Security issues related to SS7

Charles Beumier Thibault Debatty

Royal Military Academy, Brussels, Belgium

Objective

This project aims at detecting attacks in the SS7 (Signaling System 7) traffic of the 2G and 3G mobile networks. Vulnerabilities arising from the early design of SS7 in the 70ties allow an attacker to track a Mobile Station (MS), to intercept, modify or redirect SMS or calls and to perform a Denial of Service (DoS). Although the security improved with 4G, the legacy 2G and 3G networks must be maintained for 5 to 10 more years for compatibility with old mobile or network equipment.

We aim at detecting SS7 anomalies which may reveal suspicious activities. We are building detectors analysing the SS7 traffic between network nodes. We will combine detector outputs in the MARk framework (developed at the Cyber Defence Research Unit [1]) to highlight anomalies.

2G, 3G, 4G networks

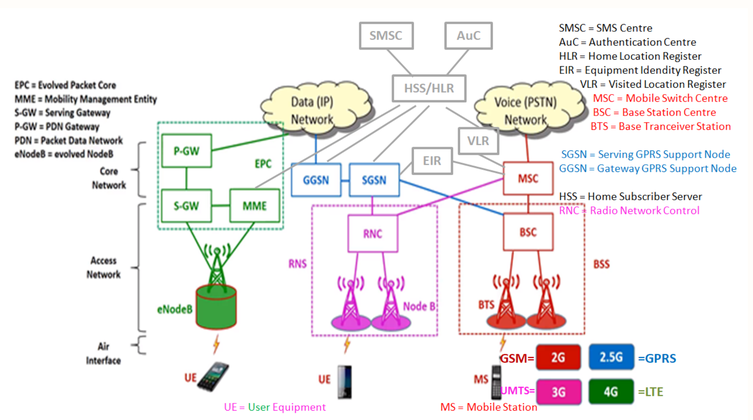

Figure 1: 2G, 3G and 4G Networks

Some important network nodes:

- HLR / HSS: home register holding subscriber location (current VLR) and subscription details
- VLR: local copy of HLR info for visiting roamers
- MSC: switch for interconnection and routing of signaling and voice
- SMSC: for Short Message storage and delivery
- AUC: centre for MS authentication and ciphering.

SS7 stack of protocols

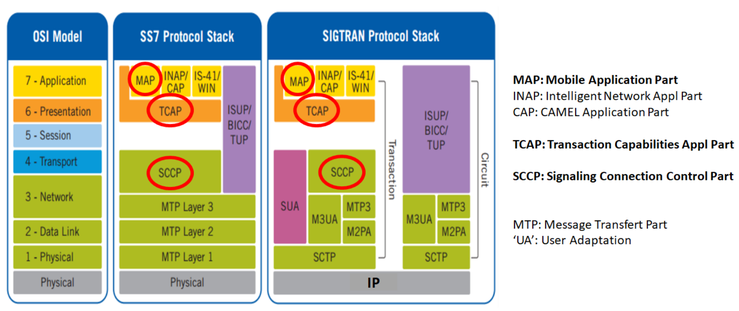

Figure 2: SS7 and SIGTRAN protocol stacks

- MAP: communication between nodes (2G..3G)
- TCAP: provides concurrent dialogs between nodes
- SCCP: routing (Global Titles OR PointCode + SSN)
- Numbering plans:

Standard	Name	Example
E.212	IMSI	206 01 0123456789
E.214	MGT	32 475 0123456789
E.164	MSISDN	32 475 322535

Vulnerabilities

- SS7 was designed in the 70's, when operators (national) trusted each other
  - 2G: MS authenticated by network but not vice versa
  - 2G: no encryption in core but on Radio (may be weak)
  - 3G: MS and network authenticated
- More risk from more SS7 accesses due to Telecom deregulation (Mid 90's) and SS7 on IP (SIGTRAN)
- Equipment can be spoofed by attacker to get personal info (IMSI, subscription plan) and change values (barring calls, redirect calls and SMS)
- 4G (all IP) uses DIAMETER: better, but similar vulnerabilities. Less attacked so far

SS7 Exploits with MAP

1. Get IMSI <-> MSISDN for later exploits
   - *MAP_SendRoutingInfoforSM* (SRISM) and *MAP_AnyTimeInterrogation* (ATI) return IMSI
2. Denial Of Service (DOS)
   - fake *MAP_UpdateLocation* of MS (MS looses access)
   - *MAP_InsertSubscriberData* with fake subscription details
3. Tracking position
   - ATI or SRISM return current VLR (rough position)
   - *MAP_SendRoutingInfoLCS* gives precise position (Lat Lon)
4. Call interception
   - *MAP_UpdateLocation* to set compromised serving MSC which routes calls (MITM)
   - *MAP_RegisterSS* to set call forwarding
5. SMS interception
   - *MAP_SendRoutingInfoForSM* to redirect messages
   - 2017: German bank '02' accounts emptied at night: customer mail hacked + 2FA (2-Fact Authent. by SMS)

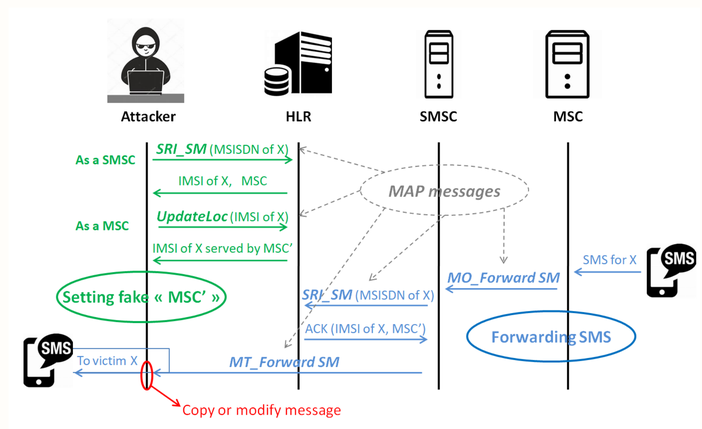

Figure 3: SMS interception

Data

- Useful SS7 Message info:
  - layer MAP: to find attacks
  - layer TCAP: may reveal fake requests (request <-> answer)
  - layer SCCP: Network node addresses (Global Titles)
- SS7 traffic from operators, thanks to IBPT
  - Respect subscriber privacy (RGPD)
    - ! pseudonymisation needed (IMSI, MGT, MSISDN)
  - Respect operator sensitive info
  - 1 week .. 1 month of traffic (huge quantity)
- Only passive (No msg injection, No penetration test)

Possible Clues

- MAP messages as those in section 'SS7 Exploits'; But all messages are a priori legitimate
- GSMA recommendation for MAP message checking
  - Cat 1 msg: Block if not from home network
  - Cat 2 msg: Check message origin of inbound roamer
  - Cat 3 msg: Check location of outbound roamer
- Scanning IMSIs or GTs: Many requests from 1 GT
- Message Timing: For DOS (overflow) or scanning
- Fake Global Titles: From TCAP errors

Challenges

- SS7 Data difficult to obtain
  - Legal frame to respect RGPD
  - SS7 samples disappeared from the net
- Limited support in the field:
  - wireshark: tool to dissect packet
  - Crucial info held by GSMA (GSM Association) restricted to members (Mobile Industry, Operators)
  - Operators protect sensitive info
- Huge data to be handled (Tb)
- Detect new attacks / vulnerabilities

Work

- Getting data from operators:
  - Data Protection Impact Analysis
  - pseudonymise IMSI, MGT, MSISDN
- Look for clues (GTs, Timing, Location, specific MAP oper, Cat 1,2,3) with a measure for anomality
- Detect anomalies, possibly fusing clues (with MARk)
- Detect Patterns (rules) <-> Machine Learning

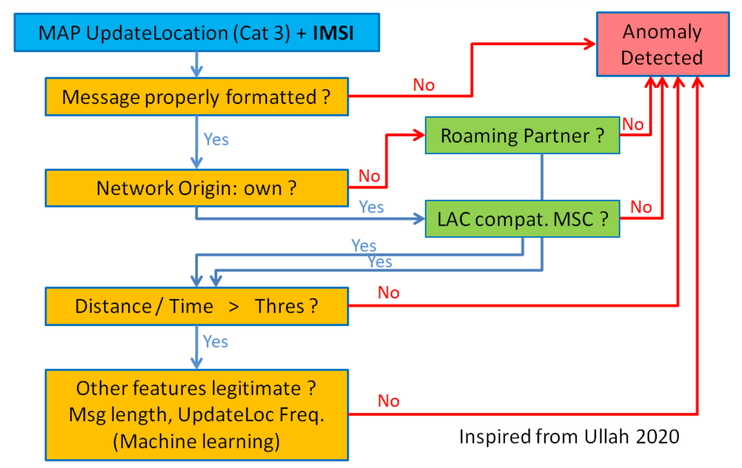

Figure 4: Attack detection for *MAP_UpdateLocation*

Acknowledgments

[1] G. Nikolov, T. Debatty, W. Mees, "Evaluation of a Multi-agent Anomaly-based Advanced Persistent Threat Detection Framework", In 12th Int. Conf. on Evolving Internet (INTERNET 2020).

[2] The project "Security Issues related to SS7 and Diameter" is funded by MDN [DAP20-01, Jul2020-Jun2024].