A Novel Detection Mechanism for SMS Attacks on Cellular Network
Eun Kyoung Kim, Thomas La Porta

In cellular network, SMS message traffic shares the control channels (CCHs) with call traffic. Abnormal increase of SMS traffic results in high occupancy of the control channels causing high call blocking rate. Therefore, detecting any malicious attempts to deplete the channel resource by extremely high SMS traffic is very important.

However, it is not trivial to distinguish malicious SMS attack from benign bursty traffic created by legitimate requests since they induce very similar phenomena in cellular network even though they need to be treated differently. We propose a novel detection mechanism that distinguishes malicious SMS attack from benign bursty traffic to quickly discard malicious requests while continuing to serve legitimate ones.

### Network/SMS Characteristics

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Average value</th>
<th>Distribution</th>
</tr>
</thead>
<tbody>
<tr>
<td>Normal traffic arrival rate</td>
<td>0.7 msg/sec</td>
<td>Poisson</td>
</tr>
<tr>
<td>Holding time at CCH</td>
<td>4 sec.</td>
<td>Exponential</td>
</tr>
<tr>
<td>Response time from the recipient</td>
<td>60 sec.</td>
<td>Pareto</td>
</tr>
<tr>
<td>Thread length</td>
<td>5 msg.</td>
<td>Exponential</td>
</tr>
<tr>
<td>Thread duration</td>
<td>8 min.</td>
<td>Exponential</td>
</tr>
</tbody>
</table>

Table 1. Message- and thread-level SMS characteristics

It is observed that a normal SMS thread consists of a series of five messages on average. That means a normal SMS is supposed to have a reply with a high probability, while an attack message typically cannot expect a high reply rate.

### Detection Algorithm

/* Forming message threads for all incoming messages */
for each message M observed in W do
  if M is an outgoing message from L to R then
    if T = (R, L) exists then
      Increase R by 1
    else
      Create T = (R, L)
      Increase R by 1
  end if
  if M is an incoming message from R to L then
    if T = (R, L) exists then
      if M is delivered to L then
        Increase R by 1
      else
        if M is delivered to L then
          Mark R as malicious
        end if
      end if
    end if
  end if
end for

/* Setting response rate threshold */
\[ \tau_r = \frac{1 - B_{avg}}{\rho} \]

/* Updating attack-likelihood score for each remote host according to its response rate and marking it as malicious once if its score exceeds the score threshold */
for each remote host R do
  if R send or receive a message then
    if \( R_\mathrm{rr} < \tau_r \) then
      \( R_\mathrm{c} += 1 \)
    else
      \( R_\mathrm{c} = \max\{R_\mathrm{c} - 1, 0\} \)
    end if
    if \( R_\mathrm{c} > \tau_c \) then
      Mark R as malicious
    end if
  end if
end for
Delete M

M : SMS messages collected during one time window W
L : local handsets
R : remote hosts
T : message threads represented by a pair of (sender, receiver)
R_s : the number of sent messages from R
R_r : the number of replied messages to R
R_\mathrm{rr} : the score representing the likelihood that R is an attacker
B_{avg} : average blocking rate during W
\tau_c : attack-likelihood score threshold for identifying the attack
\tau_r : response rate threshold to determine the likelihood score
\rho : times for which we regard the missing responses as normal

We set \( \tau_r \) to the probability that an outbound message can get a response divided by \( \rho \) and set \( \tau_c \) to a constant, 2.

### Simulation Results

We simulated one hour long SMS attacks which consist of evenly mixed traffic of benign and malicious messages or merely attack traffic, with 50 or 1950 compromised handsets among total 2000 handsets with varying attack intensity. One time window is 1 minute long.

Figure 2. Cumulative number of true positives
Figure 3. False positive rate and false negative rate

(1) 50 compromised handsets, 4 times intensity, mixed traffic
(2) 1950 compromised handsets, 4 times intensity, mixed traffic

Sponsored By National Science Foundation