Security issues related to SS7

Charles Beumier Thibault Debatty

Royal Military Academy, Brussels, Belgium

A. Aim

- SS7 (Signaling System 7) in 2G/3G mobile networks:
  - Has intrinsic Vulnerabilities (D.)
  - Showed many Exploits (E.) dangerous for privacy
  - Is used as Fallback when no 4G / 5G coverage
  - Is expected to remain 5-10 years more
- This Project (DAP20-01 [1]) aims to:
  - Detect attacks in real SS7 traffic with Machine Learning
  - Combine detector outputs by the MARk framework ([2])
  - Explain suspicious traffic and Derive recommendations

B. 2G, 3G, 4G networks

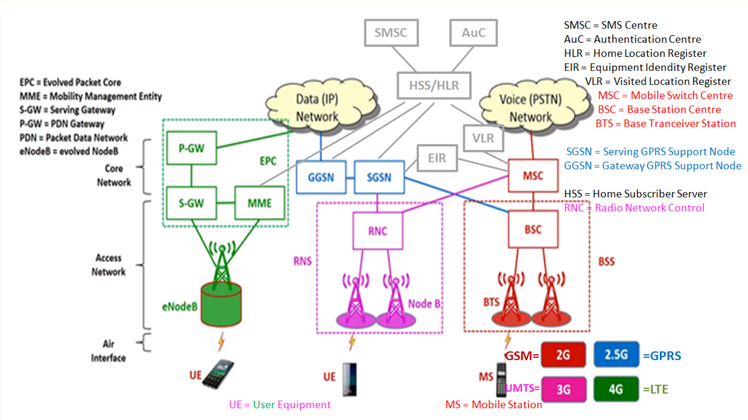

Figure 1: 2G, 3G and 4G Networks

Some important network nodes:

- HLR: home register: subscriber and location (VLR)
- VLR: local copy of HLR info for visiting roamers
- MSC: switch to route signaling and voice
- SMSC: for Short Message storage and delivery
- AUC: centre for MS authentication and ciphering

C. SS7 = stack of protocols

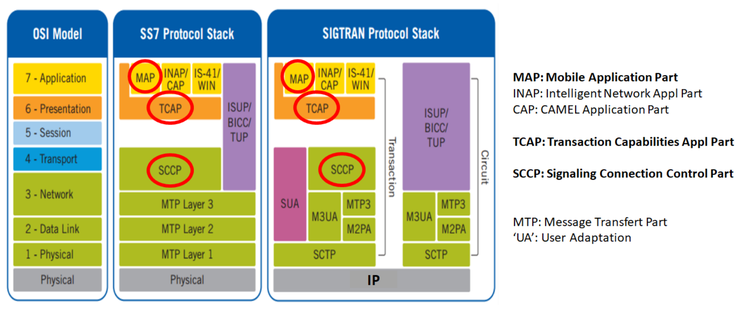

Figure 2: SS7 and SIGTRAN protocol stacks

- MAP: communication between nodes (2G..3G)
- TCAP: provides concurrent dialogs between nodes
- SCCP: routing (**G**lobal **T**itle OR **P**oint**C**ode + SSN)
- Numbering plans:

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

D. SS7 Vulnerabilities

- Designed in 70's (operators trusted each other)
  - 2G: MS authenticated by network but not vice versa
  - 2G: no encryption in core but on Radio (may be weak)
  - Equipment can be spoofed to get/set subscriber info
- Mid 90's: Telecom deregulation and SS7 on IP !
- Mid 2010's: Public demos of risks by researchers

E. Exploits with SS7/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 fake serving MSC (MITM)
   - *MAP_RegisterSS* to set call forwarding
5. SMS interception
   - *MAP_SendRoutingInfoForSM* to redirect messages
   - 2017: Bank '02' accounts emptied (2FA codes intercepted)

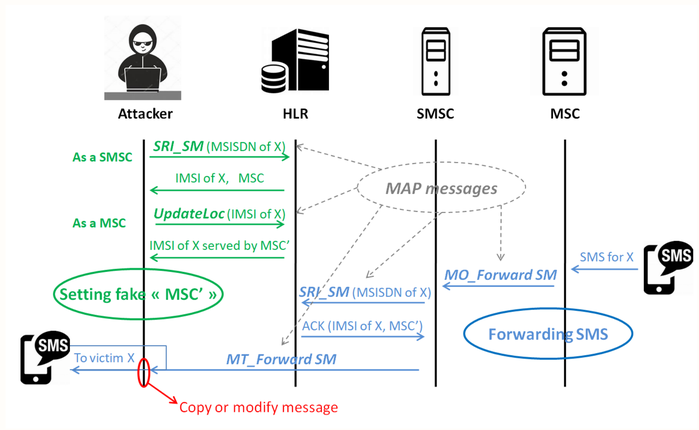

Figure 3: SMS interception

F. Project Challenges

- SS7 Data difficult to obtain
  - Respect RGPD (Web SS7 samples disappeared)
- Limited support in the field:
  - GSM Association restricts critical info to their members
  - Operators protect sensitive info
- Huge data to be handled (Tb)
- Machine Learning for detection
  - Detect new attacks / vulnerabilities

G. SS7 Data

- Useful SS7 Message info:
  - layer MAP: see E. Exploits, but a priori all legitimate
  - layer TCAP: may reveal fake requests (no answer), fake GT
  - layer SCCP, MTP3: incoherent / fake Network node addr
  - Message timing for overflow (DOS) or scanning
- 1 Month of traffic from operators, thanks to IBPT
  - Respect subscriber privacy (RGPD)
    - ! pseudonymisation needed (IMSI, MGT, MSISDN)
- Data Acquisition Progress
  1. Project presentation to Mobile Network Operators (MNOs)
  2. Data Protection of subscribers → DPIA (Impact Analysis)
  3. Small traffic sample before conventions
  4. Conventions: RMA ↔ IBPT and IBPT ↔ each MNO
  5. **Change: Binding Decision IBPT → each MNO**
  6. **Technical details**
  7. Traffic capture by MNO
  8. Pseudonymisation at MNOs (RMA soft)
  9. Transfer by RMA on encrypted medium

H. Preprocessing

- Format Conversion (ASN.1, JSON, CSV) → WSV
  - WSV = CSV with Fixed column width (fast access)
  - Conversion of some attribute values
- Message Sorting on IMSI numbers
  - So, grouped by Country, by Operator, by Subscriber
- Attribute Filtering (Time, MNO, MAP code, ...)

I. Analysis with User Interface

- Display / Interpret Msg attributes (statistics)
- Filter and Sort Messages
- 'Exec': Python interface to add functionality
- 'Pages': doc + ref about SS7, the Project, this GUI

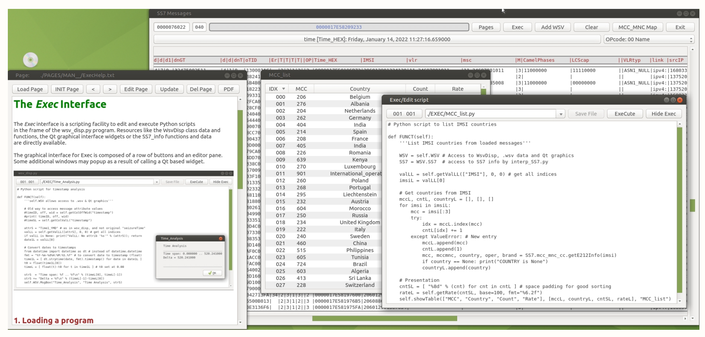

Figure 4: Graphical user Interface for SS7 messages

J. Prospective Detection

- Analyse timing (Time to answer, Brute Force)
- Detect incoherence PC (MTP3) ↔ GT (SCCP)
- Check TCAP dialogs (Begin-Continue-End, TID)
- Statistics on Countries, Operators, PC, ...
- Verify Patterns by Machine Learning
- Check GSMA 'Cat3' MAP messages
  - GSMA 'Cat 3' msg: check location of outbound roamer

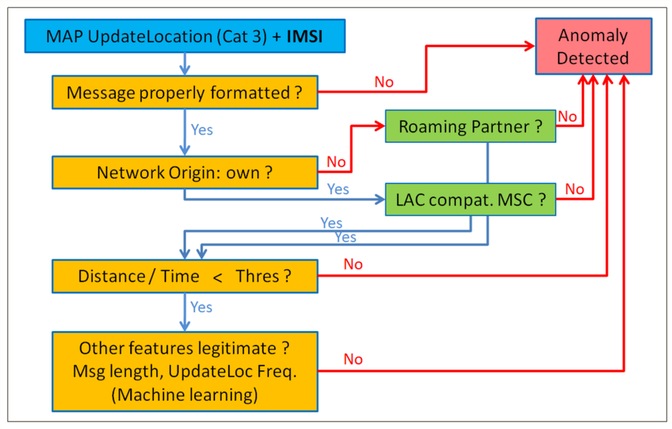

Figure 5: Attack detection for *MAP_UpdateLocation* (E.2, E.4)

References

[1] The project "Security Issues related to SS7 and Diameter" is funded by MDN / RHID [DAP20-01, Jul2020-Jun2025].

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

[3] C. Beumier, T. Debatty, "Attack Detection in SS7", Int. Conf. MCSS 2022, Proc. Dziech, A., Niemiec, M. Mees, W. (eds.). Springer, (vol. 1689 CCIS).