Lecture 12
Cellular Network Exploits

ENGG5105/CSCI5470 Computer and Network Security

Spring 2014

Patrick P. C. Lee

Motivation

- Mobile Internet access is getting popular with emergence of smartphones and 3G network infrastructures
- Yet, is our cellular network secure enough to maintain the quality of service?

Cellular Network Exploits

- SMS attack on a cellular network core
  - "Exploiting open functionality in SMS-capable cellular networks", Journal of Computer Security, 2008 (conference version in CCS'05)
- Threat Model:
  - Launch denial of service attacks against the entire cellular network core

Short Messaging Service (SMS)

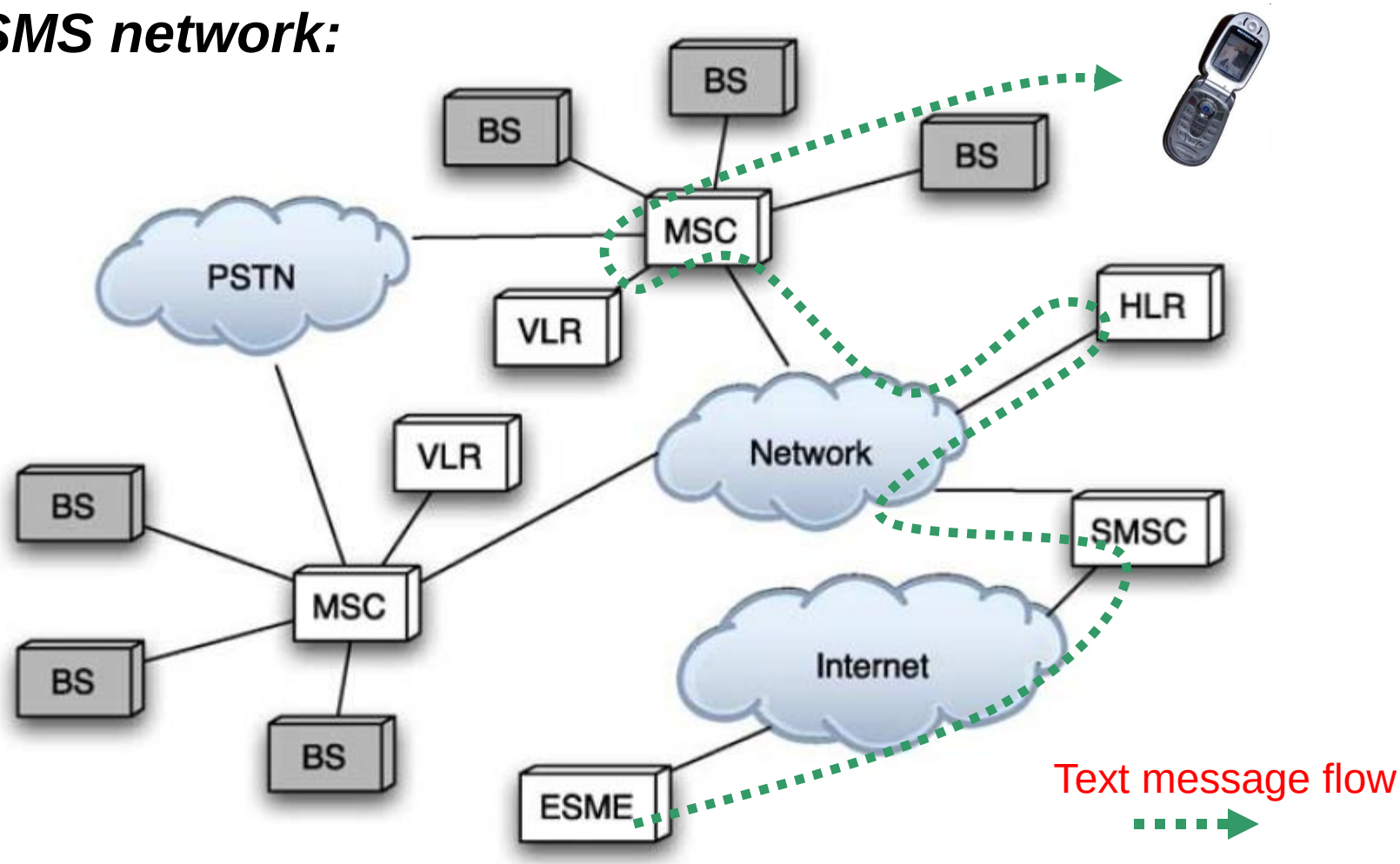
- What is SMS?
  - The text communication service for exchanging **short** text messages between fixed line or mobile phone devices
  - Each text msg. has at most 160 7-bit chars.
  - Very popular
    - In the US, 5 billion messages per month (as of 2005) http://www.usatoday.com/money/2005-07-27-text-messaging_x.htm
    - The volume of SMS messages and the number of active SMS users continue to surge

Internet-Originated SMS

- How to generate a text message?
  - Use a cell phone
  - Through Internet, e.g., service provider website interfaces, email, and applications that include instant messaging
- Such open functionality makes things worse
- **Goal of the paper: to understand the security impact of Internet-originated text messages on the network**

SMS Network Overview

An SMS network:



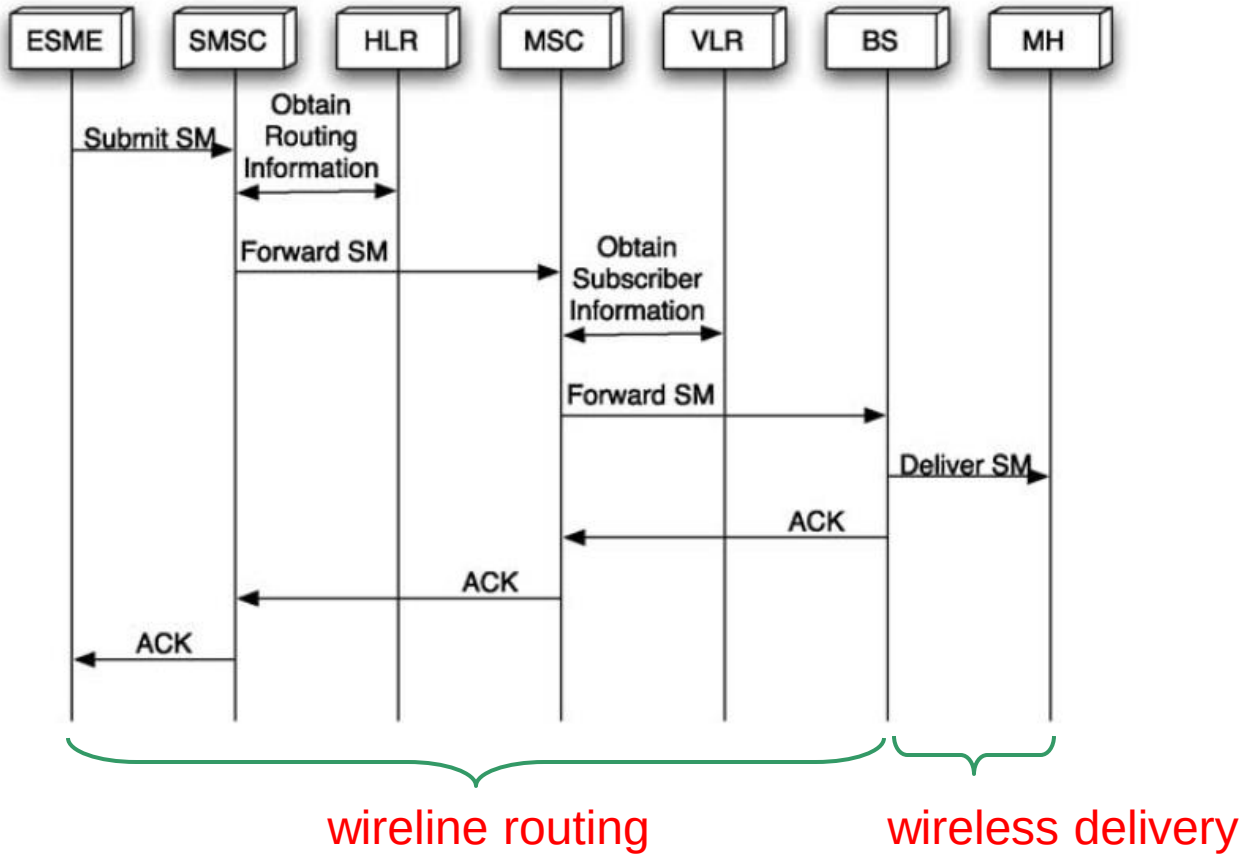
SMS Network Components

- External short message entities (ESMEs) are devices or interfaces (aside from phones) that can generate text messages
  - Examples: email, web portals, voice mail services)
- Short Messaging Service Center (SMSC) handles all SMS traffic and decides how a text message is router
- Home Location Register (HLR), the permanent repository of subscriber information

SMS Network Components

- Mobile Switching Center (MSC) handles call routing, mobile device authentication, location management for base stations, and all handoffs
- Visitor Location Register (VRL) holds information of locally served mobiles
- Base station (BS) connects mobiles over the air interface

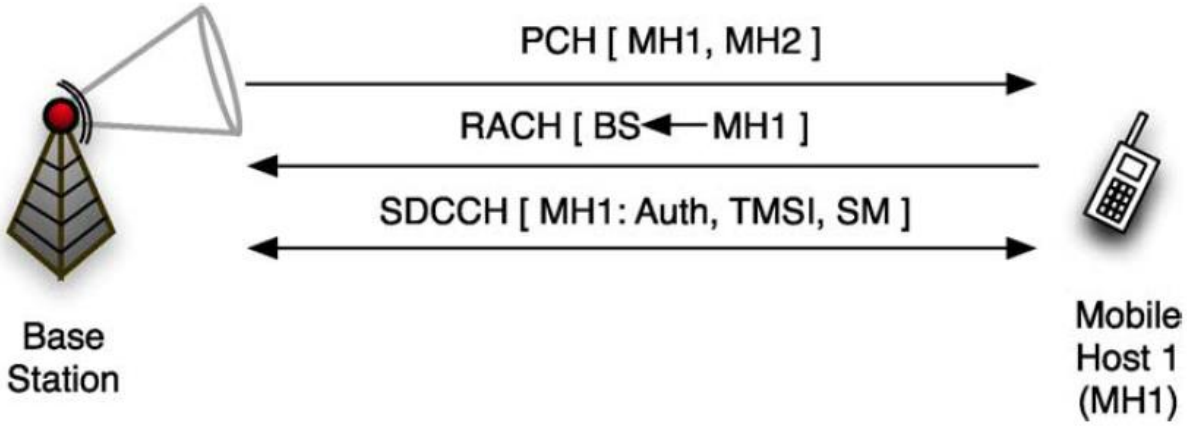
How Text Messages Routed?



Text Delivery over Wireless

- Air interface is divided into:
  - Traffic channels (TCHs)
    - for voice traffic
  - Control channels (CCHs)
    - further divided into common CCH and dedicated CCH
    - for control signaling messages
    - all mobile devices constantly listen to common CCH for voice and SMS signaling

Text Delivery over Wireless



- **PCH**: Paging Channel
- **RACH**: Random Access Channel
- **SDCCH** – Standalone Dedicated Control Channel

- Base station notifies the mobile over PCH that a text message is available, and the mobile responds over RACH
- An SDCCH is set up:
  - an authentication channel is set up between BS and mobile
  - more than one signaling message is sent
  - SMS message is delivered over SSH
  - the setup of a voice call is also carried out over SDCHH

Bottlenecks in Cellular Networks

- Main bottleneck in cellular networks:
  - Air interface
- SMS delivery discipline:
  - SMSCs are the locus of SMS message flow; all message pass through them
  - Each SMSC only holds a finite number of SMS messages
- If the air interface is constantly congested, SMS messages will be dropped at SMSCs

Sending SMS over ESMEs

- To send a 160-byte SMS message, we send a few IP packets
  - user data and ACKs
- Typical IP packet payload to trigger an SMS message is less than 900 bytes
- Let's assume the worst case 1500 bytes

A brief sampling of SMS access services

Service	URL
Instant Messaging	
AOL IM	mymobile.aol.com/portal/index.html
ICQ	www.icq.com/sms/
MSN Messenger	mobile.msn.com
Yahoo Messenger	messenger.yahoo.com/messenger/wireless/
Information Services	
CNN	www.cnn.com/togo/
Google	sms.google.com
MSNBC	net.msnbc.com/tools/alert/sub.aspx
Bulk SMS	
Clickatell	www.clickatell.com
SimpleWire	www.simplewire.com/services/smpp/
START Corp.	www.startcorp.com/StartcorpX/Mobile_Developer.aspx

Finding a Phone to Send SMS

- Hit-list creation:
  - In the US, phone formatting follows a North America Number Plan (NANP)
    - NPA-NXX-XXXX
      - NPA/NXX – prefix administered by single service provider
      - E.g., 814-876-XXXX is owned by AT&T Wireless in Pennsylvania state
  - Web scraping
    - Just search for the phone numbers on Google

Overloading Air Interface

- But each SMS message has a very small size (160 bytes), how do we congest the air interface easily?
- We actually exploit the SMS **control plane**, not the data plane

Overloading Air Interface

- To deliver a single text message, the SDCCH will do many things:
  - carry out authentication with the mobile
  - enable encryption over the air
  - deliver a fresh TMSI (Temporary Mobile Subscriber ID) for identifying the mobile
  - deliver the SMS message
- Each SDCCH is commonly held by an individual session for between **4 to 5 seconds**

Overloading Air Interface

- The air interface is a shared medium and only allows a finite number of SDCCHs at one time
- Each sector (i.e., cell region) can support 8 to 12 SDCCHs
- A metropolitan area typically has ~100 sectors

Overloading Air Interface

- Find the SDCHH capacity of an area:

C = (# sectors) * (# SDCCHs per sector) * (message rate per SDCHH)

- Consider Washington DC, with ~120 sectors
  - let 8 SDCCHs per sector
  - ~900 messages / hour (each msg needs 4s)

$$C \approx (120 \text{ sectors}) \left(\frac{8 \text{ SDCCH}}{1 \text{ sector}} \right) \left(\frac{900 \text{ msgs/h}}{1 \text{ SDCCH}} \right)$$

$$\approx 864{,}000 \text{ msgs/h}$$

$$\approx 240 \text{ msgs/s}.$$

Putting It All Together

- To launch a DoS attack from the Internet, required upload bandwidth is
  1500 bytes * 240 msg/s ~ 2.8Mbps
  - well supported with today's home broadband

Putting in All Together

- The attack should target multiple phones
  - Each phone has a buffer for text messages (from 30 to 500 messages)
  - If a phone exhausts its buffer, it stops receiving text messages, and no SDCHH will be set up
- If an attacker creates a hit list of 2500 phone numbers, just send a text message to each phone every 10.4 seconds
  - Make the attack last longer before each phone exhausts its buffer to store the text messages
  - If a phone holds 50 msgs, attack duration ~ 8.7min

Impact of the Attack

- Messages are lost due to overflow of buffers
- Messages are delayed longer than shelf-life
- Users miss important messages due to influx of attack messages
- Voice calls are also blocked, since SDCCHs are also used to set up voice calls
- Mobile phone batteries may be depleted as well with text messages

Potential Defense

- Suggested defense solutions:
  - Eliminating Internet-originated text messages
    - This could cause a big loss of revenue to service providers. Not realistic
  - Separation of voice and data
  - Resource provisioning
  - Rate limitation
- See paper for their pros and cons