Taking Over Telecom Networks

Hardik Mehta
(@hardw00t)
Loay Abdelrazek
(@sigploit)
Press Release: some highlights

- SS7 Attacks to Hack Phone, WhatsApp to Read Messages 2018
- Real-World SS7 Attack — Hackers Are Stealing Money From Bank Accounts
- Bank Account Hackers Used SS7 to Intercept Security Codes
- T-Mobile Hacked — 2 Million Customers' Personal Data Stolen

Taking Over Telecom Networks - Hardik Mehta (@hardw00t) and Loay Abdelrazek (@sigploit)
## Glossary

<table>
<thead>
<tr>
<th>Acronyms</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Operator</td>
<td>Telecom service provider</td>
</tr>
<tr>
<td>Subscriber</td>
<td>A user using the services of the telecom operator</td>
</tr>
<tr>
<td>SS7</td>
<td>Signalling System 7 is a signalling protocol</td>
</tr>
<tr>
<td>MME</td>
<td>Mobility Management Entity (MME) is responsible for initiating paging and authentication of the mobile device in LTE networks</td>
</tr>
<tr>
<td>SGW</td>
<td>Serving Gateway (SGW) is responsible for creating and maintaining subscriber’s data traffic in LTE networks</td>
</tr>
<tr>
<td>HLR</td>
<td>Home Location Register (HLR) is the main database containing subscriber information</td>
</tr>
<tr>
<td>MSC</td>
<td>Mobile Switching Centre (MSC) is a telephone exchange which makes connection between mobile users within the network</td>
</tr>
<tr>
<td>CRBT</td>
<td>Caller Ring Back Tone (CRBT) solution is part of value added services which enables subscriber to opt for a personalised ring back tone</td>
</tr>
<tr>
<td>IMSI</td>
<td>International Mobile Subscriber Identity (IMSI) is an internationally standardized unique number to identify a mobile subscriber</td>
</tr>
</tbody>
</table>
Architecture Illustration
Possible Entry Points
Possible Entry Points

Taking Over Telecom Networks - Hardik Mehta (@hardw00t) and Loay Abdelrazek (@sigploit)
Attack Vectors
**Attack Vectors**

**Mobile Stations (3G/ 4G):**
- Enumeration and exploitation of internal core network nodes
- Sending crafted SIP messages to perform tasks like, Caller ID spoofing
- Identifying nodes running signaling stacks (e.g. SIGTRAN stack) and sending malicious signaling traffic using SigPloit
Attack Vectors

Fiber to The Home (FTTH):
- Enumeration and exploitation of internal core network nodes
- VLAN hoping possible between VoIP, ITPV and Data
- Using VoIP, Crafted SIP messages can be sent to perform SIP attacks like DoS
- Using IPTV, Send crafted IGMP messages to subscribe unbilled channels
Attack Vectors

Internet:
- Compromise web applications deployed in DMZ
- Exploitation of internal network components possible if there is lack of segregation between DMZ and core network
- Possible to connect with network nodes (e.g. PGW/GGSN or SGSN) exposed on the public domain
- Sending crafted SIP messages to SBCs exposed on the public domain

![Diagram showing attack vectors in telecom networks](image)
Attack Vectors

Roaming interfaces:
- Using SS7, perform HLR lookup to get subscriber information like, IMSI and serving MSC
- Using GTP, identify active tunnel session and hijack the session
- Using SS7/ Diameter, perform attacks leading to fraud like over-billing
- Using SS7/ Diameter, perform interception attacks like, SMS and Call

Reference: SS7 Locate Track Manipulate - Tobias Engel
Attack Vectors

Passive IMSI Sniffing using RTL-SDR and OsmocomBB phone
Attack Vectors

Passive IMSI Sniffing using RTL-SDR and OsmocomBB phone
Taking Over Telecom Networks - Hardik Mehta (@hardw00t) and Loay Abdelrazek (@sigploit)
Attack Vectors

Example Realm Format

epc.mnc<MNC>.mcc<MCC>.3gppnetwork.org

dnslookup for exposed LTE nodes “3gppnetwork.org”

DNS Lookups for exposed LTE nodes “3gppnetwork.org”
Attack Scenario
**Attack Scenario**

- Internal network enumeration resulted in identification of node part of VAS networks, CRBT

- Caller Ring Back Tone (CRBT), is connecting with HLR ,MSC and IN charging nodes and it enables customers to subscribe for personalized audio, in place of regular tone

- Due to lack of basic security controls, it was possible to gain root access of the node from subscriber network segment

---

Taking Over Telecom Networks - Hardik Mehta (@hardw00t) and Loay Abdelrazek (@sigploit)
Attack Scenario

- The compromised node is connected to the core.

- It is then possible to use the node to initiate other core related attacks (i.e using protocol vulnerabilities like SS7, Diameter of GTP).

- Using a global title scanner, we can gather more info about the SS7 core.

https://github.com/SigPloiter/GTScan

Taking Over Telecom Networks - Hardik Mehta (@hardw00t) and Loay Abdelrazek (@sigploit)
Attack Scenario

- HLR(s) are identified.
- Query the HLR(s) to retrieve the IMSI.
- Bypassing SMS Home Routing if implemented.
- IMSI is the key to any mobile operation.

https://github.com/SigPloiter/SigPloit

Taking Over Telecom Networks - Hardik Mehta (@hardw00t) and Loay Abdelrazek (@sigploit)
### Attack Scenario

Identification of IMSI and MSC GT can help attackers perform various further attacks

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Impact</th>
</tr>
</thead>
<tbody>
<tr>
<td>IMSI</td>
<td>Impersonation</td>
</tr>
<tr>
<td></td>
<td>Data overbilling</td>
</tr>
<tr>
<td></td>
<td>Authentication Vector Retrieval</td>
</tr>
<tr>
<td>MSC GT</td>
<td>Subscriber profile Manipulation</td>
</tr>
<tr>
<td></td>
<td>Interception</td>
</tr>
<tr>
<td></td>
<td>Tracking</td>
</tr>
<tr>
<td></td>
<td>DoS</td>
</tr>
</tbody>
</table>
Attack Scenario

- Internet at the expense of others.
- Works for EPC and UMTS packet core.
- Using GTPv1 or GTPv2.
- Hijack the data connection of a subscriber using his retrieved IMSI.

Reference: Positive Technologies EPC Research 2018

Taking Over Telecom Networks - Hardik Mehta (@hardw00t) and Loay Abdelrazek (@sigploit)
Take control of Telecom Networks - Hardik Mehta (@hardw00t) and Loay Abdelrazek (@sigploit)
Attack Demonstration
Best Practices
Best Practices to Reduce Attack Exposure

- Implement network traffic segregation.
- Bind services to correct network interfaces.
- Limit the reachability of internal nodes from UEs.
- Limit the reachability of network nodes from Internet by configuring correctly routing protocols.
- Deploy secure configuration of network nodes
  - Secure configuration of all network services;
  - Disabling of insecure and unneeded network services;
  - Changing of default passwords;
  - Hardening;
  - Configuration and enabling of authentication and access control; Logging of all access attempts and other security-relevant events;
  - Configuration of the network node to not disclose unnecessary information;
  - Continuous deployment of the latest security patches.
  - Security testing and regular vulnerability scanning;
- Implement traffic filtering policies at the boundaries.
  - Basic IP Filtering;
  - Signaling FW;
- Monitor network traffic to discover anomalies.
- Deploy a Security Signaling Monitoring (Intrusion Detection System / IDS).
- Effective Threat modelling.
Q&A

Thank You