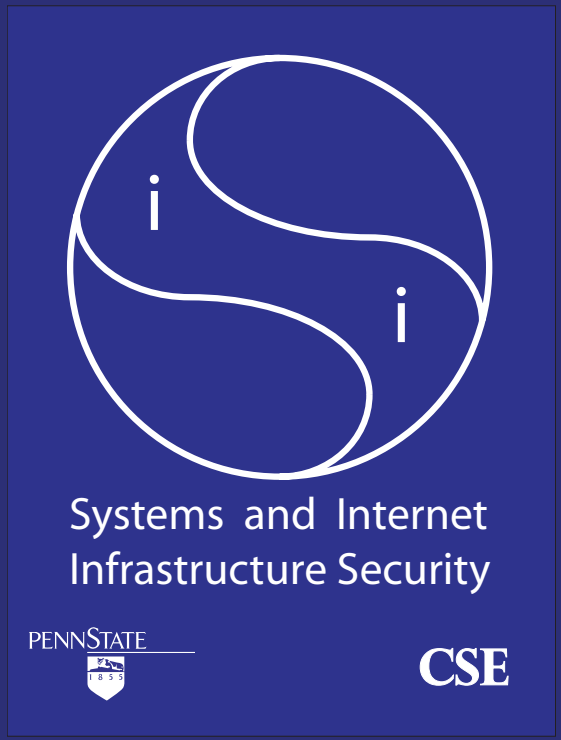
Exploiting Open Functionality in SMS-Capable Cellular Networks



NSRC Industry Day
October 5th, 2005 - State College, PA

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

Unintended Consequences

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

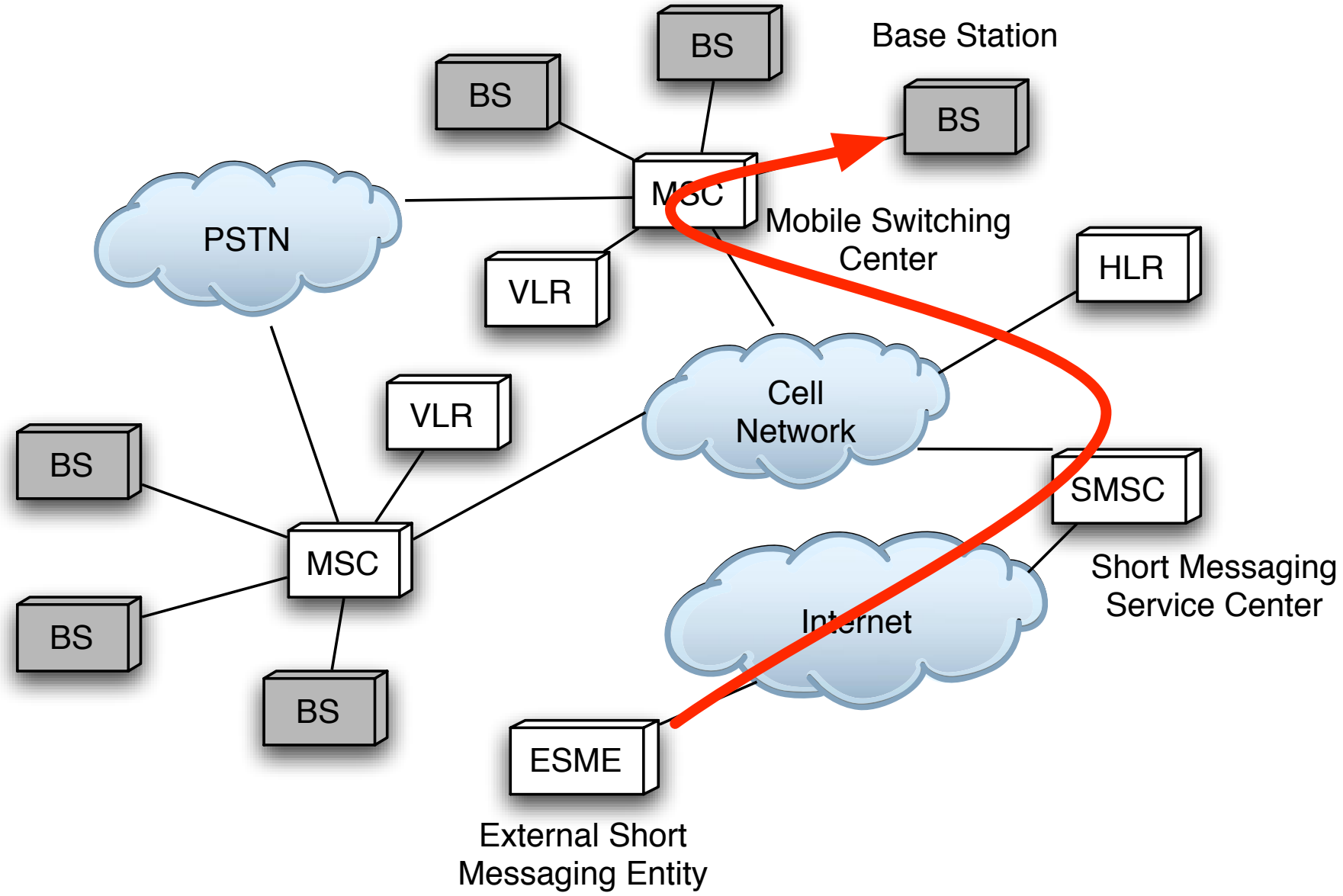
Preventing Large Scale Attacks

- Past truly damaging attacks follow a pattern ...
  - Bad guys find the vulnerability ...
  - Do some work ...
  - Then exploit it ..
  - The exploit evolves in the following way:
    1. *Recognition/discovery*
    2. *Reconnaissance*
    3. *Exploit*
    4. *Recovery/fix*

SMS Messaging

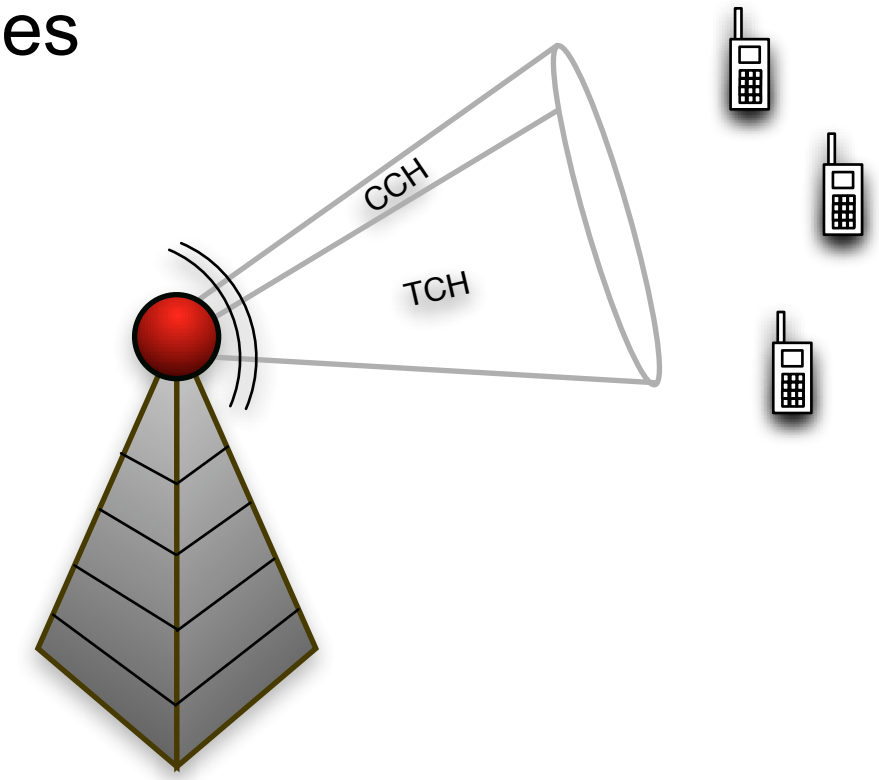
- What is SMS?
  - Allows mobile phones and other devices to send small messages containing text.
  - Extremely popular with younger demographics.
  - Ubiquitous internationally (Europe, Asia)
  - Often used in environments where voice calls are not appropriate or possible.
  - On September 11th, SMS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

SMS message delivery in 30 seconds ...



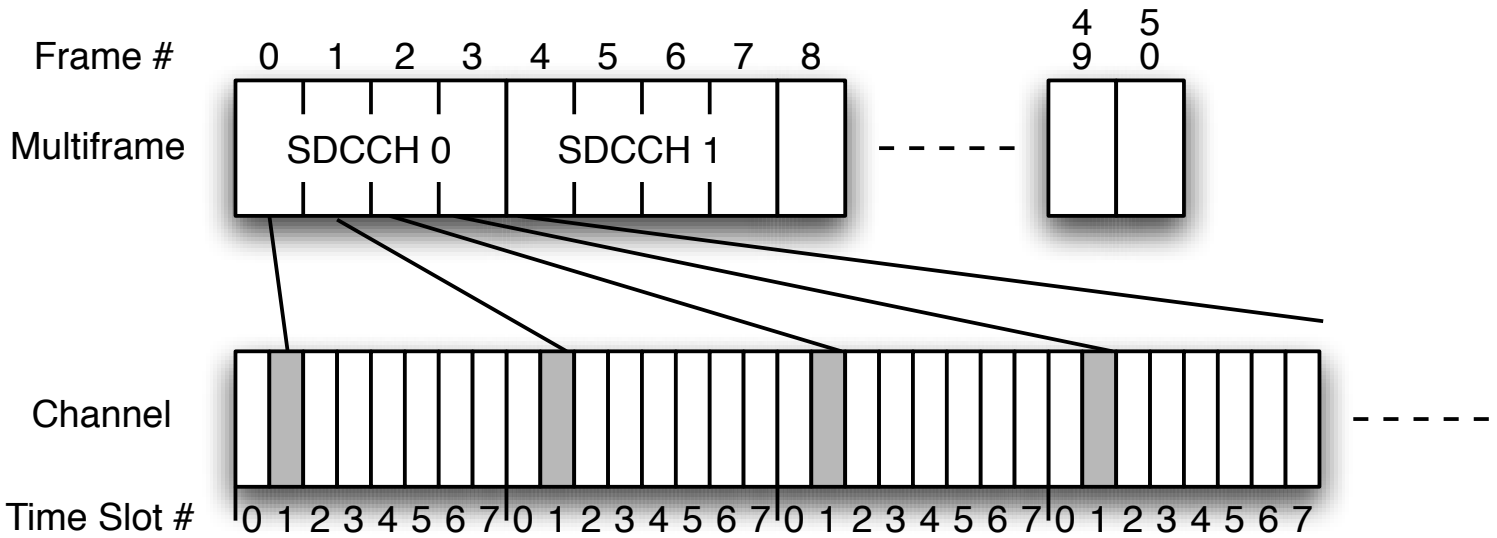
The “air interface”

- Traffic channels (TCH)
  - used to deliver voice traffic to cell phones (yak yak ...)
- Control Channel (CCH)
  - used for signaling between base station and phones
  - used to deliver SMS messages



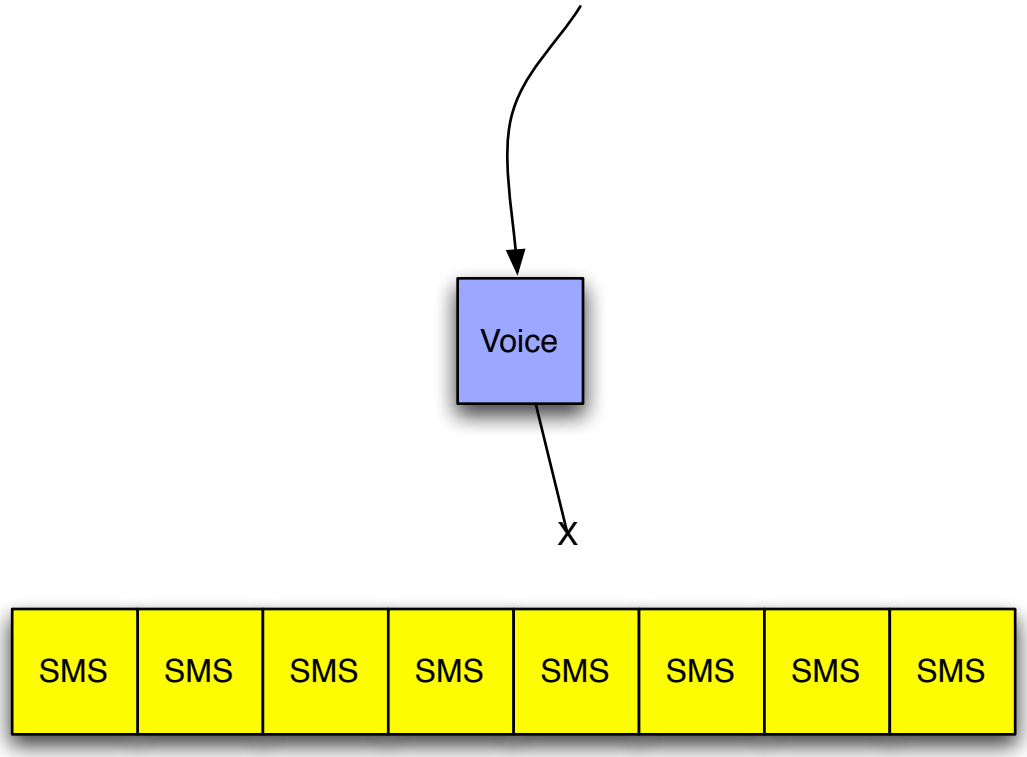
GSM as TDM

- GSM Analysis
  - Each channel divided into 8 slots
  - Each call transmits during its slot
  - BW: 762 bits/sec (96 bytes) per SDCCH
  - Number of SDCCH is 2 * number of channels
  - Number of channels averages 2-6 per sector
-



The vulnerability

- Once you fill the SDCCH channels with SMS traffic, call setup is blocked



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

Reconnaissance

- What does an adversary need to know?
  - How messages are handled in the network?
  - What targets are available in the network?

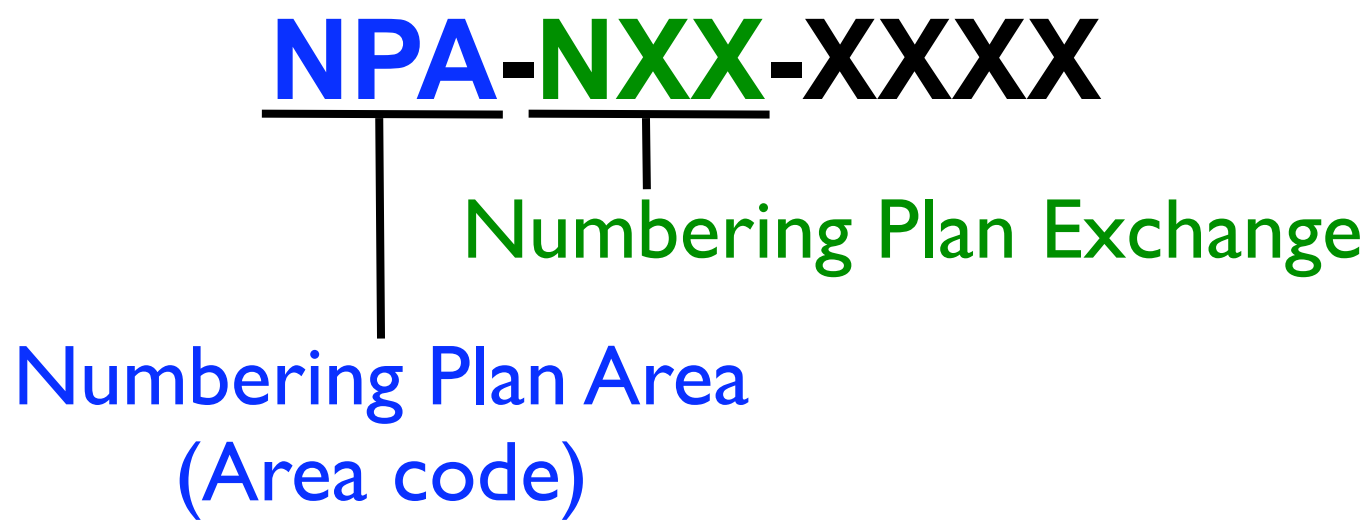
Delivery Discipline

- Details are not specified in the standards documentation
- Messages can be injected faster than received
- How many messages does the network buffer per user?
  - Varied by provider, ranging from 30 to hundreds
- What happens when the buffer is full?
  - One provider ignored new messages
  - Another provider dropped older messages

- An ***effective*** attack must target many users

Finding cell phones ...

- 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)

Web scraping

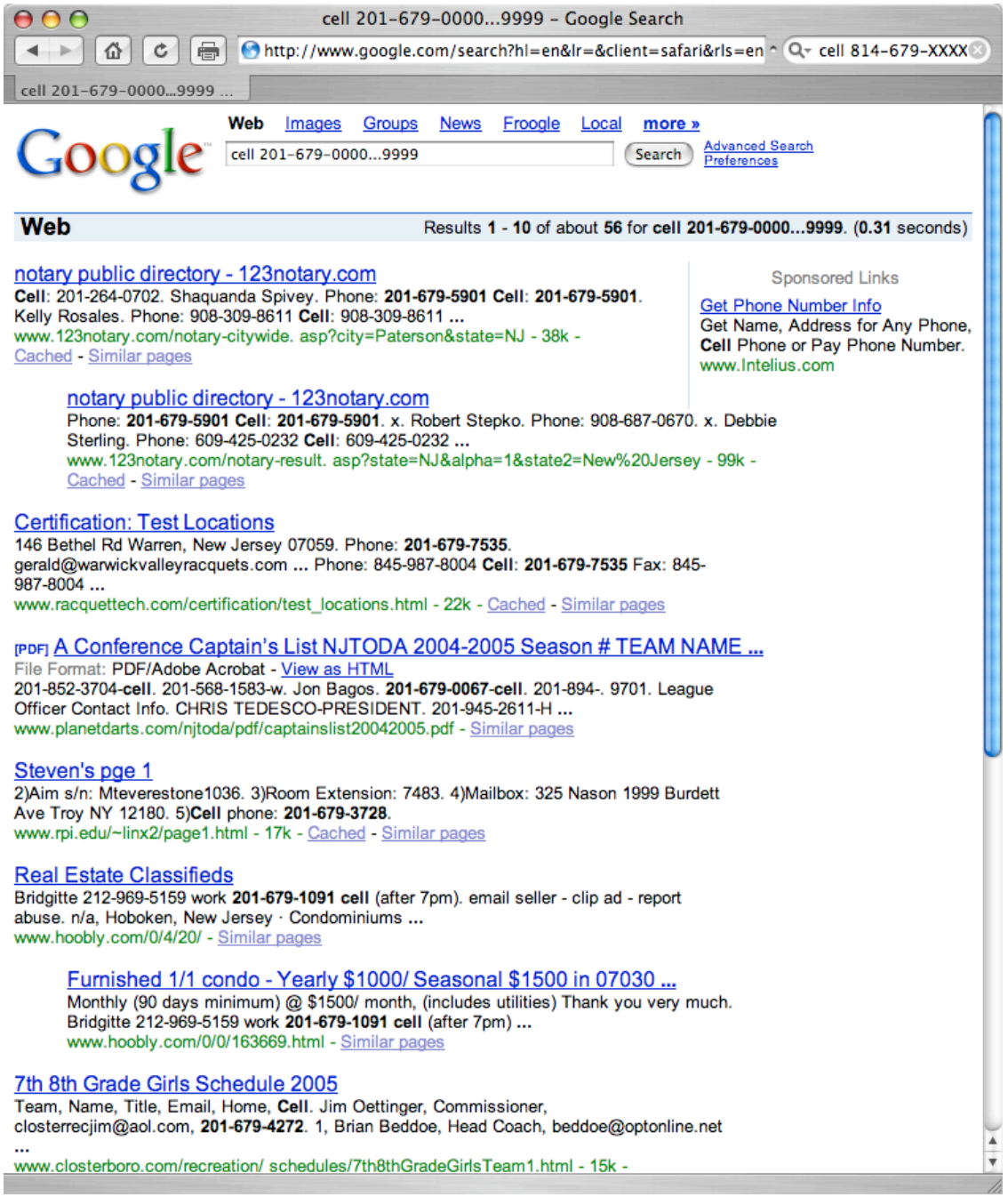
- Googling for phone numbers

  865 numbers in SC

  7,300 in NYC

  6,184 in DC

  ... *in less than 5 seconds*



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
[redacted]	[redacted]	[redacted]	Sending your message	NONE

The Exploit (Metro)

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

Sectors in Manhattan — SDCCHs per sector — Messages per SDCCH per hour

$$C \simeq (55 \text{ sectors}) \left(\frac{12 \text{ SDCCH}}{1 \text{ sector}}\right) \left(\frac{900 \text{ msg/hr}}{1 \text{ SDCCH}}\right)$$
$$\simeq 594,000 \text{ msg/hr}$$
$$\simeq 165 \text{ msg/sec}$$

- **165** msgs/sec * 1500 bytes (max message length) = **1933.6** kb/sec (193.36 on multi-send interface)
- Comparison: cable modem ~= **768** kb/sec
- Data Source: National Communication System NCS TIB 03-2 (SMS over SS7 networks)

Regional Service

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

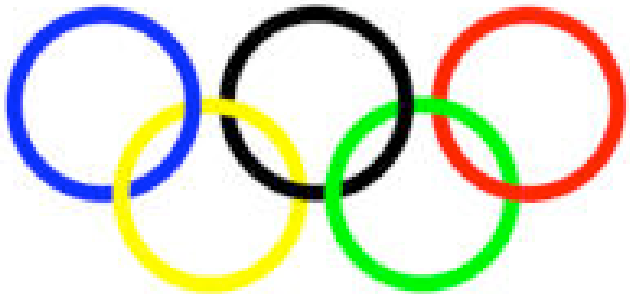
$$
\begin{aligned}
C &\simeq \left(\frac{8\ \text{SDCCH}}{1\ \text{sector}}\right)\left(\frac{900\ \text{msg/hr}}{1\ \text{SDCCH}}\right)\left(\frac{1.7595\ \text{sectors}}{1\ \text{mi}^2}\right) \\
&\quad (92,505\ \text{mi}^2) \\
&\simeq 1,171,890,342\ \text{msg/hr} \\
&\simeq 325,525\ \text{msg/sec}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

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

The solutions (today)

- *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: complex to do correctly
- *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?

The Reality

- What is in place may prevent trivial exploits of the cell phone network
  - SMS messaging 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

Recommendations

- 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 ...

Thank you

More info:

http://www.smsanalysis.org/

http://siis.cse.psu.edu/

Contact: mcdaniel@cse.psu.edu