Exploiting Open Functionality in SMS-Capable Networks

William Enck, Patrick Traynor, Patrick McDaniel, and Thomas La Porta
Systems and Internet Infrastructure Security Laboratory
Department of Computer Science and Engineering
The Pennsylvania State University

Your host today: Stuart Saltzman

Agenda

- Overview of research paper
  - SMS/Cellular Network overview
    - Submitting a message
    - Routing
    - Delivery
  - SMS/Cellular Vulnerability Analysis
  - Modeling DOS Attacks
  - Solution(s)

Overview & Introduction

Cellular Overview

- Cellular networks are critical component to economic and social infrastructures
- Cellular networks deliver alphanumeric text messages via Short Messaging Service (SMS)
- Telecommunication companies offer connections between their networks and the internet
  - Open functionality creates negative consequences

Goal of Paper

- To evaluate the security impact of SMS interface on the availability of the cellular phone network
- Demonstrate the ability to deny voice service to cities the size of Washington, D.C. and Manhattan
- Provide countermeasures that mitigate or eliminate DoS threats

SMS/Cellular Network (GSM)

- Two methods to send a text message
  - 1) via another mobile device
  - 2) through an External Short Messaging Entities (ESME)
    - Email
    - Web-bases messaging portals
    - Paging systems
    - Software
Submitting a Message

- All messages delivered to a server that handles SMS traffic known as the Short Messaging Service Center (SMSC)
  - Provider (Verizon, AT&T, etc.) MUST provide at least SMSC
- If necessary, the message is converted to SMS format
  - Example: internet originated message. Once formatted, the message becomes indistinguishable from there original originator
- Queued in SMSC for forwarding

Routing

- Home Location Register (HLR)
  - Queried by the SMSC for message routing
  - Permanent repository of user data
    - Subscriber information (call waiting, text messaging)
    - Billing data
    - Availability of targeted user
  - Determines routing information for the destination device

Routing (cont.)

- If SMSC receives a reply stating that the current user is unavailable, it stores the text message for later delivery
  - It is queued
- Otherwise, HLR responds with address of Mobile Switching Center (MSC) providing service to user/device

Routing – Mobile Switching Center

- MSC
  - Responsible for mobile device authentication
  - Location management for attached Base Stations (BS)
  - Act as gateways to Public Switched Telephone Network (PSTN)
    - Queries Visitor Location Register (VLR)
      - Local copy of the targeted devices information when away from its HLR
    - Forwards text message on to the appropriate base station for transmission over the air interface

Routing Figure

Delivery

- Air Interface
  - 1) Control Channels (CCH)
    - A) Common CCH
      - Logical channels:
        1) Paging Channel (PCH)
        2) Random Access Channel (RACH)
      - Used by base station (BS) to initiate the delivery of voice and SMS data
      - All connected mobile devices are constantly listening to the Common CCH for voice and SMS signaling
    - B) Dedicated CCHs
    - 2) Traffic Channels (TCH)
**SMS Delivery Diagram**

1. Base Station (BS) sends a message on the Paging channel (PCH) containing the Temporary Mobile Subscriber ID (TMSI).
2. Network uses the TMSI instead of the targeted devices phone number in order to thwart eavesdroppers.

**SMS Delivery Diagram (cont.)**

3. Devices contact BS over the Random Access Channel (RACH) and alert the network of its availability to receive incoming call or text data.
4. Response (from above) arrives at BS, the BS instructs the targeted device to listen to a specific Standalone Dedicated Control Channel (SDCCH).

**Delivery Discipline - Analysis**

- **Goal**: Find delivery discipline for each provider.
- Study the flow of the message.
- Standards documentation provides the framework from which the system is built, but it lacks implementation specific details.
- SMSC are the locus of all SMS message flow.
- SMSC queues only a finite number of messages per a user.
  - Message is held until:
    - Target device successfully receives it.
    - It is dropped (buffer capacity, eviction policy).

**Delivery Discipline - Results**

- **AT&T's**:
  - Buffered the entire 400 messages (160 bytes each = 62.4kB).
- **Verizon**:
  - Last 100 messages received (first 300 missing).
  - Buffer of 100, FIFO eviction policy.
- **Sprint**:
  - First 30 messages received.
  - Buffer of 30, LIFO eviction policy.
Delivery Rate - Analysis

Definition: the speed at which a collection of nodes can process and forward a message

Goal: Find bottlenecks - compare injection rates with delivery rates

Exact number of SMSCs in a network is not publicly known or discoverable

Delivery Rate - Results

- Verizon & AT&T: 7-8 seconds for delivery
- Sprint: Unknown
- Conclusion: imbalance between the time to submit and the time to receive
- SMS message size - Maximum: 160 bytes
- Using TcpDump:
  - HTTP Post and IP headers = approximately 700 bytes to send SMS message (not considering TCP overhead)
  - Web page upload sizes:
    - Verizon: 1600 bytes
    - Spring: 1300 bytes
    - AT&T: 1100 bytes
  - Email submission:
    - All emails less than 500 bytes to send

Interfaces - Analysis

- Lost messages and negatively acknowledged submit attempts were observed
- Believe it was a result of web interface limitations imposed by the service providers
- Goal: find the mechanism used to achieve rate limitation on these interfaces and the conditions necessary to activate them
- Experiment - used delivery rate analysis:
  - Verizon:
    - After 64 messages, negative acknowledgements resulted
    - Blocked messages by subnet value
  - AT&T:
    - Blindly acknowledged all submissions, but stopped delivering after 50 messages sent to single phone
    - Subnet value did not matter
    - Differentiated between its inputs
- Conclusion:
  - SMSC's typically hold far more messages than the mobile devices
  - To launch successfully DoS attack that exploits the limitations of the cellular air interface, an adversary must target multiple end devices (must have valid phone numbers)
The ability to launch a successful assault on a mobile phone network requires the attacker to do more than simply attempt to send text messages to every possible phone number. The North American Numbering Plan (NANP) created a number format, "NPA/NXX-XXXX". This format includes a number plan area, exchange code, and terminal number. Traditionally, terminal numbers were administered by a single service provider. Example: 814-876-XXXX => AT&T Wireless; 814-404-XXXX => Sprint PCS. The numbering system is very useful for an attacker as it reduces the size of the domain.

November 24, 2004, number portability went into effect, allowing numbers to be reallocated to other service providers.

Technique commonly used by spammers to collect information on potential targets through the use of search engines and scripting tools. An individual is able to gather mobile phone numbers. Example: Google search.

- 865 unique numbers from the greater State College, PA region
- 7,308 from New York City
- 6,184 from Washington D.C.

Downside - numbers might not be active.

All major wireless service providers offer a website interface through which anyone can at no charge to the sender submit a SMS message. The web user is given acknowledgement when submitting the SMS message.

Question: How many SMS messages are needed to induce saturation?

Air interface overview needed to understand SMS saturation.
Voice call establishment is very similar to SMS delivery, except a Traffic Channel (TCH) is allocated for voice traffic at the completion of control signaling. Voice and SMS traffic do NOT compete for TCHs which are held for significantly longer periods of time.

BOTH voice and SMS traffic use the same channels for session establishment, thus contention for these limited resources still occur!

Given enough SMS messages, the channels needed for session establishment will become saturated, thus preventing voice traffic in a given area.

Air Interface Overview

- 4 carriers, each a single frame
- First time slot of the first carrier is the Common CCH
- Second time slot of the first channel is reserved for SDCH connections
- Capacity for 8 users is allocated over the use of a multiframe
- Remaining timeslots across all carriers are designated for voice data

Air Interface Overview

- 8 timeslots = 1 frame = 4.65ms transmission
- 1 timeslot is assigned to a user who receives full control of the channel
- User assigned to a given TCH is able to transmit voice data once per a frame

Air Interface Overview

- 160 byte text message, the 160 byte text message, the
- multiframe cycle time of 235.36 ms => multiframe cycle time of 235.36 ms => 782 bps
- up to 900 SMS sessions per hour on each SDCH

Air Interface Overview

- Bandwidth is limited within frame, therefore data must span over multiple frames => multiframe => typically 51 frames
- Timeslot 1 from each frame in a multiframe creates the logical SDCH channel
- Within a single multiframe, up to 8 users can receive SDCH access

Air Interface - Bottleneck

- Each SDCH spans four logically consecutive timeslots in a multiframe
- Bandwidth: With 184 bits per a control channel unit and a multiframe cycle time of 235.36 ms => 762 bps
- Given authentication, TMSI renewal, encryption, and the 160 byte text message, the SDCH is held by an individual session for 4-5 seconds
- Results: Service time translates into the ability to handle up to 900 SMS sessions per hour on each SDCH

- PCH is used to signal each incoming call and text message, its commitment to each session is limited to the transmission of a TMSI
- TCHs remain occupied for the duration of a call which averages minutes
- SDCH is occupied for a number of seconds per session establishment (typical 4 seconds)
  - This SDCH channel becomes the bottleneck!
  - Must find/understand the bandwidth of the bottleneck
Air Interface – Bottleneck

Calculations – Example A

- Study from National Communications System (NCS)
  - Washington D.C. has 40 cellular towers
  - 68.2 sq miles
  - 120 total sectors
    - Each sector 0.5 to 0.75 sq. miles
    - Each sector has 8 SDCCHs
- **FIND**: Total number of messages per second needed to saturate the SDCCH capacity $C$ in Washington D.C.

- **900 msg/hr** from service time translation
  - \[ C \approx (120 \text{ sectors}) \left( \frac{8 \text{ SDCCH}}{1 \text{ sector}} \right) \left( \frac{900 \text{ msgs/hr}}{1 \text{ SDCCH}} \right) \]
  - \[ C \approx 894,000 \text{ msgs/hr} \]
  - \[ C \approx 240 \text{ msgs/sec} \]

- **240 messages** a second will saturate the SDCCH channel

Air Interface – Bottleneck

Calculations – Example B

- Study from National Communications System (NCS)
  - Manhattan
  - 31.1 sq miles
  - 55 total sectors
    - Each sector 0.5 to 0.75 sq. miles
    - Each sector has 12 SDCCHs
- **FIND**: Total number of messages per second needed to saturate the SDCCH capacity $C$ in Manhattan

- **900 msg/hr** from service time translation (previous step)
  - \[ C \approx (55 \text{ sectors}) \left( \frac{12 \text{ SDCCH}}{1 \text{ sector}} \right) \left( \frac{900 \text{ msg/hr}}{1 \text{ SDCCH}} \right) \]
  - \[ C \approx 504,000 \text{ msg/hr} \]
  - \[ C \approx 165 \text{ msg/sec} \]

- **165 messages** a second will saturate the SDCCH channel

Air Interface – Bottleneck

Calculations Results

- Use a source transmission size of 1500 bytes described in the Delivery Discipline section to submit an SMS from the internet
- Table shows the bandwidth required to saturate the control channels and thus incapacitate legitimate voice and text messaging services
Air Interface – Bottleneck

**Conclusion**

- Due to the analysis and the results from the delivery discipline and delivery rate sections, sending that many messages to a small number of recipients would degrade the effectiveness of any attack.
  - Phones buffers would reach capacity.
  - Undeliverable messages would be buffered on the network until user allocated space was exhausted.
  - Accounts could possibly be disabled temporarily.
- Hit-lists would prevent individual phones from reaching capacity and below possible service provider thresholds.
- Is it possible?

3/26/08

---

Air Interface DoS Attack

**Attack A**

- To saturate Washington DC:
  - Assumptions:
    - Washington D.C. has 572,000 people.
    - 60% wireless penetration.
    - 8 SDCCHs.
    - All devices powered on.
    - 50% of Washington D.C. use the same service provider.
  - Result:
    - An even distribution of messages would be 5.04 messages to each phone per an hour (1 message every 11.92 minutes).

3/26/08

---

Air Interface DoS Attack

**Attack B**

- Same assumptions from attack A, except:
  - Hit-list of 2500 phone numbers.
  - Phone buffer size: 50.
- Results:
  - An even distribution of messages would deliver a message every 10.4 seconds.
  - Attack would last 8.68 minutes before buffer was exhausted.
  - Previous bandwidth table shows these attacks are feasible from a standard high-speed internet connection.

3/26/08

---

Air Interface DoS Attack

**Prevention/Solution**

- Current mechanism are NOT adequate to protect these networks.
- Proven practicality of address spoofing or distributed attacks via zombie networks makes the use of authentication based upon source IP addresses an ineffective solution.
- Due to service provider earnings ($) from SMS messages, they are unlikely to restrict access to SMS messaging.

3/26/08

---

Air Interface DoS Attack

**Prevention/Solution (Cont.)**

- Separation of Voice and Data:
  - Most effective solution would be to separate all voice and data communications.
  - Insertion of data into cellular networks will no longer degrade the fidelity of voice services.
  - Dedicating a carrier on the air interface for data signaling and delivery eliminates an attacker’s ability to take down voice communications.
  - Ineffective use of the spectrum.
  - Creates bottleneck on air interface.
  - Until the offloading schemes are created, origin priority should be implemented.
  - Internet originated messages = low priority.
  - Messages from inside network = high priority.
  - Messages from within network = high priority.

- Temporary Solutions:
  - Additional Mobile Switching Centers (MSC) and Base Stations (BS).
  - Events such as the Olympics.
  - Cellular-on-Wheels (COW) (United States).
  - The increased number of handoffs puts more strain on the network.

3/26/08
Air Interface DoS Attack Solutions

- Rate Limitation
  - Within the air interface, the number of SDCCS channels allowed to deliver text messages should be restricted
  - Attack still successful, but it would only affect a small number of people
  - Slows the rate of legitimate messages can be delivered
  - Prevent hit-lists
  - Do NOT show successfulness of internet based submission
  - Web interfaces should limit the number of recipients to which a single SMS submission is sent
  - Verizon and Cingular allow 10 recipients per a submission
  - Reduce the ability to automate submission
    - Force the computer to calculate some algorithm prior to submitting
    - Close web interfaces
    - Not likely

Conclusion

- Cellular networks are a critical part of the economic and social infrastructures
- Systems typically experience below 300 seconds of communication outages per year ("five nines" availability)
- The proliferation of external services on these networks introduces significant potential for misuse
- An adversary injecting messages from the internet can cause almost twice the yearly expected network downtime using hit-lists as few as 2,500 targets
- The service providers potential problems outlined in this paper must be addressed in order to preserve the usability of these critical services