Security issues related to SS7

Charles Beumier Thibault Debatty

Royal Military Academy, Brussels, Belgium

A. Aim

E. Exploits with SS7/MAP

- ► 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
- 1. Get IMSI \leftrightarrow 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)

H. Preprocessing

- Format Conversion (ASN.1, JSON, CSV) \rightarrow 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

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

- 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

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

| | | | | | | | ×. | | | | | |
|--|--|-------------------------|-------------------|----------------------|----------------------------------|--|---|-----------------------|-------------------|------------------|-------------------------------|--|
| | 0000076022 040 | | | 0000017 | 'E58209233 | Pages Exec Add WSV Clear | | | | MCC_MNC Map Exit | | |
| | | | time [Time_H | IEX]: Friday, Januar | y 14, 2022 11:27:16.659000 | 659000 | | | OPcode: 00 Name 🗘 | | | |
| | | | | | | | | | | | | |
| | d d d1 dnGT d d | dnT oTID | Er T T 1 | T T OP Time_HE | (IMSI | vlr | msc | M CamelPhases | LCScap | VLRtyp | link srcIP | |
| Page: ./PAGES/MAN_/ExecHelp.txt | | B 8 38241 | MCC_list | 12112-10000017 | 1010003313000330 | 01324330133-24662663633 | 000 | 3 11000000 2 | 11110000 | ASN1_NULL | ipv4: 168033 ipv4: 137520 | |
| Load Page INIT Page < > Edit Page | Update Del Page PD | F 18223 | IDX 🔻 | MCC | Country | Count | Rate | 3 11000000 | | ASN1_NULL | ipv4: 137520 | |
| The <i>Exec</i> Interface | | 2FCA0 28CF0 | 000 | 206 276 204 | Albania Netherlands | Exec/Edit script | Acc list av | | Cours File | [Fun Cuba | | |
| he Exec interface is a scripting facility to edit and exec | ute Python scripts | 24040 54440 90070 | 003 004 | 262 404 | Germany India | # Python script to li | st IMSI countries | v | Save File | Execute | HIde Exec | |
| i the rrame of the wsv_disp.py program. Resources like the wsvDisp class data and unctions, the Qt graphical interface widgets or the SS7_info functions and data re directly available. | | | 005 006 007 | 214 208 405 | Spain France India | def FUNCT(self): '''List IMSI coun | <pre>'FUNCT(self): '''List IMSI countries from loaded messages'''</pre> | | | | | |
| he graphical interface for Exec is composed of a row of buttons and an editor pane. ome additional windows may popup as a result of calling a Ot based widget. | | | 008 | 226 639 | Romania Kenya | WSV = self.WSV # Access to WsvDisp, .wsv data and Qt graphics SS7 = WSV.SS7 # access to SS7 info by interp SS7.pv | | | | | | |
| wav_disp.py | 000 | 57009 33F10 | 010 | 270 901 In | Luxembourg ternational_operat | valLL = self.getV | alLL(["IMSI"], 0, 0) ; | # get all indices | | | | |
| 001 001 /EXEC/Time_Analysis.py | Save File ExeCute Hide Exec | 91335 | 012 | 260 | Poland | imsiL = ValLL[0] | | | | | | |
| # Python script for timestamp analysis | | 48110 | 014 | 295 | Liechtenstein | # Get countries f | rom IMSI | | | | | |
| '''self.WSV allows access to .wsv & Qt graphics''' | | 81880 | 015 | 232 | Austria | mccL, cntL, count | ryL = [], [], [] | | | | | |
| # Old way to access message attribute values | | 80261 | 016 | 604 | Morocco | TOF 1ms1 1n 1ms1L mcc = imsi['3 | 1 | | | | | |
| <pre>#print(timeID, off, wid) #time[= set(getters time(timestamp) #time[= set[set(a) wid)</pre> | | 94990 | 017 | 250 | Russia | try: | | | | | | |
| stand = stingetotrate(tangtamp) | | 0D4C0 | 018 | 234 | United Kingdom | idx = mcc | L.index(mcc) | | | | | |
| valLL = self.getValLL([attr5], 0, 0) # get all indices | | 97330 | 019 | 222 | Italy | cntL[idx] | += 1 | | | | | |
| <pre>datelL = valLL[0]</pre> | Time_Analysis 🙁 😕 | 98353 | 020 | 240 | Sweden | except ValueE | rror: # New entry | | | | | |
| # Convert dates to timestamps | Time Analysis | BD140 | 021 | 515 | Philippines | cntL.appe | nd(1) | | | | | |
| fmt = "%Y-%m-%d%H:%H:%S.%f" # to convert date to timestamp (float) | Time span: 0.000000 520.241000 Delta = 520.241000 | LACCO | 023 | 605 | Tunisia | mcc, mccm | nc, country, oper, bra | and = SS7.mcc_mnc_cc. | getE212Info(i | .msi) | | |
| <pre>timelL = [dt.strptime(date, fmt).timestamp() for date in dateLL] t0 = float(timeLL[0])</pre> | | FACOO | 024 | 724 | Brazil | if countr | y == None: print("COU | NTRY is None") | | | | |
| timeL = [float(t)-t0 for t in timelL] # t0 set at 0.00 | | 54002 | 025 | 603 | Algeria | countryL. | append(country) | | | | | |
| <pre>strS = "Time span: %f %f\n* % (timeL[0], timeL[-1]) strS += "Delta = %f\n* % (timeL[-1]-timeL[0])</pre> | | BD160 | 026 | 413 | Sri Lanka | # Presentation | | | | | | |
| <pre>self.WSV.MsgBox(*Time_Analysis*, "Time Analysis", strS)</pre> | | D100 | 027 | 228 | Switzerland | cntSL = ["%8d" % | (cnt) for cnt in cnt |] # space padding f | or good sorti | na | | |
| | | | AT3/1713131 | 113113 10000017 | 591076001206012 | rateL = self.getR | ate(cntSL, base=100, | fmt="%6.2f") | | | | |
| | | 5500B01 | 3 2 3 | 1 2 3 0000017 | E581976B5 2060880 | self.showTable([" | MCC", "Country", "Coun | nt", "Rate"], [mccL, | countryL, cnt | SL, rateL], "MC | :_list") 🖕 | |
| | | 9E3136F | 6 23 | 1 2 3 0000017 | E581975FA 2060125 | 01001001 | | 191 | | | | |
| | | | | | | | | | | | | |
| . Loading a program | | - | | | | | | | | | | |
| | | | | | | | | | | | | |

Figure 4: Graphical user Interface for SS7 messages

J. Prospective Detection

- Analyse timing (Time to answer, Brute Force)
- ▶ Detect incoherence PC (MTP3) \leftrightarrow GT (SCCP)

C. SS7 = stack of protocols





Figure 2: SS7 and SIGTRAN protocol stacks

- ► MAP: communication between nodes (2G..3G)
- TCAP: provides concurrent dialogs between nodes
- \blacktriangleright 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 | | |



- ► 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

- 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

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

1. Project presentation to Mobile Network Operators (MNOs)

- 2. Data Protection of subscribers \rightarrow DPIA (Impact Analysis)
- 3. Small traffic sample before conventions
- 4. Conventions: RMA \leftrightarrow IBPT and IBPT \leftrightarrow each MNO
- 5. Change: Binding Decision IBPT \rightarrow each MNO
- 6. Technical details
- 7. Traffic capture by MNO
- 8. Pseudonymisation at MNOs (RMA soft)
- 9. Transfer by RMA on encrypted medium

- [1] The project "Security Issues related to SS7 and Diameter" is funded by MDN / RHID [DAP20-01, Jul2020-Jun2025].
- 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).
- C. Beumier, T. Debatty, "Attack Detection in SS7", Int. Conf. 3 MCSS 2022, Proc. Dziech, A., Niemiec, M. Mees, W. (eds.). Springer, (vol. 1689 CCIS).



Cyber Defence Lab

Royal Military Academy

www.cylab.be

