CSE 543 - Computer Security (Fall 2006)

Lecture 25 - Cellular Network Security
Guest Lecturer: William Enck
November 30, 2006
URL: http://www.cse.psu.edu/~tjaeger/cse543-f06
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, ...
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
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?

Cellular Network
Gray-box Testing Summary

- Individual phones are only capable of accepting so many messages.
  - Low end devices: ~30-50 messages
  - High end devices: 500+ (battery drain)
- Messages can be injected orders of magnitude faster than they can be delivered
  - Delivery time is multiple seconds
- Interfaces have trivial mass insertion countermeasures
  - Address-based authentication, bulk senders, etc

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

- North American Numbering Plan (NANP)

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

- 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>9999999999</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/1 sector</td>
<td>900 msg/hr</td>
</tr>
</tbody>
</table>

\[ C \approx (55 \text{ sectors}) \left( \frac{12 \text{ SDCCH}}{1 \text{ sector}} \right) \left( \frac{900 \text{ msg/hr}}{1 \text{ SDCCH}} \right) \]

\[ \approx 594,000 \text{ msg/hr} \]

\[ \approx 165 \text{ msg/sec} \]

- **165** msgs/sec * 1500 bytes (max message length) = **1933.6** kb/sec

- Comparison: cable modem \( \approx = 768 \) kb/sec

- **193.36** on multi-send interface

- What happens when we have broadcast SMS?
Regional Service

- 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: 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?
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 ...