AdaptiveMobile Security

Protecting Mobile Networks and Infrastructure from External Threat Actors

22nd of October 2021

Introduction

Welcome!

Presenter: Qusai Qaryouti & Mohamed Darweesh

SS7 & Signaling Basics

- What is SS7?

  A standard (devised in an era where security was not a primary concern) that defines how network elements in a public switched telephone network (PSTN) exchange information over a digital signalling network. For the purposed of this session, we care mostly about 2 application layer protocols, MAP (Mobile Application Part) & CAMEL (Customised Applications for Mobile networks Enhanced Logic).

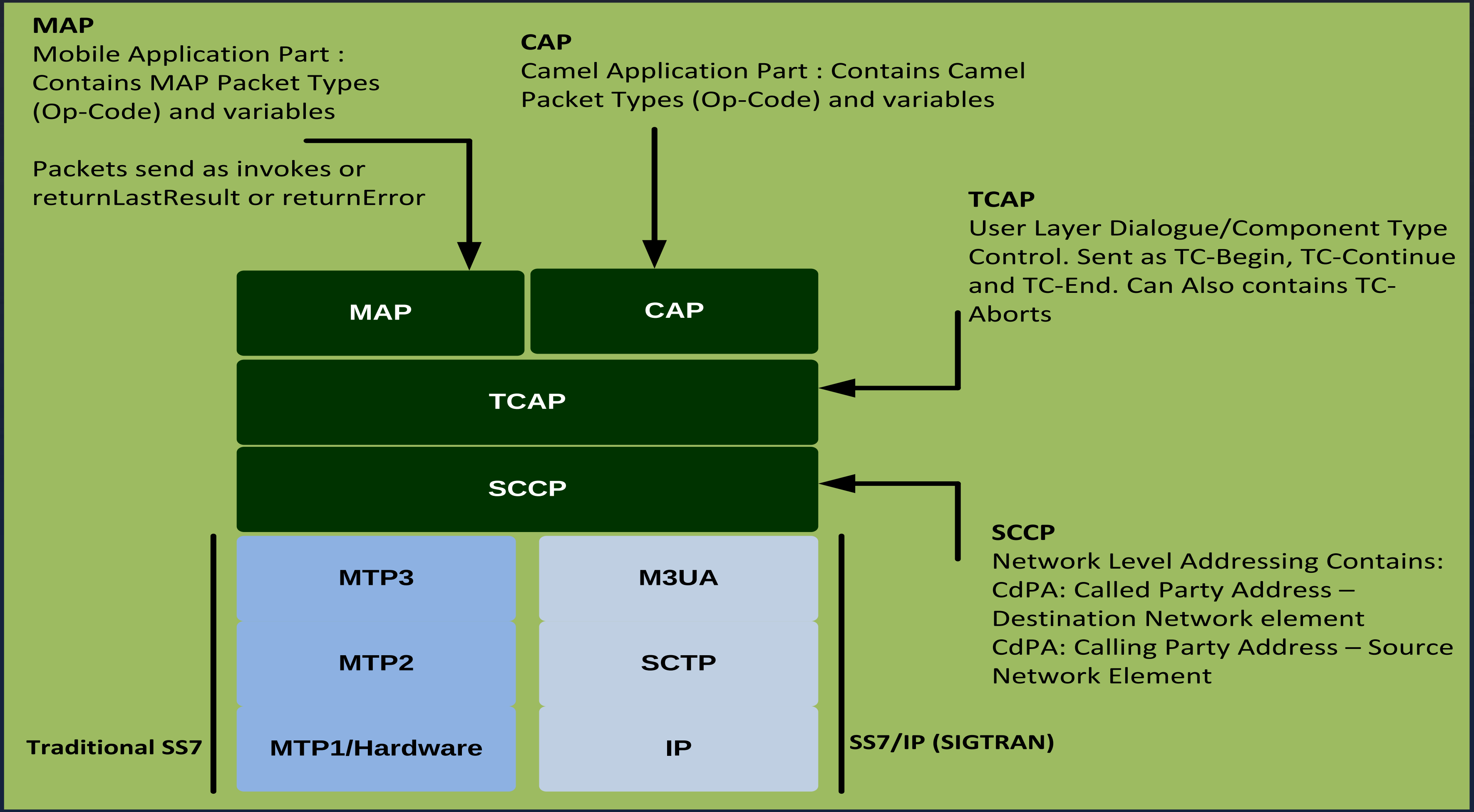
- Key Concepts:
  - Global Title or GT is a numeric address by which we can address the nodes (HLRs / VLRs / MSCs / gsmSCF)
  - Subscriber IDs (IMSIs & MSISDNs)

SS7 is superseded (technologically) by other signaling protocols such as DIAMETER & GTP in more modern network technologies. All these are bearers, or networks, are leveraged by malicious groups ∴ cross protocol correlation of signaling is necessary for comprehensive Threat Intelligence

In 5G, a dedicated security focused network function, the SEPP (security edge protection proxy), will exist at each network periphery. All inter-carrier traffic will traverse through a SEPP & the N32 interface towards OLO or foreign networks.

SS7 Stack

There are several layers or protocols within the SS7 Stack, we will focus on 4 main protocols.



MAP
Mobile Application Part : Contains MAP Packet Types (Op-Code) and variables

Packets send as invokes or returnLastResult or returnError

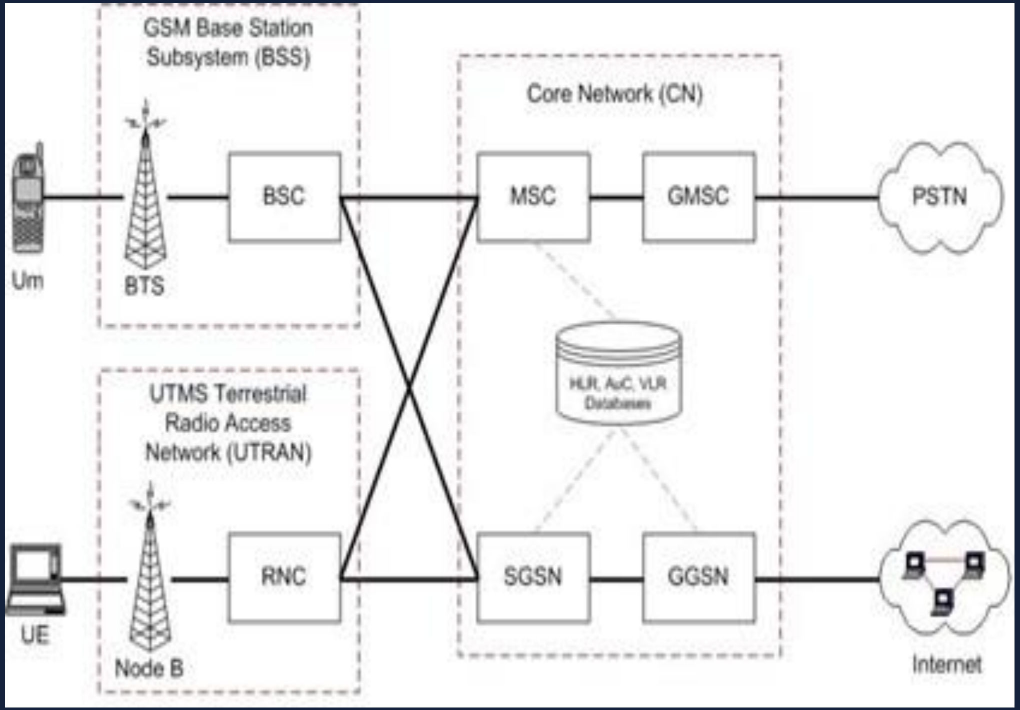
CAP
Camel Application Part : Contains Camel Packet Types (Op-Code) and variables

TCAP
User Layer Dialogue/Component Type Control. Sent as TC-Begin, TC-Continue and TC-End. Can Also contains TC-Aborts

SCCP
Network Level Addressing Contains:
CdPA: Called Party Address – Destination Network element
CdPA: Calling Party Address – Source Network Element

Mobile Network Architecture (2G/3G)

- STP: Signalling Transfer Point
  - A Router that relays / transfer SS7 messages between the Signalling End Points
- HLR: Home Location Register
  - Central database that contains details of each mobile phone subscriber that is authorized to use the GSM core network.
- MSC: Mobile Switching Centre
  - The centrepiece of a network switching subsystem (NSS). The MSC is mostly associated with communications switching functions, such as call set-up, release, and routing.
- VLR: Visitor Location Register
  - Database that contains information about the subscribers roaming within a mobile switching center's (MSC) location area
- SMSC: Short Message Service Center
  - Value Added Service Node responsible for storing, forwarding and delivering SMS Messages between mobile subscribers
- SGSN: Serving Gateway Supporting Node
- GGSN: GPRS Gateway Supporting Node
  - Data handling in 2G/3G including authentication, authorization and accounting, IP allocation etc.



Network Expressions

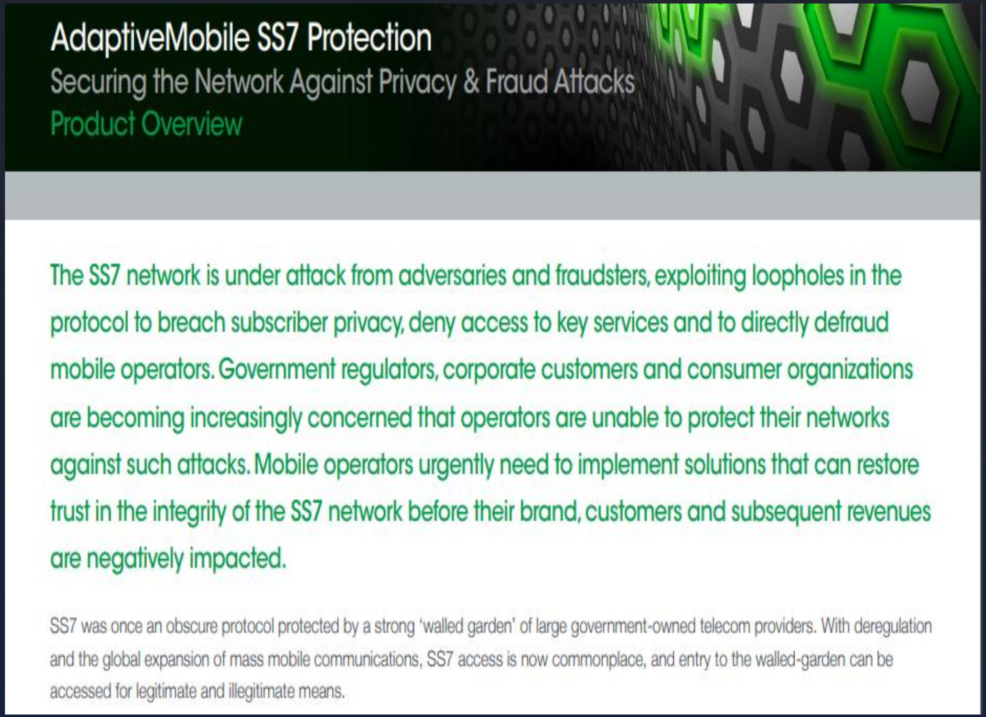
- MSISDN: Mobile Subscriber Integrated Services Digital Network Number (simply you mobile number)
  - MSISDN = CC + NDC + SN e.g. +216 9x xxxxxxx
  - CC = Country Code (represents the country)
  - NDC = Network Destination Code (represents the MNO)
  - SN = Subscriber Network (represents the subscriber)

- IMSI: International Mobile Subscriber Identity
  - IMSI = MCC + MNC + MSIN e.g. 605 01 xxxxxxxxx
  - MCC = Mobile Country Code (represents the country)
  - MNC = Mobile Network Code ((represents the MNO)
  - MSIN = Mobile Subscriber Identification Number (represents the subscriber)

- GT: Global Title (the address of the core node) e.g. HLR, MSC similar to the MSISDN

- IMEI: International Mobile Equipment Identity
  - Unique address to identify Mobile phones

Security Issues Are Widely Reported & Often Exploited



AdaptiveMobile SS7 Protection

Securing the Network Against Privacy & Fraud Attacks

Product Overview

The SS7 network is under attack from adversaries and fraudsters, exploiting loopholes in the protocol to breach subscriber privacy, deny access to key services and to directly defraud mobile operators. Government regulators, corporate customers and consumer organizations are becoming increasingly concerned that operators are unable to protect their networks against such attacks. Mobile operators urgently need to implement solutions that can restore trust in the integrity of the SS7 network before their brand, customers and subsequent revenues are negatively impacted.

SS7 was once an obscure protocol protected by a strong 'walled garden' of large government-owned telecom providers. With deregulation and the global expansion of mass mobile communications, SS7 access is now commonplace, and entry to the walled-garden can be accessed for legitimate and illegitimate means.

16.12.20 STATE SCRUTINY › DECISION MACHINES

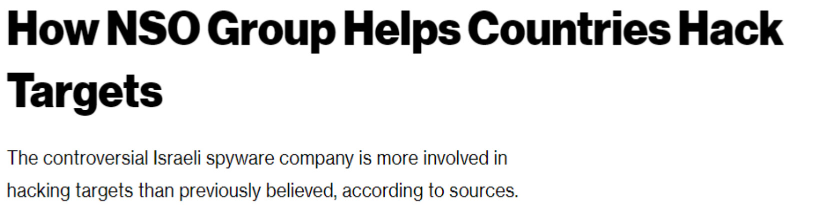
SPY COMPANIES USING CHANNEL ISLANDS TO TRACK PHONES AROUND THE WORLD

Inside the shadowy world of spyware makers that target activists and dissidents

There's some new competition for NSO, the Israeli company which boasts of its ability to take over phones and computers on behalf of high-paying government clients: Dozens upon dozens of spyware firms that offer a range of surveillance options.

For $500, this site promises the power to track a phone and intercept its texts

Paid access to a deeply insecure phone network



How NSO Group Helps Countries Hack Targets

The controversial Israeli spyware company is more involved in hacking targets than previously believed, according to sources.

Real-World SS7 Attack – Hackers Are Stealing Money From Bank Accounts

Risks in Cyber Telecom Domains

- Interception of calls & SMSs
- Eavesdropping
- Tracking of location
- Fraudulent activity
- Denial of service attacks against individual or locations
- Identity Manipulation (Spoofing)
- Man in the middle
- Information Harvesting
- Ransomware & Smishing
- Even encrypted phones can still be tracked and denied service

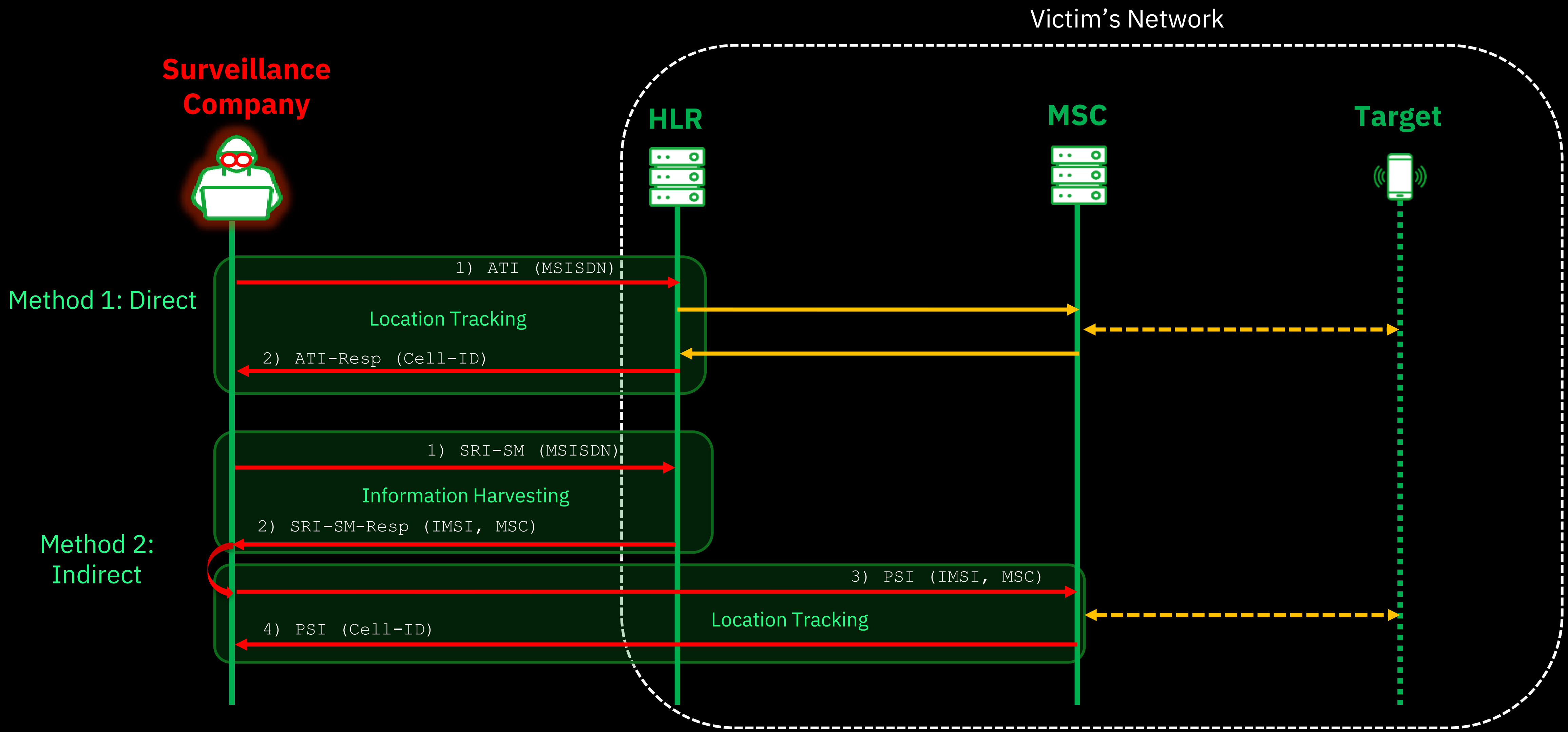
...attacks are conducted remotely and without detection

Signaling Attack Scenarios

Attack Scenario	PDUs	Frequency	Severity
Information Retrieval	SRI, ATI, Send IMSI, Restore Data, SRI-SM	High (monthly)	Medium - High
Location Tracking	ATI, PSI, PSL, MT-FSM	High (monthly)	High
Interception / Redirection	ISD, PRN, Update Location, Update GPRS Location, Initial DP	Low - High (varies by market)	High - Critical
DoS	ISD, DSD, Cancel Location, Update Location, Update GPRS Location	Low	High
Fraud	ISD, PRN, USSD, RegisterSS, MO-FSM, MT-FSM	Low	High

- **NB**, these are extremely high-level abstractions or summarizations of complex attacks.
- Periodic information retrieval attacks are encountered that often reveals or uncovers a gap in protection at a network. These policy gaps can then be exploited later in more complex attacks. Some of these information retrieval attacks can be difficult to detect and block since they might employ PDUs which are commonly exchanged between networks such as SRI-SM.
- Each attack incident requires in-depth analysis and the severity of such attacks is highly subjective. For instance, revenue & billing teams may consider fraud scenarios to be greater problem than the continuous tracking or call interception of a VIP which might be a greater concern the security team.

How Location Tracking is done via SS7 : Example

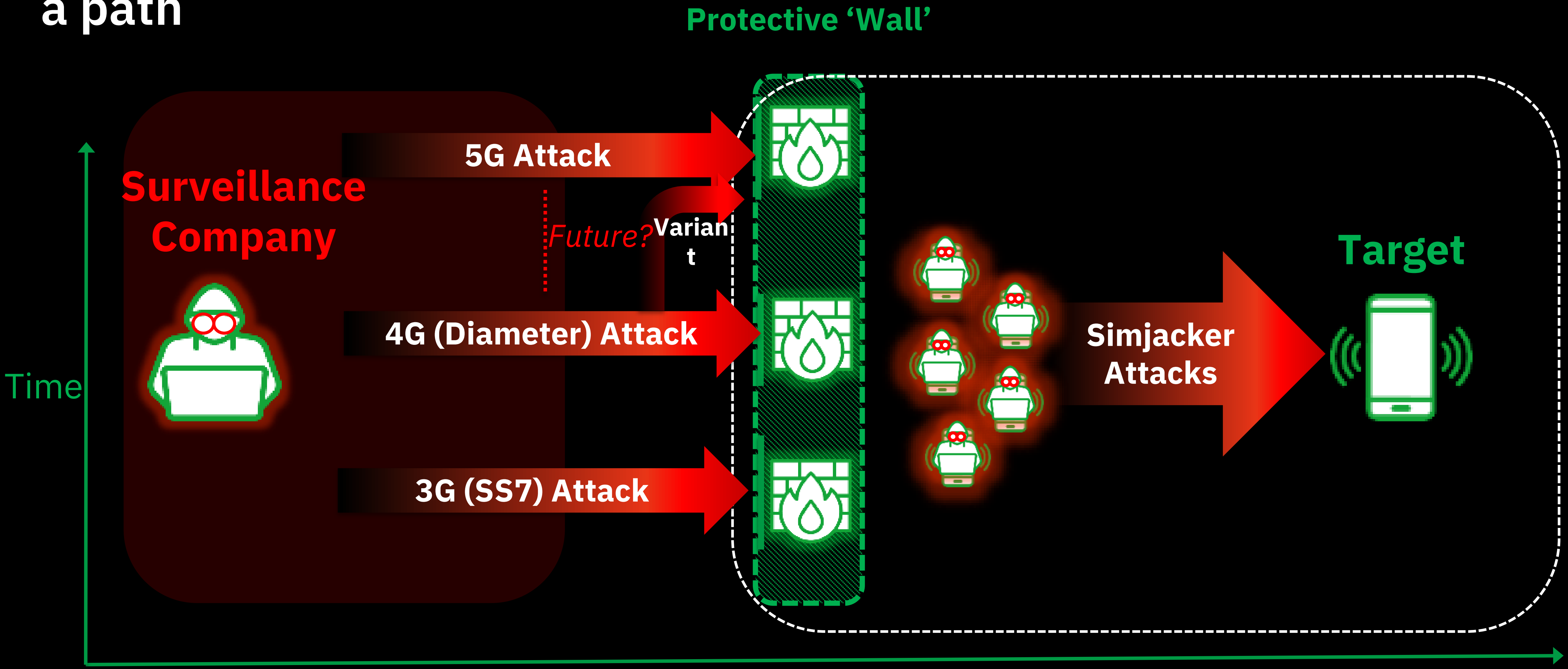


Simplified views, for more public information see:
#31C3 Karsten Nohl, Tobias Engel

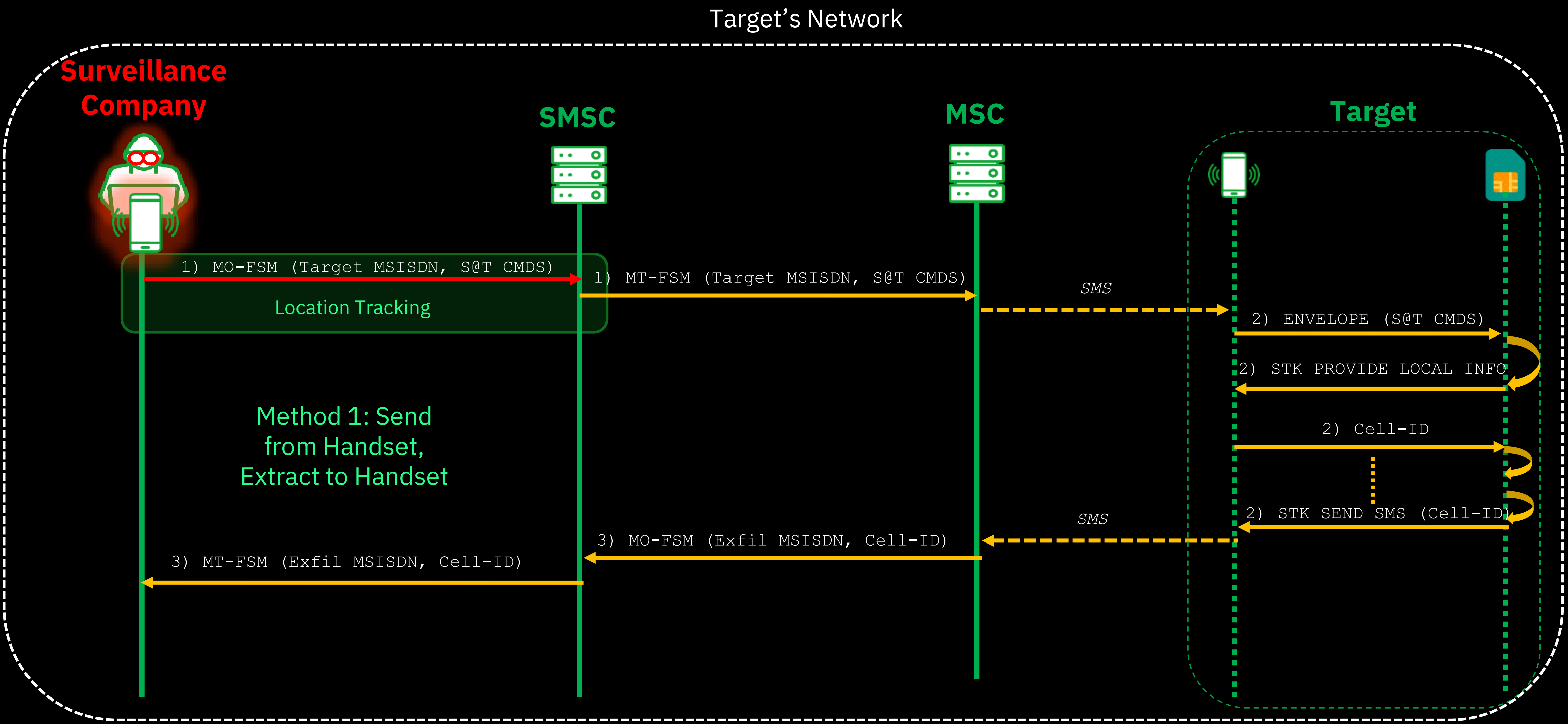
SS7 Location Tracking Command ‘Toolbox’ – Attacker Pros and Cons

GSM-MAP Command	Pre-requisite(s)	Pros	Cons
ANY-TIME-INTERROGATION (ATI)	MSISDN (or IMSI)	No other info needed	Can often be blocked by operator legacy equipment
PROVIDE-SUBSCRIBER-INFO (PSI)	IMSI, Serving MSC	Difficult for Operators to block	Requires possession of IMSI and Serving MSC
PROVIDE-SUBSCRIBER-LOCATION (PSL)	MSISDN (or IMSI) Serving MSC	Gets most precise location	Can normally be blocked by legacy equipment. Requires possession of serving MSC. May not be supported by target network

Surveillance Companies see mobile technology as a tool, not as a path



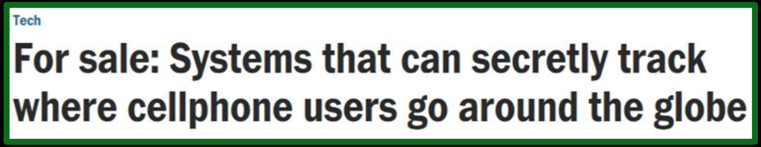
How Location Tracking is done via Simjacker SMS


Target's Network
Surveillance Company
SMSC
MSC
Target
1) MO-FSM (Target MSISDN, S@T CMDS)
Location Tracking
1) MT-FSM (Target MSISDN, S@T CMDS)
SMS
2) ENVELOPE (S@T CMDS)
2) STK PROVIDE LOCAL INFO
2) Cell-ID
2) STK SEND SMS (Cell-ID)
SMS
3) MO-FSM (Exfil MSISDN, Cell-ID)
3) MT-FSM (Exfil MSISDN, Cell-ID)
Method 1: Send from Handset, Extract to Handset

Simplified view, for more public information see:
www.simjacker.com

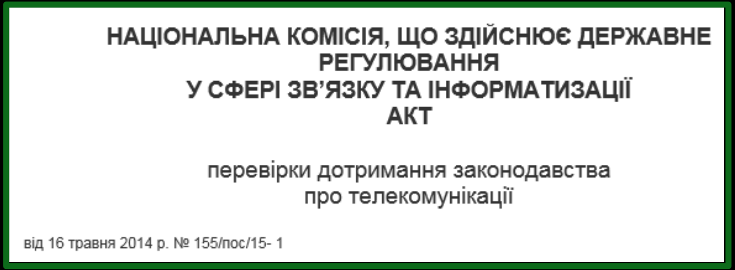
3 Types of Exploiters of Mobile Signalling Networks

1) Surveillance Companies


Tech

For sale: Systems that can secretly track where cellphone users go around the globe

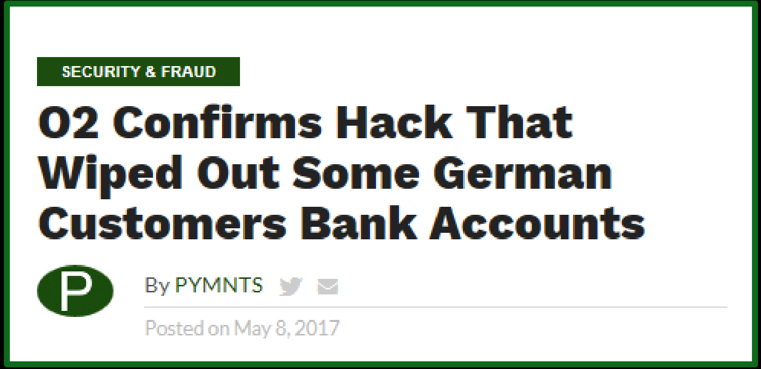
2) Governments


НАЦІОНАЛЬНА КОМІСІЯ, ЩО ЗДІЙСНЮЄ ДЕРЖАВНЕ РЕГУЛЮВАННЯ
У СФЕРІ ЗВ'ЯЗКУ ТА ІНФОРМАТИЗАЦІЇ
АКТ

перевірки дотримання законодавства
про телекомунікації

від 16 травня 2014 р. № 155/пос/15- 1

3) Criminals / Fraudsters


SECURITY & FRAUD

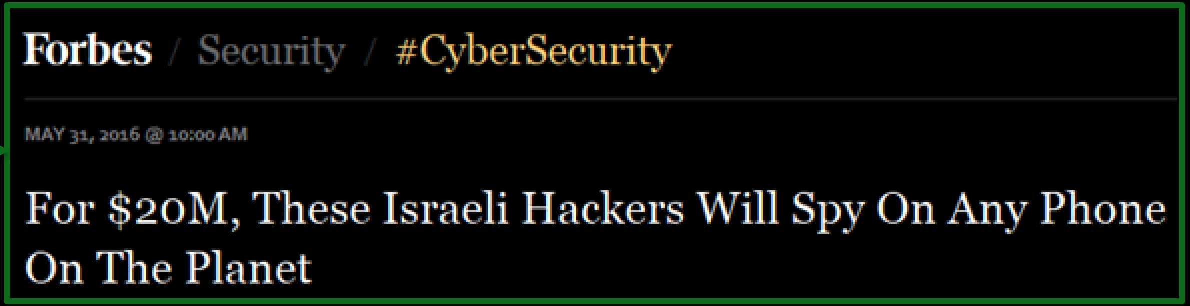
O2 Confirms Hack That Wiped Out Some German Customers Bank Accounts

By PYMNTS

Posted on May 8, 2017

- Considerable overlap between sources used by Surveillance Companies and Governments
- Criminal activity is the smallest activity, some overlap between sources used by these and Surveillance Companies

Surveillance companies have large resources ($$)


Forbes / Security / #CyberSecurity

MAY 31, 2016 @ 10:00 AM

For $20M, These Israeli Hackers Will Spy On Any Phone On The Planet

How do these Surveillance Companies gain access?

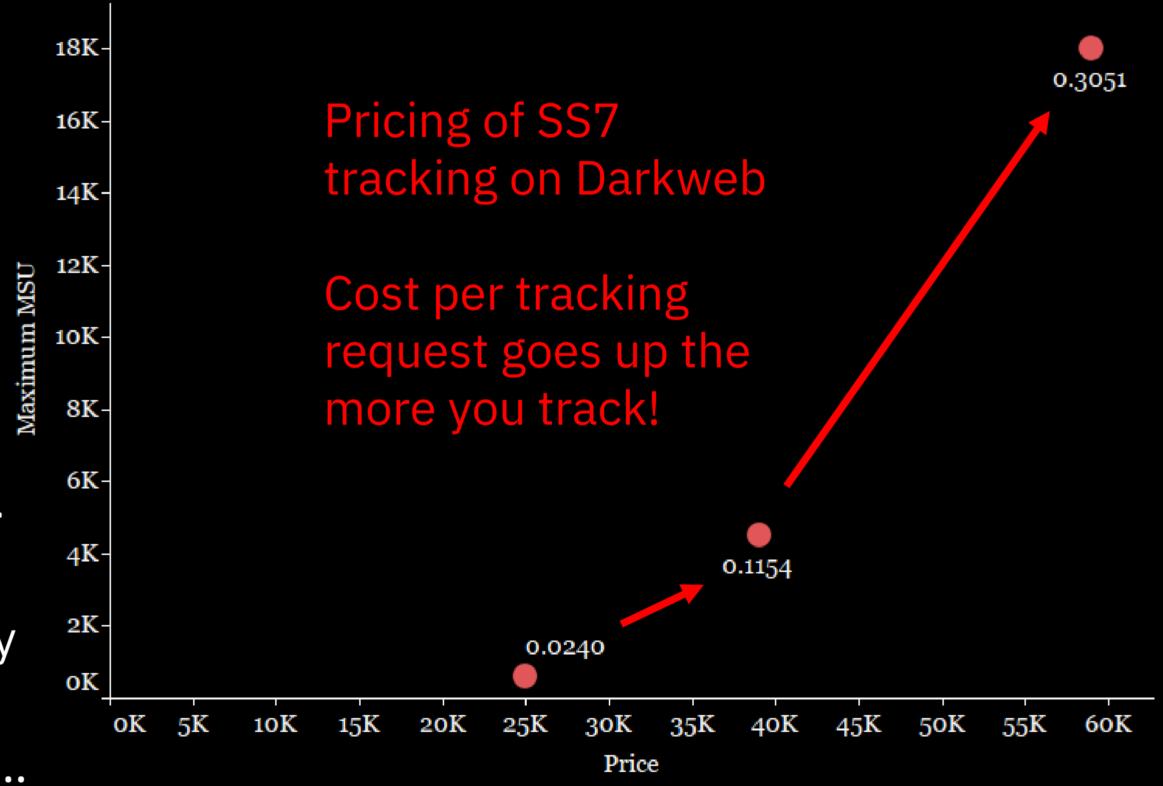
Multiple methods, most common:

1. Pay for Link :
   – Commercial agreements via front companies , who then negotiate access to other companies reselling access to mobile operators. Can be many layers. Works best in areas with poor regulations/oversight
2. Use Big Brother:
   – Governments buy surveillance solution, mandate system to be installed in 'captive' Operator, or add directly onto link (bypassing Operator)
3. Find old link :
   – Old/legacy connections - rare. Defunct companies whose access is not completely removed. Less of an issue in Diameter than SS7
4. Others

Pricing not opaque, access is normally between €0.02 -> €0.10 per MSU

- The more SS7/Diameter access a surveillance company has, the more valuable it is
- Leads to some strange business cases when re-selling...

Pricing per MSU



Pricing of SS7 tracking on Darkweb

Cost per tracking request goes up the more you track!

SS7 Commands & GSMA Classifications

The MAP & CAMEL protocols essentially comprise of a set of commands (opcodes) that are exchanged between signaling end points to achieve a purpose (e.g Location updating or Information Retrieval).

To reduce misuse of SS7 signaling, the GSMA Fraud & Security Group devised guidelines to help operators reduce their exposure to signalling attacks. At a high level there would be three main classifications of rules that PDUs would be filtered by:

- Category-1, PDUs which should normally **not** be exchanged between operators.
- Category-2, PDUs which must be exchanged between operators, however, only the home network (HPMN) of a home subscriber should originate these PDUs.
- Category-3, PDUs which must be exchanged between operators due to the subscribers mobility or roaming on a Visited Network (VPMN).

- The PDUs do not always strictly fit into a single Category, there are many examples where the call flow, or use case of a PDU will result in a PDU matching a rule or a different Category.

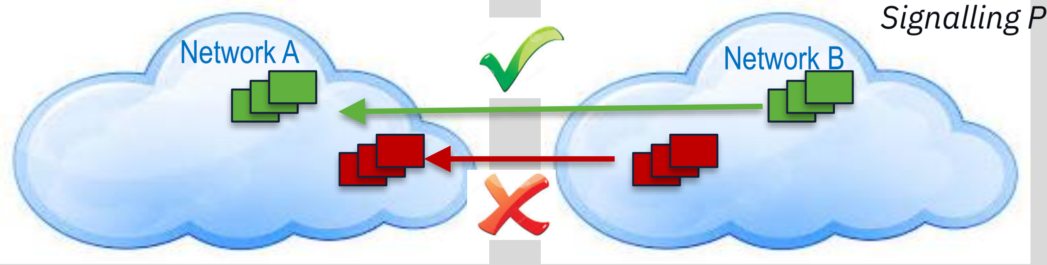
Signalling Threat Categories

– Allowed/Disallowed Messages

Low Layer

Malformed *Messages*

Messages abusing the protocol standards, aimed at "infecting" home network, services or subscribers



Signalling Protection with out-of-box policies

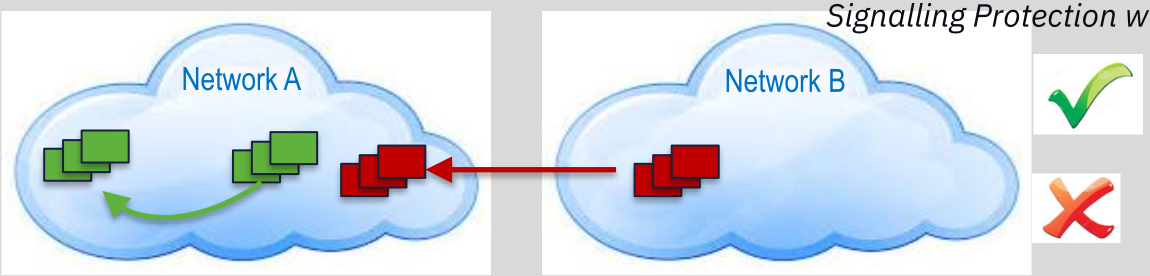
Command format is standard

Command contains nested AVPs, corrupted info, or malware

Category 1

Prohibited Interconnect *Messages*

Messages that should only normally be received from within the same network or networks with bilateral agreements



Signalling Protection with out-of-box policies

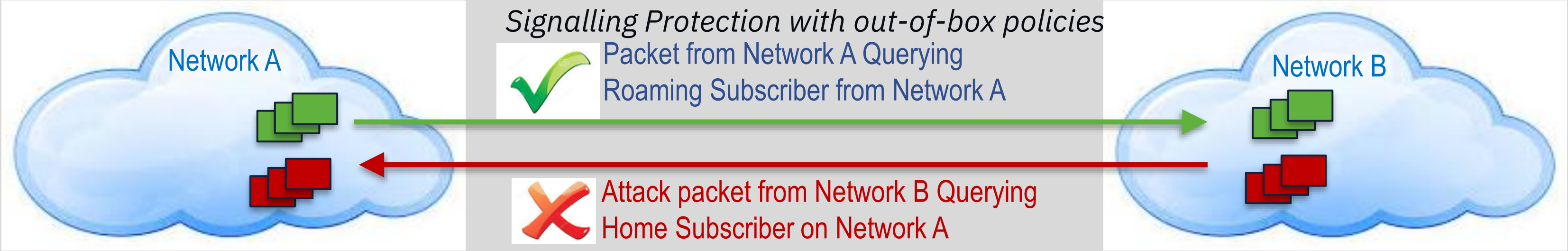
✓ Command from Network A Querying Network A Subscriber whilst at home

✗ Command from other Network B Querying Network A Subscriber whilst at home or roaming

Category 2

Unauthorised *Messages*

Messages that should only be sent about a visiting subscriber from that subscriber's home network



Signalling Protection with out-of-box policies

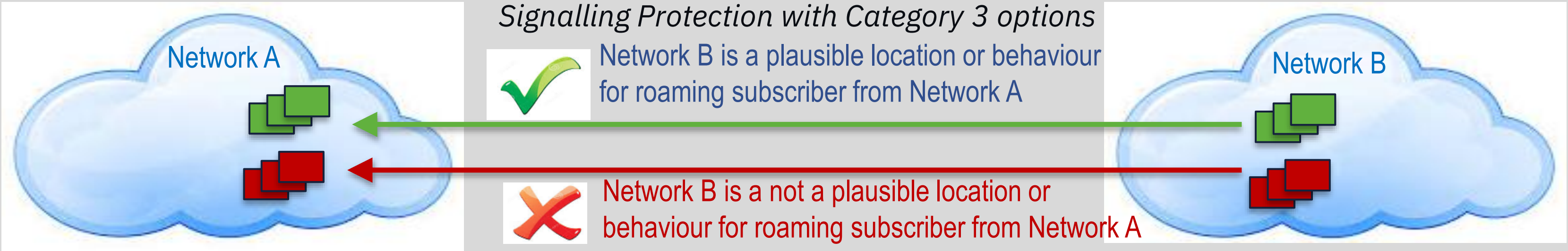
✓ Packet from Network A Querying Roaming Subscriber from Network A

✗ Attack packet from Network B Querying Home Subscriber on Network A

Category 3

Suspicious Location *Messages*

Messages that should only be sent about a visiting subscriber from that subscriber's current visited network



Signalling Protection with Category 3 options

✓ Network B is a plausible location or behaviour for roaming subscriber from Network A

✗ Network B is a not a plausible location or behaviour for roaming subscriber from Network A

Category-1

The most basic category, these are PDUs which should simply **not** be exchanged between operators normally. In most cases these are Intra-network PDUs.

Category-1 PDUs can be addressed to the MSISDN or IMSI however more often than not, we observe genuine hostile Category-1 based attack PDUs targeting MSISDNs (why is this?)

Category-1 PDUs include (see GSMA FS.11 for full matrix):

- Send IMSI (opcode 58)
- Send Routing Info (opcode 22)
- Send Routing Info For LCS (opcode 85)
- Any Time Interrogation (opcode 71)

Other illegal variants of Category-2 or Category-3 PDUs might also be considered Category-1, for example PRN (VLR →VLR) or SRI-SM sent to Dest SSN 8 (MSC). Or illegal combinations of GSM MAP PDUs delivered within a single TCAP component.

Category-2

The next PDU grouping, Category-2 relates to PDUs that must be exchanged between operators however we should expect that only the home network (HPMN) for a subscriber is authorized to send PDUs for that subscriber.

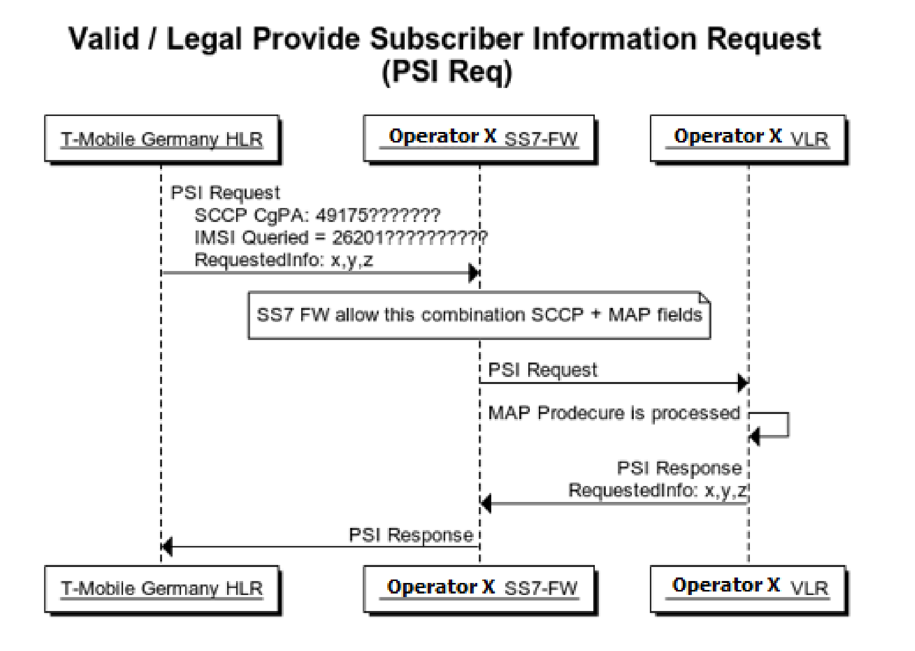
Category-2 PDUs include:

- Provide Subscriber Info (opcode 70)
- Provide Subscriber Location (opcode 22) * some operators consider this a Category-1 PDU.
- Insert Subscriber Data (opcode 7)
- Provide Roaming Number (opcode 4)

In addition to screening PDUs to enforce source (SCCP CgPA) vs subscriber consistencies, other inter-packet consistency checks may be performed. It’s therefore important to understand that the label “Category-2” can be used in relation to a rule, if that rule is comparing 2 fields within the PDU.

Category-2 (Valid Example)

SCCP CgPA (addressing layer) vs MAP MSISDN or IMSI (subscriber level) consistency checks are applied to certain PDUs to ensure that no foreign GTs (nodes) are illegally sending PDUs for unauthorised subscribers. Foreign networks may only send these PDUs for their own expected subscribers



Valid / Legal Provide Subscriber Information Request (PSI Req)

T-Mobile Germany HLR

Operator X SS7-FW

Operator X VLR

PSI Request
SCCP CgPA: 49175???????
IMSI Queried = 26201??????????
RequestedInfo: x,y,z

SS7 FW allow this combination SCCP + MAP fields

PSI Request

MAP Prodecure is processed

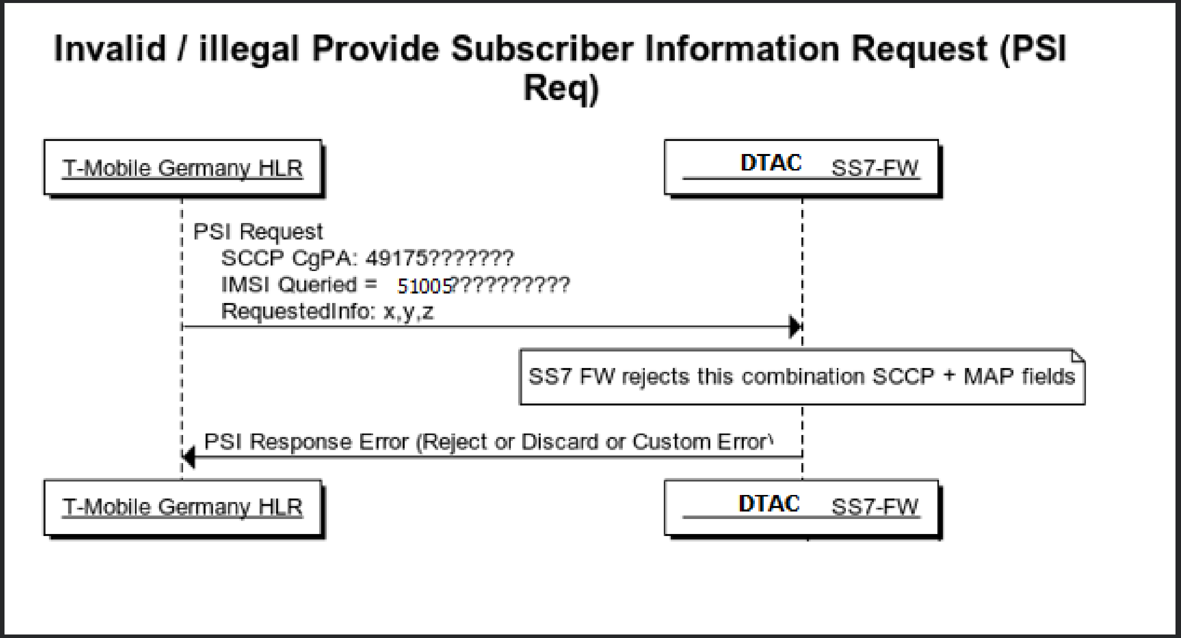
PSI Response
RequestedInfo: x,y,z

PSI Response

The SS7-FW screens these packets & will only blocks PDUs that is are violation of these consistency checks. Therefore only a small percentage of the overall CAT2 traffic that is processed will be blocked.

Category-2 (Invalid Example)

If a foreign GT attempts to query a home network IMSI (or in some cases MSISDN), the PDU is rejected.



Invalid / illegal Provide Subscriber Information Request (PSI Req)

PSI Request
SCCP CgPA: 49175???????
IMSI Queried = 51005??????????
RequestedInfo: x,y,z

SS7 FW rejects this combination SCCP + MAP fields

PSI Response Error (Reject or Discard or Custom Error)

Category-2 consistency checks are normally only enforced for home network IMSIs which means that attacks on inbound roaming IMSIs are likely to be successful.

Category-3

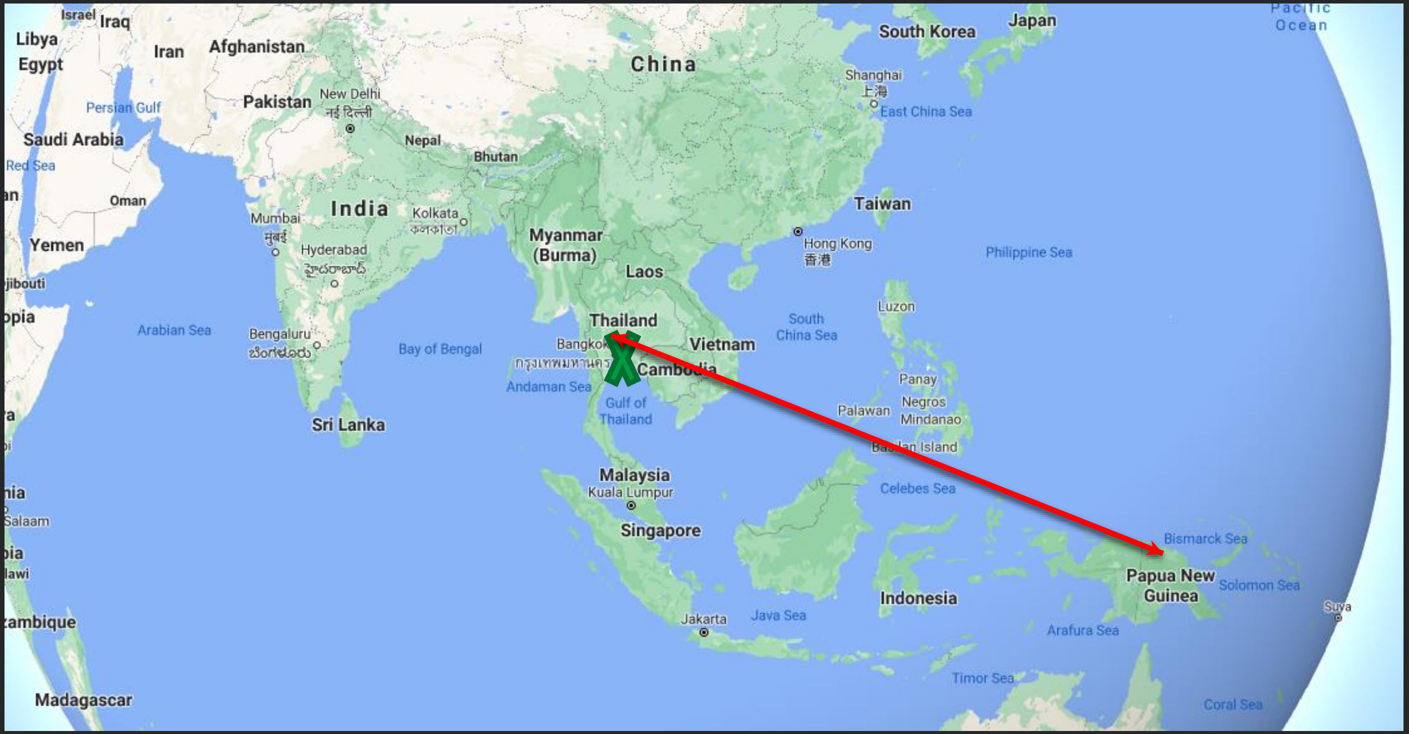
The third grouping, Category-3, relates to the protection of PDUs which we must expect to be received from the visited network for outbound roaming subscribers. These PDUs are screened by "trajectory plausibility" (velocity) and "network memory" protection features.

While information retrieval and location tracking attacks may be possible if attackers only possess the MSISDN of the target, attacks involving Category-3 PDUs are only possible if the IMSI is known to the attackers. The most important line of defense against Category-3 attacks is therefore to prevent the IMSI from being leaked from the network. If the IMSI is known to attackers then Category-3 protection will provide security against these attacks*.

- Category 3.1 Network Memory PDUs include:
  - ActivateSS, InterrogateSS, MO-Forward-SM, Restore Data, Send Parameters*
- Category 3.2 Trajectory Plausibility PDUs include:
  - Update Location (opcode 2), Update GPRS Location (opcode 23), Send Authentication Info (opcode 56)

Category 3 Trajectory Plausibility (Invalid Scenario)

Trajectory plausibility is a type of protection where the plausibility of new roaming signaling is evaluated against previous subscriber locations.

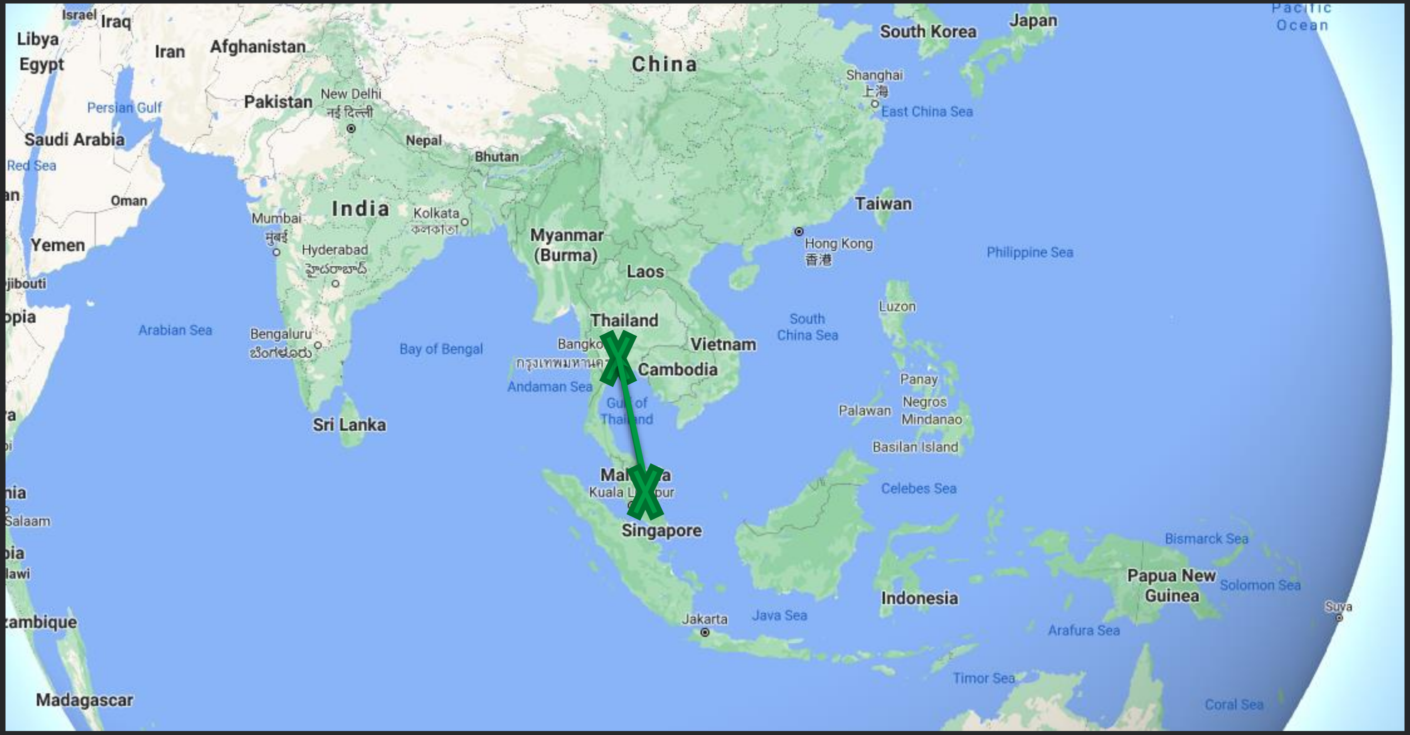


1. Subscriber is in home network
2. ULOC signalling is received from PNG
3. Subscriber was last known to be active in home country 30 minutes earlier therefore PNG roaming signalling cannot be valid
4. Error response returned to source of fake ULOC

TP protection robustness or effectiveness is variable & dependant on multiple factors.

Category 3.2 Trajectory Plausibility (“Valid” Scenario)

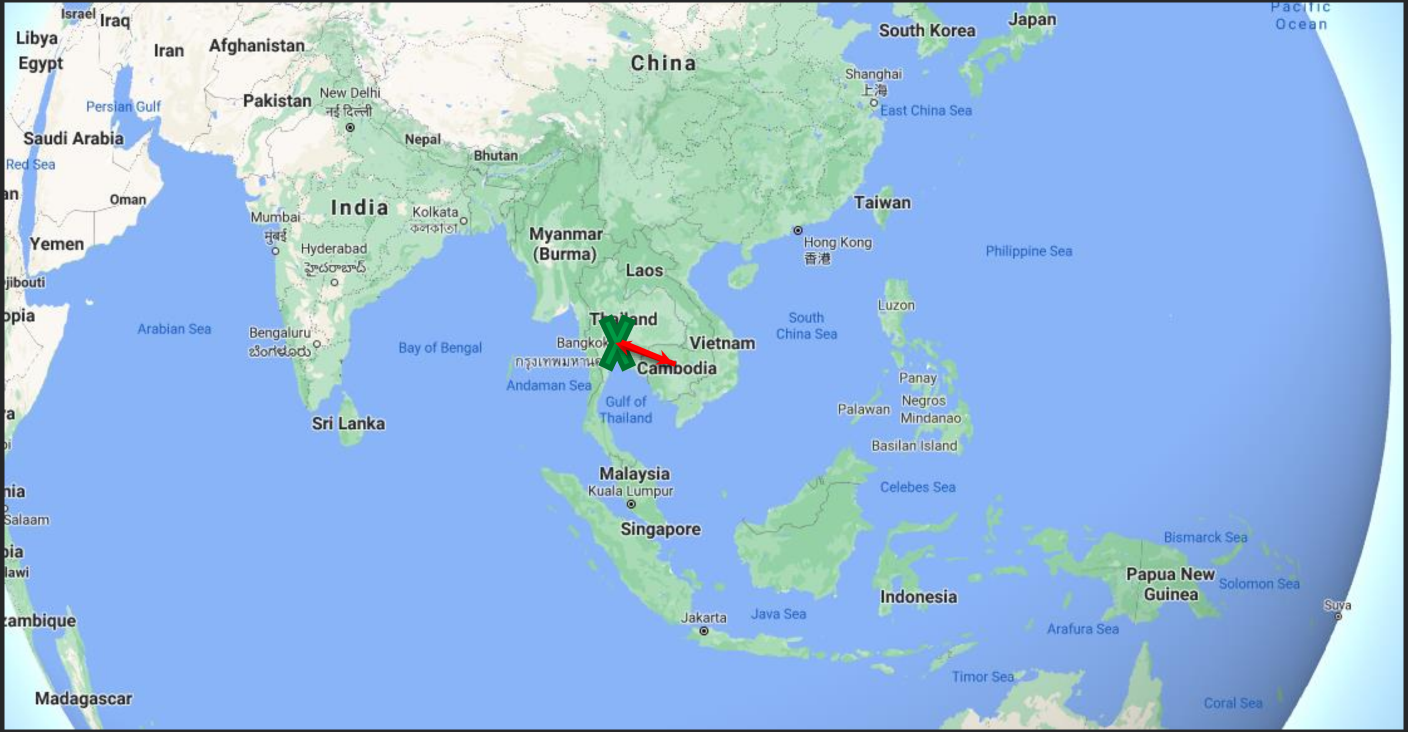
Roaming “transitions” between neighboring or bordering countries may occur at any instant.



1. Subscriber is in home network
2. ULOC signalling is received from Malaysia
3. Subscriber was last known to be active in home country 15 minutes earlier therefore roaming to Malaysia is permitted
4. HPMN HLR now expected subscriber to be in Malaysia

Category 3.1 Network Memory (Invalid Scenario)

Network memory protection applies to PDUs that a subscriber might generate from a roaming location, when a PDU is received from a country which is not the current visited country, it is rejected.



1. Subscriber is in the home network.
2. Category 3.1 PDU such as a MO-Forward-SM or a RestoreData PDU is received from any foreign network, in this example, Cambodia
3. The PDU is rejected because the subscriber is currently known, or expected to be in Thailand

Basic Attack Anatomy

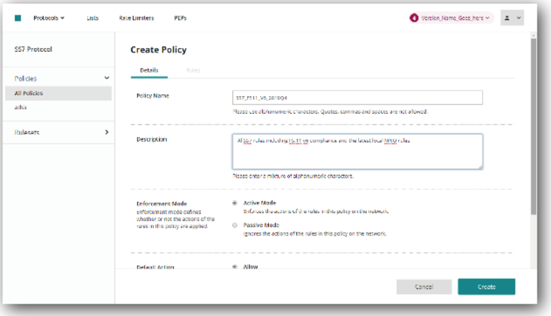
Subscriber focused targeted attacks typically comprise multiple stages, or phases.

- Stage 1, attacks often begin with some form of information gathering attacks on MSISDNs (why?).
  - PDUs: SendIMSI, ATI, SRI, SRI-SM, PSL
- Stage 2, if the IMSI is known, or can be obtained from the network by querying a MSISDN, the attack might develop into more complex scenarios (e.g. interception, fraud).
  - PDUs: RestoreData, UpdateLocation, PSI, MT-FSM, PSL

Complex attacks may be witnessed on networks which do not leak IMSIs, this can happen because the IMSI may be known to attackers from an earlier time before protection was enabled (SIMs are rarely changed), or the IMSI could be obtained via another means such as monitoring of SCCP links or an IMSI catcher.

Signalling Protection (SS7 Firewall)

Seamlessly fits into existing network flows



Create Policy

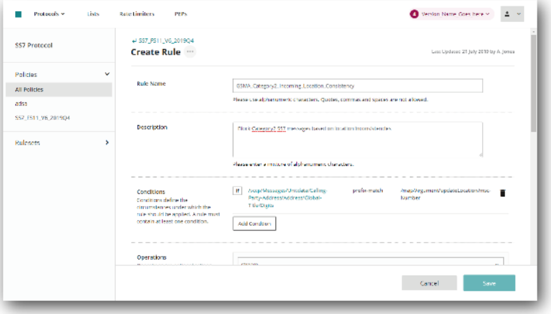
Policy Name: SS7_FS11_V6_2019Q4
Please use alphanumeric characters. Quotes, commas and spaces are not allowed.

Description: All SS7 rules including FS.11 v6 compliance and the latest local MNO rules
Please enter a mixture of alphanumeric characters.

Enforcement Mode
Enforcement mode defines whether or not the actions of the rules in this policy are applied.
● Active Mode
Enforces the actions of the rules in this policy on the network.
○ Passive Mode
Ignores the actions of the rules in this policy on the network.

Default Action: ● Allow

Policy Management



↵ SS7_FS11_V6_2019Q4

Create Rule

Last Updated 21 July 2019 by A. Jones

Rule Name: GSMA_Category2_Incoming_Location_Consistency
Please use alphanumeric characters. Quotes, commas and spaces are not allowed.

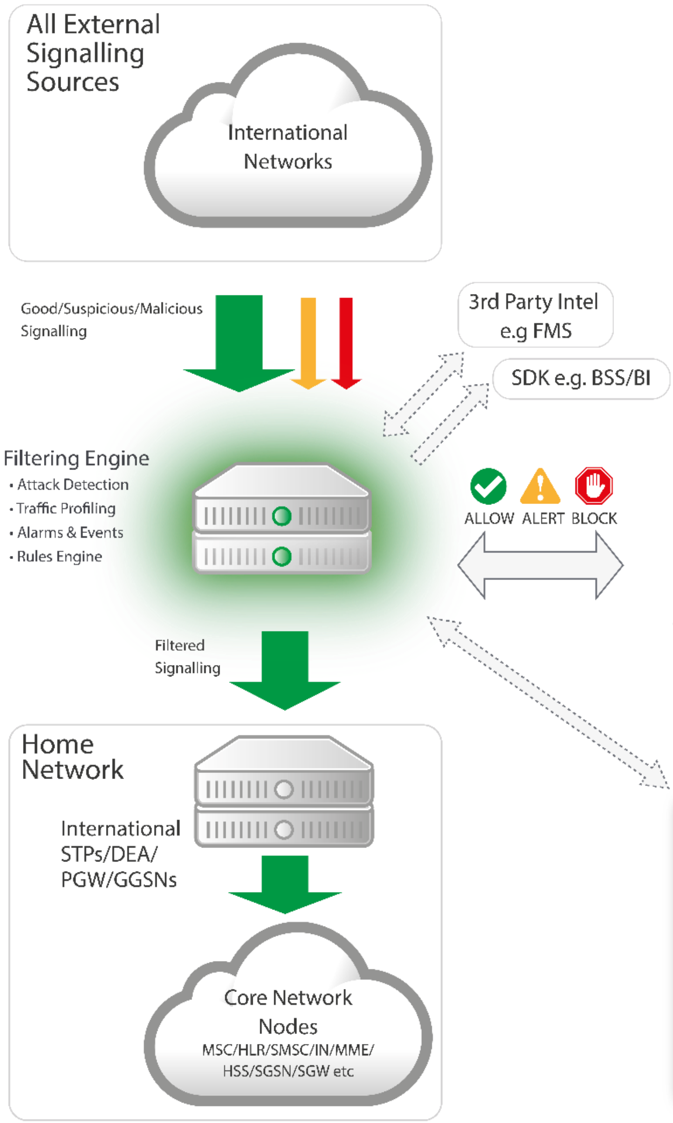
Description: Block Category2 SS7 messages based on location inconsistencies.
Please enter a mixture of alphanumeric characters.

Conditions
Conditions define the circumstances under which the rule should be applied. A rule must contain at least one condition.
If /sccp/Messages/Unitdata/Calling-Party-Address/Address/Global-Title/Digits prefix-match /map/Argument/updateLocation/msc-Number

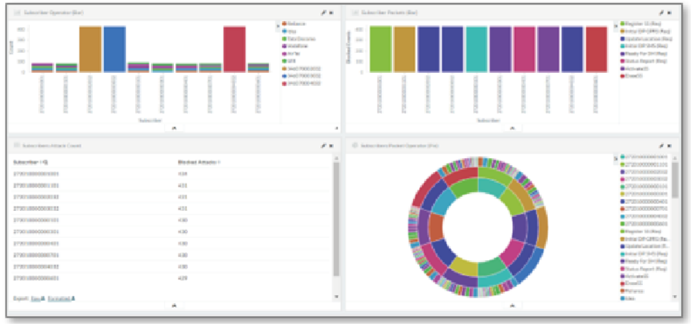
Operations

Signalling Rules Configuration UI

Intelligent and flexible signalling control configuration to respond to new threats and attacks

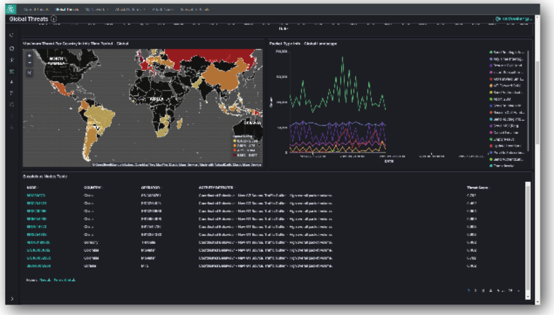


Policy Management
Threat Reporting & Analysis
System Administration

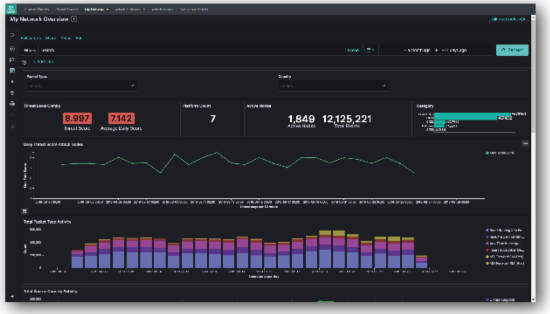


Advanced Threat Reporting

Support for SS7, Diameter, GTP, ISUP, SIP



Global SIGIL



Local SIGIL

Combine with SIGIL to understand suspicious signalling activity, to predict and defend from future attacks

The Need for Industry-Wide Signalling Intelligence

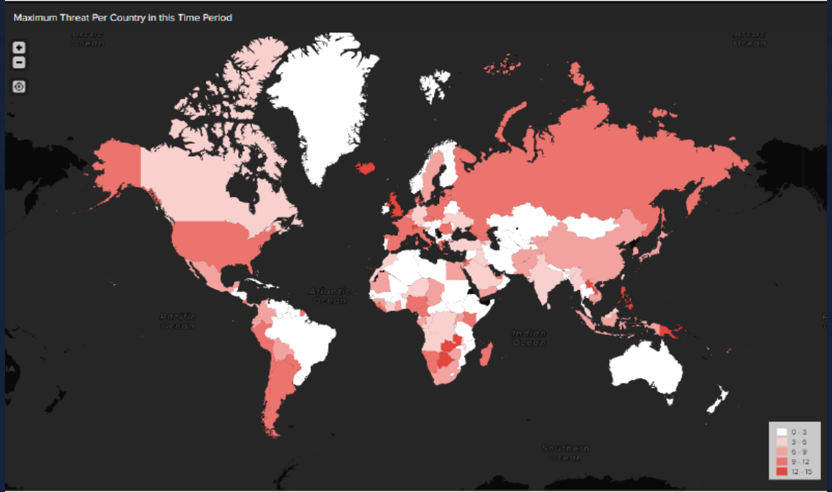
Many mobile operators have made changes to their network to deal with threats: signalling infrastructure updates, signalling firewall deployments, etc.

However, there are still many challenges:

- New rules and detection methods are slow or unable to be applied rapidly in the face of evolving attack scenarios and techniques across SS7, Diameter and GTP
- There is a lack of signalling security knowledge/personnel to perform in-depth triaging of attacks
- Operators have difficulty in finding the ‘real’ malicious attacks in the overall suspicious activity detected
- Global threat knowledge is a must in order to understand and defend local attacks
- Attackers are adapting to GSMA and industry implementations
- Successful 5G rollouts will require advanced security preparation now

The complexity of detected signalling abuses indicates Nation State actors i.e. heavily funded & highly skilled attackers

Promotional material for SS7 Attacker Interception platform



Sources of AdaptiveMobile detected suspicious SS7 activity in one recent quarter

Challenges to secure Signalling critical infrastructure from Nation State Attacks

- Do you know who is infiltrating your network?
- Do you know the level of complexity they use to get to your subscribers?
- Do you know the subscribers being targeted?
- Do you know how frequently they adapt to your defences?

Proper Defence Architecture

Signalling Protection

Securing the backbone of telecom networks from SS7, Diameter, GTP, SIP and 5G based attacks and malicious use.

Protect List

Proactively Securing critical individuals and resources. Alerting when Cyber Telecom intrusion attempts are detected.

SIGIL – Signalling Intelligence Layer

Combining AdaptiveMobile’s signalling intelligence expertise and global footprint, enabling operators to increase their effectiveness in preventing signalling attacks.

We have developed series of strategies to defend critical resources:

- Detect mobile network intrusion and block all unauthorized access with signalling protection platforms
- It is critical that all interconnections are secured, attackers will exploit the interfaces that are unprotected
- Pay particular attention of critical resources. Any attempt to exploit the mobile services for these individuals (or resources they used e.g. vehicles, mobile enabled computing or personal devices) should be escalated and investigated
- Attack networks and infrastructure will be used until they become ineffective, so Threat Intelligence is key and it’s recommended to share intelligence to understand your adversary and defend proactively.

The Value of Threat Intelligence and Sharing The Intelligence

- Threat Intelligence is a kind of “safety built” for Telecommunications Providers

- **Cyber Attacks are not entirely predictable, but with TI you manage to get ahead of the situation and recognize attack patterns as quickly as possible**

- Therefore, information must be exchanged and analysed

The Benefits of Telcos using Threat Intelligence

Attacks are coming from everywhere!

TI helps to take the inventory and filters out which data is relevant for further analysis. Thus TI helps to:

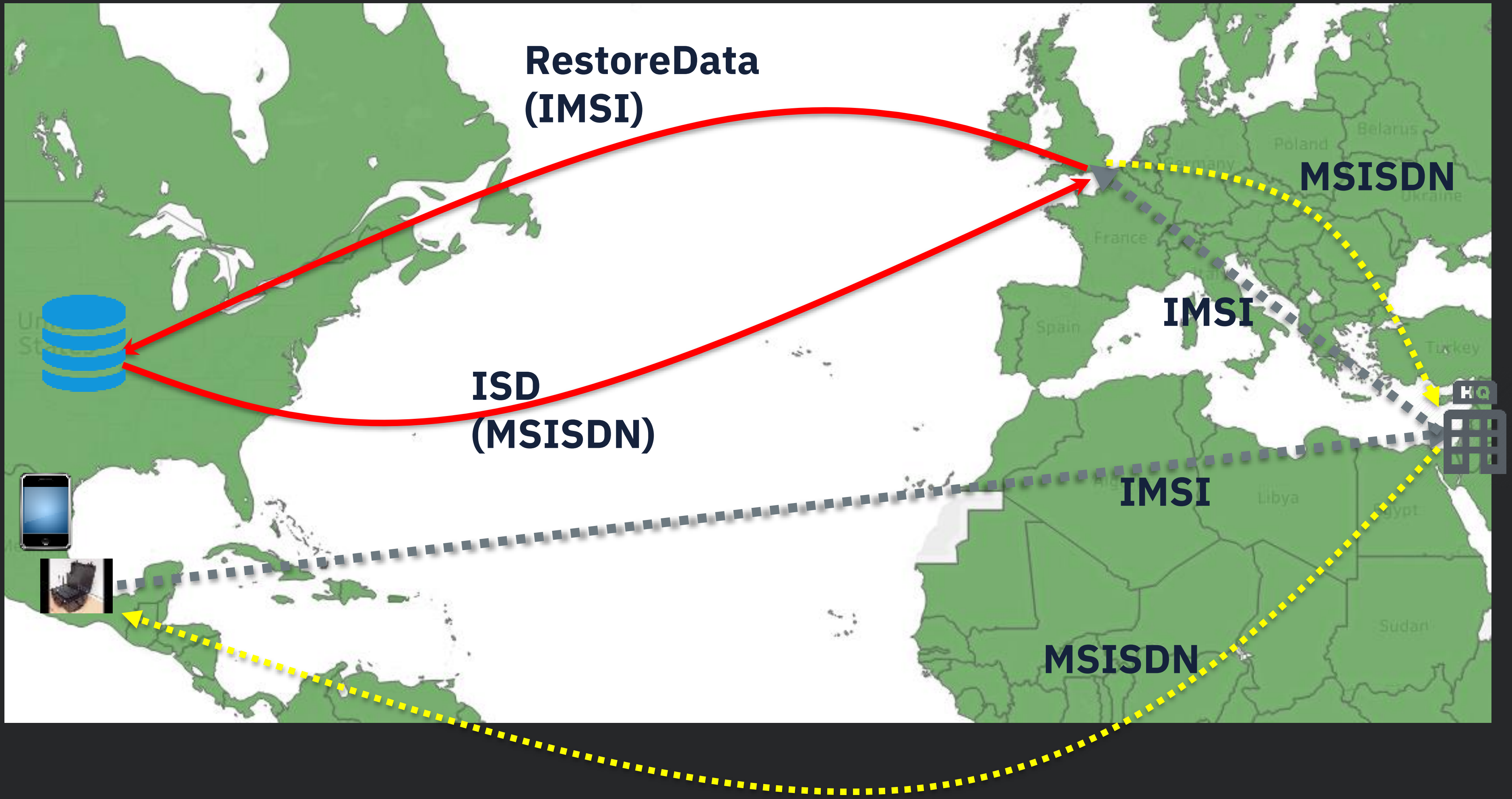
- Understand why you are an attractive target
- Understand where the vulnerabilities are
- Understand who is the actual target of an attack
- Understand who the attackers are, how they operate, what techniques, methods they use
- Understand how to mitigate an attack and how to implement security measures in the best possible way

So overall understanding how to act proactively...

Signalling Intelligence e.g. *Remote IMSI Catcher Behaviour Detection*

1. Subscriber A is from country 1 (e.g. USA)
2. Subscriber A is currently roaming in country 2 ,(e.g. Mexico),
3. IMSI catcher in Mexico picks up IMSI from Subscriber A
4. IMSI Catcher sends details (A-IMSI) sent to HQ in Country 3 (e.g. Israel).
5. HQ issues request to Node with SS7 Connection in Country 4 (e.g. Channel Islands in the UK)
6. SS7 Node sends RestoreData with A- IMSI to Country 1 (USA)
7. USA responds with ISD with A-MSISDN and other details
8. SS7 Node sends this back to HQ

Attackers can then obtain MSISDN of any IMSIs picked up



Signalling Intelligence Layer (SIGIL)

SIGIL is a signaling security threat intelligence platform, implemented as a supervised machine learning cloud platform, it applies security correlation algorithms and prioritize security threats automatically based on risk score in real-time. Supervision and security expert analysis is provided by our TIU team

Defend

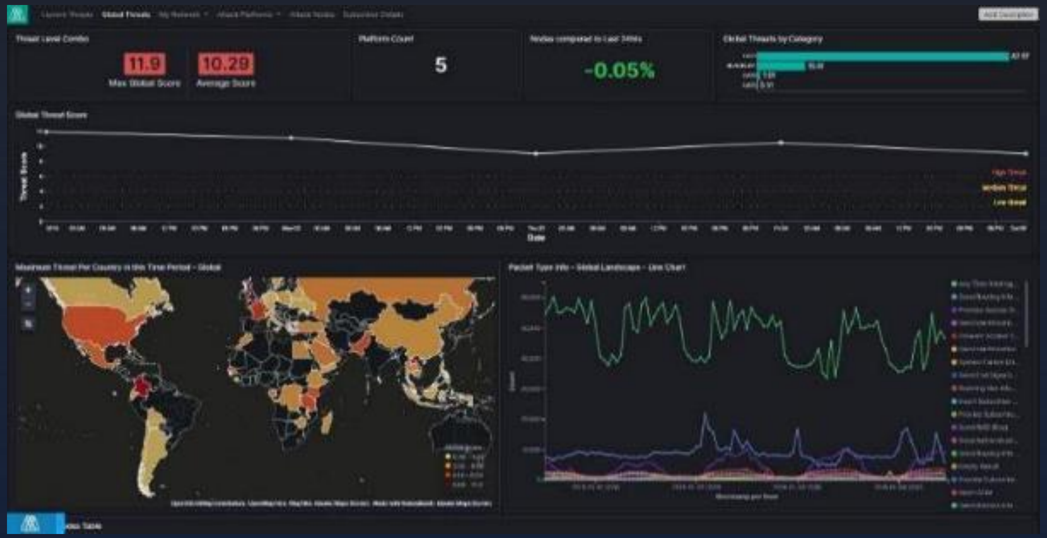
- Make faster decisions to block security threats to your network
- Prioritize the serious signalling security alerts over operational noise

Understand

- Monitor & block known sources of malicious attacks proactively
- Complete expert analysis with investigations supported by our TIU Team

Predict

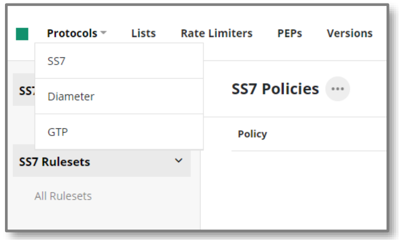
- Understand the Global Signalling Threat landscape and your threat level


Global Threats
Threat Level Combo
11.9
Max Global Score
10.29
Average Score
Platform Count
5
Nodes compared to Last 24Hrs
-0.05%
Global Threats by Category
Global Threat Score
Threat Score
Date
Maximum Threat Per Country in this Time Period - Global
Packet Type Info - Global Landscape - Line Chart

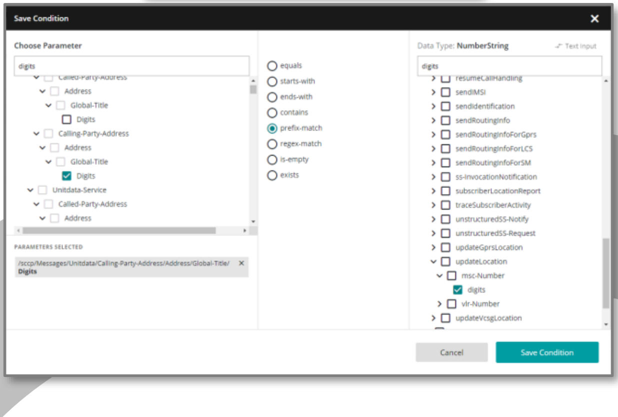
SIGIL Analytics Dashboard – Threat Level

The Signalling Circle of Trust

Baseline
Out-of-the-box
GSMA rules



Adapt
Flexible Signalling
Control Configuration



Choose Parameter: digits

- Called-Party-Address
  - Address
    - Global-Title
      - □ Digits
- Calling-Party-Address
  - Address
    - Global-Title
      - ☑ Digits
- Unitdata-Service
  - Called-Party-Address
    - Address

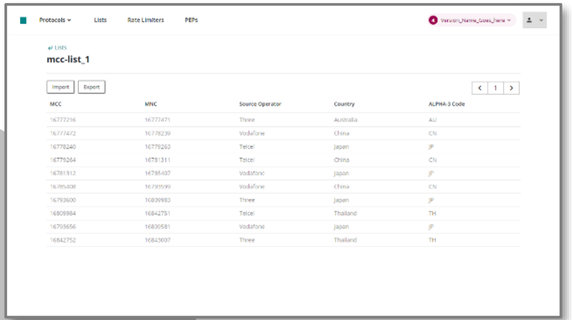
○ equals
○ starts-with
○ ends-with
○ contains
● prefix-match
○ regex-match
○ is-empty
○ exists

PARAMETERS SELECTED
/sccp/Messages/Unitdata/Calling-Party-Address/Address/Global-Title/ **Digits**

Data Type: **NumberString**: digits

- □ resumeCallHandling
- □ sendIMSI
- □ sendIdentification
- □ sendRoutingInfo
- □ sendRoutingInfoForGprs
- □ sendRoutingInfoForLCS
- □ sendRoutingInfoForSM
- □ ss-InvocationNotification
- □ subscriberLocationReport
- □ traceSubscriberActivity
- □ unstructuredSS-Notify
- □ unstructuredSS-Request
- □ updateGprsLocation
- □ updateLocation
  - □ msc-Number
    - ☑ digits
  - □ vlr-Number
- □ updateVcsgLocation

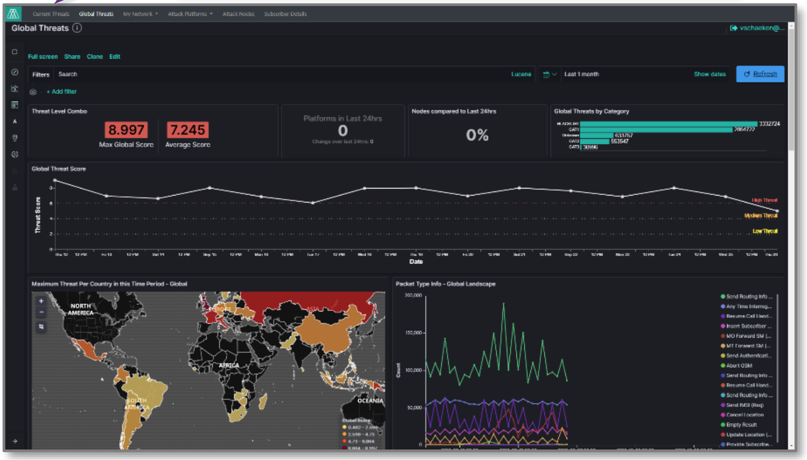
External Intelligence
Use lists, lookups, mappings



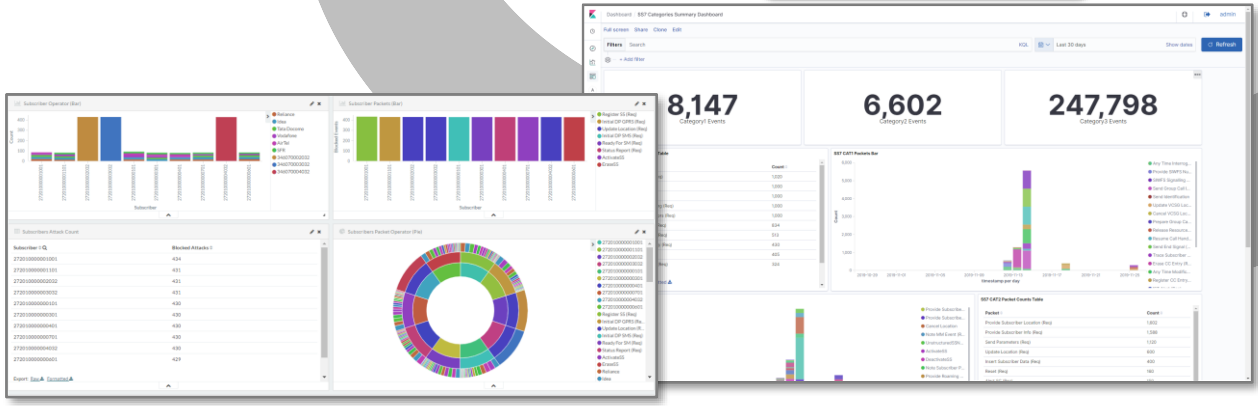
mcc-list_1

MCC	MNC	Source Operator	Country	ALPHA-3 Code
16777216	16777471	Three	Australia	AU
16777472	16778239	Vodafone	China	CN
16778240	16779263	Telcel	Japan	JP
16779264	16781311	Telcel	China	CN
16781312	16785407	Vodafone	Japan	JP
16785408	16793599	Vodafone	China	CN
16793600	16809983	Three	Japan	JP
16809984	16842751	Telcel	Thailand	TH
16793656	16809581	Vodafone	Japan	JP
16842752	16843007	Three	Thailand	TH

Understand, Predict, Defend
Global Intelligence (SIGIL ML/AI)
Plus TIU Signalling Protection Services



Insight
Observe and Learn



AdaptiveMobile
Security