

Exploiting Open Functionality in SMS-Capable Cellular Networks

William Enck, Patrick Traynor, Patrick McDaniel, and Thomas La Porta

Lecture 2 - CSE 544 - Advanced Systems Security

Presenter: William Enck

January 18, 2007

URL: <http://www.cse.psu.edu/~mcdaniel/cse544>

Unintended Consequences

- The *law of unintended consequences* holds that almost all human actions have at least one unintended consequence.



Large Scale Attacks

- Past damaging attacks follow a pattern ...
 - ▶ Bad (or good) guys find the vulnerability ...
 - ▶ Somebody does some work ...
 - ▶ Then exploit it ...
- Hence, an exploit evolves in the following way:
 - 1. Recognition*
 - 2. Reconnaissance*
 - 3. Exploit*
 - 4. Recovery/Fix*

Recognition: SMS Messaging

- What is SMS?
 - ▶ Allows mobile phones and other devices to send small *asynchronous* messages containing text.
 - ▶ Ubiquitous internationally (Europe, Asia)
 - ▶ Often used in environments where voice calls are not appropriate or possible.
 - ▶ On September 11th, SMS helped many people communicate even though call channels were full
 - ▶ Can be delivered via *Internet*
 - Web-pages (provider websites)
 - Email, IM, ...

The screenshot shows the Verizon Wireless 'get it NOW' website interface for sending text messages. The page features a navigation bar with links for 'SEND TXT', 'MY TXT', 'TXT INT'L', 'ALERTS', 'RINGTONES', and 'TXT PLAY'. Below the navigation bar is a 'get TTX' banner with 'R U TTX MESSAGING?' and buttons for 'JOIN UP', 'ARE YOU IN?', and 'HELP'. The main content area is divided into three sections: 'Sign In', 'Send TXT Message', and 'More Messaging'. The 'Sign In' section includes fields for 'Mobile Number' and 'Password', a 'GO' button, and checkboxes for 'Remember My: Mobile Number' and 'Remember My: Mobile Number & Password'. The 'Send TXT Message' section has a 'Send To:' field, a 'From:' field, a 'Reply To Address:' field, a 'Your Message:' text area, and a 'Callback Number:' field. It also includes a 'Priority:' dropdown menu with 'Normal' and 'Urgent' options, and a 'Characters Remaining: 160' indicator. The 'More Messaging' section contains links for 'Text to Landline', 'Send PIX/FLIX MSG', and 'Instant Messaging', along with a promotional banner for 'Stay cool Stay organized Stay in touch Join Up 2Day!'. The footer contains links for 'FAQs', 'Service Availability', 'Store Locator', 'Website Use', 'Privacy Statement', and 'getTXT & getAlerts Terms & Conditions'.

Reconnaissance: Understanding the System



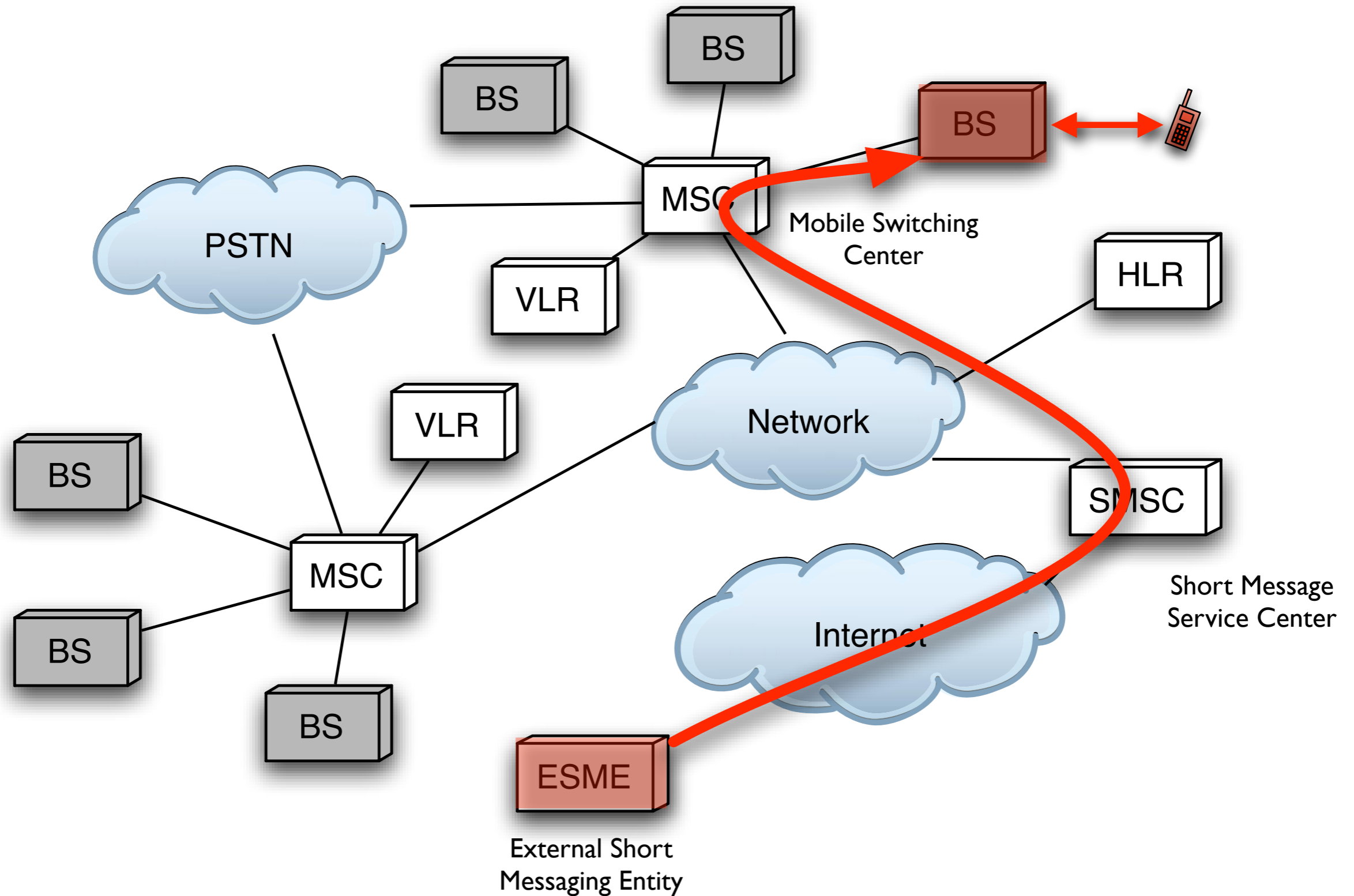
Cellular
Network
?



Telecommunications Vocabulary

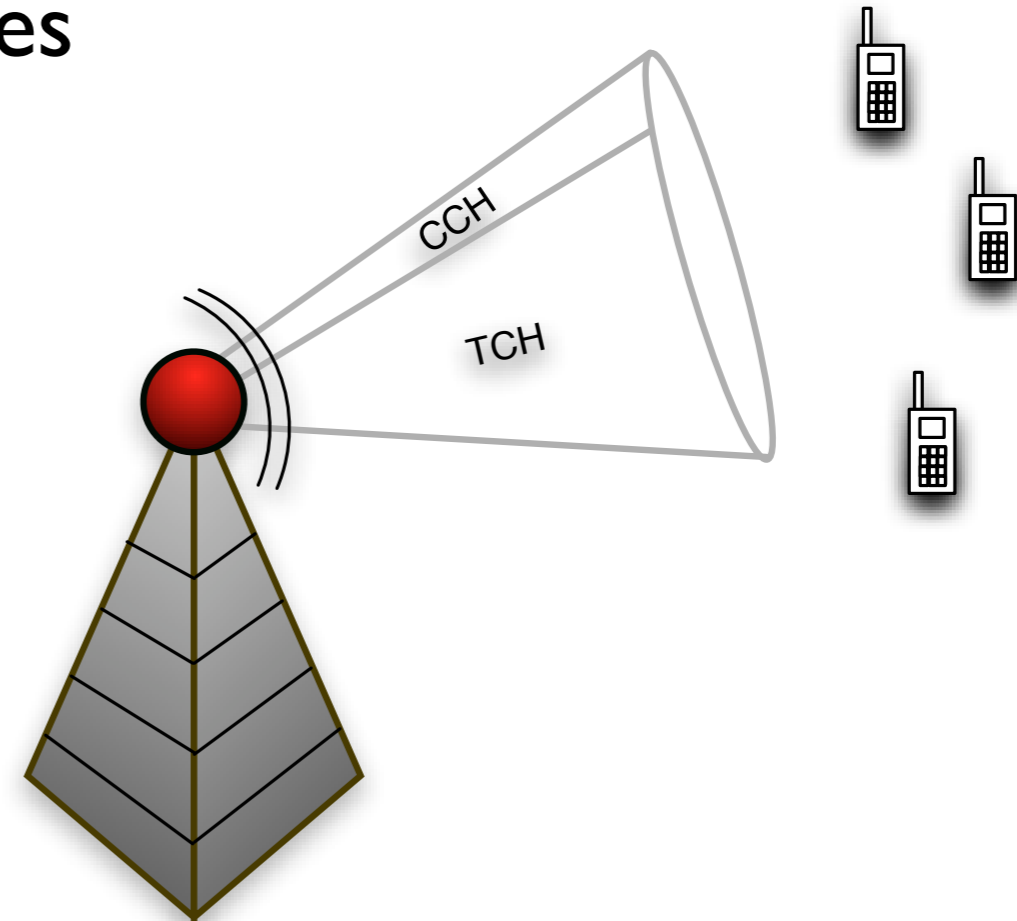
- Signaling System 7 (SS7): The phone network
- POTS: Plain-old telephone service
- Cellular network: Radio network and infrastructure used to support mobile communications (phones)
- Base Station (BS): Cellular towers for wireless delivery
- Channel: A frequency (carrier) over which cell phone communications are transmitted
- Sector: A cell region covered by fixed channels

Overview of SMS Delivery

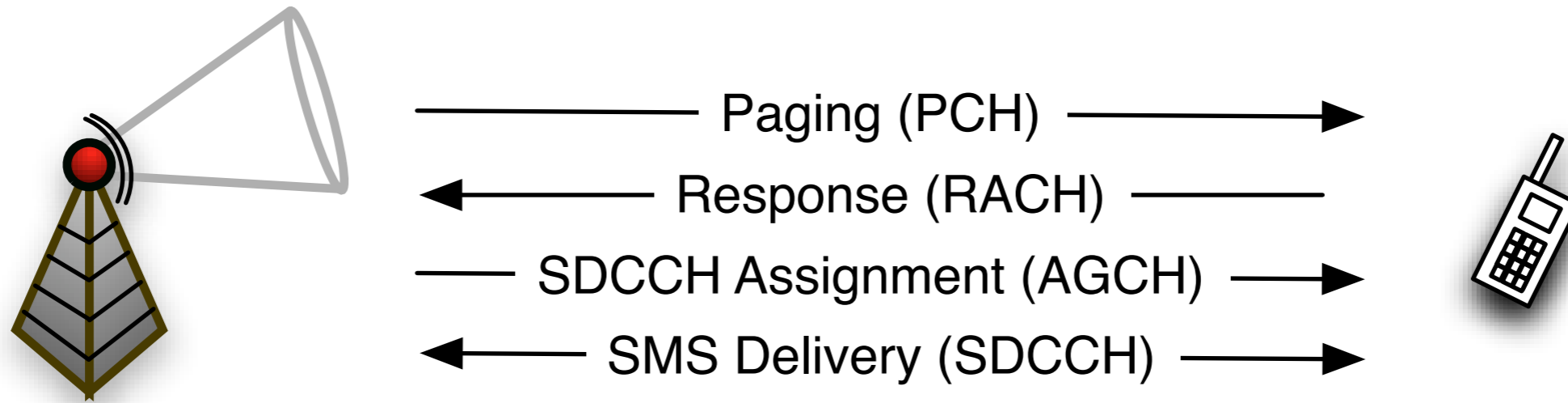


The “air interface”

- Traffic Channels (TCH)
 - ▶ Used to deliver voice traffic to cell phones
- Control Channels (CCH)
 - ▶ Used for signaling between base stations and cell phones
 - ▶ Used to deliver SMS messages



Wireless Delivery of SMS

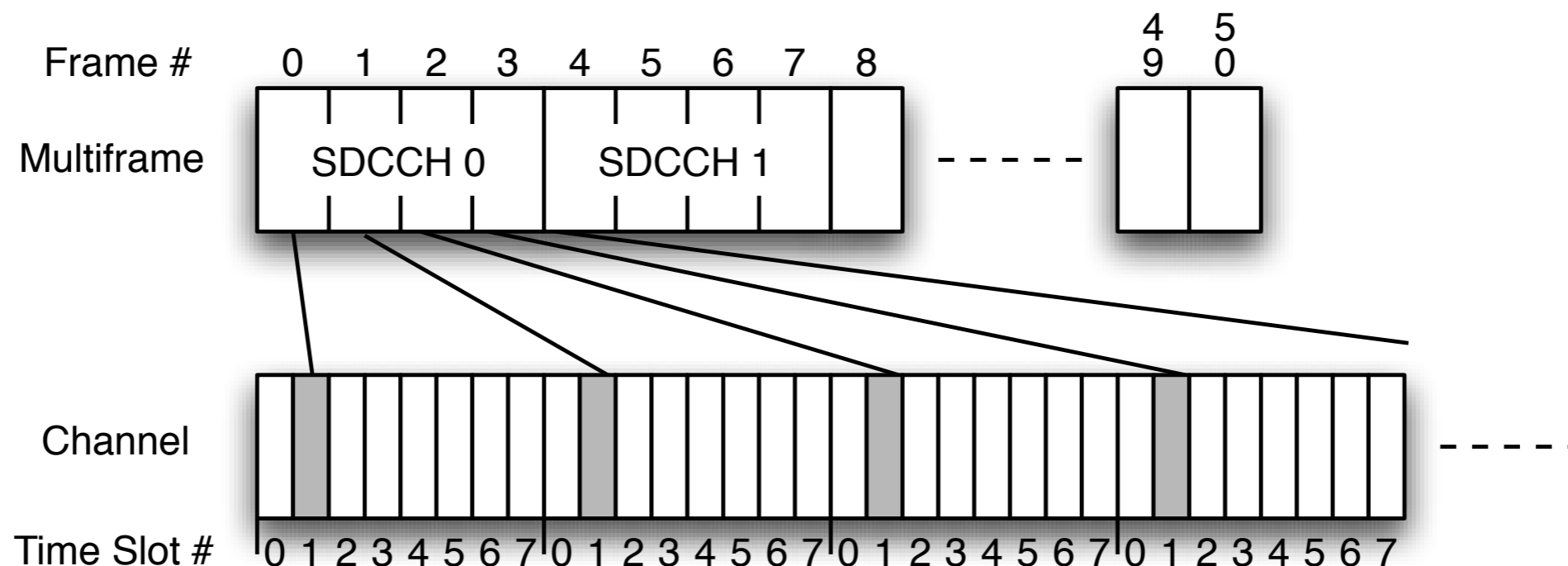


- Once the destination is found, it requests an Standalone Dedicated Control Channel (SDCCH)
- The SDCCH is used to deliver the SMS message
- The SDCCH is also used to setup voice calls

GSM as TDM

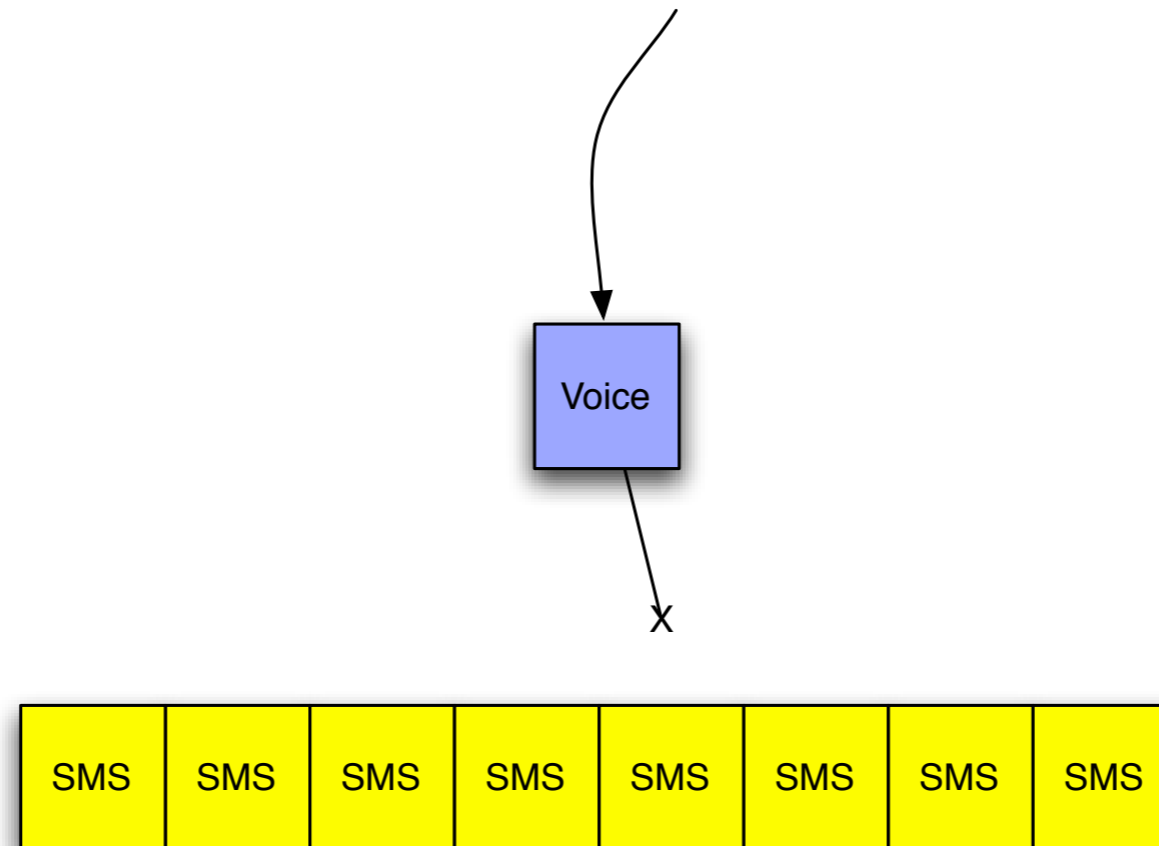
- GSM Analysis

- ▶ Each channel divided into 8 time-slots
 - Each call transmits during its time-slot (TCH)
 - Paging channel (PCH) and SDCCH are embedded in CCH
- ▶ BW: 762 bits/sec (96 bytes) per **SDCCH**
- ▶ Number of SDCCH is $2 * \text{number of channels}$
- ▶ Number of channels averages 2-6 per sector (2/4/8/12/??)



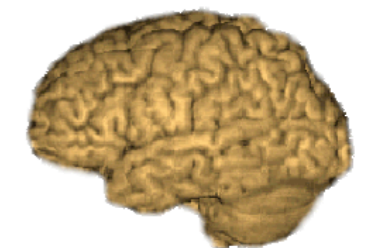
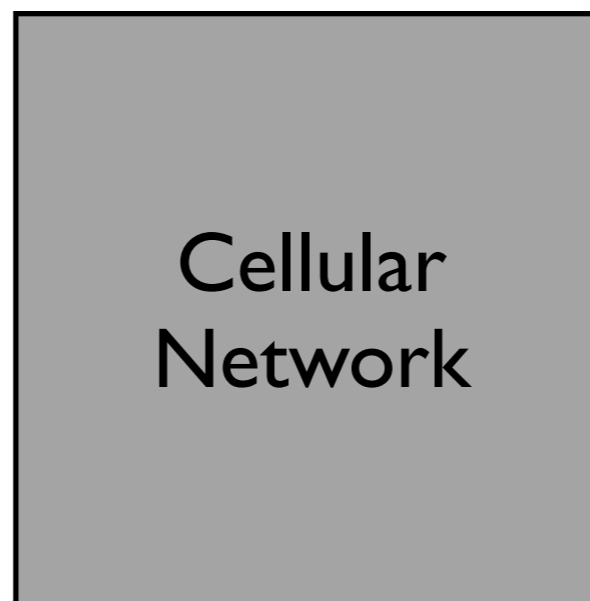
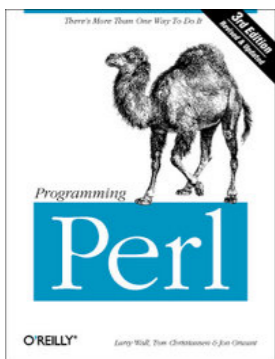
The Vulnerability

- Once you fill up the SDCCH channels with SMS messages, call setup is *blocked*



- So, the goal of the adversary is to fill the cell network with SMS traffic
 - ▶ Not as easy as you might think ...

- Standards documentation only tells half the story
- Open Questions (Implementation Specific)
 - ▶ How are messages stored?
 - ▶ How do injection and delivery rates compare?
 - ▶ What interface limitations currently exist?

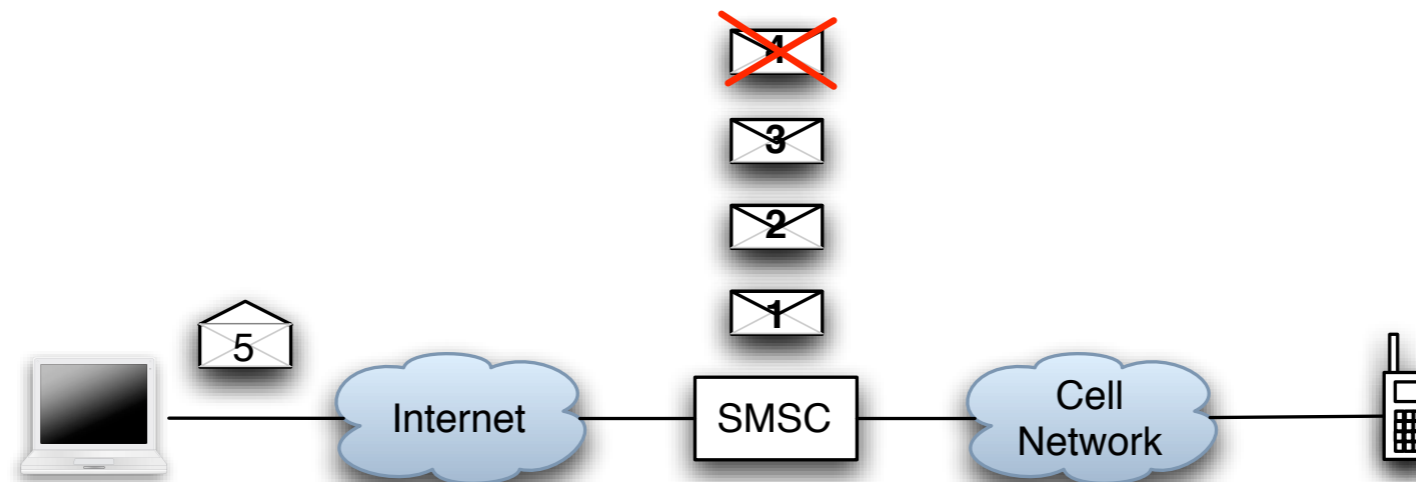


- Methodology
 - ▶ Determine phone capacity by slowly injecting messages while target phone is powered on
 - ▶ Each phone in our sample set displayed the number of new messages
- Result:
 - ▶ Low end phones observed 30-50 message buffers
 - ▶ High end phone drained power before max found (500+)
- Some phones were *incapable* of receiving new messages without user intervention



Delivery Discipline

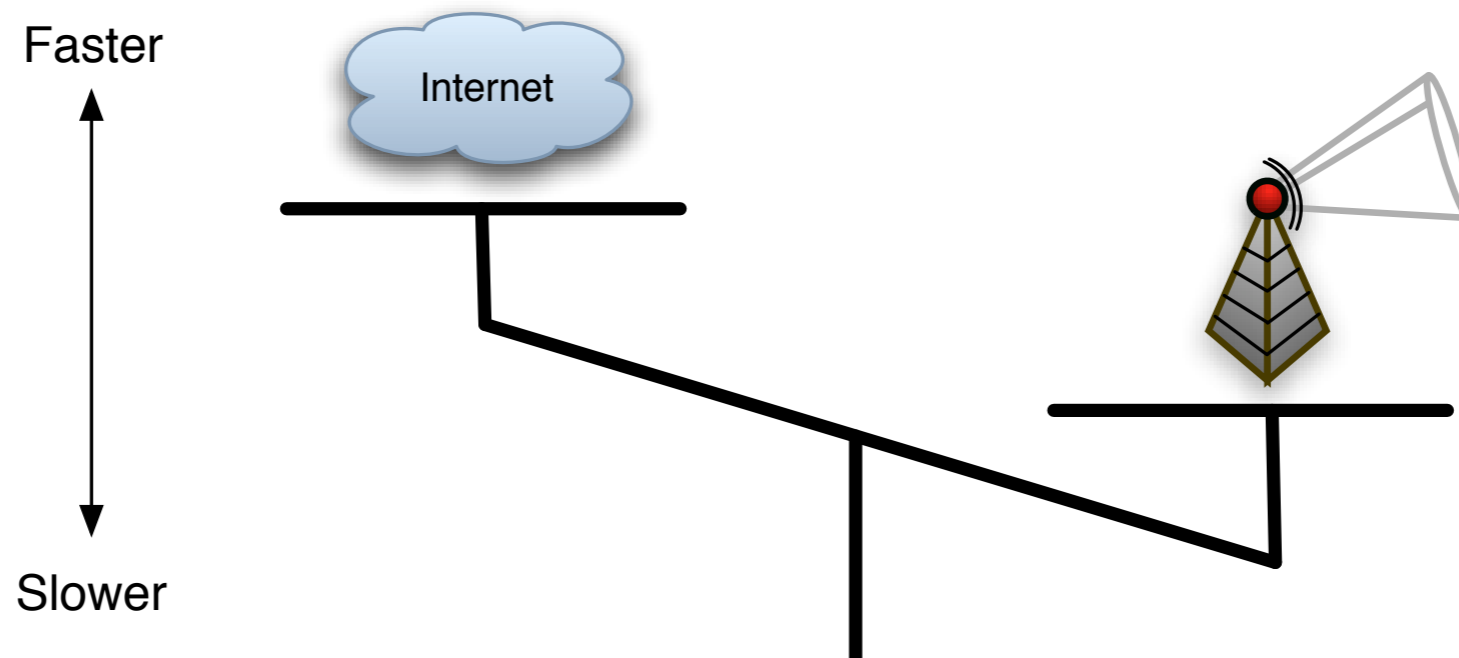
- Methodology
 - ▶ Determine network queueing policy by slowly injecting hundreds of (enumerated) messages while target phone is powered off
 - ▶ Set of received messages indicates both the buffer size and dropping policy for each user at the SMSC
- Result:
 - ▶ Buffer sizes varied by provider (range of 30 to a few hundred)
 - ▶ Message dropping policy (SMSC) also varied (drop-tail and head)



- We caused messages to be *lost*

Injection vs. Delivery Rate

- Methodology
 - ▶ Find a bottleneck by comparing injection and delivery rates
- 7-8 second interarrival times observed on phones
- Experimentally finding maximum injection rate is dangerous
 - ▶ Google found many websites selling bulk SMS sending
 - ▶ Estimate hundreds to thousands of messages can be sent per second

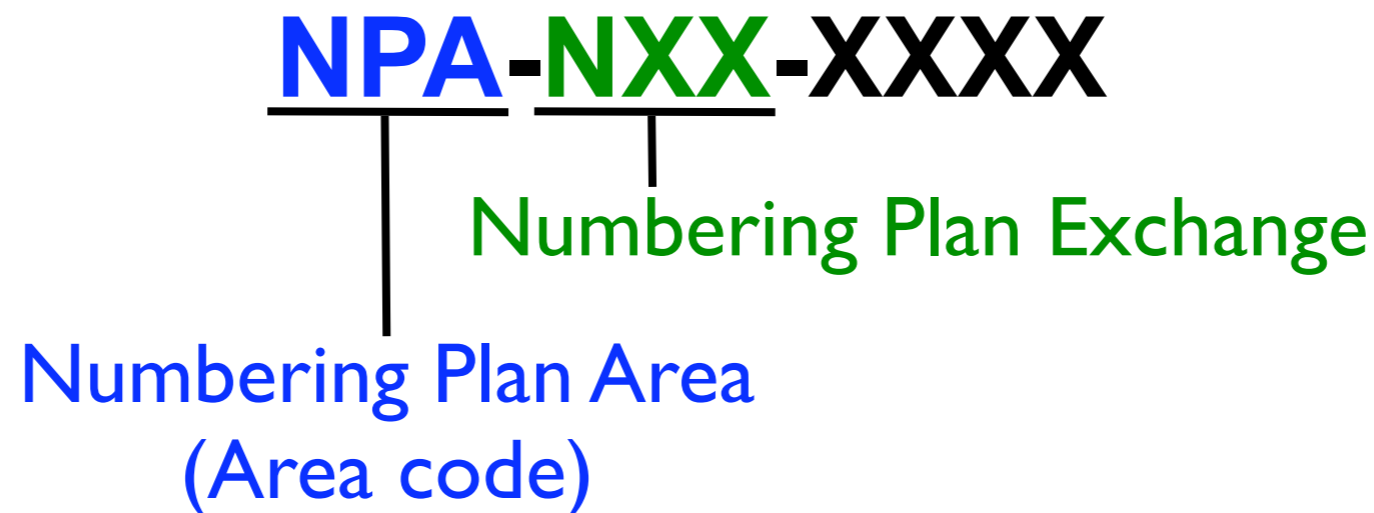


- **Large imbalance** between injection and delivery

- Methodology
 - ▶ Determine limitations on provider web interfaces using automated scripts to inject messages at a moderate rate
 - ▶ Record HTML response to each message sent
- Result:
 - ▶ Rudimentary restrictions (IP-based, Session cookie)
 - ▶ Unable to determine if messages dropped due to SPAM filtering
 - ▶ Bulk senders advertise 30-25 messages per second
 - Multiple bulk senders can be used
- All observed interface regulations are *trivially circumvented*

- Not all messages injected will be delivered
- Messages can be injected orders of magnitude faster than they can be delivered
 - ▶ Delivery time is multiple seconds
- Interfaces have trivial regulations
- **Result:** An attack must be distributed and must target many users

- North American Numbering Plan (NANP)



- ▶ NPA/NXX prefixes are administered by a provider
 - ▶ Phone number mobility may change this a little
 - ▶ Mappings between providers and exchanges publicly documented and available on the web
- *Implication:* An adversary can identify the prefixes used in a target area (e.g., metropolitan area)

Example NPA-NXX

local calling guide: [home](#)

browse: [region](#) | [area code](#) | [LATA](#) search: [area code/prefix](#) | [rate centre](#) | [switch](#) | [telco](#) | [local calling area activity](#) | [dial-around code](#) | [local call finder links](#): [tariffs](#) | [other](#)

Area code/prefix search

Search by area code/prefix (NPA/NXX) or OCN

NPA: NXX: Block: OCN: Region: LATA: Switch: Effective date within past or next days

[New search](#)

- Effective date searches are available only for US area codes. Our sources for non-US NPA-NXX data do not provide this information.
- If you want to search an entire area code regardless of activity, leave both the next and past days fields set to zero.

[How to use this page](#)

NPA: [814](#) [[Rate centres in NPA 814](#)] [[More information about NPA 814](#)]

NXX: [404](#)

NPA-NXX BLOCK	RATE CENTRE	REGION	SWITCH	OCN	LATA	EFF DATE	DISC DATE	MAP
814-404	Bellefonte	PA	JHTWPADPCM2	8392 CELLCO PARTNERSHIP DBA VERIZON WIRELESS - PA	230			

Web Scraping

- Googling for phone numbers
 - ▶ 865 numbers in SC
 - ▶ 7,300 in NYC
 - ▶ 6,184 in DC
 - ▶ ... *in less than 5 seconds*

The screenshot shows a Google search results page in a Safari browser window. The search query is 'cell 201-679-0000...9999'. The page displays several search results, including:

- notary public directory - 123notary.com**: Cell: 201-264-0702. Shaquanda Spivey. Phone: 201-679-5901 Cell: 201-679-5901. Kelly Rosales. Phone: 908-309-8611 Cell: 908-309-8611 ... www.123notary.com/notary-citywide.asp?city=Paterson&state=NJ - 38k - [Cached](#) - [Similar pages](#)
- notary public directory - 123notary.com**: Phone: 201-679-5901 Cell: 201-679-5901. x. Robert Stepko. Phone: 908-687-0670. x. Debbie Sterling. Phone: 609-425-0232 Cell: 609-425-0232 ... www.123notary.com/notary-result.asp?state=NJ&alpha=1&state2=New%20Jersey - 99k - [Cached](#) - [Similar pages](#)
- Certification: Test Locations**: 146 Bethel Rd Warren, New Jersey 07059. Phone: 201-679-7535. gerald@warwickvalleyracquets.com ... Phone: 845-987-8004 Cell: 201-679-7535 Fax: 845-987-8004 ... www.racquettech.com/certification/test_locations.html - 22k - [Cached](#) - [Similar pages](#)
- [PDF] A Conference Captain's List NJTODA 2004-2005 Season # TEAM NAME ...**: File Format: PDF/Adobe Acrobat - [View as HTML](#)
201-852-3704-cell. 201-568-1583-w. Jon Bagos. 201-679-0067-cell. 201-894-. 9701. League Officer Contact Info. CHRIS TEDESCO-PRESIDENT. 201-945-2611-H ... www.planetdarts.com/njtoda/pdf/captainslist20042005.pdf - [Similar pages](#)
- Steven's pge 1**: 2)Aim s/n: Mteverestone1036. 3)Room Extension: 7483. 4)Mailbox: 325 Nason 1999 Burdett Ave Troy NY 12180. 5)Cell phone: 201-679-3728. www.rpi.edu/~linx2/page1.html - 17k - [Cached](#) - [Similar pages](#)
- Real Estate Classifieds**: Bridgitte 212-969-5159 work 201-679-1091 cell (after 7pm). email seller - clip ad - report abuse. n/a, Hoboken, New Jersey · Condominiums ... www.hoobly.com/0/4/20/ - [Similar pages](#)
- Furnished 1/1 condo - Yearly \$1000/ Seasonal \$1500 in 07030 ...**: Monthly (90 days minimum) @ \$1500/ month, (includes utilities) Thank you very much. Bridgitte 212-969-5159 work 201-679-1091 cell (after 7pm) ... www.hoobly.com/0/0/163669.html - [Similar pages](#)
- 7th 8th Grade Girls Schedule 2005**: Team, Name, Title, Email, Home, Cell. Jim Oettinger, Commissioner, closterrecjim@aol.com, 201-679-4272. 1, Brian Beddoe, Head Coach, beddoe@optonline.net ... www.closterboro.com/recreation/schedules/7th8thGradeGirlsTeam1.html - 15k -

Using the SMS interface

- While google may provide a good “hit-list” it is advantageous to create a larger and fresher list
 - ▶ Providers entry points into the SMS are available, e.g., email, web, instant messaging
 - ▶ Almost all provider web interfaces indicate whether the phone number is good or not (not just ability to deliver)
 - ▶ Hence, web interface is an oracle for available phones

Sent At	Tracking ID	Recipient	Status	Date Delivered
N/A	N/A	9999999999	Delivery to this destination failed due to invalid address.	N/A
Sent At	Tracking ID	Recipient	Status	Date Delivered
██████████	████████████████████	██████████████████	Sending your message	NONE

- Determining the capacity of an area is simple with the above observations

$$C = (\text{sectors/area}) * (\text{SDCCHs/sector}) * (\text{throughput/SDCCH})$$

- Note that this is the *capacity* of the system. An attack would be aided by normal traffic
- Model Data
 - ▶ Channel Bandwidth: 3GPP TS 05.01 v8.9.0 (GSM Standard)
 - ▶ City profiles and SMS channel characteristics: National Communications System (NCS) TIB 03-2
 - ▶ City and population profiles: US Census 2000

The Exploit (Metro)

- Capacity = sectors * SDCCH/sector * msgs/hour

	Sectors in Manhattan	SDCCHs per sector	Messages per SDCCH per hour
C	$\approx (55 \text{ sectors})$	$\left(\frac{12 \text{ SDCCH}}{1 \text{ sector}} \right)$	$\left(\frac{900 \text{ msg/hr}}{1 \text{ SDCCH}} \right)$
	$\approx 594,000 \text{ msg/hr}$		
	$\approx 165 \text{ msg/sec}$		

- **165** msgs/sec * 1500 bytes = **1933.6** kb/sec
- Comparison: cable modem \approx **768** kb/sec
- **193.36** on a multi-send interface

- How much bandwidth is needed to prevent access to *all* cell phones in the United States?

$$\begin{aligned} C &\approx \left(\frac{8 \text{ SDCCH}}{1 \text{ sector}} \right) \left(\frac{900 \text{ msg/hr}}{1 \text{ SDCCH}} \right) \left(\frac{1.7595 \text{ sectors}}{1 \text{ mi}^2} \right) \\ &\quad (92,505 \text{ mi}^2) \\ &\approx 1,171,890,342 \text{ msg/hr} \\ &\approx 325,525 \text{ msg/sec} \end{aligned}$$

- About 3.8 Gbps or 2 OC-48s (5.0 Gbps)

- **Solution 1**: separate Internet from cell network
 - ▶ pros: essentially eliminates attacks (from Internet)
 - ▶ cons: infeasible, loss of important functionality
- **Solution 2**: resource over-provisioning
 - ▶ pros: allows a mitigation strategy without re-architecting
 - ▶ cons: costly, just raises the bar on the attackers



The solutions (tomorrow)

- **Solution 3: Queuing**
 - ▶ Separate queues for control vs. SMS
 - ▶ Control messaging should preempt with priority
 - ▶ Cons: complexity?
- **Solution 4: Rate limitation**
 - ▶ Control the aggregate input into a network/sector
 - ▶ Cons: complex to do correctly
- **Solution 5: Next generation networks**
 - ▶ 3G networks will logically separate data and voice
 - ▶ Thus, Internet -based DOS attacks will affect data only
 - ▶ Cons: available when?

- Attacks occur accidentally
 - ▶ “Celebration Messages Overload SMS Network” (Oman)
 - ▶ “Mobile Networks Facing Overload” (Russia)
 - ▶ “Will Success Spoil SMS?” (Europe and Asia)
- In-place tools may prevent trivial exploits
 - ▶ message filtering, Over-provisioning
- Sophisticated adversaries could likely exploit this vulnerability without additional counter-measures
 - ▶ Many possible entry points into the network
 - Zombie networks
 - ▶ Little *network internal* control of SMS messaging
 - Note: Edge solutions are unlikely to be successful

Reality check: SMS Over SS7

- The National Communications System issued a report about the use of SMS messages in times of disaster.
- In this report, everyone with a cellular phone in a major city tried to send text messages at a rate of 1/60 seconds.
- In a conservative estimate, Manhattan would need *100 times* more capacity to meet such a load.



- Short term: reduce number of SMS gateways and regulate input flow into cell phone network
- Remove any feedback on the availability of cell phones or success of message delivery
- Implement an emergency shutdown procedure
 - ▶ Disconnect from Internet during crisis
 - ▶ Only allow emergency services during crisis
- Seek solutions from equipment manufacturers
 - ▶ Separate control traffic from SMS messaging
 - ▶ Advanced cell networks

A cautionary tale ...

- Attaching the Internet to any critical infrastructure is *inherently* dangerous
 - ▶ ... because of the *unintended consequences*
- *Will/have* been felt in other areas
 - ▶ electrical grids
 - ▶ emergency services
 - ▶ banking and finance
 - ▶ and many more ...

Teaching a Lecture

- What was the arc of the Lecture?
- Teaching how to go about vulnerability analysis
 - ▶ Recognition
 - ▶ Reconnaissance (a lot of work, be responsible)
 - ▶ Exploit (beat the bag guys to the punch)
 - ▶ Recovery
- Larger picture

