DDoS for your Cell Networks

Benjamin Mood
Contents

• Opening
• SMS paths
• Vulnerability Analysis
• The attack
• Mitigation
• Can this still be done (or still as “easy” to do)?
Imagine...

• Imagine one day you want to talk on the phone
  • And you can’t place a call
  • And no one can place a call
  • Or text
Imagine... (cont.)

• This was the attack reported in *Exploiting Open Functionality in SMS Capable Cellular Networks*
Term Define

- **DDoS** – Distributed Denial of Service
  - From multiple platforms, this attack attempt to use enough resources of a given service to prevent legitimate business from taking place.
- **Cell** – Place between three towers with three towers at different corners. Typically represented as a hexagon
- **Sector** – How a cell is divided. Typically 3 per cell but could be more or less.
  - (Directional)
Network Structure

• We focus on GSM and not CDMA networks but the existence of the bottlenecks should be similar
SMS structure

• Why do we care?
  • Find a bottleneck to attack
Cell Networks - sms

- Sms paths
  - Two starting blocks
    A. From phones
    B. From ESME (External Short Messaging Entities)
External Short Messaging Entities

• Include web forms or various sorts, different devices, and from email

• From the ESME the sms is sent to the SMSC (Short Messaging Service Center)
Short Messaging Service Center

- At the SMSC the message is converted to the SMS format.
- Each Service Provider has their own SMSC.
- SMSC then looks at a database which knows where the phones are and the status of the phones called Home Location Registration.
- If the sms can be delivered the SMSC delivers them to the MSC (Mobile Switching Center).
Mobile Switching Center

• Notes which base station the message should be delivered too for the phone to receive the sms.
• Sends queries to multiple base stations to find the phone
Wireless Transmissions

- Two types of Channels, Control Channels (CCH) and Transmission Channels (TCH).

- CCH is divided into Paging Channels (PCH) and Random Access Channels (RACH).
Actual Communications

- When a phone hears its ID on the paging channel, it responds on a RACH.
- The rest of the communication then takes place on a Standalone Dedicated Control Channel (SDCCH)
  - Including the encryption and SMS messages.
Vulnerability Analysis

- Buffers of carriers for overflow or off phones are different sizes, handle the overflow differently, and return messages at different rates.
- The send rate and the receiving rate on the phone were different.
  - This demonstrated a bottleneck existed.
- Estimated several hundred to several thousand messages per second per computer.
- Bulk SMS exists if an attacker can pay for it.
- Lots of ESME. The paper had a relatively small list.
Vulnerability (cont.)

- Takes under 1500 bytes to send 160 byte SMS message from the computer.
- Some limitations were observed over web EMSE.
  - When sending at 1 message per second:
    - After 44 messages verizon blocked the senders IP
    - After 50 messages AT&T was also observed to block by IP
- Based on results, the target for this attack must be during transmission to the phone.
  - I.e. the phone is the bottleneck somehow. (more on this later)
Hit Lists

• Find phone numbers of a given network that are ready to be used for the attack
• The way phone numbers work (with an area code) greatly reduces the space to try to find mobile phones.
• Can use scripting to gather phones much like emails
• Upon searching for phone numbers like the paper suggested I came across:
  • www.007numbers.com/###/###/1/
  • Supposedly lists all cell phone numbers in service in a given range
    • (did not have my number)
• Only way to really verify a phone number for a given provider is to send a message and get an acknowledgement.
  • Like what the carriers do on their websites for phones that are in their network
    • (I tested Verizon yesterday)
• So far we have a cell phone listing and a way to determine who the provider is with high accuracy
• Or use a worm to gather information from a computer
More About Bottlenecks

• Given enough SMS messages, the control channels have been saturated.
• Each base station has a finite number of controls channels
  • When this limit is exceeded it stops working as it should.
• Each channel is divided into eight timeslots. For a given timeslot a user has complete access to the channel.
• More specifically, 4.615 ms per sample. In a phone conversation this gives the illusion of constant communication even though the conversation is only sampled.
Bottlenecks (cont.)

• The SDDCH can be a bottleneck since for each connection it might be taken for 4 to 5 seconds per user.
• This means 900 SMS sessions per hour on each SDDCH.
  • Typically twice as many SDDCHs as carriers in the area.
    • 1 SDDCH per 3 or 4 voice channels.
Capacity

• Capacity of a area is = Sectors * SDCCH * 900

• For Washington D.C.
  • 120 * 8 * 900 messages per hour
  • 240 messages/second

• for Manhattan
  • 55 * 12 * 900 messages per hour
  • 165 messages/second

• Observations, thoughts?
Attack

• Since there are limits per phone, the only logical recourse is to use lots of phones.

• Assuming 50% of users had the same provider, sending a message to each phone ever 11.92 minutes would suffice.
  • Assuming 25% of users had the same provider, sending a message every 5.96 minutes would work

• What if we don’t have all the numbers?
  • Assuming 2500 phones were know, the attack could go on for 8 minutes before the buffers overflowed
Attack (cont.)

- What about a large scale attack on the United States urban areas?
  - Apx 92,505 mi$^2$ area
  - Apx 1.7595 sectors per mile
  - Which is $1.7595 \times 92,505 \times 900$
    - Or 325,525 messages per second
    - Or 3.8 Gbps of bandwidth
Prevention

• As noted, the largest counter measure was rate limitation
  • Also, as was pointed out, this is an annoyance, not a blocker of the attack after some thought is put into it

  Including:
  block by IP after 50 messages
  filter “spam” messages

Why don’t these work?

Suggested:
  Eliminate Internet based texts
  Separate voice and data
  Better resource provisioning
  Rate Limitation
The second paper

- *Mitigating Attacks on Open Functionality in SMS-Capable Cellular Networks*
  - Mentioned some mitigation techniques

- Any ideas?
Current solutions

• Still rate limitation
• Spam detection
  • However using messages from the terms of service prevented this from working.
Mitigation Techniques

• Improving the way message queues are handled
  • Give voice priority or messages.
  • Dropping messages when the queue is full
    • But then we lose some good messages
    • Solution is to drop based on content

• Resource provisioning
  • Give voice some dedicated resources over messages
    • (or only give SMS some SDDCH channels to use)
  • Or give resources dynamically when needed
  • Or by separate channels for voice and messages that do not interfere with each other
Can rate limiting work?

- Would putting a limit on the number of messages a given network can process at the SMSCs?
Other attack mentioned

- DDos from cell phones themselves
Can this still be done?

- Is the cell phone network still connected to the internet?
- Closed System
Let's see how....

- There are several pieces to a possible attack
  - A. Can we make a script to automate through web forms?
    - More precisely, has anything been done to prevent this?
  - B. Can we enter into the phone network some other way?
    - Is there any other holes
      - Such as email
My Observations

• Most of the ESME web forms have some form of question (be it enter the text or answer a math problem)
• Sprint appears to have some rate limiting on its text by email service
  • When sending multiple emails at the same time only one is actually gets to the phone (where same time > 15 seconds and less then 30)
  • Unless you send from multiple email accounts, in which case it works

• Bulk senders still exist if you want to pay for it
Conclusion

• It can probably happen