

SS7 Attacker Heaven turns into Riot: How to make Nation-State and Intelligence Attackers' lives much harder on mobile networks

SigFW Open Source SS7/Diameter firewall for Antisniff, Antispoof & Threat Hunt

blackhat USA 2017

Martin Kacer, Philippe Langlois



© 2017 – P1 Security, All Rights Reserved

Introduction

Martin Kacer, Core Network Security Researcher Philippe Langlois, Security Researcher & CEO P1 Security

P1 Security (<u>http://www.p1sec.com</u>) is dedicated to providing top security products and services for high-expertise security areas.

P1 Labs is the research department of P1 Security. Conducting research on many subjects related to telecom systems and protocols, mobile apps and platforms, embedded systems, Core Network protocols, etc.

Introduction

Open-source SigFW

- SS7 and Diameter Firewall created under P1 Labs
- Source code is available at https://github.com/P1sec/SigFW

The open-source SigFW should be considered as **reference implementation** and **research project** but **without any warranty** and it is not carrier grade solution.

Motivation of this work

blackhat USA 2017

4

Motivation for this work Background

Telecom networks (SS7, IPX) are the key infrastructure transmitting subscribers' locations, metadata and communication content

These networks are vulnerable to both active signalling attacks and to passive eavesdropping attacks

blackhat USA 2017



5

Motivation for this work Current status

On conferences and publicly in past, most time the attacks were covered There is a lack of public defense solutions

There is intensive work at the GSMA level (trade body that represents the interests of mobile operators worldwide) and by telecom and private security companies
But there is lack of open-source and affordable tools to improve the security on a wide scale

Some specifications are written

But take a lot of time to become mainstream, if ever adopted. blackhat USA 2017

Motivation for this work Will SS7 be phased-out soon?



Let's evaluate this...

- The circuit switched voice service could be replaced by VoLTE (4G) with IMS home routed architecture, but such deployment requires VoLTE capable devices and VoLTE networks with a similar radio coverage compared to 2G & 3G. So before an operator decides to shut-down both 2G and 3G networks, **all the home subscribers should be VoLTE enabled**.
- And still, haven't we forgot the inbound-roamers?
- Moreover, similar pitfalls as in SS7 are still present in GRX/IPX networks used for mobile data for GTP protocol and in 4G for Diameter protocol.

...so maybe not so soon

Motivation for this work The Signal App and other mobile encryption Apps

Not covering everything ...

- Subscribers are not always attached to mobile data
- Not all users are using it, so there is still fallback to standard Voice and SMS
- The location data could be present in signalling in 4G over Diameter and for 3G, 2G in SS7. This will also apply for VoLTE.
- Most of the time A2P SMS are delivered over SS7
- ... there is still need to protect the signalling

Motivation for this work Main Goal

Try to improve telecom security on a wide scale and try to provide solution to address vulnerabilities in SS7 and IPX networks.

Secure messages against advanced attacks:

- Spoofing
- Interception
- Illegal injection

Decision to try make a difference in the World:

- Humbly, with what we can
- Even if P1 Security is doubling size every Year
- Still small (compared to huge Telecom and Mobile giants)

Current status

Current status SS7 / Sigtran stack overview

Decoding is done from lower layers to upper layers

Filtering should be performed based on decoding different layers



Current status Major Core Network Elements overview

STP - Like router, but capable also doing filtering/screening

HLR/HSS - Home Location Register. The main database storing home subscribers, profiles, authentication information and locations.

MSC/VLR - switching center connecting the circuits and VLR is storing the subscriber profile received from HLR in HPLMN or VPLMN. Every subscriber in 2G/3G is served by some MSC/VLR.

SGSN - Like MSC/VLR, but for mobile data. Creating data tunnel (GTP) to home GGSN to allow internet connectivity. Every subscriber in 2G/3G with enabled data is served by some SGSN.

SMSC - SMS center. Storing and delivering SMS messages.

Other - IN, GGSN, PCRF, IVR, P-GW, S-GW, MME, IMS, ... blackhat USA 2017

Current status Perimeters of SS7 overview



Current status SS7 messages categories

"Category" is just a naming indicating a group of similar messages. For messages in the same category the same protection logic could be implemented. Mainly the message direction is important to decide to which category a message belongs. The normal call flows and normal use of the message are well described in 3GPP specifications.

MAP Cat1 messages are messages which should not be allowed towards HPLMN.

MAP Cat2 messages are messages which should be allowed towards HPLMN only if foreign network is targeting it's own subscribers (inbound-roamers).

MAP Cat3 messages are messages which should be allowed towards HPLMN from own subscribers in roaming (outbound-roamers) only if location condition matches.

SMS Cat: SMS messages which require to decode SMS layer.

CAP Category 2 messages are Camel messages which should be allowed for inbound-roamers from HPLMN towards foreign network (inbound-roamers).

CAP Category 3 messages are Camel messages which should be allowed for outbound-roamers from VPLMN towards HPLMN.

Current status And we can then create protocol matrices for SS7 and also for Diameter and GTP

Command Cols Command Name App Bandwill App Castland Aum 0.252 MOREL SCHLER (SALE) (SALE) SALE SCHLER (SALE) SALE SCHLER (SALE) SALE SCHLER (SALE) Application Control 2261 CALE (SALE) (SALE) (SALE) SALE SCHLER (SALE) <td< th=""><th></th><th>IPX - Conve</th><th>Mand-Codes</th><th></th><th></th><th></th><th></th></td<>		IPX - Conve	Mand-Codes					
Backbar Backbar <t< th=""><th>Comm and Code</th><th>Comman d Name</th><th></th><th>App ligation-ld</th><th>Application4d name</th><th></th><th></th></t<>	Comm and Code	Comman d Name		App ligation-ld	Application4d name			
BAREAR BAR Organization BAR Organization Application Application <thapplication< th=""></thapplication<>		RADIUS COMPANYING COMP						
127 CR1 CED - CapUch S Bud way 2 4 4 4 4 4 4 268 SAC(RAA, A. Stack B. Bud way 2 account water 0.4 MA PC previow 1 account water 0.4 268 SAC(RAA, A. Max b. Bud water 0.4 4 account water 0.4 1 account water 0.4 <t< td=""><td>255.</td><td>Unsakared</td><td></td><td></td><td></td><td></td><td></td></t<>	255.	Unsakared						
Add Constraint MAR P Operation MAR Add Code Approache Contact 200 Add Code Code Add Code 2 Approache Contact 200 Add Code 2 Approache Contact 2 Approache Contact 200 Add Code 2 Approache Contact 2 Approache Contact 201 Add Code 2 Approache Contact 2 Approache Contact 201 Add Code 2 Approache Contact 2 Approache Contact 202 Add Code 2 Approache Contact 2 Approache Contact 202 Add Code 2 Add Code 2 Approache Contact 202 Add Code 2 Add Code 2 Approache Contact 202 Add Code 2 Add Code 2 Add Code 2 203 Add Code 2 Add Code 3 Add Code 3 Add Code 204 Add Code 2 Add Code 3 Add Code 3 Add Code 203 Add Code 2 Add Code 3 Add Code 3 Add Code 204 Add Code 2 Add Code 3 Add Code 3 <td>257</td> <td>CONTRACTOR CONTRACTOR</td> <td>88</td> <td></td> <td>BAP CC - INA</td> <td>12</td> <td>30</td>	257	CONTRACTOR CONTRACTOR	88		BAP CC - INA	12	30	
Biol Mail Ref. Ref. Biol Bigsell J prestantion J prestantion 280 Monit Add. Add State Hole 4 rescaledants 3 prestantiants 280 Monit Add. Add State Hole 4 rescaledants 3 prestantiants 281 Monit Add. Add State Hole 4 rescaledants 3 prestantiants prestantiants prestantiants prestantiants prestantiants prestantiants prestantiants prestantiants prestantiants prestantiants </th <th>400</th> <th>CERTODAL CODAL AND AND AND AND AND AND AND AND AND AND</th> <th>Dparation Col</th> <th></th> <th>MAP Operation</th> <th>MAP AC Code</th> <th>Application Costant</th>	400	CERTODAL CODAL AND	Dparation Col		MAP Operation	MAP AC Code	Application Costant	
200 Management 2 method sector 2 method sector 201 Management 4 Tachel Andreas 3 method sector 202 Management 4 Tachel Andreas 3 method sector 202 Management 6 Tachel Andreas 3 method sector 202 Management 6 Tachel Andreas 3 method sector 202 Management 6 Tachel Andreas 3 Tachel Andreas 203 Management 6 Tachel Andreas 3 Tachel Andreas 204 Management 6	255	RAR (RAA - Re-auto Request	2	untitalization		1	two studio	
Bits Mail (AM, AM, Mailler 1990) F product bits product bits <td>239</td> <td>sharespeet.</td> <td>1</td> <td>Conception in</td> <td></td> <td>1 2 1</td> <td>In an Constation</td>	239	sharespeet.	1	Conception in		1 2 1	In an Constation	
201 Distancy and particular structures Distance and particular structures and constructures and particular structures and particular structures particular structures particular structures and par	250	APRILAWA - AA-MUN-NAGE	4 4	array h Buarris	an at a		Concept Property	
Bits Bits Description Description Description 283-264 MAIL (AAI, Allocata (Unit of the Name) 1 <td>201</td> <td>Unasigned</td> <td></td> <td colspan="2">a service of the second s</td> <td></td> <td>and services of the filled in output for the star</td>	201	Unasigned		a service of the second s			and services of the filled in output for the star	
281 284 Main State State 1 matching State 1 matching State 285 MAI AMA - Advance Main State 1 matching State 1 matching State 286 MAI State 1 matching State 1 matching State 286 MAI State 1 matching State 1 matching State 287 Main State 1 matching State 1 matching State 287 MAI State 1 matching State 1 matching State 287 MAI State 1 matching State 1 matching State 287 MAI State 1 matching State 1 matching State 287 MAI State 1 matching State 1 matching State 288 MAI AMA - Advance 1 matching State 1 matching State 289 OWE (VMA - State 1 matching State 1 matching State 280 OWE (VMA - State 1 matching State 1 matching State 281 OPAI State 1 matching State 1 matching State 282 OWE (VMA - State 1 matching State 1 matching State </td <td>252</td> <td>HAR IN A - PUTE Agent Mit</td> <td></td> <td>Construction of the local division of</td> <td>Search and an</td> <td></td> <td></td>	252	HAR IN A - PUTE Agent Mit		Construction of the local division of	Search and an			
284 MAI, IAA, Autority Municipal I In an Autority Municipal 284 CAN, IAA, Autority Municipal I Interfactority Autority 284 CAN, IAA, Autority Municipal I Interfactority Autority 284 CAN, IAA, Autority Municipal I Interfactority Autority 287 CAN, IAA, Autority Massall I Interfactority Autority 288 CAN, IAA, Autority Massall I Interfactority Autority 289 CAN, IAA, Autority Massall I Interfactority Autority 280 CAN, IAA, Autority Massall I Interfactority Autority 281 Canada Autority II Interfactority Autority 283 Canada Autority II Interfactority Autority 284 CAN, IAAA, Autority Autority III Interfactority Autority 285 CAN, IAAA, Autority Autority	103 - 104	Urangred		Comparison of the other	A.M	4	Carto on this Time after	
201 201 201 3 If it is the set of data If it is the set of data If it is the set of data 202 201	200	ALE TAXA - ALE STAR AUTORISCH		IL BRITCH BOLLOW	A#4	4	reading	
283 OK (2) Constrained with intermed with intermed and intermed by i	200-201	Unably of		T martStaszbaDita		4	auto action (2 et all http:	
AMOUNT Constraint State Image: State State Image: State State State State Image: State St	200,200	DERIDUA - DIA DIA CARTA		1 mertSubscrberDeta		-	apolocato Opter	
1072 COS. (Col. A coll. C	271	STREAM AND STREAM		1 martinezoata			regrestrupte	
Addition Image: State of the second state of t	372	CORP. COL. Credit Control Restor	1	8 defailed up set her Cala		16	subsector Outstagt	
1974 AGD / 2004. School freedom official and a second match official and a	773	ite animat		8 undParameters		1	releasedup	
372 372 <td>274</td> <td>ALC LASA Abort Session Requer</td> <td>1</td> <td colspan="2">soutPatienators</td> <td></td> <td>india Plantia wal</td>	274	ALC LASA Abort Session Requer	1	soutPatienators			india Plantia wal	
With Prov User provide Statement With Provide Statement With Provide Statement 200 OPR / DVA - Devide Vacandard User provide Statement With Provide Statement With Provide Statement 201 OVR / DVA - Devide Vacandard User provide Statement With Provide Statement With Provide Statement 202 OPR / DVA - Devide Vacandard User provide Statement With Provide Statement With Provide Statement 203 OPR / DVA - Devide Vacandardown With Provide Statement With Provide Statement With Provide Statement 203 OPR / DVA - Devide Vacandardown With Provide Statement With Provide Statement With Provide Statement 204 OPR / DVA - Devide Vacandardown With Provide Statement With Provide Statement With Provide Statement 204 OPR / DVA - Devide Vacandardown With Provide Statement With Provide Statement With Provide Statement 204 OPR / DVA - DVA	275	STR / STA - Session Termination 7	Contract of the local division of the local	8 antiPersonators			international and	
240 OVAR / DVA Device Vacon-val 11 areasistic 12 areasistic 12 areasistic 12 areasistic 12 areasistic 13 areasistic 13 areasistic 13 areasistic 13 areasistic 14 14	275.279	in the second		again 12		14	releaseFundaretEs	
280 OVM (10M-Levids Valorind) U mesod valorind) U mesod valorind) 281 Meansamed U exclusion M exclusion 284 Meansamed U exclusion M exclusion 284 PRI (DAFL - Decomposition of the main of the finance) W exclusion of the main of th			5 15	th scale 10		18	resolvindumba	
241 Manufacture 30 Personality of the second secon	280	DWR / DWA - Device Visionidog		12 activate Still		16	rewol/indunitia	
242 OPR (c)PA - Decompeñ/Per 9 andres/detar/staftand 90 meastar/staftand 265 CAR (C)AA - Samu Alegional Per 10 andres/data france 90 andr	261	Unassigned		U padrando		18	reword in the refo	
No. Dir. Letter balance durch son auf and son auf and son automatic problem. Dir. Dir. Letter balance durch son automatic problem. Dir. 265 OART (VAA - Loss - Automatic problem. 17 - angle data son automatic problem. 18 - andore data son automatic problem. 266 OART (VAA - Loss - Automatic problem. 17 - angle data son automatic problem. 18 - andore data son automatic problem. 266 DART (VAA - Loss - Automatic problem. 18 - andore data son automatic problem. 18 - andore data son automatic problem. 267 DART (VAA - Loss - Automatic problem. 18 - andore data son automatic problem. 18 - andore data son automatic problem. 268 DART (VAA - Loss - Automatic problem. 28 - andore data son automatic problem. 28 - andore data son automatic problem. 268 DART (VAA - Loss - Automatic problem. 28 - andore data son automatic problem. 28 - andore data son automatic problem. 268 DART (VAA - Loss - Automatic problem. 28 - andore data son automatic problem. 28 - andore data son automatic problem. 269 DART (VAA - Loss - Automatic problem. 28 - andore data son automatic problem. 28 - andore data son automatic problem. 261 DART (VAA - Loss - Automatic problem. 28 - andore d	282	DRR IDRA - Disconned-Peer	14	alaring as 55		14	retwo Munderal Ss	
253 DAR (DAR): Subschulzborg (DAR) IN IN IN 264 SAR (DAR): Subschulzborg (DAR) IN IN IN 264 SAR (DAR): Subschulzborg (DAR) IN IN IN 265 UR (DAR): Subschulzborg (DAR) IN IN IN 266 UR (DAR): Subschulzborg (DAR) IN IN IN 267 UR (DAR): Subschulzborg (DAR) IN IN IN 268 UR (DAR): Subschulzborg (DAR) IN IN IN 269 VIIII (TAR): Subschulzborg (DAR) IN IN IN 261 UR (DAR): Subschulzborg (DAR) IN IN IN 262 UR (DAR): Subschulzborg (DAR) IN IN IN 263 UR (DAR): Subschulzborg (DAR) IN IN IN 264 UR (DAR): Subschulzborg (DAR) IN IN IN 265 UR (DAR): Subschulzborg (DAR) IN IN IN 265 UR (DAR): Subschulzborg (DAR) IN IN IN 266 UR (DAR): Subschulzborg (DAR) IN IN IN 267 UR (DAR): Subschulzborg (DAR) IN IN IN 268 UR (DAR): Subschulzborg (DAR)			-	autantistant	at a france		authorite activation and another part	
253 DAR (10, 4), Sover A arguing and Sover A server Arguing and Sover Arguing an		and the second second second		ALLER S				
244 MR (1944, Saver Augment R) 3 4 4 285 LR / DA - Saver Augment R) 3 4		CAR CAR CAR	17	17 InstatePassaret			and and and and a second se	
244 MK (* Starts: Adaption at 10 10			- 11	-		-	The second se	
Bits Bits <td>284</td> <td>SAR / SAA - Samer Assontant Ho</td> <td>-</td> <td colspan="2"></td> <td>-</td> <td>Patto w undernites</td>	284	SAR / SAA - Samer Assontant Ho	-			-	Patto w undernites	
Bits UNIT UNIT <th< td=""><td></td><td></td><td></td><td colspan="2">16 Price and Preventing data Links</td><td>A</td><td>Participar un du nuis e</td></th<>				16 Price and Preventing data Links		A	Participar un du nuis e	
The Control and the state of t	285	LIR/UA-Locator-InfoReport		20 PELIS data Property Comp			Transa Jawas all constit	
THE MORE 148.4.1. Multiment schedunffilm D Call of schedung D Call of schedung D D Schedung Schedun				2 ¹ PAPamarAlativ des			staining the states many	
20 21 24<	206	And Allen In Course Auto Real		A DESCRIPTION OF		4	The widtant wide	
State Control (Control (Contro) (Control (Contro)(Control (Control (Control (Con			23	splateGpnLoatian		32	spina.coato eUptaine	
20 No.46	1000	RTR / RTA - Registration Terrenal		A STREET, STRE	Pardens.;	-	The second state of the second	
P2 Color Barlow Barlo	201	A Design of the second second	the state of the s	Designed and the		A	Internal and Inter	
20 000000000000000000000000000000000000		25 delete as pr		THE R. LOW DO. NO.	a Sen	-	and they	
27 Addition State 27 Addition State 27 Addition State 28 Addition State Addition State <td></td> <td>24 eror indicate</td> <td>2</td> <td>a provinciane d</td> <td></td> <td>A DESCRIPTION OF</td> <td></td>		24 eror indicate	2	a provinciane d		A DESCRIPTION OF		
State Advance Description Description Description 20 dot, confictioner, yeard, report point, confictioner, confictioner, report point, confictioner, con		27 pdu notificati		Last section and		A second second	burstone-Contest	
22 Mol. / collicities/, reports Mol. / collicities/, reports Mol. 23 Adu. / collicities/, reports Mol. / collicities/, reports Mol. 24 Mol. / collicities/, reports Mol. / collicities/, reports Mol. 25 Mol. / collicities/, reports Mol. / collicities/, reports Mol. 26 Mol. / collicities/, reports Mol. / collicities/, reports Mol. 27 Mol. / collicities/, reports Mol. / collicities/, reports Mol. 28 Mol. / collicities/, reports Mol. / collicities/, reports Mol. / collicities/, reports 28 Mol. / collicities/, reports Mol. / collicities/, reports Mol. / collicities/, reports 29 Mol. / collicities/, reports Mol. / collicities/, reports Mol. / collicities/, reports 29 Mol. / collicities/, reports Mol. / collicities/, reports Mol. / collicities/, reports 20 Mol. / collicities/, reports Mol. / collicities/, reports Mol. / collicities/, reports 20 Mol. / collicities/, reports Mol. / collicities/, reports Mol. / collicities/, reports 21 Mol. / collicities/, reports Mol. / collicities/, reports Mol. / collicities/, reports 21 Mol. / collicities/, reports Mol. / collicities/, reports Mol. / collicities/, reports <td></td> <td>25 poly notificati</td> <td>Constant of the local division of the local</td> <td>In section of the sec</td> <td></td> <td>The second second</td> <td>tastos Control</td>		25 poly notificati	Constant of the local division of the local	In section of the sec		The second second	tastos Control	
30 Pails / postication / reject / response Pails / postication / reject / response NA 31 BA expcorted ent / backer / rollbuildon MA 32 BA expcorted ent / backer / rollbuildon MA 33 BA expcorted ent / backer / rollbuildon MA 33 BA expcorted ent / backer / rollbuildon MA 33 BA expcorted ent / backer / rollbuildon MA 34 BA expcorted ent / backer / rollbuildon MA 35 BA roll / backer / rollbuildon MA 36 BA roll / backer / rollbuildon Rollbuildon 37 Roll / rollbuildon Roll / backer / rollbuildon Rollbuildon 38 Roll / rollbuildon Rollbuildon Rollbuildon Rollbuildon 39 Rollbuildon / rollbuildon Rollbuildon Rollbuildon Rollbuildon Rollbuildon 30 Rollbuildon / rollbuildon Rollbuildon / rollbuildon Rollbuildon Rollbuildon Rollbuildon 31 Rollbuildon / rollbuildon Rollbuildon		20 pdu notificati	Taket Int	1.44	and politication reject request	and and		
31 DA. Decipionid ant Peaker Profile. Decipionid ant Peaker Decipionid ant Peaker 32 Decipionid and Peaker New Restance Decipionid ant Peaker Decipionid ant Peaker 33 Decipionid and Peaker New Restance Decipionid ant Peaker Decipionid ant Peaker 34 Decipionid ant Peaker New Restance Decipionid ant Peaker Decipionid ant Peaker 34 Decipionid ant Peaker Decipionid ant Peaker Decipionid ant Peaker 35 Decipionid ant Peaker Decipionid ant Peaker Decipionid ant Peaker 34 Decipionid ant Peaker Decipionid ant Peaker Decipionid ant Peaker 35 Decipionid ant Peaker Decipionid ant Peaker Decipionid ant Peaker 36 Decipionid ant Peaker Decipionid ant Peaker Decipionid ant Peaker 36 Decipionid ant Peaker Decipionid ant Peaker Decipionid ant Peaker 36 Decipionid ant Peaker Decipionid ant Peaker Decipionid ant Peaker 37 Decipionid ant Peaker Decipionid ant Peaker Decipionid ant Peaker 38 Decipionid ant Peaker Decipionid ant Peaker Decipionid ant Peaker 39 Decipionid ant Peaker Decipionid ant Peaker Decipionid ant Peaker 39 Decip		20 100 10000	and and and	and the second second	and and ballets minut anyone	- Carlo	Ta'A	
21 Bend Tracking this inspose Bend Round gifting the preparate and county gifting preparate and county g	7	31 100	Contraction of the local division of the loc		and other and header politication	and the second second		
20 Instruction of the properties Instruct instruction Other properties 31 Instruct instruction Instruct instruction Other properties 32 Instruct instruction Instruct instruction Other properties 32 Instruct instruction Instruct instruction Other properties 33 Instruct instruction Other properties Other properties 33 Instruct instruction Other properties Other properties 34 Instruct instruction Other properties Other properies 35 Instruction Other properties Other properties Other properties 35 Instruction Other properties Other properties Other properties 36 Instruction Other properties Other properties Other properties 37 Instruction Other properties Other properties Other properties 38 Instruction Other properties Other properties Other properties 38 Instruction Other properties Other properies Other properies <td></td> <td>11 And In Frank</td> <td>And in case of the local division of the loc</td> <td></td> <td>Supported and reader include</td> <td>Carl Company</td> <td>and the second se</td>		11 And In Frank	And in case of the local division of the loc		Supported and reader include	Carl Company	and the second se	
22 des const de properties 22 des const des const des const de properties 22 des const des const des const de properties 22 des const des const des const de properties 22 des const des const des const de properties 22 des const des const des const de properties 22 des const des const des const de properties 22 des const des const des const de properties 22 des const des const des const de properties 22 des const des const de properties 22 des const des const des const de properties 22 des const des const des const de properties 22 des const des const des const des const des const de properties 22 des const des const des const des const des const de properises 22 des cons		11 June 1 1			And the second second		logudat	
Al discussion reasons al discussion reasons		31 500 00 000		And the owner of the	and the second		apone	
A time store (model) A time store (model) Control (applied), model Control (applied),		24. 24. 24. 24. 24. 24. 24. 24. 24. 24.	ALCONO.		HAVE SHELL VERY	- Diente start Start	9.8%	
B 20 000 ms preier, morres mol na preier, neores preier, neores preier, neores preier, neores	And the second	26. June 100 100			AUG MUT STREET	Contract of the second	\$2009R	
2 State Control of the state of		11 Mar 10 Mar			COR. CA DINING COMMA	Contrast and some	Canton Social Contraction	
		24 AU	AN A LANDON DR.		THE PASSAGE CONTRACTOR	dama autorica includ		
					Para.	Contract Internation	A. 190.8%	
							State of the second	

Current status SS7 screening categories grouped by protocol layers



Current status Currently available solutions

Signalling Firewalls

Focused on protecting home network (HPLMN) and filtering illegal traffic originating from different PLMN countries implementing mainly GSMA recommendations

Currently commercial only

Filtering inside the Network elements

Depending on the vendor's capabilities

IDS and monitoring

Current status Possible SS7 filtering by existing infrastructure without FW

Better then no filtering

No easy path to enable message confidentiality and integrity protection

Every network element should protect itself

Most STPs can provide Cat1, Cat0 protections



Current status Conclusion

All these filtering categories more strictly validate the signalling messages according to 3GPP specification and the context of their use.

But no authenticity, integrity protection and confidentiality

Advanced signalling attacks

Advanced signalling attacks Category 2 attack example VLR profile manipulation

In Cat2 there is also manipulation of VLR profile

- MSISDN, SS, Camel trigger points manipulation, etc

blackhat USA 2017

VPLMN

IPLMN

Profile manipulation in VLR - Change of MSISDN - Provisioning of rogue Camel IN platform - Provisioning the CFx - Possible to change other attributes in VLR profile

MAP message to manipulate of the profile

Advanced signalling attacks Category 2 attack example GPRS/LTE profile manipulation

In Cat2 there is also manipulation of GRPS profile in SGSN or MME.

 Accessing the private APNs if there is no AAA used to authenticate APN VPLMN

MAP or Diameter message to manipulate of the profile (and for Diameter additionally to get back the cell-ID of the user)



Profile manipulation in SGSN/MME

- Change of MSISDN - Provision APN - Possible to change other attributes in GPRS profile (like QoS)

Advanced signalling attacks Category 3 attack example Hostile Location Update

In Cat3 there is also manipulation of GRPS profile in SGSN or MME.

MT SMS and MT Call interception or targeted MT DoS

VPLMN

MAP hostile locationUpdate to intercept mobile terminating call and SMS

HPLMN

Change MSC/VLR address in HLR ogue MSC/VLR address

Advanced signalling attacks Category 3 attack example Register/Activate SS

In Cat3 there is also manipulation of SS.

- CFx frauds, SMS forwarding and other

VPLMN

MAP message to manipulate the supplementary services of the subscriber

HPLMN

Change supplementary services - Provision call forwarding (CFx) - Manipulate other supplementary services



attributes in VLR profile

25

Advanced signalling attacks Category 3 protection bypass

Outbound-roamer in VPLMN: Attacker first performing hostile LocationUpdate (if need could use additionally spoofed Cancel Location) After performing Cat3 messages.

blackhat USA 2017



HPLMN is protected by

PSI check or by time/location comparison with previous

carrier

HPI N

Spoofed Cancel Location

Hostile Update Location

Advanced signalling attacks **MITM**

Man In The Middle traffic manipulation:

- Access into SS7 network by MITM in SCTP
- Possibility to inject traffic
- ISD/profile modification
- Authentication vectors modification (RES, IK, CK, AUTN)
- Possibility to modify the Result messages

SCTP (RFC 3257)

5.3 Security Issues with both TCP and SCTP

It is important to note that neither TCP nor SCTP protect itself from

man-in-the-middle attacks where an established session might be

hijacked (assuming the attacker can see the traffic from and inject

its own packets to either endpoints).

Advanced signalling attacks Passive Attacks

Mass collection of signalling data including mainly:

- SMS content with A-party, B-party information
- Locations (MAP, CAP, Diameter)
- From SS7 MAP it is possible to get CK, IK
- Decoding of TCAP TID which could be used for later attacks



Advanced signalling attacks Combining Passive and Active Attacks (MoTS)

By knowing the TCAP TID in real time and exact user location it could lead to more sophisticated attacks.

- Injection of messages into TCAP dialog, possibly hijacking the state machine in network elements and other effects
- Camel manipulation towards the IN platforms
- Better targeted spoofing of the SCCP messages
- Capturing the result messages to spoofed messages



Advanced signalling attacks Malformed messages

There are various ways of manipulating and malforming the messages. Various effects and possible impacts on the network.

Could lead to DoS or Exploitation Even DoS of the whole network



Advanced signalling attacks Conclusion

To address the above advanced types of attacks the signalling should be <u>confidentially and integrity protected</u>.

A firewall with only filtering could well protect the home subscribers in HPLMN. But the home subscribers in VPLMN or inbound-roamers in HPLMN could not be easily protected mainly because the SS7, Diameter is vulnerable to spoofing and the Location Update is not authenticated.

The encryption can be done on TCAP layer or Diameter/AVP. (the current work is using proprietary implementation using asymmetric encryption)

Messages can be integrity protected carrying signature. (the current work is using proprietary implementation

*IPSec is not suitable, because the SCCP and IPX network is required to perform routing. blackhat USA 2017

SigFW Open SS7 Firewall

Open SS7 Firewall Well positioned for signaling security enhancement



Open SS7 Firewall Features of Open SS7 Firewall

SS7 FW functionalities:

- Open SS7 TCAP encryption and signing of the SS7 messages, including auto encryption setup
- SS7 SCCP blacklists (Category 0)
- SS7 TCAP blacklists (Category 1)
- SS7 MAP firewall rules (Category 2)
- Signalling IDS integration (for Category 3 and advanced detection)
- SS7 Filtering and honeypoting
- Centralized threat reporting with mThreat integration
- Collaboration with other SS7 and signaling security systems
- Management through open APIs
- LUA programmable firewall rules
- Scalable/Decentralized solution

blackhat USA 2017

Mayen Restcomm

Build in Java Maven Using free Telestax Passive run (re-run traffic from pcap or passive interface to test the firewall).

Open SS7 Firewall Architecture

Frames are forwarded on SCCP layer (using SCCP state-machine)

Filtering is possible up to the application layer (in code SCCP, TCAP, MAP are currently implemented)



Open SS7 Firewall Architecture

Firewall is acting like M3UA server and M3UA client, without having SCCP GT.

Below is an illustration of the direction of links and associations establishment.


Open SS7 Firewall **Deployment**

Loopback on STP towards the FW



Open SS7 Firewall Progressive deployment & support in networks

Can be used by individual Network Element owner (e.g. HLR owner, SMSC owner)

Not the whole network == progressive introduction

Could provide protection of the individual Network Elements

Allows to deploy FW in limited scope to protect just select network elements, parts of the networks or individual links. blackhat USA 2017 © 2017 – P1 Security, All Rights Reserved

38

Open SS7 Firewall APIs

- Signaling Filter Push API (Manage Firewall Rules)
- Signaling Message Evaluation API (Message evaluation with external IDS signalling system)
- mThreat API (to report the detected attacks)

APIs allows to manage the FW and integrate it with other systems.

Open SS7 Firewall Config

JSON syntax (Compatible with P1 PTM IDS)

IP, SCTP, M3UA configuration

Firewall filtering rules

Config is periodically saved to store the changes

blackhat USA 2017

"firewall_rules": {

"firewall_rules_comment": "# Firewall filtering rules con

"firewall_policy_comment": "# Allowed value is one from: |
"firewall_policy": "DROP_WITH_SCCP_ERROR",

```
"SCCD": {
         "sccp comment": "# SCCP firewall rules",
        "calling gt whitelist": [
                 "/*"
        1,
        "calling gt blacklist": [
                 "10000000000",
                 "777*"
},
"tcap": {
        "tcap_comment": "# TCAP Cat1 firewall rules",
        "oc blacklist": [
                 "5",
                 "6".
                 "9",
                 "16",
                 "20",
                 "21".
                 "22",
                 "24",
                 "25",
```

Open SS7 Firewall Signaling Messages Evaluation API

- FW forwards the SCCP message to the Signalling IDS
- Signalling IDS responds back with the result (allow/filter message)
- FW performs the filtering action
- By this integration no need for the FW to contain it's own centralized DB and there could be deployed multiple FW instances
- Signalling IDS can handle more advanced Cat2, Cat3 detection, anomaly detection or threat intelligence decision



Open SS7 Firewall Open SS7 FW Passive Mode

Example of replayed traffic on localhost

"Passive mode"

8		*any																
File	Edit	<u>V</u> iew <u>G</u>	o <u>C</u> a	pture <u>A</u> na	alyze	Statisti	cs T	elephony	Wireles	s <u>T</u> ool	ls <u>H</u> elp							
		2 📀			3	9	(• 🐕	주 👱			÷,	Q					
	n3ua																Expression	4
	44077 44078 44078 44078 44078 44078 44078 44088 44088 44089 44089 44089 44089 44089 44089 44089	6 158695 8 158695 9 158695 2 158695 2 158695 8 158695 8 158699 1 158699 9 158699 1 158699 2 158699 8 158699 8 158699 3 158699 7 158703 7 158703	542 553 554 556 753 576 576 577 578 777 732 783 929	234 343 343 234 343 234 343 234 343 234 343 234 234	5 3 3 5 3 3 5 3 3 4 4 4 4 4 4 4 5 4 5 5 5 5	3433 2345 2345 3433 2345 3434 2344 2344	127.0 127.0 127.0 127.0 127.0 127.0 127.0 127.0 127.0 127.0 127.0 127.0 127.0 127.0 127.0	.0.1 .0.1 .0.1 .0.1 .0.1 .0.1 .0.1 .0.1	127. 127. 127. 127. 127. 127. 127. 127. 127. 127. 127. 127. 127. 127. 22. 2	0.0.1 0.0.1 0.0.1 0.0.1 0.0.1 0.0.1 0.0.1 0.0.1 0.0.1 0.0.1 0.0.1 0.0.1 0.0.1 0.0.1 0.0.1		43UA 43UA 43UA 43UA 43UA 43UA 43UA 43UA	(RFC (RFC (RFC (RFC (RFC (RFC (RFC (RFC	466 466 466 466 466 466 466 466 466 466	3:	80 96 104 104 96 80 96 104 104 96 300 296 1644	0 ASPUP 0 ASPUP_ACK 6 NTFY 4 SACK ASPAC_ACK 6 NTFY 0 ASPUP_ACK 6 NTFY 4 SACK ASPAC_CK 6 NTFY 4 SACK ASPAC_CK 6 NTFY 6 Invoke forwardSM 6 Invoke forwardSM 6 Invoke forwardSM	
	44099 44100 44100 44101 44102 44102 44102 44103 44103	9 158703. 5 158704. 7 158704. 9 158704. 7 158704. 1 158704. 5 158704. 9 158704. 9 158704. 1 158704. 7 158704. 7 158704.	981 129 181 329 381 529 581 729 781 929	234 234 234 234 234 234 234 234 234 234	4 5 4 5 4 5 4 5 4 5 4 5 4 5 4 5	3434 3433 3434 3433 3434 3433 3434 3433 3434 3433	1 1 1 1 1 1 1 1		2 2 2 2 2 2 2 2 2 2 2 2 2 2 2 2 2 2 2		0 1 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0	3SM N 3SM N TCAP GSM N GSM N GSM N GSM N GSM N GSM N	MAP MAP MAP MAP MAP MAP MAP MAP		10 30 15 30 30	9344 9776 6856 0716 5248 0000 5176 0852 2420 9560	4 returnResultast updatelocation invoke sendAuthenticat. 6 invoke sendAuthenticationInfo invoke insertSubscriberD. 6 returnResultast sendAuthenticationInfo invoke insertS. 8 invoke sendAuthenticationInfo invoke sendAuthenticatio. 6 invoke sendAuthenticationInfo returnResultast sendAut. 6 returnResultast sendAuthenticationInfo invoke updat. 9 returnReror invoke sendAuthenticationInfo invoke updat. 9 invoke sendAuthenticationInfo returnError invo. 9 invoke sendAuthenticationInfo invoke updat. 9 invoke sendAuthenticationInfo invoke updat. 9 invoke.sendAuthenticationInfo invoke sendAuthenticatio. 9 invoke.sendAuthenticationInfo invoke sendAuthenticationInfo invoke invoke.	100 00 50 500 10 50 500 0
<pre>+ LISMSTG + + + + + + + + + + + + + + + + + + +</pre>	rame 4 inux c nterne tream TP 3 L ignall ransac SM Mob ► Comp ► i SM SMS	40974: 3 socked ca th Protoc Control Iser Adap ing Conn tion Cap ing Cap Cap ing Cap Cap ing Cap Cap Cap ing Cap Cap Cap Cap Cap Cap Cap Cap Cap Cap	00 byt pture pl Ver Transm tation ection abilit icatio NVOKE SM 03.	es on wir sion 4, S ission Pr Capter Control ies Appli (1) (1) 40) SMS-E	e (24 Src: 1 Otoco Part Licatio	00 bits 27.0.0. 1, Src n Part R), 30 1, Ds Port:	00 bytes st: 127.6 : 2345 (2	capture).0.1 2345), D	d (2400	0 bits) t: 3433	on i (343	Lnter1 33)	face (9		$ \begin{array}{c} \begin{array}{c} \begin{array}{c} \begin{array}{c} \begin{array}{c} \begin{array}{c} \begin{array}{c} \begin{array}{c}$	
0	💙 м	TP 3 User	Adapta	tion Layer	: Proto	col										1	Packets: 745383 · Displayed: 2923 (0.4%) Profile: Default	ĺ

Open SS7 Firewall Open SS7 FW Passive Mode

Passive mode is implemented in VM in the following way:

- 1. tshark live capture to Json EK
- SS7ClientLiveInput is reading sccp_raw from named pipe and forwarding it to FW
- 3. SS7FW performs the filtering
- 4. SS7Server receives the unfiltered traffic

Passive mode can enable to evaluate and validate the FW without deploying it actively into the network

Open SS7 Firewall SS7 Encryption / Signatures

Current version is also capable of

- Signing/Verifying the SS7 message
- Encrypting/Decrypting SS7 messages

Public/Private keys are used and the security model is similar to email security (signing, encrypting).

Encryption is performed on TCAP level to pass through the STPs. SCCP layer is not encrypted, but the SCCP addresses are used to calculate signature. Encryption or Signatures could be optionally enabled. blackhat USA 2017

Open SS7 Firewall SS7 Encryption Config

"encryption_rules": {

"called_gt_encryption": [

"called_gt": "0*",

GT prefix defining the PLMN where this public key should be used

"public_key":

"MIGfMA0GCSqGSIb3DqEBAQUAA4GNADCBiQKBgQCm/PAsX0j7cjirJsQsiIfHauFNLwBIuM1brkUm3aVXeraDIej2BWXmW1KMmX/FRZh4Qhe9mUy6YgwT08PndWdMDRWMw8vvXJ FI7HPJpsNfcBykefSqhr5X4h6HyQr63V800U5PtgCBuVoyu0FIj84WFwaLuajHiQgps7N0loeH1WIDAQAB"

Public Key Encoded by Base64

"called_gt_decryption": [

},

"signature_rules": {

"calling_gt_verify": [

Open SS7 Firewall SS7 Encryption Flow



Open SS7 Firewall SS7 Encryption Algorithm

- 1. The whole TCAP layer is encrypted
- 2. The following payload is created:
 - a. version (4 bytes)
 - b. encrypted(timestamp (4 bytes) + tcap_layer) // If the key is short the multiple similar blocks are created
- Encryption algorithm should be mapped with version. Currently only RSA/ECB/PKCS1Padding is used in the code
- 4. Timestamp is verified after decryption to prevent attacks replay

Open SS7 Firewall SS7 Encryption Example

25890 2017-04-04 2344	3434 111111111111	VLR	(Visitor Location Re.	00000000000	HLR	(H	1111111 GSM M	P 226 000003b	invoke processUnstructuredSS-R
25891 2017-04-04., 2345	3433 11111111111	HLR	(Home Location Regis	00000000000	VLR	(V	111111. GSM M	P 222 0000003c	invoke unstructuredSS-Request
25893 2017-04-04 2349	3439 111111111111.11	HLR	(Home Location Regis	00000000000	VLR	(V	TCAP	614	XUDT (Message reassembled) XUD
25895 2017-04-04 2344	3434 11111111111	HLR	(Home Location Regis	00000000000	VLR	(V	111111 GSM M/	P 226 0000003c	invoke unstructuredSS-Request
25897 2017-04-04. 2345	3433 11111111111	HLR	(Home Location Regis	00000000000	VLR	ív.	111111. GSM M	P 210 0000003d	invoke unstructuredSS-Notify
25899 2017-04-04 2349	3439 11111111111	HLR	(Home Location Regis.	000000000000	VIR	(V.	SCCP	362	XUDT (Message reassembled)
• 25903 2017-04-04 2349	3439 11111111111	HLR	(Home Location Regis	000000000000	VLR	(V	TCAP	170	XUDT (Message reassembled)
25904 2017-04-04., 2344	3434 11111111111	HLR	(Home Location Regis	00000000000	VLR	(V	111111 GSM M	P 218 0000003d	invoke unstructuredSS-Notify
25905 2017-04-04 2345	3433 1111111111	asmS	CF (MAP) or IM-SSF (00000000000	HLR	сн.	GSM M	P 206 000003e	invoke anvTimeSubscriptionInte
25909 2017-04-04 2345	3433 1111111111	HLR	(Home Location Regis	00000000000	MSC	(M	GSM M	P 182 0000003f	invoke informServiceCentre
25910 2017-04-04 2349	3439 1111111111	HLR	(Home Location Regis	00000000000	MSC	(M	SCCP		XUDT (Message reassembled)
25913 2017-04-04 2349	3439 1111111111	HLR	(Home Location Regis	00000000000	MSC	(M	TCAP	170	XUDT (Message reassembled)
25914 2017-04-04 2344	3434 1111111111	HLR	(Home Location Regis	00000000000	MSC	(M	GSM MA	P 190 0000003f	invoke informServiceCentre
25915 2017-04-04 2345	3433 1111111111	HLR	(Home Location Regis	00000000000	MSC	(M	GSM M	P 190 00000040	invoke alertServiceCentre
25917 2017-04-04 2349	3439 11111111111, 11	HLR	(Home Location Regis	00000000000,	MSC	(M	TCAP	486	XUDT (Message reassembled) XUD
25919 2017-04-04 2344	3434 11111111111	HLR	(Home Location Regis	00000000000	MSC	(M	GSM M	P 198 00000040	invoke alertServiceCentre
25921 2017-04-04 2345	3433 1111111111	gsmS	CF (MAP) or IM-SSF (00000000000	HLR	(H	GSM MA	P 206 00000041	invoke anyTimeModification
25925 2017-04-04 2345	3433 1111111111	HLR	(Home Location Regis	00000000000	VLR	(V	GSM MA	P 190 00000042	invoke readyForSM
25926 2017-04-04 2349	3439 1111111111	HLR	(Home Location Regis	000000000000	VLR	(V	SCCP	362	XUDT (Message reassembled)
25929 2017-04-04 2349	3439 1111111111	HLR	(Home Location Regis	00000000000	VLR	(V	TCAP	170	XUDT (Message reassembled)
25930 2017-04-04 2344	3434 1111111111	HLR	(Home Location Regis	00000000000	VLR	(V	GSM MA	P 194 00000042	invoke readyForSM
25931 2017-04-04 2345	3433 1111111111	VLR	(Visitor Location Re	00000000000	HLR	(H	GSM M	P 194 00000043	invoke purgeMS
25933 2017-04-04 2349	3439 11111111111, 11	VLR	(Visitor Location Re	00000000000,	HLR	(H	TCAP	486	XUDT (Message reassembled) XUD
25935 2017-04-04 2344	3434 11111111111	VLR	(Visitor Location Re	00000000000	HLR	(H	GSM M	P 198 00000043	invoke purgeMS
25937 2017-04-04 2345	3433 1111111111	MSC	(Mobile Switching Ce	00000000000	MSC	(M	GSM M	P 186 00000044	invoke prepareHandover
25941 2017-04-04 2345	3433 1111111111	MSC	(Mobile Switching Ce	00000000000	MSC	(M	GSM M	P 182 00000045	invoke prepareSubsequentHandov
25943 2017-04-04 2345	3433 1111111111	HLR	(Home Location Regis	000000000000	VLR	(V	GSM M	P 190 00000046	invoke provideSubscriberInfo
Erame 25003: 170 bytes on Wi	re (1360 bits) 170 b	tes c	antured (1260 bits) (n interface O		0000	00 00 00 00	00 00 00 00 75	19 20 27 2d 20 bb f6
Ethernet II Src: 00:00:00 0	0:00:00 (00:00:00:00:00:00:00:00:00:00:00:00:00:	00.001	Det: 00:00:00 00:00).00 (00.00.00	· 00 ·	0010	63 ae ad 1b	57 ea dd 52 Af	ce a7 de 55 e5 7e h3 c W R O
Internet Protocol Version 4	Src: 127 0 0 1 Det:	127 6	0 1			0020	8d of ed be	a5 83 2h h8 da	32 dh ed 07 he 8h 6a
Stream Control Transmission	Protocol Src Port: 2	249 (2	(349) Det Port · 3439	(3439)		0030	b6 ad 3e 31	62 20 9h 7f 50	8e 27 97 c7 e8 0c 0f >1h P
MTP 3 User Adaptation Laver	1000001, 510 POIL. 20	(2		(0400)		0040	ff d3 c2 9h	4f a3 83 0h 7d	3f c4 03 3d 34 3b 73
Signalling Connection Control	1 Part					0050	45 ac 96 44	Af b4 55 7b db	3a 7f 3d 5c c6 a3 ed E D U
E2 Message fragments (264 by)	tes): #25899(229) #2	5903(3	5)1			0060	82 ab 38 30	a9 46 2d 6b 6c	48 8d e6 7e cd 3e 20 80 E-k 1
Transaction Capabilities App	lication Part					0070	6f d0 f0 f5	ee 1a 31 f6 cc	11 81 94 d3 2c 56 ff 01.
The second secon						0080	03 09 5f ee	3d 69 0c e7 9c	5a 60 81 01 77 47 82
						0000	f5 o6 47 09	14 01 51 61 49	c7 ac fa f2 59 dd bf

00a0

ce 40 fb d6 1d 12 b3 fc 80 e0 c0 88 ca a1 93 41

Open SS7 Firewall SCCP UDT / XUDT

XUDT messages has been seen on the previous slide.

The XUDT is used instead of UDT if the payload size has increased and reached the maximum limit of UDT message.

After decryption on the other end the message is again reconstructed into UDT message.

Open SS7 Firewall SS7 Encryption Autodiscovery

Feature to enable encryption autodiscovery

- 1. The FW #1 will send a MAP Invoke (New OpCode 99) for destinations with no known Public Keys
- 2. If there FW #2 is in the path, it processes the Invoke and sends Result (including GT prefix and Public Key)
- 3. FW #1 config is updated with gathered Public Keys



Autodiscover should enable easier key management blackhat USA 2017

© 2017 – P1 Security, All Rights Reserved 50

Open SS7 Firewall SS7 Encryption Flow - autodiscovery



Open SS7 Firewall TCAPsec comparison

	Current Encryption	TCAPsec
Last update	2017	3GPP Rel.7 2006
History	Reuse email security principles	Evolved from MAPsec (Mapsec was deprecated)
Type of encryption	Asymmetric Integrity and Confidentiality is independent (like in email security: signature and encryption)	Symmetric AES Point to Point Protection Mode 1 and 2 (with Confidentiality)
Key exchange	Public Keys Autodiscovery	Manual exchange between every 2 operators

Open SS7 Firewall SS7 Signature

For every TCAP Begin, the signature Invoke is added, containing the TCAP signature



Open SS7 Firewall SS7 Signature Algorithm

- 1. Only TCAP Begins are signed
- 2. Check if the TCAP already contains some TCAP Invoke signature component. If not, sign it.

3. TCAP signature component will contain:

- a. version
- b. timestamp
- c. signature

4. Signature is calculated:

- a. String dataToSign = calling_gt_digits + called_gt_digits + timestamp + tcap_layer
- b. String tcap_layer = base64(tcap_component_1) + ... + base64(tcap_component_N);
- c. String dataToSign is then hashed (currently in code SHA256WithRSA is used)

Open SS7 Firewall SS7 Signature

79324 2017-04-07 2344	3434					M3UA	(78	3	ASPUP		
79326 2017-04-07 3434	2344					M3UA	(78	3	ASPUP_A	CK	
79328 2017-04-07 3434	2344					M3UA	(94	4	NTFY		
79329 2017-04-07 2344	3434					M3UA	(102	2	SACK AS	PAC	
79330 2017-04-07 3434	2344					M3UA	(10;	2	SACK AS	PAC ACK	
79332 2017-04-07 3434	2344					M3UA	(94	1	NTEY		
79334 2017-04-07 2345	3433 1111111111	MSC (Mobile Switching	Ce 0000000000	MSC	(M.,	GSM M	AP 170	00000000	invoke U	Jnknown GSM-MAP opcou	le
79336 2017-04-07 2345	3433 11111111111	MSC (Mobile Switching	Ce 0000000000	MSC	(M	GSM M	AP 170	00000001	invoke I	Inknown GSM-MAP onco	le
79356 2017-04-07 2344	3434 11111111111	MSC (Mobile Switching	Ce 0000000000	MSC	(M	GSM M	AP 318	3 00000000	invoke l	Inknown GSM-MAP oncou	ie .
79360 2017-04-07 2345	3433 11111111111	VIR (Visitor Location	Re. 00000000000	HIR	ζH.	GSM M	AP 200	5 00000002	invoke i	indatel ocation	
79365 2017-04-07 2344	3434 111111111111111111	MSC (Mobile Switching	Ce 0000000000	MSC	(M	GSM M	AP 620	6 00000001	invoke l	Inknown GSM-MAP oncor	ie .
79367 2017-04-07 2345	3433 11111111111	HLR (Home Location Re	dis 0000000000	A VIR	(V	GSM M	AP 186	6 00000003	invoke (cancellocation	
79369 2017-04-07 2344	3434 11111111111	HLR (Home Location Re	die 33333333333	8 MSC	(M	GSM M	AP 33/	1 000000003	invoke	cancellocation invoke	
79372 2017-04-07 2345	3/33 11111111111	HLR (Home Location Re	dis 000000000000000000000000000000000000		(M	GSM M	AD 220	5 00000000	invoke	arovideRoamingNumber	-
79374 2017-04-07 2345	3/23 11111111111	HLR (Home Location Re	gis 00000000000	a a man	CE.	GSM M	AD 10/	1 00000000	invoke	ateSubscriberDataMo	tif
79375 2017-04-07 2344	3434 11111111111	HLR (Home Location Re	die 333333333333	s MSC	(M	GSM M	AD 343	2 000000005	invoke	noteSubscriberDataMo	lif
79405 2017-04-07 2345	3/33 11111111111	MSC (Mohile Switching	Ce 000000000000000000000000000000000000	A MSC	(M	GSM M	AD 180	6 00000000	invoke	cosumeCallHandling	
70406 2017 04 07 2244	2424 1111111111	MSC (Mobile Switching	Co. 2222222222	MSC	(M	CSM M	AD 22	1 00000000	invoko	cocumeCallHandling i	
										esullecarrialiurriu ri	
70400 0047 04 07 0045	0400 4444444444	100 (100110 001100110g		100	N.	CON N	10 04	00000007			
FEXPERT Info (Warr	/Malformed): Unknown :	invokeData 100]		0160 0	1 12 00 0	00 01 0	00 00	00 02 03 0	0 00 05 0	9 80	
<pre>Expert Info (Warr <malformed packet)<="" pre=""></malformed></pre>	n/Malformed): Unknown :	invokeData 100]	-1- 000000000	0160 0 0170 0	1 12 00 00 3 0e 19 0	00 01 0	00 00	00 02 03 C 04 00 00 C		9 80	
Expert Info (Warr <malformed packets<br="">> Stream Control Transmission</malformed>	n/Malformed): Unknown :	invokeData 100]		0160 0 0170 0 0180 1	1 12 00 00 3 0e 19 01 2 07 00 1	0 00 01 0 0 12 06 0 1 04 11 1	00 00	00 02 03 0 04 00 00 0 11 11 01 e	0 00 05 0 0 00 00 0 4 62 81 e	9 80 9 0b 1 48	
 Expert Info (Warr <malformed li="" packetz<=""> Stream Control Transmission MTP 3 User Adaptation Laver </malformed>	//Malformed): Unknown : > Protocol	invokeData 100]		0160 0 0170 0 0180 1 0190 0	1 12 00 00 3 0e 19 01 2 07 00 1: 4 00 00 00	0 00 01 0 0 12 06 0 1 04 11 1 0 02 6b 1	00 00 00 11 11 11 Le 28	00 02 03 0 04 00 00 0 11 11 01 e 1c 06 07 0	0 00 05 0 0 00 00 0 4 62 81 e	9 80 9 0b 1 48k.(эн
 Expert Info (Warr <malformed li="" packet)<=""> Stream Control Transmission MTP 3 User Adaptation Layer Signalling Connection Control </malformed>	h/Malformed): Unknown : Protocol	invokeData 100]		0160 0 0170 0 0180 1 0190 0 01a0 0	1 12 00 00 3 0e 19 00 2 07 00 1: 4 00 00 00 1 01 a0 1:	0 00 01 0 0 12 06 0 1 04 11 1 0 02 6b 1 1 60 0f 8	00 00 00 11 11 11 Le 28 30 02	00 02 03 0 04 00 00 0 11 11 01 e 1c 06 07 0 07 80 a1 0	0 00 05 0 0 00 00 0 4 62 81 e 0 11 86 0 9 06 07 0	9 80 0 0b 1 48	н
 Expert Info (Warr Malformed Packet: Stream Control Transmission MTP 3 User Adaptation Layer Signalling Connection Contro Transaction Capabilities App 	n/Malformed): Unknown : Protocol DI Part Dication Part	InvokeData 100]		0160 0 0170 0 0180 1 0190 0 01a0 0 01b0 0	1 12 00 0 3 0e 19 0 2 07 00 1 4 00 00 0 1 01 a0 1 0 01 00 0	0 00 01 0 0 12 06 0 1 04 11 1 0 02 6b 1 1 60 0f 8	00 00 00 11 11 11 Le 28 30 02 31 b8	00 02 03 0 04 00 00 0 11 11 01 e 1c 06 07 0 07 80 a1 0 a1 2a 02 0	0 00 05 0 0 00 00 0 4 62 81 e 0 11 86 0 9 06 07 0	9 80 9 80 1 48 5 01k.(4 00	н
<pre>> [Expert Info (Warn</pre>	/Malformed): Unknown : Protocol Pl Part Nication Part	invokeData 100]		0160 0 0170 0 0180 1 0190 0 01a0 0 01b0 0 01c0 3	1 12 00 00 3 0e 19 00 2 07 00 1 4 00 00 00 1 01 a0 1 0 01 00 0 0 22 04 00	0 00 01 0 0 12 06 0 1 04 11 1 0 02 6b 1 1 60 0f 8 1 02 6c 8 3 11 11 1	00 00 00 11 11 11 Le 28 30 02 31 b8	00 02 03 0 04 00 00 0 11 11 01 e 1c 06 07 0 07 80 a1 0 a1 2a 02 0 11 11 11 f	0 00 05 0 0 00 00 0 4 62 81 e 0 11 86 0 9 06 07 0 1 01 02 0	9 80 0 0b 1 48k.(5 01k.(4 00 1 021*	рн
 Expert Info (Warr	h/Malformed): Unknown : Protocol Pl Part Dication Part	invokeData 100]		0160 0 0170 0 0180 1 0190 0 01a0 0 01b0 0 01b0 3 01c0 3 01d0 1	1 12 00 00 3 0e 19 00 2 07 00 1 4 00 00 00 1 01 a0 1 0 01 00 0 0 22 04 00 1 11 11 1	0 00 01 0 0 12 06 0 1 04 11 1 0 02 6b 1 1 60 0f 8 1 02 6c 8 3 11 11 1	00 00 00 11 11 11 Le 28 30 02 31 b8 11 11 07 11	00 02 03 0 04 00 00 0 11 11 01 e 1c 06 07 0 07 80 a1 0 a1 2a 02 0 11 11 11 1	0 00 05 0 0 00 00 0 4 62 81 e 0 11 86 0 9 06 07 0 1 01 02 0 1 81 07 1 1 11 f1 a	9 80 9 80 1 48 5 91k.(4 00 1 02l 1 11 0"	рн
<pre>> [Expert Info (Warr</pre>	n/Malformed): Unknown : Protocol DI Part Lication Part	InvokeData 100]		0160 0 0170 0 0180 1 0190 0 01a0 0 01b0 0 01c0 3 01c0 1 01c0 8	1 12 00 00 3 0e 19 00 2 07 00 1 4 00 00 00 1 01 a0 1 0 22 04 0 1 11 11 1 0 02 07 8	0 00 01 0 0 12 06 0 1 04 11 1 0 02 6b 1 1 60 0f 8 1 02 6c 8 3 11 11 1 1 f1 04 0 0 a1 81 8	00 00 00 11 11 11 Le 28 30 02 31 b8 L1 11 07 11	00 02 03 0 04 00 00 0 11 11 01 e 1c 06 07 0 07 80 a1 0 a1 2a 02 0 11 11 11 f 11 11 11 1	0 00 05 0 0 00 00 0 4 62 81 e 0 11 86 0 9 06 07 0 1 01 02 0 1 81 07 1 1 11 f1 a 1 64 64 8	9 80 0 0b 1 48 0 0 1 400 1 02 1 02 1 02 1 02 1 0" 6 04	р Н
<pre>> [Expert Info (Warr</pre>	/Malformed): Unknown : Protocol DI Part Dication Part	invokeData 100]		0160 0 0170 0 0180 1 0190 0 01a0 0 01b0 0 01c0 3 01d0 1 01e0 8 01f0 8	1 12 00 00 3 0e 19 00 2 07 00 1: 4 00 00 00 1 01 a0 1: 0 01 00 0: 0 22 04 00 1 11 11 1: 0 02 04 00 1 11 11 1: 0 02 04 00 1 11 1: 1 1: 1 1: 1 1: 0 02 07 00 00 0 00 00 0 00 00 0 00 00 0 00 00 0 00 0	0 00 01 0 1 2 06 0 1 04 11 1 0 02 6b 1 1 60 0f 8 1 02 6c 8 3 11 11 1 1 10 4 6 a1 81 8 7 7 5 5	00 00 00 11 11 11 12 28 00 02 01 b8 11 11 07 11 07 11 09 02	00 02 03 0 04 00 00 0 11 11 01 e 1c 06 07 0 07 80 a1 0 a1 2a 02 0 11 11 11 f 11 11 11 1 01 01 02 0	0 00 05 0 0 00 00 00 0 0 04 62 81 e 0 11 86 0 0 0 19 06 07 0 0 1 10 11 86 0 1 0 1 10 04 02 0 0 1 0 1 11 14 07 1	9 80 0 9b 1 48 5 01 4 00 1 02 1 02 1 11 0 04 1 101 1 101 1 102 1 101 1 101 1 101 1 102 1 101 1 101 1 102 1 102 1 101 1 102 1 103 1 103 1 103 1 103 1 103 1 103 1 103 1 103 1 103 1 104 1 105 1 104 1 105 <td>р н</td>	р н
<pre>> [Expert Info (Warr</pre>	h/Malformed): Unknown : Protocol DI Part Dication Part	invokeData 100]		0160 0 0170 0 0180 1 0190 0 01a0 0 01b0 0 01c0 3 01c0 3 01c0 1 01e0 8 01f0 8 0200 0	1 12 00 00 3 0e 19 00 2 07 00 1: 4 00 00 00 1 01 a0 1: 0 01 00 0: 0 22 04 00 1 11 11 1 0 02 07 80 a df 3c ff 4 c5 9f 80	0 00 01 0 1 2 06 0 1 04 11 1 0 02 6b 1 1 60 0f 8 1 02 6c 8 3 11 11 1 1 f1 04 6 0 a1 81 8 6 7f 55 a	00 00 00 11 1 11 1 28 30 02 31 b8 11 11 07 11 39 02 b 0b 00 e2	00 02 03 0 04 00 00 0 11 11 01 0 1c 06 07 0 07 80 a1 0 a1 2a 02 0 11 11 11 1 11 11 11 1 01 01 02 0 61 8a 67 0 91 f4 56 6	0 00 05 0 0 00 00 0 0 4 62 81 e 0 11 86 0 9 06 07 0 1 01 02 0 1 101 02 0 1 11 12 0 11 11 1 1 1 14 c4 c4 8 1 9 6 03 c 1 9 06 07 0 1 1 1 1 1	9 80 0 0b 1 48 5 01 1 02 1 02 1 02 1 02 1 01 1 02 1 01 1 02 1 01 1 01 1 03 1 04 1 03 1 03 1 04 1 03 1 04 1 05 1 04 1 05 1 05 1 05 1 05 1 05 1 05 1 05 1 05 1 05 1 05 1 05 1 05 <tr td=""></tr>	р Н
<pre>> [Expert Info (Warr</pre>	/Malformed): Unknown : Protocol D Part lication Part	InvokeData 100]		0160 0 0170 0 0180 1 0190 0 01a0 0 01b0 0 01c0 3 01d0 1 01e0 8 01f0 8 0210 5	1 12 00 00 3 0e 19 00 2 07 00 1: 4 00 00 00 1 01 a0 1: 0 22 04 00 1 11 11 1: 0 02 07 80 a df 3c ff 4 c5 9f 80	0 00 01 0 12 06 0 1 04 11 1 0 02 6b 1 1 60 0f 8 1 02 6c 8 3 11 11 1 1 f1 04 6 0 a1 81 8 6 ae db a 5 5 5 7 2	00 00 00 11 1 11 1 28 00 02 31 b8 11 11 07 11 39 02 00 00 00 00 00 00 00 00 00 00 00 00 0	00 02 03 0 04 00 00 0 11 11 01 e 1c 06 07 0 07 80 a1 0 a1 2a 02 0 11 11 11 1 11 11 11 1 01 01 02 0 61 8a 67 e 91 f4 56 6	0 00 05 0 0 00 00 00 0 02 00 01 4 62 81 e 0 11 86 01 9 06 07 0 1 11 161 07 1 11 17 1 1 64 c4 8 1 9b fb 1 7 9b fb 1 7 9c b3 1	9 80	рн
<pre>> [Expert Info (Warr</pre>	Protocol Plart Plication Part	invokeData 100]		0160 0 0170 0 0180 1 0190 0 01a0 0 01b0 0 01c0 3 01d0 1 01e0 8 01f0 8 0210 0 0210 0	1 12 00 00 3 0e 19 00 4 00 00 00 1 01 a0 1: 0 01 00 00 0 22 04 00 1 11 11 1: 0 02 07 80 a df 3c fo 4 c5 9f 80 9 a4 d3 b	0 00 01 0 1 2 06 0 1 04 11 1 0 02 6b 1 1 60 0f 8 1 11 11 1 f1 04 0 0 a1 81 8 6 7f 55 a 6 ae db a 5 5f 2 8 0 0f 2 8	00 00 00 11 11 11 12 28 00 02 11 b8 11 b8 11 11 07 11 09 02 10 02 10 02 10 02 10 02 10 02 10 02 10 02 10 02 10 00 11 11 11 11 11 11 11 11 11 11 11 11 1	00 02 03 0 4 00 00 0 11 11 01 e 1c 06 07 0 07 80 a1 0 11 11 11 f 11 11 11 f 11 11 11 1 01 01 02 0 61 8a 67 e 91 f4 56 6 cc 69 9 fb	0 00 05 0 0 00 00 00 0 0 0 00 00 0 4 62 81 e 0 11 86 0 9 06 07 0 1 01 02 0 1 11 11 11 1 64 c4 8 1 9b fb 1 7 06 b3 c 5 a4 c6 1 3 da 8.5 4	9 80 0 9b 1 48 5 91 4 40 1 92 1 92 1 92 1 92 1 92 1 92 1 92 1 93 6 94 1 80 5 92 YU.X.11.	р Н 1
<pre>> [Expert Info (Warr</pre>	n/Malformed): Unknown : Protocol DI Part Dication Part	invokeData 100]		0160 0 0170 0 0180 1 0190 0 0140 0 0140 0 0140 3 0140 1 0140 3 0140 3 0140 3 0140 3 0200 0 0210 5 0220 0 0220 2	1 12 00 00 3 0e 19 00 2 07 00 1 4 00 00 00 1 01 a0 1 0 01 00 0 0 22 04 00 1 11 11 1 1 11 1 1 11 1 4 c5 9f 8 9 a4 d3 b 9 ca bc d0 84 7a 1	000011 01206 01206 01411 0266 10411 0266 1104 0266 1111	00 00 11 1 11 1 2 28 1 58 1 11 07 11 07 11 09 02 10 0b 10 e2 10 0b 10 e2 11 0b 11 11 11 11 10 02 11 11 11 11 11 11 10 02 10 0 10 0 11 11 11 11 10 0 10 0	00 02 03 0 04 00 00 0 11 11 01 e 1c 06 07 0 07 80 a1 0 a1 2a 02 0 11 11 11 1 11 11 11 1 11 11 11 1 01 01 02 0 61 8a 67 e 91 f4 56 6 cc 69 9f b 0e 8a aac 0 da aa 6f 0	0 00 05 0 0 00 00 0 4 62 81 e 0 11 86 0 9 06 07 0 11 101 02 0 1 81 07 1 1 11 f1 a 1 14 c4 c4 1 90 65 c4 1 90 65 c4 1 90 65 c4 1 90 63 c1 3 da 8f 4 4 0d 7d 7d	9 80	р Н
<pre>> [Expert Info (Warr</pre>	A/Malformed): Unknown : Protocol Dl Part Llication Part Dcated (100)	InvokeData 100]		0160 0 0170 0 0180 1 0190 0 0140 0 0140 0 0140 3 0140 1 0140 8 0210 5 0220 0 0210 5 0220 2 0230 2 0240 3	1 12 00 00 3 0e 19 00 2 07 00 1: 4 00 00 01 1 01 a0 1: 0 01 00 0: 0 22 04 00 1 11 11 1: 1 11 1: 0 02 07 80 a df 3c fi 4 c5 9f 80 9 a4 d3 b 9 ca bc do 0 84 7a 1: 0 a9 3e 1:	0 00 01 0 01 0 1 1 0 0 0 0 0 0 1 1 0 0 1	00 00 11 1 11 1 21 1 21 1 21 20 02 1 58 1 11 07 11 07 11 09 02 1 05 0 02 1 58 1 11 07 10 07 100 07 100 07 100 07 100 07 100 07 100 07 100 07 100 07 1000	00 02 03 0 4 00 00 0 11 11 01 e 1c 06 07 0 a1 2a 02 0 11 11 11 1 11 11 11 1 11 11 11 1 01 01 02 0 61 8a 67 e 91 f4 56 6 0e 8a aa c 03 aa 6f 0 05 95 9a 1	0 00 05 0 0 00 00 00 0 4 62 81 e 0 1 86 0 71 86 9 06 07 0 1 81 07 1 1 01 02 0 1 81 07 1 1 11 11 11 11 11 1 <td>9 80 </td> <td>)H</td>	9 80)H
<pre>> [Expert Info (Warr</pre>	A/Malformed): Unknown : Protocol DI Part Dication Part Docated (100) 00 0/Malformed): Unknown :	invokeData 100]		0160 0 0170 0 0180 1 0190 0 01a0 0 01c0 3 01c0 3 01c0 3 01c0 8 0200 0 0210 5 0220 c 0230 2 0240 a 0250 7	1 12 00 00 3 0e 19 00 2 07 00 1: 4 00 00 00 1 01 a0 1: 0 01 00 0: 0 22 04 00 1 11 11 1: 1 11 1: 0 02 07 80 a df 3c ff 4 c5 9f 81 9 a4 d3 b 9 ca bc d0 0 84 7a 1: d a9 3e 1!	0 00 01 0 0 12 06 0 1 04 11 1 0 02 6b 0 1 60 0f 8 1 102 6c 8 3 11 11 0 0 a1 81 8 5 7f 55 a 6 ae db a 18 5 7f 55 a b 6 ae db a 5 c 0f 62 8 5 c 0f 62 8 6 6 ae db 6 8 6 af 6 7 5 6 ad 6 7 5 6 df 6 7 5 1 bd 0 7 5	00 00 00 00 11 11 12 12 13 02 14 11 15 02 16 02 17 11 19 02 10 00 11 00 12 00 13 00 14 00 15 00 16 00 17 11 18 00 10 02 10 02 11 00 12 02 13 02 14 00 15 00 16 02 17 02 18 00 19 02 10 02 11 03 12 04	00 02 03 0 04 00 00 0 11 11 01 01 1C 06 07 0 07 80 a1 2 11 11 2 02 0 11	0 00 05 0 0 00 00 0 4 62 81 e 0 1 81 0 1 9 06 07 0 1 01 02 0 1 11 11 11 1 1 14 64 0 5 1 9b fb 1 7 1 14 164 04 66 1 5 a4 c6 1 3 da 8f 4 4 0d 7d f 1 1 a a 44 0d 7d f 1 5a b5 e (2 97 5b 9 9 7 9 9	9 80	2H
<pre>> [Expert Info (Warr</pre>	A/Malformed): Unknown : Protocol Di Part Dication Part Dicated (100) 00 //Malformed): Unknown :	invokeData 100]		0160 0 0170 0 0180 1 0190 0 01a0 0 01a0 0 01b0 0 000 0 01b0 0 000 0 01b0 0 000 000 0000 000000	1 12 00 01 3 0e 19 01 2 07 00 1: 4 00 00 01 4 00 00 01 0 01 00 00 0 01 00 00 0 02 07 84 1 11 11 11 0 02 07 84 4 c5 of 84 9 a4 d3 b 9 ca b 9 0 84 7a 1 d a9 3e 11 3 0c 5a 13 4 25 9f 84 3 0c 5a 13 4 2 3 0c 5a 4 2 5 14 3	0 00 01 0 0 00 01 0 0 12 06 0 1 00 02 60 1 0 02 60 1 1 1 0 02 60 1 1 1 0 0 60 1 1 01 02 65 1 1 1 0 0 1 1 0 0 1 1 0 0 0 1 1 0 0 1 1 0 0 1 1 0 0 1 1 0 0 1 1 0 0 1 1 0 0 1 0 0 1 0 0 1 0 0 1 0 0 1 0 0 0 0 0 0 0 0 0 0 0 0	00 00 10 11 11 11 12 28 30 02 11 b8 11 11 39 02 10 0b 10 0b 10 0b 10 0b 10 0b 10 0b 10 0b 10 0b 11 11 11 11 10 0b 11 11 10 0b 10 11 10 0 10 02 10 05 10 05 100	00 02 03 0 04 00 00 0 1 11 11 01 6 07 0 1 <td< td=""><td>0 00 05 0 0 00 00 0 4 62 81 e 0 11 86 0 9 06 07 0 1 01 02 0 1 81 07 1 1 11 f1 a 1 64 c4 8 1 9b fb 1 1 16 dc4 8 1 9b fb 1 5 a4 c6 1 3 da 8f 4 1 5a b5 e c 97 5b 9 1 bc 9 5</td><td>9 80 0 0b 1 48 1 48 1 02 1 02 1 02 1 02 1 02 1 02 1 02 1 02 1 02 1 01 5 02 1 02 5 02 1 02 5 02 1 02 5 02 1 02 1 03 1 04 1 04 1 02 2 28 2 28 2 28 2 28 2 28 2 28 2 28 2 28 2 28 2 34 4 35 10</td><td>2H</td></td<>	0 00 05 0 0 00 00 0 4 62 81 e 0 11 86 0 9 06 07 0 1 01 02 0 1 81 07 1 1 11 f1 a 1 64 c4 8 1 9b fb 1 1 16 dc4 8 1 9b fb 1 5 a4 c6 1 3 da 8f 4 1 5a b5 e c 97 5b 9 1 bc 9 5	9 80 0 0b 1 48 1 48 1 02 1 02 1 02 1 02 1 02 1 02 1 02 1 02 1 02 1 01 5 02 1 02 5 02 1 02 5 02 1 02 5 02 1 02 1 03 1 04 1 04 1 02 2 28 2 28 2 28 2 28 2 28 2 28 2 28 2 28 2 28 2 34 4 35 10	2H

TCAP Signature in Additional Invoke with new OpCode

Open SS7 Firewall **DNAT to Honeypot**

After detecting an attack the FW could perform DNAT for a defined time period for the attacker's GT



56

FW supported actions: DROP_SILENTLY, DROP_WITH_SCCP_ERROR, DNAT_TO_HONEYPOT, ALLOW blackhat USA 2017 © 2017 – P1 Security, All Rights Reserved

Open SS7 Firewall **DNAT to Honeypot**

DNAT to new called GT

_															
	81418 2017-04-07 2345	3433 1111111111	MSC ((Mobile Switching	Ce 0000000000	O MS	C (M		GSM MAP	170	00000000	invoke	Unknown	GSM-MAP opco	ode
	81437 2017-04-07 2345	3433 1111111111	MSC ((Mobile Switching	Ce 0000000000	0 MS	C (M		GSM MAP	170	00000001	invoke	Unknown	GSM-MAP opco	ode
	81439 2017-04-07 2344	3434 1111111111	MSC (Mobile Switching	Ce 0000000000	O MS	C (M		GSM MAP	170	00000000	invoke	Unknown	GSM-MAP opco	ode
	81445 2017-04-07 2344	3434 1111111111	MSC ((Mobile Switching	Ce 0000000000	0 MS	C (M		GSM MAP	170	00000001	invoke	Unknown	GSM-MAP opco	ode
	81446 2017-04-07 2345	3433 1111111111	VLR (Visitor Location	Re 0000000000	0 HL	R (H		GSM MAP	206	00000002	invoke	updateL	ocation	1000000
	81451 2017-04-07 2344	3434 1111111111	VLR (Visitor Location	Re., 0000000000	0 HL	R (H		GSM MAP	206	00000002	invoke	updateL	ocation	
	81453 2017-04-07 2345	3433 11111111111	HLR (Home Location Reg	is. 00000000000	O VLI	R (V		GSM MAP	186	00000003	invoke	cancelL	ocation	
	81455 2017-04-07 2344	3434 11111111111	HLR ((Home Location Rec	is 33333333333	3 MS	C. (M		GSM MAP	186	00000003	invoke	cancelL	ocation	
	81458 2017-04-07 2345	3433 11111111111	HLR ((Home Location Rec	is 0000000000	0 VL	R (V		GSM MAP	226	00000004	invoke	provide	RoamingNumber	r
	81459 2017-04-07 2344	3434 11111111111	HLR	(Home Location Rec	is 333333333333	3 MS	C (M.		GSM MAP	226	00000004	invoke	provide	RoamingNumber	r
	81462 2017-04-07 2345	3433 11111111111	HIR	(Home Location Rec	is 00000000000	a asi	ISCE		GSM MAP	194	00000005	invoke	noteSub	scriberDataM	odif.
	81463 2017-04-07 2344	3434 11111111111	HIR	(Home Location Rec	15 333333333333	3 MS	C (M		GSM MAP	194	00000005	invoke	noteSub	scriberDataM	lodif.
	81466 2017-04-07 2345	3433 11111111111	MSC ((Mohile Switching	000000000000000000000000000000000000000	A MS	C (M		GSM MAP	186	00000006	invoke	resumeC	11Handling	Contraction of the second
	91467 2017-04-07 2344	2434 111111111111	MSC /	(Mobile Switching	Co. 3333333333333	2 MS	C (M		GSM MAP	186	000000000	invoke	resumeC	11Handling	
	91470 2017-04-07 2345	2422 11111111111	HIR	(Home Location Rec	10 000000000000000000000000000000000000				GSM MAP	214	00000000	invoke	insertS	theriberDate	
	91471 2017-04-07 2344	2424 11111111111	HR	(Home Location Reg	ic 22233333333	2 MS	C (M		GSM MAD	214	00000007	invoke	incertS	bacriberDat	a
	91471 2017 04 07 2245	2422 11111111111	ULP /	(Home Location Reg	ic 000000000000000000000000000000000000		CAL /		GSM MAD	104	00000000	invoko	dolotoS	ubcoriborDate	d
	31474 2017-04-07 2343	3433 1111111111	HIP	Home Location Reg	15	0 30	SIN (COM MAD	194	00000000	invoke	deletes	ibscriberDate	a
	314/5 2017-04-07 2344	3434 11111111111	HLR	Home Location Reg	1S. 33333333333	3 113	C (M		COM MAD	194	00000000	invoke	Geretes	ubscriber baca	a
	314/8 2017-04-07 2345	3433 1111111111	VLR	Visitor Location	Re 00000000000		R (H		GSM MAP	190	00000009	Invoke	SenuPar	ameters	
	314/9 2017-04-07 2344	3434 1111111111	VLR	Visitor Location	Re. 33333333333	3 113	C (M	144114	GSM MAP	190	00000009	invoke	Senural	ameters	
	81482 2017-04-07 2345	3433 111111111	VLK	VISITOR LOCALION	Re. 00000000000	0 HL	2 (H.	111	IT SM MARK	111	()()()()()()()()()()()()()()()()()()()	TOWNER	registe	SS	
	NAME 0047 04 07 0044	0101 11111111111	LUD (uttaiter Loostion		A MC		144444		000	22000000	invoke	registe		
	81486 2017-04-07 2344	3434 1111111111	VLR (Visitor Location	Re. 33333333333	3 MS	C (M	111111	L GSM MAP	222	0000000a	invoke	registe	rSS	
	81486 2017-04-07 2344	3434 1111111111	VLR ((Visitor Location	Re. 3333333333	3 MS	C (M	111111	L. GSM MAP	222	0000000a	invoke	registe	rSS	F
	81486 2017-04-07 2344 Called Party Address lengt	3434 11111111111 th: 11	VLR (Visitor Location	Re. 33333333333	3 MS	00 00	00 00	00 00 00 40 00 40	222 00 0	0000000a 0 00 00 00 00	invoke 0 08 00	45 02	rSS	E.
	81486 2017-04-07 2344 Called Party Address lengt Called Party address (11 t	3434 1111111111 th: 11 bytes)	VLR (Visitor Location	Re 33333333333	3 MS 0000 0010 0020	00 00 00 ac	111111 00 00 00 00 00 28	00 00 00 40 00 40	222 00 0 84 3	0000000a 0 00 00 00 b ca 7f 00	08 00 00 01	45 02 7f 00	rss	E.
	<pre>81486 2017-04-07 2344 Called Party Address leng Called Party address (11 t > Address Indicator SubSystem Number: MSC (</pre>	3434 1111111111 th: 11 bytes)	VLR	Visitor Location	Re. 33333333333	3 MS 0000 0010 0020 0030	00 00 00 ac 00 01	111111 00 00 00 00 09 28 65 00	00 00 00 40 00 40 0d 6a 15	222 00 0 84 3 34 e	0000000a 0 00 00 00 b ca 7f 00 a f9 00 00	invoke 0.08 00 0.00 01 0.00 00 0.00 00 0.00 00 0.00 03	registe 45 02 7f 00 00 03	····.@.@. ; (.j.4	E.
	Called Party Address leng ← Called Party Address (11 → Address Indicator SubSystem Number: MSC (← Called party address [MS]	3434 1111111111 th: 11 bytes) Mobile Switching Cent	VLR :er) (8	(Visitor Location	Re. 33333333333	3 MS 0000 0010 0020 0030 0040	00 00 00 ac 00 01 00 8c	111111 00 00 00 00 09 28 6b 0c	00 00 00 40 00 40 0d 6a 15 16 0e 00	222 00 0 84 3 34 e 06 0	0000000a 0 00 00 00 b ca 7f 00 a f9 00 00 0 03 00 00	invoke 0 08 00 0 00 01 0 00 00 0 00 03 0 00 64	registe 45 02 7f 00 00 03 01 00 02 10	SS @.@. ; (.j.4 k	E.
	Called Party Address leng ← Called Party Address (11 ← Called Party address (11 ← Address Indicator SubSystem Number: MSC (← Called or Calling SubS Cliptod to TCAP, TCAP, SCAP	3434 1111111111 th: 11 bytes) Mobile Switching Cent iystem Number: MSC (Mo DEN linked to GSW MADE	VLR (8) (8) (8) (8) (8)	(Visitor Location)) witching Center)	Re. 333333333333333333333333333333333333	3 MS 0000 0010 0020 0030 0040 0050	00 00 00 ac 00 01 00 8c 01 01	111111 00 00 00 00 09 28 6b 0c 00 00	00 00 00 40 00 40 0d 6a 15 16 0e 00 00 7c 00	222 00 0 84 3 34 e 06 0 06 0 06 0	0000000a 0 00 00 00 b ca 7f 00 a f9 00 00 0 03 00 00 0 08 00 00	invoke 0 08 00 0 00 01 0 00 00 0 00 03 0 00 64 0 00 05	registe 45 02 7f 00 00 03 01 00 02 10 02 80	rss @.@; (.j.4 k	E.
	<pre>81486 2017-04-07 2344 Called Party Address leng Called Party address (11) Address Indicator SubSystem Number: NSC (</pre>	3434 1111111111 bytes) Mobile Switching Cent system Number: MSC (Mo SN linked to GSM_MAP]	VLR (8) bile Su	(Visitor Location)) witching Center)	Re. 333333333333 (8)>	3 MS 0000 0010 0020 0030 0040 0050	00 00 00 ac 00 01 00 8c 01 01 00 6b	111111 00 00 00 00 09 28 6b 0c 00 00 00 00	00 00 00 40 00 40 0d 6a 15 16 0e 00 00 7c 00 00 01 00	222 222 244 24 34 26 06 06 06 00 00 00 00	0000000a 0 00 00 00 b ca 7f 00 a f9 00 00 0 03 00 00 0 08 00 00 0 02 03 00	invoke 0 08 00 0 00 01 0 00 03 0 00 64 0 00 05 0 0 05	45 02 7f 00 00 03 01 00 02 10 09 80	rss @.@; (.j.4 k 	E.
	<pre>81486 2017-04-07 2344 Called Party Address leng Called Party address (11) Address Indicator SubSystem Number: MSC (</pre>	3434 1111111111 th: 11 bytes) Mobile Switching Cent ystem Number: MSC (Mo iSN linked to GSM_MAP] es)	VLR ter) (8 bbile St	(Visitor Location)) Witching Center)	(8)>	3 MS 0000 0010 0020 0030 0040 0050 0060 0060	00 00 00 ac 00 01 00 8c 01 01 00 6b 03 0e	111111 00 00 00 00 09 28 6b 0c 00 00 00 00 19 0b	00 00 00 40 00 40 0d 6a 15 16 0e 00 00 7c 00 00 01 00 12 08 00	222 00 0 84 3 34 e 06 0 06 0 00 0 11 0	00000000a 0 00 00 00 b ca 7f 00 a f9 00 00 0 03 00 00 0 08 00 00 0 02 03 00 4 33 33 3	invoke 0 08 00 0 00 01 0 00 03 0 00 03 0 00 04 0 00 05 3 33 33 0 02 20	45 02 7f 00 00 03 01 00 02 10 09 80 03 0b	-SS (.j.4 	E. d
	<pre>S1486 2017-04-072344 Called Party Address leng Called Party address (11 Address Indicator SubSystem Number: NSC (</pre>	3434 1111111111 th: 11 bytes) Mobile Switching Cent Jystem Number: MSC (Mo IsN linked to GSM_MAP] ies) 00	VLR ter) (8 bbile Sr	(Visitor Location)) witching Center)	(8)>	0000 0010 0020 0030 0040 0050 0060 0060	00 00 00 ac 00 01 00 8c 01 01 00 6b 03 0e 12 06	111111 00 00 00 00 09 28 6b 0c 00 00 00 00 19 0b 00 11	GSM MAP 00 00 00 40 00 40 0d 6a 15 16 0e 00 00 7c 00 00 01 00 12 08 00 04 11 11	222 00 0 84 3 34 e 06 0 06 0 00 0 11 0 11 1	00000000a 0 00 00 b ca 7f 01 a f9 00 01 0 03 00 01 0 03 00 01 0 03 00 01 0 03 00 01 0 03 00 01 0 02 03 01 4 33 33 31 1 11 01 31	invoke 0 08 00 0 00 01 0 00 03 0 00 03 0 00 64 0 00 05 3 33 33 1 62 3b 0 0 5	registe 45 02 7f 00 00 03 01 00 02 10 09 80 03 0b 48 04 48 04	-55 (.j.4 	E. d 3333 =b;H.
	<pre>81486 2017-04-07. 2344 Called Party Address leng Called Party address [11] Address Indicator SubSystem Number: MSC (<called (9="" 0001="Numbering</td" 0x="" 0x4="" [linked="" byt="" calling="" global="" or="" s="" subs="" tcap="" tcap,="" title="" to="" translation="" type:=""><td>3434 1111111111 bytes) (Mobile Switching Cent System Number: MSC (Mc SSN linked to GSM_MAP] es) 00 g Plan: ISDN/telephony</td><td>VLR ter) (8 pbile Sr y (0x01</td><td>(Visitor Location) witching Center) 1)</td><td>Re</td><td>0000 0010 0020 0030 0040 0050 0060 0070 0080</td><td>00 00 00 ac 00 01 00 8c 01 01 00 6b 03 0e 12 06 00 00</td><td>111111 00 00 00 00 09 28 6b 0c 00 00 00 00 19 0b 00 11 00 03</td><td>00 00 00 40 00 40 0d 6a 15 16 0e 00 00 7c 00 00 01 00 12 08 00 04 11 11 6b 1a 28</td><td>00 0 84 3 34 e 06 0 06 0 00 0 11 0 11 1 18 0</td><td>00000000 0 00 00 00 b ca 7f 00 a f9 00 00 0 03 00 00 0 08 00 00 0 02 03 00 4 33 33 33 1 11 01 36 6 07 00 11 </td><td>invoke 0 08 00 0 00 01 0 00 00 0 00 03 0 00 64 0 00 05 3 33 33 d 62 3b 1 86 05 2 60 00</td><td>registe registe 45 02 7f 00 00 03 01 00 02 10 09 80 03 0b 48 04 01 01 02 02 03 0b 04 01 01 01 02 02 04 02 05 02 05 02 05 02 06 03 07 00 00 03 00 05 00 05 00 00 00 00 00 00 00 00 00</td><td>-SS (.j.4 </td><td>E. d 3333 =b;H.</td></called></pre>	3434 1111111111 bytes) (Mobile Switching Cent System Number: MSC (Mc SSN linked to GSM_MAP] es) 00 g Plan: ISDN/telephony	VLR ter) (8 pbile Sr y (0x01	(Visitor Location) witching Center) 1)	Re	0000 0010 0020 0030 0040 0050 0060 0070 0080	00 00 00 ac 00 01 00 8c 01 01 00 6b 03 0e 12 06 00 00	111111 00 00 00 00 09 28 6b 0c 00 00 00 00 19 0b 00 11 00 03	00 00 00 40 00 40 0d 6a 15 16 0e 00 00 7c 00 00 01 00 12 08 00 04 11 11 6b 1a 28	00 0 84 3 34 e 06 0 06 0 00 0 11 0 11 1 18 0	00000000 0 00 00 00 b ca 7f 00 a f9 00 00 0 03 00 00 0 08 00 00 0 02 03 00 4 33 33 33 1 11 01 36 6 07 00 11 	invoke 0 08 00 0 00 01 0 00 00 0 00 03 0 00 64 0 00 05 3 33 33 d 62 3b 1 86 05 2 60 00	registe registe 45 02 7f 00 00 03 01 00 02 10 09 80 03 0b 48 04 01 01 02 02 03 0b 04 01 01 01 02 02 04 02 05 02 05 02 05 02 06 03 07 00 00 03 00 05 00 05 00 00 00 00 00 00 00 00 00	-SS (.j.4 	E. d 3333 =b;H.
	<pre>81486 2017-04-07. 2344 Called Party Address leng Called Party address [11] Address Indicator SubSystem Number: MSC (<called calling="" or="" subs<br="">[Linked to TCAP, TCAP S Global Title 0x4 (9 byt Translation Type: 0x4 0001 = Numbering 0001 = Encoding</called></pre>	3434 1111111111 th: 11 bytes) (Mobile Switching Cent ystem Number: MSC (Mc SN linked to GSM_MAP] es) 00 g Plan: ISDN/telephony Scheme: BCD, odd num	VLR ter) (8 obile S y (0x01 ber of	(Visitor Location)) witching Center) 1) digits (0x01)	Re. 3333333333 (8)>	3 MS 0000 0010 0020 0030 0040 0050 0060 0070 0080 0090	C (M 00 00 00 ac 00 01 00 8c 01 01 00 6b 03 0e 12 06 00 00 01 a0	111111 00 00 00 00 09 28 6b 0c 00 00 00 00 19 0b 00 11 00 03 0d 60	00 00 00 40 00 40 0d 6a 15 16 0e 00 00 7c 00 00 01 00 12 08 00 04 11 11 6b 1a 28 0b a1 09	222 00 0 84 3 34 e 06 0 00 0 11 0 11 1 18 0 06 0	00000000 0 00 00 00 0 ca 77 00 0 3 00 00 0 03 00 00 0 08 00 00 0 02 03 00 4 33 33 33 1 11 01 33 6 07 00 1: 7 04 00 00	invoke 0 08 00 0 00 01 0 00 03 0 00 04 0 00 05 3 33 33 1 62 3b 1 86 05 0 0 00 0 00 01 0 00 01 0 00 00 0 00 03 0 00 05 3 3 33 1 62 3b 1 86 05 0 0 00 0 00 00 0 00 05 0 05 0 00 00 0 00 00 0 00 00 0 00 000 0 00 000 0 00 000 0 00000000	registe 45 02 7f 00 00 03 01 00 02 10 09 80 03 0b 48 04 01 01 02 03 04		E. d 3333 .=b;H.
	<pre>81486 2017-04-07 2344 Called Party Address leng Called Party address (11) Address Indicator SubSystem Number: MSC (</pre>	3434 1111111111 th: 11 bytes) (Mobile Switching Cent System Number: MSC (Mc SSN linked to GSM_MAP] :es) 00 g Plan: ISDN/telephony Scheme: BCD, odd num f Address Indicator: 1	VLR bbile S l y (0x01 ber of Interna	(Visitor Location)) Witching Center) 1) digits (0x01) ational number (0x	Re. 3333333333 (8)>	3 MS 0000 0010 0020 0030 0040 0050 0060 0070 0080 0090 0090 0080	C (M 00 00 00 ac 00 01 00 8c 01 01 00 6b 03 0e 12 06 00 00 01 a0 6c 17	111111 00 00 00 00 09 28 6b 0c 00 00 00 00 19 0b 00 11 00 03 0d 60 a1 15	00 00 00 40 00 40 0d 6a 15 16 0e 00 00 7c 00 00 01 00 12 08 00 04 11 11 6b 1a 28 0b a1 09 02 01 01	222 00 0 84 3 34 e 06 0 00 0 11 0 11 1 18 0 06 0 02 0	00000000 b ca 7f 00 b ca 7f 00 0 00 00 00 0 03 00 00 0 08 00 00 0 02 03 00 4 33 33 33 1 11 01 34 7 04 00 01 1 03 a3 00	invoke 0 08 00 0 00 01 0 00 00 0 00 03 0 00 64 0 00 05 3 33 33 1 62 3b 1 86 05 0 1 00 1 00 0 4 08	registe 7f 00 00 03 01 00 02 10 09 80 03 0b 48 04 01 01 02 03 11 11	-55 (.j.4 	E.
	<pre>81486 2017-04-07. 2344 Called Party Address leng Called Party address [11] > Address Indicator SubSystem Number: MSC (</pre>	3434 1111111111 th: 11 bytes) (Mobile Switching Cent System Number: MSC (Mc SSN linked to GSM_MAP] ies) 00 g Plan: ISDN/telephony Scheme: BCD, odd num f Address Indicator: 1 333333333333	VLR bbile S) y (0x01 ber of Interna	(Visitor Location)) wwitching Center) 1) digits (0x01) ational number (0x	Re. 333333333 (8)> (8)>	3 MSI 0000 0010 0020 0040 0050 0060 0070 0080 0090 0080 0090 0080 0090	00 00 00 ac 00 01 00 8c 01 01 00 6b 03 0e 12 06 00 00 01 a0 6c 17 11 11	111111 00 00 00 00 09 28 6b 0c 00 00 00 00 19 0b 00 11 00 03 0d 60 a1 15 11 11	00 00 00 40 00 40 0d 6a 15 16 0e 00 00 7C 00 00 11 00 12 08 00 04 11 11 6b 1a 28 0b a1 09 02 01 01 11 f1 0a	222 00 0 84 3 34 e 06 0 00 0 11 0 11 1 18 0 06 0 02 0 01 0	00000000a 0 00 00 00 0 0 0 00 00 a f9 00 00 00 0 0.3 00 0 0 0 0 0 0 0	Invoke 0 08 00 0 00 01 0 00 03 0 00 64 0 00 05 3 33 33 1 62 3b 1 86 05 0 01 00 1 86 05 0 01 00 0 01 00 0 00 01 0 00 05 0 00 00 0 00 000 0 00 000 0 00000000	registe 7f 00 00 03 01 00 02 10 09 80 03 0b 48 04 01 01 02 03 11 11	SS (.j.4 	E. d.
	<pre>81486 2017-04-07 2344 Called Party Address leng Called Party address (11) Address Indicator SubSystem Number: MSC (<called calling="" or="" subs<br="">[Linked to TCAP, TCAP S Global Title 0x4 (9 byt Translation Type: 0x4 0001 9 Numbering 0001 = Encoding .000 0100 = Nature of Called Party Digits: Calling Party Address leng</called></pre>	3434 1111111111 th: 11 bytes) (Mobile Switching Cent System Number: MSC (Mc SSN linked to GSM_MAP] :es) 00 g Plan: ISDN/telephony Scheme: BCD, odd num f Address Indicator: 1 3333333333 jth: 11	VLR bbile S] y (0x01 ber of Interna	(Visitor Location)) witching Center) 1) digits (0x01) ational number (0x	Re. 3333333333 (8)> (04)	3 MS/ 0000 0010 0020 0030 0040 0050 0060 0050 0060 0070 0080 0090 00a0 00b0	00 00 00 ac 00 01 00 8c 01 01 00 6b 03 0e 12 06 00 00 01 a0 6c 17 11 11	111111 00 00 09 28 6b 0c 00 00 00 00 19 0b 00 11 00 03 0d 60 a1 15 11 11	GSM MAP 00 00 00 40 00 40 0d 6a 15 16 0e 00 00 01 00 00 01 00 00 01 00 00 01 00 00 01 00 00 01 00 04 11 11 6b 1a 28 0b a1 09 02 01 01 11 f1 0a	2222 00 0 84 3 34 e 06 0 06 0 00 0 11 0 11 1 18 0 06 0 02 0 01 0	00000000 00000000 ca 7f 00 a 79 00 00 0 03 00 01 0 02 03 00 1 11 01 33 6 07 00 11 7 04 00 01 1 03 a3 00 0 00	Invoke 0 08 00 0 00 01 0 00 03 0 00 04 0 00 05 3 33 33 1 62 3b 1 86 05 0 1 00 1 04 08	registe 7f 00 00 03 01 00 02 10 09 80 03 0b 48 04 01 01 02 03 11 11	SS 	E. d 3333 =b;H.
	<pre>81486 2017-04-07. 2344 Called Party Address leng Called Party address (11) Address Indicator SubSystem Number: MSC (<called (11)="" (9="" .000="" 0001="Encoding" 0100="Nature" 0x4="" 0xx="" <="" [linked="" address="" byt="" calling="" global="" leng="" of="" or="" party="" pre="" s="" subs="" tcap="" tcap,="" title="" to="" translation="" type:=""></called></pre>	3434 1111111111 th: 11 bytes) (Mobile Switching Cent System Number: MSC (Mc SSN linked to GSM_MAP] :es) 00 g Plan: ISDN/telephony Scheme: BCD, odd num f Address Indicator: 1 3333333333333 gth: 11 bytes)	VLR bbile S) y (0x01 ber of Interna	(Visitor Location)) Witching Center) 1) digits (0x01) ational number (0x	Re. 3333333333 (8)> (8)>	3 MS/ 0000 0010 0020 0030 0040 0050 0060 0070 0080 0090 0090 0090	C (M 00 00 00 ac 00 01 00 8c 01 01 00 6b 03 0e 12 06 00 00 01 a0 6c 17 11 11	111111 00 00 09 28 6b 0c 00 00 00 00 19 0b 00 11 00 03 0d 60 a1 15 11 11	00 00 00 40 00 40 00 6a 15 16 0e 00 00 7c 00 00 7c 00 00 12 08 00 04 11 11 6b 1a 28 0b a1 09 02 01 01 11 f1 0a	222 234 00 0 84 3 34 e 06 0 06 0 00 0 11 0 11 1 18 0 06 0 01 0 01 0	0000000a 0000000a 0000000a 00000000 15000000000 000000000000 00000000000000 000000000000000000000000000000000000	Invoke 0 08 00 0 00 01 0 00 00 0 00 00 0 00 00 0 00 00 0 00 03 0 00 05 3 33 33 1 62 3b 1 86 05 0 01 00 1 04 08	registe 45 02 7f 00 00 03 01 00 02 10 09 80 03 0b 48 04 01 01 02 03 11 11		E. d 33333 =b;H.
	<pre>81486 2017-04-07. 2344 Called Party Address leng Called Party address (11) Address Indicator SubSystem Number: MSC (</pre>	3434 1111111111 th: 11 bytes) (Mobile Switching Cent System Number: MSC (Mc SSN linked to GSM_MAP] tes) 00 g Plan: ISDN/telephony Scheme: BCD, odd numi f Address Indicator: : 333333333333 gth: 11 bytes)	VLR bbile S } y (0x01 ber of Interna	(Visitor Location)) witching Center) 1) digits (0x01) ational number (0x	Re. 333333333 (8)> (8)>	MSI 0000 0010 0020 0030 0040 0050 0060 0060 0070 0080 0090 0040	C (M 00 00 00 ac 00 01 00 8c 01 01 00 6b 03 0e 12 06 00 00 01 a0 6c 17 11 11	111111 00 00 00 00 09 28 6b 0c 00 00 19 0b 00 11 00 03 0d 60 a1 15 11 11	00 00 00 40 00 40 00 40 00 40 00 6a 15 16 0e 00 00 7c 00 00 01 00 12 08 00 04 11 11 6b 1a 28 0b a1 09 02 01 01 11 f1 0a	222 233 34 e 06 0 06 0 00 0 11 0 11 1 18 0 06 0 01 0	00000000 0 00 00 00 b ca 7f 00 a 79 00 00 0 03 00 00 0 02 03 00 0 02 03 00 4 33 33 33 1 11 01 33 6 07 00 11 7 04 00 00 1 03 a3 00 0 00	invoke 0 08 00 0 00 01 0 00 03 0 00 64 0 00 64 0 00 64 0 00 64 0 00 65 3 33 33 1 62 3b 1 86 05 0 01 00 1 04 08	registe 45 02 7f 00 00 03 01 00 02 10 09 80 03 0b 48 04 01 01 02 03 11 11	SS 	E.
•	<pre>81486 2017-04-07 2344 Called Party Address leng Called Party address [11] Address Indicator SubSystem Number: MSC (</pre>	3434 1111111111 th: 11 bytes) (Mobile Switching Cent System Number: NSC (MC SSN linked to GSM_MAP] tes) 00 g Plan: ISDN/telephon; Scheme: BCD, odd num f Address Indicator: 3 3333333333 gth: 11 bytes) lication Part	VLR bbile S] y (0x01 ber of Interna	(Visitor Location)) witching Center) 1) digits (0x01) ational number (0x	Re. 3333333333 (8)> (8)>	3 MS/ 0000 0010 0020 0030 0040 0050 0060 0070 0080 0090 0080 0090 0080	C (M 00 00 00 ac 00 01 00 8c 01 01 00 6b 03 0e 12 06 00 00 01 a0 6c 17 11 11	111111 00 00 00 00 09 28 6b 0c 00 00 00 00 19 0b 00 11 00 03 0d 60 a1 15 11 11	GSM MAP 00 00 00 0d 6a 15 16 0e 00 00 01 00 00 01 00 00 11 11 6b 14 19 02 01 01 11 f1 0a	222 222 233 24 06 06 00 00 00 01 11 11 18 06 02 00 01 0 01 0	0000000a 0 00 00 0 b ca 7f 0 a f9 00 0 0 03 00 0 0 08 00 0 0 02 03 0 0 02 03 0 0 02 03 0 0 02 03 0 0 02 03 0 1 11 01 3 6 07 04 00 1 03 a3 0 0 00 0 0	Invoke 0 08 00 0 00 01 0 00 00 0 00 03 0 00 64 0 00 05 3 33 33 1 62 3b 1 86 05 0 01 00 1 04 08	registe 45 02 7f 00 00 03 01 00 02 10 09 80 00 04 80 48 04 01 01 02 03 11 11	SS 	E. d 3333 =b;H.

Ŧ

Open SS7 Firewall mThreat

Every firewalled event can be optionally sent to mThreat over mThreat API



FW Alerts can be anonymized and reported to central Threat intelligence blackhat USA 2017 © 2017 – P1 Security, All Rights Reserved

58

Open SS7 Firewall mThreat Example



SigFW Open Diameter Firewall

Open Diameter Firewall Overview

The source code contains also a **Diameter Firewall** with similar capabilities.

To address Diameter security is mainly important for 4G and 5G.

In Diameter, message spoofing brings additional vulnerability, because of Route-Records AVPs, the attacker can get back Diameter Answers to spoofed Origin-Host and Origin-Realm messages.

Open Diameter Firewall Features of Open Diameter Firewall

Diameter FW functionalities:

- Open Diameter encryption and signing of the Diameter messages, including auto encryption setup
- Diameter host and realms blacklists (Category 0)
- Diameter Command Code blacklists and Realm whitelist (Category 1)
- Diameter firewall rules (Category 2)
- Signalling IDS integration (for Category 3 and advanced detection)
- Diameter Filtering and honeypoting
- Centralized threat reporting with mThreat integration
- Collaboration with other Diameter and signaling security systems
- Management through open APIs
- Passive run (re-run traffic from pcap or passive interface to test the firewall)**jDiameter** LUA programmable firewall rules
- Scalable/Decentralized solution

blackhat USA 2017

Mayen[®] Restcomm

Build in Java Maven Using free Telestax Mobicent/Restcomm

License AGPLv3

Open Diameter Firewall Architecture

Frames are forwarded on SCTP layer

Filtering is possible up to the application layer (Diameter layer)



Open Diameter Firewall Architecture

Firewall is acting like SCTP server and SCTP client, without having Diameter Address. The Diameter CER, DWR, DPR or forwarded. Below is an illustration of the direction of links and associations establishment.



Open Diameter Firewall Deployment

Loopback on DRA towards the FW



Open Diameter Firewall Diameter Encryption flow



Open Diameter Firewall Diameter Encryption Algorithm

- 1. Encryption is at the Diameter AVP level
- 2. AVPs required for IPX carriers are unencrypted (mainly host, realm, route)
- 3. The following payload is encrypted for every AVP:
 - a. version (4 bytes)
 - b. encrypted(timestamp (4 bytes) + avp_bytes) // If the key is short the multiple similar blocks are created
- 4. Encryption algorithm should be mapped with version. Currently only RSA/ECB/PKCS1Padding is used in the code.
- 5. Timestamp is verified after decryption to prevent replay attacks

Open Diameter Firewall Diameter Encryption Example

147 62.930384208	127.0.0.1	127.0.0.1	DIAMET	462 cmd=3GPP-Notify Request(323) flags=R appl=3GPP S6a/S6d(16777251) h2h=4a49277c e2e=6f500011
148 62.931295117	127.0.0.1	127.0.0.1	DIAMET	426 SACK cmd=3GPP-Notify Answer(323) flags=E- appl=3GPP S6a/S6d(16777251) h2h=4a49277c e2e=6f500011
151 62.939193161	127.0.0.1	127.0.0.1	DIAMET	1334 SACK cmd=3GPP-Notify Answer(323) flags=E- appl=3GPP S6a/S6d(16777251) h2h=4a49277c e2e=6f500011
155 62.957918437	127.0.0.1	127.0.0.1	DIAMET	426 SACK cmd=3GPP-Notify Answer(323) flags=E- appl=3GPP S6a/S6d(16777251) h2h=4a49277c e2e=6f500011
156 62.957935581	127.0.0.1	127.0.0.1	DIAMET	410 SACK cmd=3GPP-Update-Location Request(316) flags=R appl=3GPP S6a/S6d(16777251) h2h=4a49277d e2e
159 62.966246812	127.0.0.1	127.0.0.1	DIAMET	1514 SACK cmd=3GPP-Update-Location Request(316) flags=R appl=3GPP S6a/S6d(16777251) h2h=4a49277d e2e
164 62.985854473	127.0.0.1	127.0.0.1	DIAMET	410 SACK cmd=3GPP-Update-Location Request(316) flags=R appl=3GPP S6a/S6d(16777251) h2h=4a49277d e2e
165 62.986540937	127.0.0.1	127.0.0.1	DIAMET	350 SACK cmd=3GPP-Update-Location Answer(316) flags=E- appl=3GPP S6a/S6d(16777251) h2h=4a49277d e2e=
168 62.992970061	127.0.0.1	127.0.0.1	DIAMET	1418 SACK cmd=3GPP-Update-Location Answer(316) flags=E- appl=3GPP S6a/S6d(16777251) h2h=4a49277d e2e=
173 63.009762391	127.0.0.1	127.0.0.1	DIAMET	350 SACK cmd=3GPP-Update-Location Answer(316) flags=E- appl=3GPP S6a/S6d(16777251) h2h=4a49277d e2e=
186 92.995232305	127.0.0.1	127.0.0.1	DIAMET	142 cmd=Device-Watchdog Request(280) flags=R appl=Diameter Common Messages(0) h2h=4a492fc2 e2e=70b0
187 92.996785046	127.0.0.1	127.0.0.1	DIAMET	142 cmd=Device-Watchdog Request(280) flags=R appl=Diameter Common Messages(0) h2h=4a492fc2 e2e=70b0
188 92.998244255	127.0.0.1	127.0.0.1	DIAMET	142 cmd=Device-Watchdog Request(280) flags=R appl=Diameter Common Messages(0) h2h=4a492fc2 e2e=70b0
189 92.999627596	127.0.0.1	127.0.0.1	DIAMET	166 SACK cmd=Device-Watchdog Answer(280) flags= appl=Diameter Common Messages(0) h2h=4a492fc2 e2e=
190 93.000873609	127.0.0.1	127.0.0.1	DIAMET	166 SACK cmd=Device-Watchdog Answer(280) flags= appl=Diameter Common Messages(0) h2h=4a492fc2 e2e=
191 93.002105486	127.0.0.1	127.0.0.1	DIAMET	166 SACK cmd=Device-Watchdog Answer(280) flags= appl=Diameter Common Messages(0) h2h=4a492fc2 e2e=
▶ Flags: 0x80, Requ	uest			
Command Code: 310	6 3GPP-Update-L	ocation		
ApplicationId: 30	GPP S6a/S6d (16	777251)		
Hop-by-Hop Ident:	ifier: 0x4a4927	7d		
End-to-End Ident:	ifier: 0x6f5000	14		
[Answer In: 168]				
AVP: Session-Id(2)	263) 1=48 f=-M-	val=CretedByDiameterLiveC	lient;14937	47508867
AVP: Unknown(1100)	0) l=136 f=	val=45e945a4a0758023a778a2	6b851e619db	996671e851e34178
AVP: Destination	-Host(293) 1=28	f=-M- val=aaa://127.0.0.1	:3868	
AVP: Unknown(1100)	0) l=136 f=	val=3650b1097190e791b8d03f	53f9eb1afff	bdc34cc5afdb80f
AVP: Origin-Host	(264) 1=59 f=-M	- val=		
AVP: Unknown(1100)	0) l=136 f=	val=79d158db1690d26781fffb	cbf040ec702	23dabc728bf5556a
AVP: Unknown(1100)	0) l=136 f=	val=035f530ec93c18f991225c	f91b05cc5dc	l4e167cb6d4c463b
AVP: Unknown(1100)	0) 1=136 f=	val=013d585de64a1ef1a06838	6d375827cb2	2de27e1c720dbf51
AVP: Unknown(1100)	0) 1=136 f=	val=5a1f8a2df193160d5fe39c	3231630e09d	2447ff00b879fd9
AVP: Unknown(1100)	0) l=136 f=	val=6510ea0a4bbd1c8ed21c50	fee483110cb	0141c2f58f3d1a98
AVP: Destination	-Realm(283) 1=2	8 f=-M- val=exchange.examp	le.org	
AVP: Origin-Real	m(296) 1=34 f=-	M- val=exchangeClient.exam	ple.org	

AVP: Unknown(1100) 1=264 f=--- val=7290d5360b1fcecbf95fe43055cb5f49ef273f3ce8a43b04...

Open Diameter Firewall Diameter Encryption Autodiscovery



Open Diameter Firewall Diameter Signature Algorithm

- 1. Only Diameter Requests are signed
- 2. Check if the Diameter message already contains some Diameter signature AVP. If not, sign it.

3. Diameter signature is Octet String of the following:

- a. version (4 bytes)
- b. timestamp (4 bytes)
- c. signature

4. Signature is calculated:

- a. String dataToSign = getApplicationId + ":" + CommandCode + ":" + EndToEndIdentifier +
 ":" + timestamp + diameter_layer;
- c. String dataToSign is then hashed (currently in code SHA256WithRSA is used)

Open Diameter Firewall Diameter Signature

368	258.634106162 127.0.0.1	127.0.0.1	DIAMET	330 cmd=3GPP-Authentication-Informatio	on Answer(318) flag	s=E- appl=3GPP	S6a/S6d(167	77251) h2h=4a	.49278
370	259.889738089 127.0.0.1	127.0.0.1	DIAMET	462 cmd=3GPP-Notify Request(323) flags	=R appl=3GPP S6	a/S6d(16777251)	h2h=4a492785	e2e=6f500031	1
374	259.896722807 127.0.0.1	127.0.0.1	DIAMET	602 cmd=3GPP-Notify Request(323) flags	=R appl=3GPP S6	a/S6d(16777251)	h2h=4a492785	e2e=6f500031	
378	259.902956863 127.0.0.1	127.0.0.1	DIAMET	462 cmd=3GPP-Notify Request(323) flags	=R appl=3GPP S6	a/S6d(16777251)	h2h=4a492785	e2e=6f500031	1
379	259.903929063 127.0.0.1	127.0.0.1	DIAMET	426 SACK cmd=3GPP-Notity Answer(323) f	lags=E- appl=3GP	P S6a/S6d(16///2	251) h2h=4a49	2785 e2e=6f50	0031
382	259.909959844 127.0.0.1	127.0.0.1	DIAMET	426 SACK cmd=3GPP-Notify Answer(323) f	lags=E- appl=3GP	P S6a/S6d(167772	251) h2h=4a493	2785 e2e=6f50	0031
385	259.915694965 127.0.0.1	127.0.0.1	DIAMET	426 SACK cmd=3GPP-Notify Answer(323) f	'lags=E- appl=3GP	P S6a/S6d(167772	251) h2h=4a49	2785 e2e=6f50	0031
386	259.921751307 127.0.0.1	127.0.0.1	DIAMET	410 SACK cmd=3GPP-Update-Location Requ	iest(316) flags=R	- appl=3GPP S6a/	S6d(16777251) h2h=4a49278	6 e2e
389	259.930512885 127.0.0.1	127.0.0.1	DIAMET	550 SACK cmd=3GPP-Update-Location Requ	iest(316) flags=R	- app1=3GPP S6a/	S6d(16777251) h2h=4a49278	6 e2e
392	259.936816424 127.0.0.1	127.0.0.1	DIAMET	410 SACK cmd=3GPP-Update-Location Requ	lest(316) Tlags=R	- app1=3GPP S6a/	S60(16///251) n2n=4a49278	6 e2e
393	259.937610346 127.0.0.1	127.0.0.1	DIAMET	350 SACK cmd=3GPP-Update-Location Answ	/er(316) Tlags=E-	app1=3GPP S6a/S	56d(16///251)	h2h=4a492786	e2e=
396	259.944006943 127.0.0.1	127.0.0.1	DIAMET	350 SACK cmd=3GPP-Update-Location Answ	/er(316) flags=E-	app1=3GPP S6a/S	56d(16///251)	h2h=4a492786	e2e=
399	259.948708460 127.0.0.1	127.0.0.1	DIAMET	350 SACK cmd=3GPP-Update-Location Answ	/er(316) flags=E-	app1=3GPP S6a/S	56d(16///251)	h2h=4a492786	e2e=
 Fla Com App Hop End End	gs: 0x80, Request mand Code: 316 3GPP-Update-Locatic licationId: 3GPP S6a/S6d (16777251 -by-Hop Identifier: 0x4A492786 -to-End Identifier: 0x6f500035 swer In: 396] : Session-Id(263) 1=48 f=-M- val=C : Auth-Application-Id(258) 1=12 f=- : Destination-Host(264) 1=59 f=-M- val= : User-Name(1) 1=23 f=-M- val= : User-Name(1) 1=23 f=-M- val= : User-SNVCC-Capability(1615) 1=16 : Destination-Realm(283) 1=28 f=-M : Origin-Realm(283) 1=28 f=-M : Userian (283) 1=28 f=-M : Userian (283) 1=28 f=-M : Userian (283) 1=28 f=-M : Origin-Realm(283) 1=24 f=-M: Origin-Realm(283) 1=24 f=-M : Origin-Realm(283) 1=24 f=-M: Origin-Realm(283) 1=24 f=-M: Origin-Realm(283) 1=24 f=-M:	cretedByDiameterLi -M- val=3GPP S6a/ val=aa://127.0. M- val=N_STATE_M GPP val=34 GPP val=24 GPP val=24 GPP val=5767629a635156154	veClient;149374 S6d (16777251) 0.1:3868 AINTAINED (1) =UE-SRVCC-NOT-S ample.org xample.org cample.org	17705878 NUPPORTED (0) 164dddf85a6fbe5					
	AVP Flags: UXUU								
	AVP Length: 140 Value: 7a57cfc20a92b15d1b4o56bfdo2	o195b1264dddf95a6	fho5						

Code

Diameter Signature in Additional AVP with new

SigFW Open Source SS7/Diameter firewall

Use cases
SigFW - Open Source SS7/Diameter firewall Use cases

Encrypted and integrity protected signalling traffic



SigFW - Open Source SS7/Diameter firewall Use cases

DNAT of attacker to honeypot



74

Related Open Source contributions

Related Open Source contributions tshark + Elasticsearch

Could be used as light monitoring and analytics solution

Easier detected signalling attacks targeting HPLMN users could be monitored directly in Kibana dashboard

Also applicable to different technology domains

Related Open Source contributions tshark + Elasticsearch

Collecting tshark json files

elastic

kıbana

Indexed data



Port-mirrored traffic into tshark probe

Various Statistics Security Dashboards

Conclusion

Conclusion
Source code

Source code is available at https://github.com/P1sec/SigFW

For more details also read BlackHat whitepaper

Conclusion VM

VM is available for download at https://github.com/P1sec/SigFW/wiki/VM

Ubuntu Server

eth0 management eth1 signalling (possible to configure the firewall here) eth2 passive signalling (used by tshark to feed the VM in passive mode) Installed ElasticSearch, Kibana All firewall modules as systemd services On localhost running SS7ClientLiveInput - > SS7Firewall -> SS7Server pcap -> tshark -> SS7ClientLiveInput eth2 -> tshark -> SS7ClientLiveInput eth2 -> tshark -> SS7ClientLiveInput

Conclusion Follow up / Next steps

- Review by security researchers
- Review by industry
- Possible wider adoption
- Move towards standardization of the used extensions
- Better and multiple encryption models

We would like to encourage everyone to contribute.

Conclusion Video Example

	7Server java × 🗟 SS7Firewall java 🗙 🗟 SS7Clienti iveloput java	×		.
-				
SOC		8 B A A 0 0 8 4		
1432 1433 1434 1435 1436 1437 1438 1439 1439 1440	<pre>comps = tcb.getComponent(); //</pre>) != null) { ess().getGlobalTitle() != null) { ify .comps) == 0) { igned messages		
Find				Nomatches
			C-III- D	rao maccries
NO S	s/rw.55/Firewail 🔰 🥥 oniviessage 🧨 switch (tag) 🔰 case FCB	eginmes (= nuil) > Ir (message.ge	ccalungPartyAddress() != null) 🦻 Ir (m	essage.getCalli
0	utput 🗴 🕼 Notifications 🗙 🔍 Search Results 🗙 🛞 on Message -	Naviga		
D	Run (SS7Server) × Run (SS7FirewallSecondInstance) × Run	n (SS7Fii	.) ×	
10	86493 [pool-24-thread-1] DEBUG ss7fw.SS7Firewall	- Add. a: ZQQ0/iyo3vZaCa4+H	=pSq895th9jlf6PG7589S2VRyZnAgC	mrmjM/BLbkFm
-	86494 [pool-24-thread-1] DEBUG ss7fw.SS7Firewall	- TCAPSCCP Called GT = 000	3000000	
100	86694 [pool-24-thread-1] DEBUG ss/fw.SS/Firewall	- [[[[[[]],		D MD-0
90	86695 [pool-24-thread-1] DEBUG ss7fw SS7Firewall	- MIP-IKANSFEK: UPC=1, DPC=2, SLS=5, MsgLe	1111111111	P, MP=0
	86695 [pool-24-thread-1] DEBUG ss7fw.SS7Firewall	- Sccp Msg [Type=UD] networkId=0 sls=5 inc	ominaOpc=1 incominaDpc=2 outac	inoDpc=-1 Ca
23	86698 [pool-24-thread-1] DEBUG ss7fw.SS7Firewall	- Adding TCAP Signed Data: 111111111110000	0000002102595790oQYCAQECA fw=	
	86698 [pool-24-thread-1] DEBUG ss7fw.SS7Firewall	 Adding TCAP Signature: BiQZjxp6hU6Yt41zx. 	JVB85IVf7avRFMillXPpB20SQzUeV9	/2Tt2+CKjBUR
	86700 [pool-24-thread-1] DEBUG ss7fw.SS7Firewall	 TCAP Encryption for SCCP Called GT = 000 	30000000 I	
	86896 [pool-24-thread-1] DEBUG ss7fw.SS7Firewall	- [[[[[[[[onMtp3TransferMessage	111111111	
	2009/ [pool-24-thread-1] DEBUG ss/Tw.SS/Firewall	- MIP-IKANSFER: UPC=1, DPC=2, SLS=5, MsgLei	יייייי, NI=International, SI=SCC	P, MP=0
	86898 [pool-24-thread-1] DEBUG ss7fw SS7Firewall	- Scop Msg [Type=UDT petworkId=0 s]s=5 inc	amingOnc=1 incomingOnc=2 outgo	indDoc=-1 Ca
	86903 [pool-24-thread-1] DEBUG ss7fw.SS7Firewall	- Adding TCAP Signed Data: 111111111110000	3000000210259579200YCA0ECAf0=	Tugope-i ca
	86903 [pool-24-thread-1] DEBUG ss7fw.SS7Firewall	- Adding TCAP Signature: SR0D7iI2ZikQfI0lT	yyUYa3j7Dx+p0UjgeqvxbgR0ZqUvST	pzBdm8j86Fce
	· · · · · · · · · · · · · · · · · · ·)D
		Due (CCCC) and Looker ()		

https://github.com/P1sec/SigFW/blob/master/docs/running_from_netbeans.gif

Conclusion Work done thanks to

Special thanks to:

Open Source projects

- Telestax jSS7, jDiameter
- Wireshark
- Elastic (ELK)

Conclusion Q&A

Thank you



Takeaways

- **Open-source SS7/Diameter firewall** (the reference implementation and the research project)
- Encryption and integrity protection of the signalling
- mThreat reporting and forwarding the attacker to honeypot