Open Functionality in SMS
Cellular Networks

Johns Hopkins University
September 25, 2006 - Baltimore, MD
Patrick McDaniel, William Enck, Patrick Traynor, and Thomas La Porta
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
    • also observed anecdotally during recent hurricanes
  • Can be delivered via *Internet*
    • Web-pages (provider websites)
    • Email, IM, ...
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
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
    - *not* originally designed for SMS
Call Setup/SMS Delivery

SDCCH (Stand-alone Dedicated Control Channel)
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 * number of channels
  - Number of channels averages 2-6 per sector (2/4/8/12/??)
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: Gray-box Testing

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

• 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 queuing policy by slowly injecting hundreds of (enumerated) messages while target phone is powered off
  • Set of received messages indicates both the buffer size and eviction policy for each user at the SMSC

• Result:
  • Buffer sizes varied by provider (range of 30 to a few hundred)
  • Message eviction policy also varied (FIFO and LIFO observed)

• 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
Interface Regulation

• Methodology
  • Determine limitations on provider web interfaces using automated scripts to inject messages at a moderate rate
  • Recorded 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 30-35 messages per second
    • Some SMSC advertise up to 20,000 message/sec
    • Multiple bulk senders can be used

• All observed interface regulations are trivially circumvented
Gray-box Testing Summary

- 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 mass insertion countermeasures

**Result**: An attack must be distributed and must target many users
Reconnaissance: Finding cell phones ...

- North American Numbering Plan (NANP)

\[
\text{NPA-} \underline{\text{NXX}} - \underline{\text{XXXX}}
\]

Numbering Plan Area
(Area code)

Numbering Plan Exchange

- 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

<table>
<thead>
<tr>
<th>Sent At</th>
<th>Tracking ID</th>
<th>Recipient</th>
<th>Status</th>
<th>Date Delivered</th>
</tr>
</thead>
<tbody>
<tr>
<td>N/A</td>
<td>N/A</td>
<td>999999999</td>
<td>Delivery to this destination failed due to invalid address.</td>
<td>N/A</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Sent At</th>
<th>Tracking ID</th>
<th>Recipient</th>
<th>Status</th>
<th>Date Delivered</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td>Sending your message</td>
<td>NONE</td>
</tr>
</tbody>
</table>
Exploit: Area Capacity

• Determining the capacity of an area is simple with the above observations.

\[ C = \left( \frac{\text{sectors}}{\text{area}} \right) \times \left( \frac{\text{SDCCHs}}{\text{sector}} \right) \times \left( \frac{\text{throughput}}{\text{SDCCH}} \right) \]

• 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

<table>
<thead>
<tr>
<th>Sectors in Manhattan</th>
<th>SDCCHs per sector</th>
<th>Messages per SDCCH per hour</th>
</tr>
</thead>
<tbody>
<tr>
<td>55 sectors</td>
<td>12 SDCCH</td>
<td>900 msgs/hr</td>
</tr>
<tr>
<td></td>
<td>1 sector</td>
<td>1 SDCCH</td>
</tr>
<tr>
<td>C ≈</td>
<td></td>
<td></td>
</tr>
<tr>
<td>594,000 msg/hr</td>
<td></td>
<td></td>
</tr>
<tr>
<td>165 msg/sec</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

- 165 msgs/sec * 1500 bytes (max message length) = 1933.6 kb/sec
- Comparison: cable modem ~ = 768 kb/sec
- 193.36 on multi-send interface
- What happens when we have broadcast SMS?
How much bandwidth is needed to prevent access to all cell phones in the United States?

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

About 3.8 Gbps or 2 OC-48s (5.0 Gbps)
Recovery/Fix: 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?
Network Characterization

- To better understand such attacks, we assume a Poisson interarrival rate for SMS messages.
- Using 495 messages/second, we achieve a blocking rate of 71%. (validation of previous result)
• We apply Weighted Fair Queueing (WFQ) and Weighted Random Early Discard (WRED) as mitigation techniques.

• Both techniques maintain voice services but shed the vast majority of incoming SMS messages.
Resource Provisioning

- Dynamic Resource Provisioning (DRP) reclaims traffic channels to alleviate control contention.
- Direct Channel Allocation (DCA) allows calls to perform signaling directly on traffic channels.
The Reality

- 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
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 ...
Systems and Internet Infrastructure Laboratory

Prof. Patrick McDaniel, *co-director* (mcdaniel@cse.psu.edu)

- network security, security modeling, critical infrastructure, security-typed languages, formal security policy

Prof. Trent Jaeger, *co-director* (tjaeger@cse.psu.edu)

- operating systems security, policy design and analysis, source code analysis

Prof. Sencun Zhu (szhu@cse.psu.edu)

- ad hoc and sensor networks, buffer-overflow and worm detection, p2p security

Prof. Adam Smith (01/07)

- cryptography, applied cryptography, information science, theoretical computer science

Lead graduate student: P. Traynor (PhD - 2008)

**Funding:**

- National Science Foundation
- Army Research Office/DOD
- CISCO
- Motorola (SERC)
- Raytheon
- IBM
- AT&T, ...

**Ongoing Projects:**

- Hardware system security
- Secure Storage Systems
- Language Based Security
- Secure Linux and Virtual Machines
- Telecommunications Security
- Self-healing Sensor Networks

**Students (10 PhD, 10 MS):** K. Butler (PhD - 2008), W. Enck (PhD - 2009), Fr. B. Hicks (PhD - 2006), H. Hsu (PhD - 2007), L. Johansen (PhD - 2008), S. Rodriguez (PhD 2010), L. St. Clair (PhD - 2010), X. Wang (PhD - 2009), Y. Yang (PhD - 2009), L. Xie (PhD - 2009),

**Factoids:** Established September 2004 -- Location - 344 IST Building -- Contact siislab@cse.psu.edu

**URL:** http://siis.cse.psu.edu
Thank you

Source Publications:


• Online References:
  
  http://www.smsanalysis.org/
  
  http://siis.cse.psu.edu/

Contact: mcdaniel@cse.psu.edu