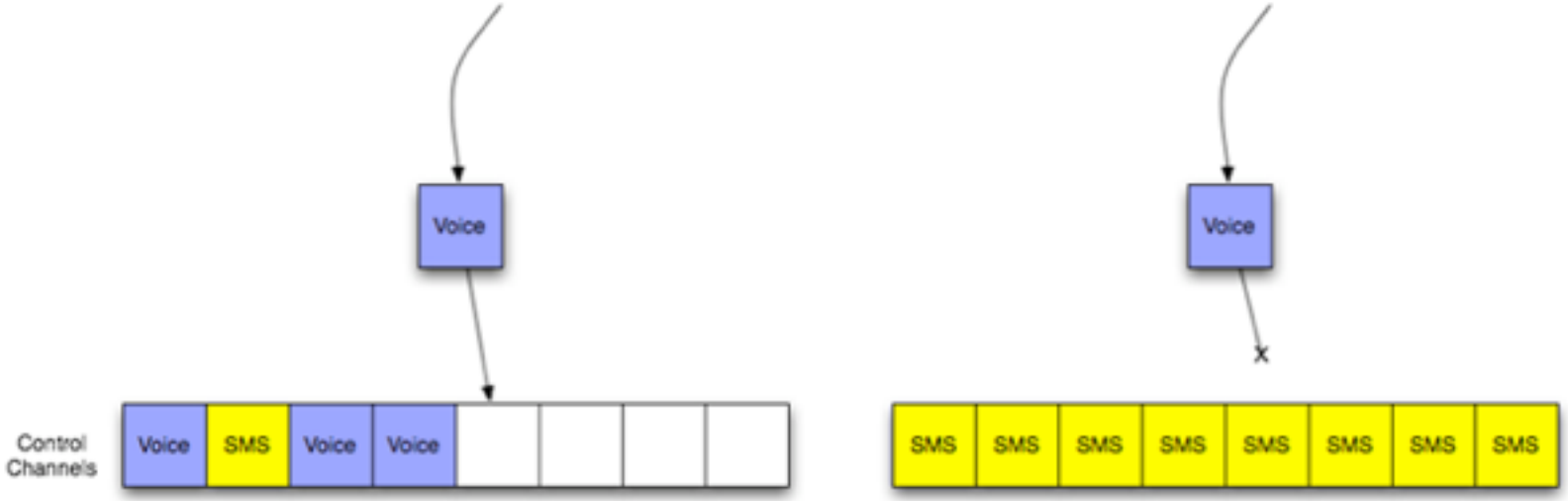


Voicemail

- Trivial hack: default password
  - Enough to make a world of trouble for Rupert Murdoch
- Many carriers use IP-based voicemail
  - Using IMAP servers (originally designed for email)

Short Message Service (SMS)

- Sent via control channel
- An SMS flood could DoS voice service for a whole city from a single attacking device
  - Link Ch 2b2



SMS Channels

- SMS messages are delivered over either
  - SDCCH when a user is not on a call
  - or the **Slow Associated Control Channel (SACCH)** if the user is talking at the time
- Reasonably achievable SMS floods wouldn't stop voice calls in practice

SMS Service Center (SMSC)

- SMSCs carry most of the SMS messages when SMS message storm happens
- It's the hardest working piece of equipment in modern cellular provider networks

Other Uses for SMS Messages

- Java implemented per-application messaging using
- Java Mobile Information Device Profile (MIDP) and Connected Limited Device Configuration (CLDC), which use a
- User Data Header (UDH) specifying a port to send the message to
  - Ports are not UDP or TCP ports, but similar

Other SMS Messages

- SMS is used not just between users
- But between network elements, like configuration servers
- For peer-to-peer Java apps
- UDH features

  - Changing reply-to phone number (UDH 22)
  - Message concatenation (UDH 08)
  - Message indicator settings—video, voice, text, email, fax (UDH 01)
  - Ported SMS message (UDH 05)

SMS Lacks Security Controls

- SMS messages have
  - No authentication
  - No integrity checking
  - No confidentiality
- So apps shouldn't trust what they get too much

SMS Origin Spoofing

- iOS displays the number in the "reply-to" field in the SMS header as the origin of an SMS message
  - Instead of the actual origin number
- So it's easy to send SMS messages that appear to come from someone else
  - Link Ch 2c

Fake SMS Messages

- On Android, a malicious app can fool your device into displaying a fake SMS message
  - Link Ch 2d

Attacks and Countermeasures

Hacking Mobile Voicemail

- MNOs often configure voicemail accounts insecurely
  - No authentication required if the user's own phone is used to fetch the messages
- With a PBX sever like Asterisk, anyone can easily spoof any caller ID value
- All they need is your phone number

Internet Spoofing Services

- Link Ch 2f

Countermeasures for Mobile Voicemail Hacks

- Set a voicemail password
- Configure access so that entering the password is required from all phones, including yours

Rogue Mobile Devices

- An evil phone could attack the mobile network (theoretical attack only)
- Phone OS is not hard to understand, basically
  - iOS is BSD
  - Android is Linux
- A modified phone could jam or modify broadcast signals from a BTS
  - But it would only affect a small area

Rogue Mobile Device Countermeasures

- The cellular network is carved up into many small parts
- Radio earshot is only a few hundred yards in a city, or a few miles on flat terrain
- Just a normal radio jammer would be more effective

Early Rogue Station Attacks

- Until recently, carriers assumed that attackers lacked the skill to build a base station, so
- Network required authentication from the phone, but
- Phone didn't require authentication from the network
- So it was simple to emulate a cellular network

Attacking in the 1990s

- A cellular phone can simply "join up" with another cellular provider's network.
- Cellular phones are generally promiscuous when it comes to joining networks (how else would roaming be so easy?).
- Cellular networks are defined by a simple three-digit number and a three-digit country code, as shown in Table 2-1.

Country	Country Code	Selected Operators
United States	310, 311, 313, 316	T-Mobile: 026; ATT: 150
United Kingdom	234, 235	T-Mobile: 030; BT: 076
Canada	302	Koodo: 220; Rogers: 720
Saudi Arabia	420	Mobily: 003
Brazil	724	Claro: 005; Vivo: 006
China	460	China Mobile: 002; China Telecom: 003
Test	001	TEST: 1

Table 2-1 GSM Network MCC/MNC Chart
(Source: Wikipedia,
en.wikipedia.org/wiki/Mobile_Country_Code_(MCC))

Base Station Hardware

- A normal cell phone could act as a base station with only a software change
- A phone in "engineering mode" could sniff radio traffic on all bands at the same time
- Packets can be logged via RS232
- You get voice and SMS traffic
- Flash phone via USB cable

Legal Warning

- This was all fantastically illegal, of course
- Wiretapping laws are scary
- We won't do illegal projects in this class
- I don't plan to do any rogue base station projects this semester

Hacking in 2002

- Rhode & Schwartz sold test gear for SMS networks, including BTS emulation
- Cost was six figures

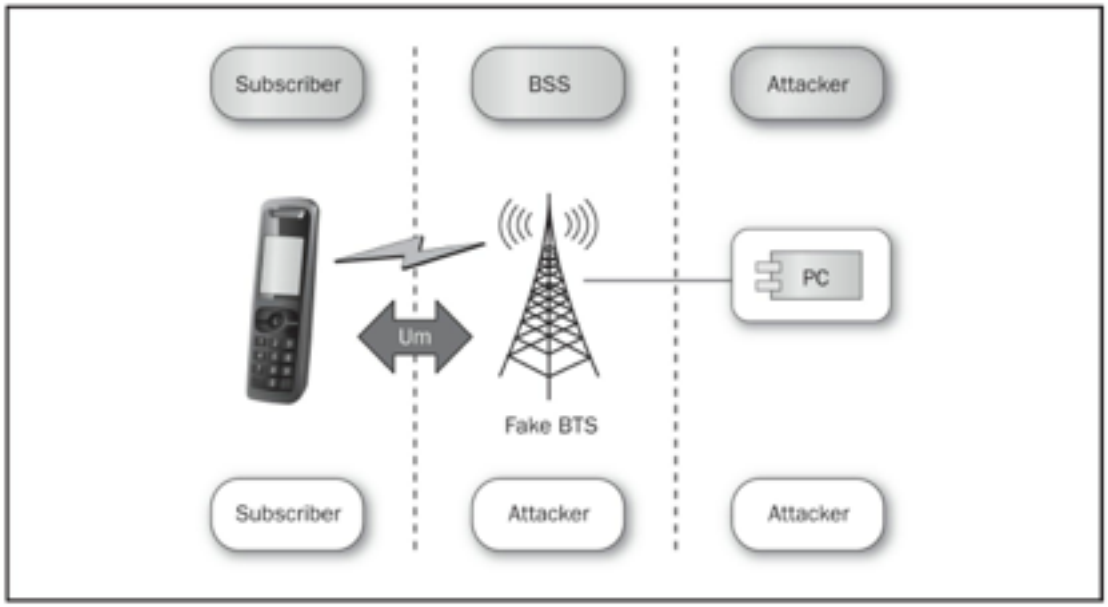


Figure 2-4 A simple GSM spoofing setup

Rogue Base Station Countermeasures

- It's up to the carriers to authenticate their networks
- There's nothing an end-user can do

Femtocell

- A device you can purchase
- Gives a stronger cell phone signal in your building
- Connects to your broadband Internet
  - Link Ch 2i

Rogue Femtocell Attacks

- OpenBTS: free software that can be used to make a fake base station for about $1500 in 2009
- Femtocells are even simpler

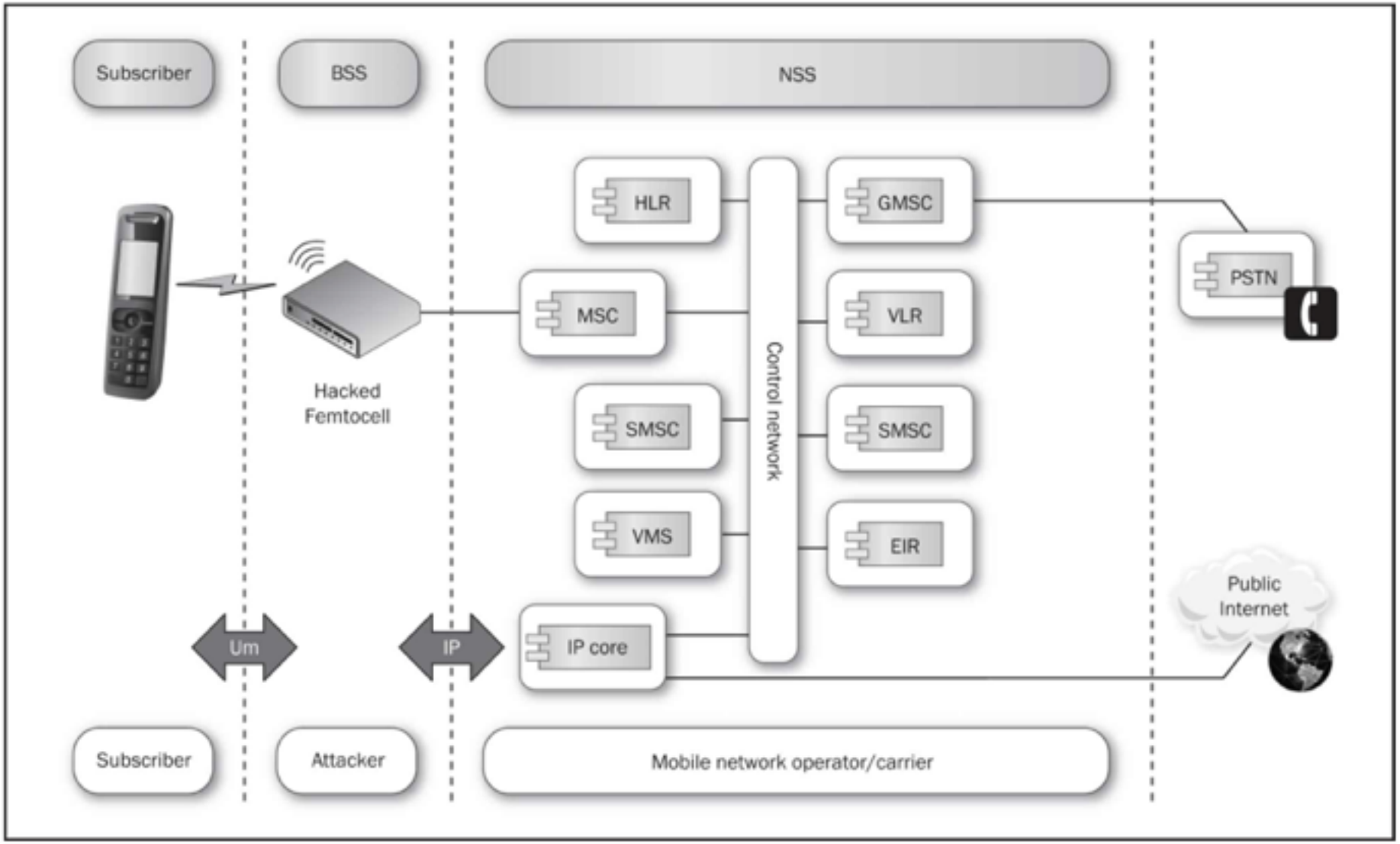


Figure 2-5 Rogue femtocell spoofing setup

Femtocell

- A tiny box with connectors for antenna, power, and Ethernet
- Generic Linux distribution running several specialized apps
- Loads a couple of drivers
- Includes some simple radios

Femtocell Functions

- Control signaling
  - Call setup and teardown and SMS messaging
- Converting normal voice calls into real-time protocol streams
- Associated SIP setup
- Backhaul link uses IPsec connections to special security gateways on the mobile network operator side

Information Disclosure

- Femtocells receive raw secrets used to authenticate devices from carriers
- They are encrypted in transit with IPsec, but they are present in the femtocell's software and hardware
  - Hacking AT&T Femtocell (link Ch 2g)
  - Hacking a Vodaphone Femtocell (link Ch 2h)

POKING AT THE FEMTOCELL HARDWARE IN AN AT&T MICROCELL

by: Mike Szczys

48 Comments

April 12, 2012

Femtocell Membership

- Carriers could limit membership to a few cell phones for a single femtocell
- But why not let everyone in? That expands their coverage for free!
- But it also means customers are using untrustworthy devices and they have no way to know that

Countermeasures for Rogue Femtocells

- Femtocells should be more limited in function
- Networks need to authenticate themselves to the handsets reliably
- SIP and IPsec allow for strong authentication
- We just need new standards that use them

The Brave New World of IP

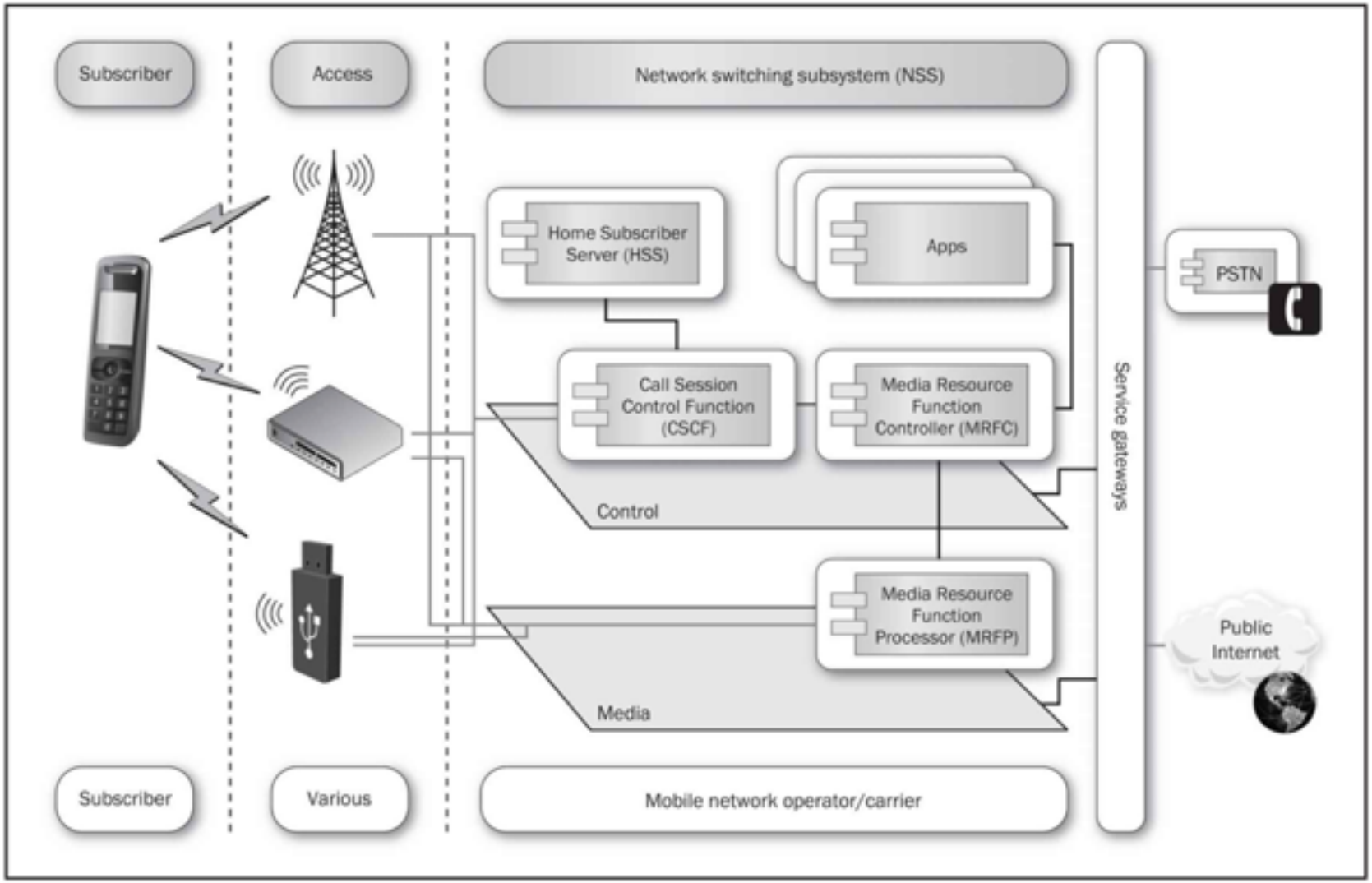
IMS (IP Multimedia Subsystem)

- Carriers are moving to an IP-only system
- No more
  - Packetized voice
  - Loss of data service while on a phone call
  - Low-speed data links
- Everything will use a baseband that connects to a high-speed IP network

Changes to Services

- Voice calls become Real-time Transport Protocol (RTP) streams delivered via UDP.
- SMS and MMS messages become Short Message Peer-to-Peer (SMPP) interactions.
- Control channels become SSL- or IPSec-protected TCP endpoints on your phone.

IMS Architecture



Long-Term Evolution (LTE)

- Devices connect via IP networks to services, protected by gateways
- As networks move from GSM or CDMA to LTE, these changes occur:
  - Unified bearer protocol—IP
  - IMS network can service any IP client, including PC, laptop, tablet, smartphone
  - All these devices could interoperate and replace one another, someday