AdaptiveMobile Security

Signaling Security

December 2021

Intro

Welcome!

Presenter: Faaez Burney

Faaez.burney@adaptivemobile.com

Karel van der Lecq

karel.vanderlecq@adaptivemobile.com

World Leader in Cyber Telecom Security

Protecting 2.5 billion mobile subscribers worldwide

Unique visibility of mobile traffic

Our software sits in the heart and Edge of an operator's network, identifying threats and securing their key services in real time

T-Mobile · airtel · at&t · Sprint · vodafone · BT · MTN · stc

Trusted in over 100 Operators, Governments and Regulators

Capturing over 50 billion events/day

Specialisation in signalling and telecom connectivity security enabling the national telecommunication protection

Industry Recognition of Leadership

GSMA GLOMO AWARDS THE GLOBAL MOBILE AWARDS · ISO 27001 certified · MEFFYS 2016 FINALIST · GLOTEL AWARDS 2016 · Gartner Cool Vendor · FROST & SULLIVAN · CARRIERS WORLD NOMINEE · AWARDS Technology Innovation & Company of the Year 2016

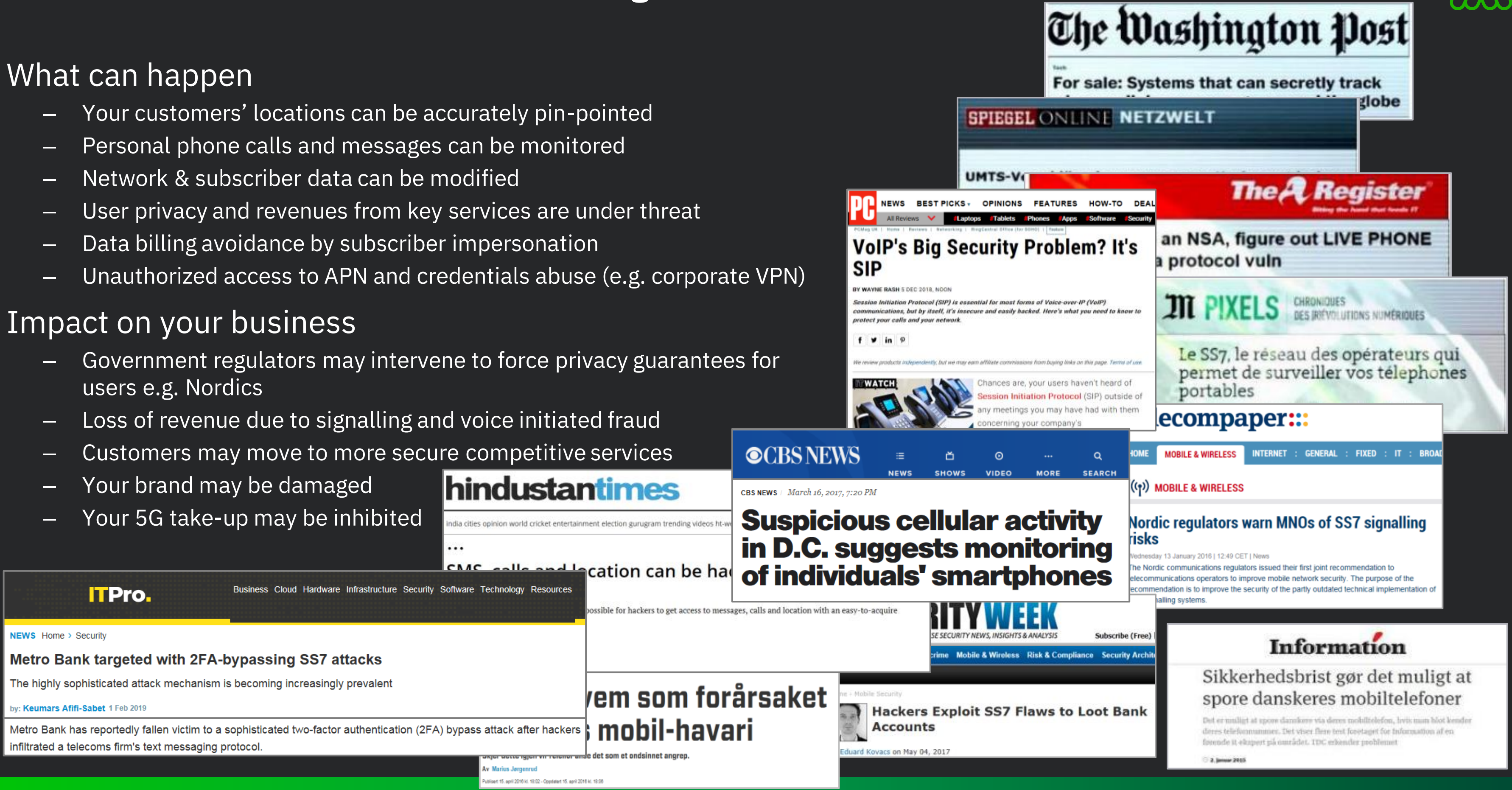
securing every nation

securing every network

securing every number

Current Situation – A Shattering of Trust in the Network

- What can happen
  - Your customers' locations can be accurately pin-pointed
  - Personal phone calls and messages can be monitored
  - Network & subscriber data can be modified
  - User privacy and revenues from key services are under threat
  - Data billing avoidance by subscriber impersonation
  - Unauthorized access to APN and credentials abuse (e.g. corporate VPN)
- Impact on your business
  - Government regulators may intervene to force privacy guarantees for users e.g. Nordics
  - Loss of revenue due to signalling and voice initiated fraud
  - Customers may move to more secure competitive services
  - Your brand may be damaged
  - Your 5G take-up may be inhibited



The Washington Post

For sale: Systems that can secretly track ... globe

SPIEGEL ONLINE NETZWELT

UMTS-V...

The Register

... an NSA, figure out LIVE PHONE ... a protocol vuln

PC NEWS BEST PICKS OPINIONS FEATURES HOW-TO DEAL

All Reviews #Laptops #Tablets #Phones #Apps #Software #Security

VoIP's Big Security Problem? It's SIP

BY WAYNE RASH 5 DEC 2018, NOON

Session Initiation Protocol (SIP) is essential for most forms of Voice-over-IP (VoIP) communications, but by itself, it's insecure and easily hacked. Here's what you need to know to protect your calls and your network.

We review products independently, but we may earn affiliate commissions from buying links on this page. Terms of use.

Chances are, your users haven't heard of Session Initiation Protocol (SIP) outside of any meetings you may have had with them concerning your company's

Le Monde PIXELS CHRONIQUES DES RÉVOLUTIONS NUMÉRIQUES

Le SS7, le réseau des opérateurs qui permet de surveiller vos téléphones portables

...ecompaper

...HOME MOBILE & WIRELESS INTERNET : GENERAL : FIXED : IT : BROAD...

MOBILE & WIRELESS

Nordic regulators warn MNOs of SS7 signalling risks

...Wednesday 13 January 2016 | 12:49 CET | News

...The Nordic communications regulators issued their first joint recommendation to ...elecommunications operators to improve mobile network security. The purpose of the ...ecommendation is to improve the security of the partly outdated technical implementation of ...alling systems.

CBS NEWS NEWS SHOWS VIDEO MORE SEARCH

CBS NEWS March 16, 2017, 7:20 PM

Suspicious cellular activity in D.C. suggests monitoring of individuals' smartphones

hindustantimes

india cities opinion world cricket entertainment election gurugram trending videos ht-we...

...

SMS, calls and location can be hac...

...possible for hackers to get access to messages, calls and location with an easy-to-acquire

...RITY WEEK ...SE SECURITY NEWS, INSIGHTS & ANALYSIS Subscribe (Free)

...crime Mobile & Wireless Risk & Compliance Security Archit...

...me › Mobile Security

Hackers Exploit SS7 Flaws to Loot Bank Accounts

Eduard Kovacs on May 04, 2017

Information

Sikkerhedsbrist gør det muligt at spore danskeres mobiltelefoner

Det er muligt at spore danskere via deres mobiltelefon, hvis man blot kender deres telefonnummer. Det viser flere test foretaget for Information af en førende it-ekspert på området. TDC erkender problemet

2. januar 2015

...vem som forårsaket ...s mobil-havari

...e det som et ondsinnet angrep.

Av Marius Jørgenrud

Publisert 15. april 2016 kl. 18:02 - Oppdatert 15. april 2016 kl. 18:06

ITPro. Business Cloud Hardware Infrastructure Security Software Technology Resources

NEWS Home › Security

Metro Bank targeted with 2FA-bypassing SS7 attacks

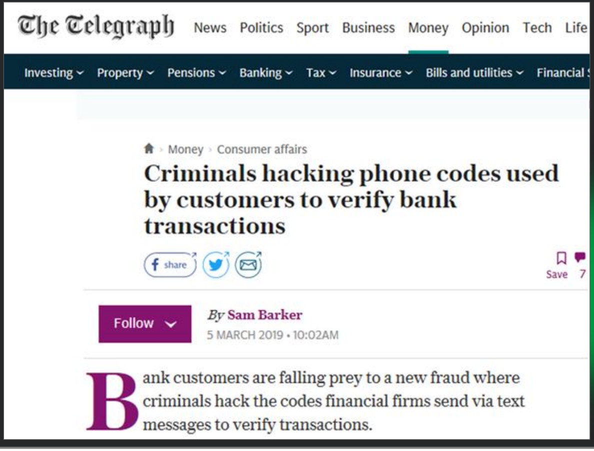
The highly sophisticated attack mechanism is becoming increasingly prevalent

by: Keumars Afifi-Sabet 1 Feb 2019

Metro Bank has reportedly fallen victim to a sophisticated two-factor authentication (2FA) bypass attack after hackers infiltrated a telecoms firm's text messaging protocol.

Example: High-profile case of SS7 Fraud

Many recent media reports

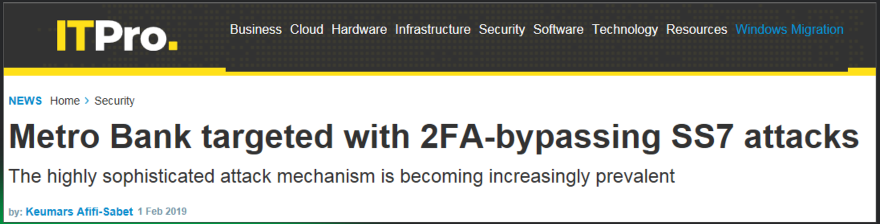

The Telegraph
News Politics Sport Business Money Opinion Tech Life
Investing Property Pensions Banking Tax Insurance Bills and utilities Financial
share
Save 7
Follow

Money › Consumer affairs

Criminals hacking phone codes used by customers to verify bank transactions

By Sam Barker
5 MARCH 2019 • 10:02AM

Bank customers are falling prey to a new fraud where criminals hack the codes financial firms send via text messages to verify transactions.

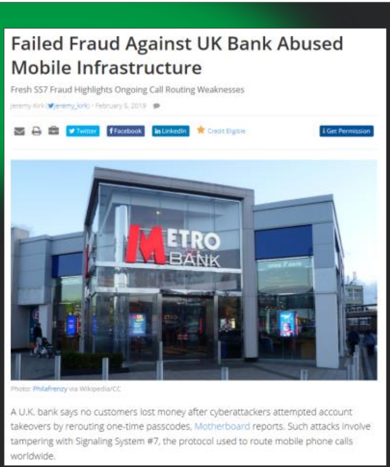

ITPro.
Business Cloud Hardware Infrastructure Security Software Technology Resources Windows Migration

NEWS Home › Security

Metro Bank targeted with 2FA-bypassing SS7 attacks

The highly sophisticated attack mechanism is becoming increasingly prevalent

by: Keumars Afifi-Sabet 1 Feb 2019



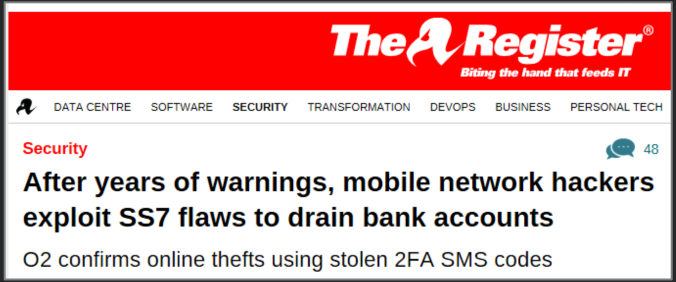
Failed Fraud Against UK Bank Abused Mobile Infrastructure

Fresh SS7 Fraud Highlights Ongoing Call Routing Weaknesses

Jeremy Kirk (jeremy_kirk) • February 5, 2019

Photo: Philafrenzy via Wikipedia/CC

A U.K. bank says no customers lost money after cyberattackers attempted account takeovers by rerouting one-time passcodes, Motherboard reports. Such attacks involve tampering with Signaling System #7, the protocol used to route mobile phone calls worldwide.


The Register®
Biting the hand that feeds IT
DATA CENTRE SOFTWARE SECURITY TRANSFORMATION DEVOPS BUSINESS PERSONAL TECH
48

Security

After years of warnings, mobile network hackers exploit SS7 flaws to drain bank accounts

O2 confirms online thefts using stolen 2FA SMS codes

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 how frequently they adapt to your defences?

The Need for Industry-Wide Signalling Intelligence

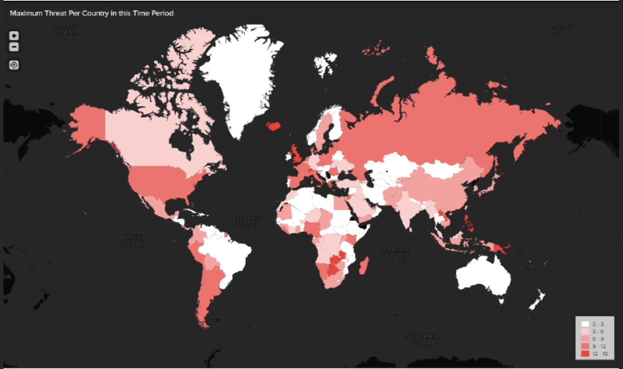
Many mobile operators have made changes to their network to deal with threats: signalling infrastructure updates, signalling firewall deployments, etc.

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

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).

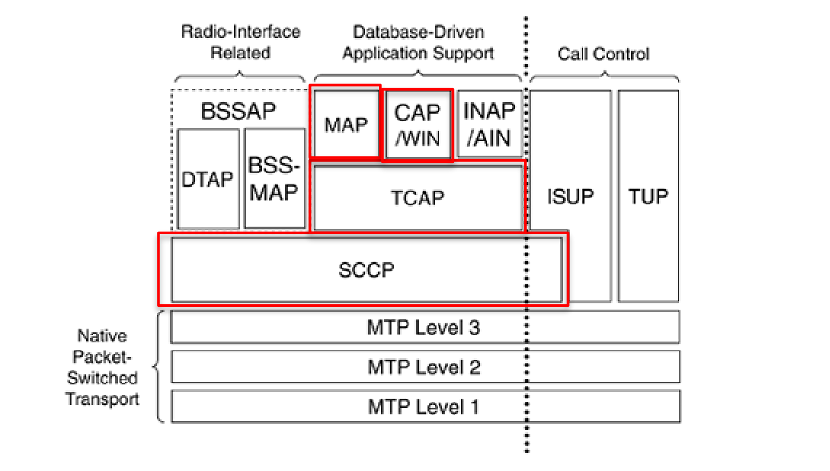
- Key Concepts:
  - Global Title or GT is a numeric address by which we can address the nodes (HLRs / VLRs / MSCs / gsmSCF)
  - Subscriber IDs (IMSIs & MSISDNs)

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.

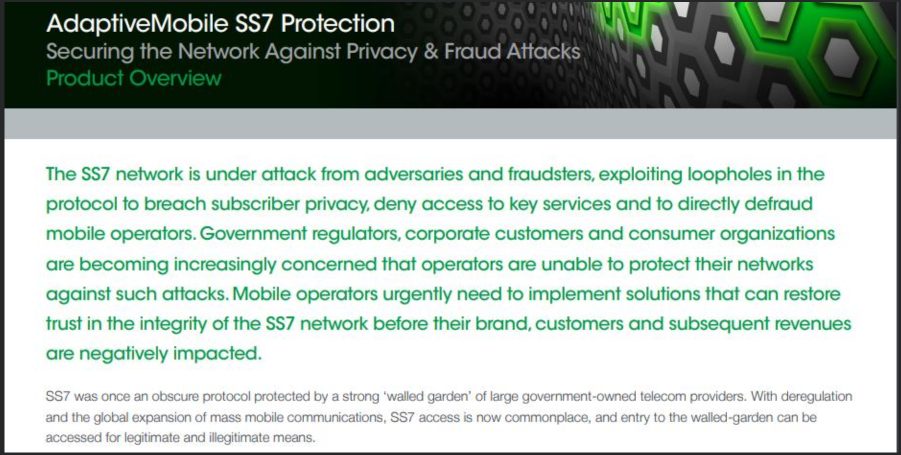
SS7 Stack

There are several layers or protocols within the SS7 Stack, FS.19 focuses on 4 main protocols.



1. SCCP, responsible for routing, addressing, subsystem management
2. TCAP, responsible for managing dialogues and structures
3. MAP, the application layer enabling GSM/UMTS/GPRS core networks to communicate
4. CAP (CAMEL), to provide additional services for roaming outside the HPMN

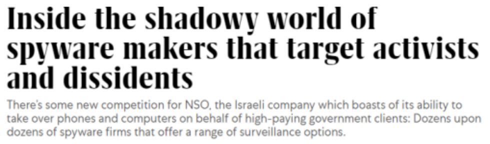
Security Issues Are Widely Reported & Often Exploited



AdaptiveMobile SS7 Protection
Securing the Network Against Privacy & Fraud Attacks
Product Overview

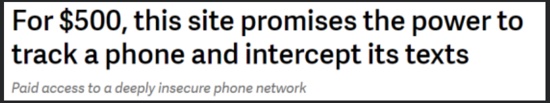
The SS7 network is under attack from adversaries and fraudsters, exploiting loopholes in the protocol to breach subscriber privacy, deny access to key services and to directly defraud mobile operators. Government regulators, corporate customers and consumer organizations are becoming increasingly concerned 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.



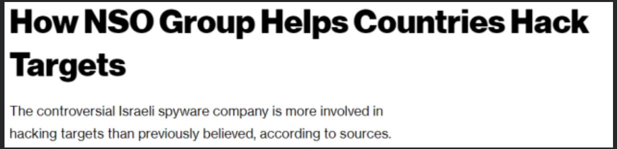
Inside the shadowy world of spyware makers that target activists and dissidents

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.



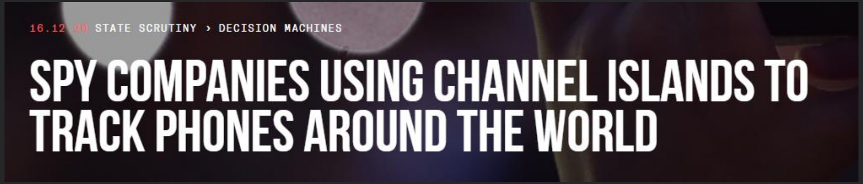
For $500, this site promises the power to track a phone and intercept its texts

Paid access to a deeply insecure phone network



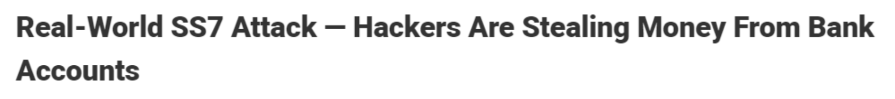
How NSO Group Helps Countries Hack Targets

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



16.12.20 STATE SCRUTINY › DECISION MACHINES

SPY COMPANIES USING CHANNEL ISLANDS TO TRACK PHONES AROUND THE WORLD



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

Signaling Attack Scenarios

Vulnerabilities in unsecured signaling networks enable diverse attack scenarios, most common of these are:

- Information Retrieval (Subscriber and Network Information)
- Location Tracking
- Traffic or Call Interception / Redirection
- DoS
- Fraud
- Phishing

These are more commonly witnessed on SS7 today but attacks are migrating to other bearers such as DIAMETER.

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.

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.

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.

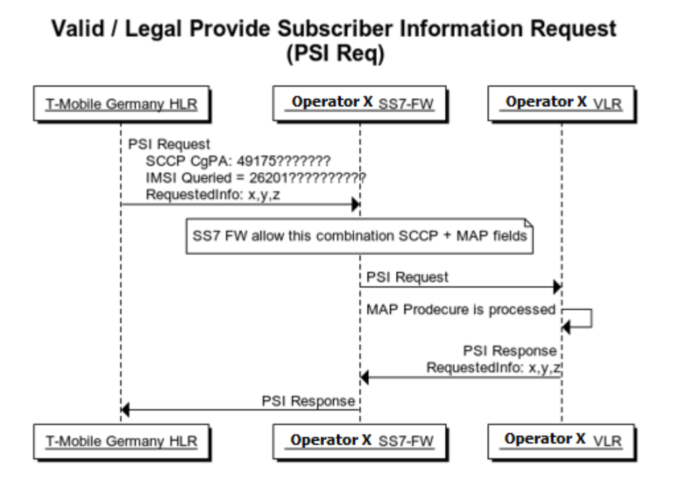
Category-2 PDUs include:

- 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

T-Mobile Germany HLR

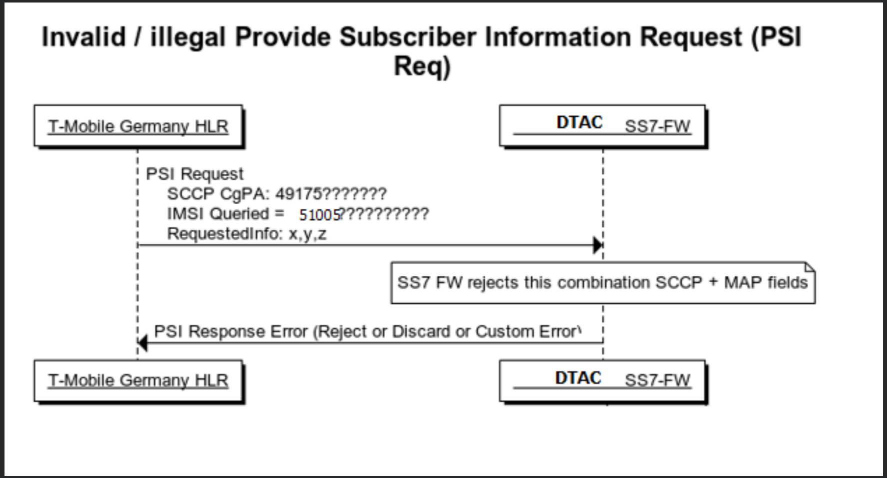
Operator X SS7-FW

Operator X VLR

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)

T-Mobile Germany HLR

DTAC SS7-FW

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)

T-Mobile Germany HLR

DTAC SS7-FW

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)

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.

Common Attack Patterns / Sequences

Each SS7 attack may be structured in a unique way, with a unique set of parameters for any single attack however some recurring patterns can be found across these incidents.

Two common attack types are information retrieval (network or subscriber focused) & location tracking.

- Network focused information retrieval are typically occur periodically where the intention of the incident is to uncover weaknesses in the protection levels, any weaknesses are documented & then used when real subscriber orientated attacks are required (for real surveillance missions later).
  - SRI-SM scanning & Category-1 PDU fuzzing attacks

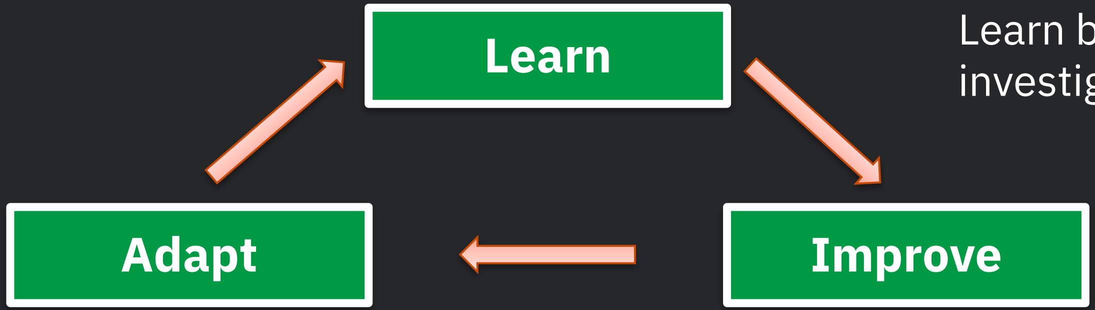
Subscriber tracking attacks tend to focus on a single MSISDN or IMSI, with the fewest set of PDUs required attempted. Some common sequences / techniques include

  - Silent SMS + PSI or PSL, PSI scanning across VLR/MSCs,
  - SRI-SM + Update Location
  - SIMTOOLKIT exploits

Threat Intelligence Lifecycle

Faced with complex and constantly evolving threats, operators should embrace a comprehensive, continuous framework that acknowledges the cyclical & ever evolving nature of the risk.

Exact operational procedures may vary but a simple model only needs to contain a few steps:



Learn by monitoring, detecting & investigating incidents in-depth.

Implementing blocking measures, Communicate findings

Improve by deploying & testing new rul improving work practices, make decisio

Knowing the enemy…

The attribution of signalling attacks often requires repeated in-depth investigations which are complicated by various factors:

- GT leasing arrangements
- Forensic or technical intelligence data availability (time constraints)
- Uncooperative 3rd parties
- Spoofing of source addresses

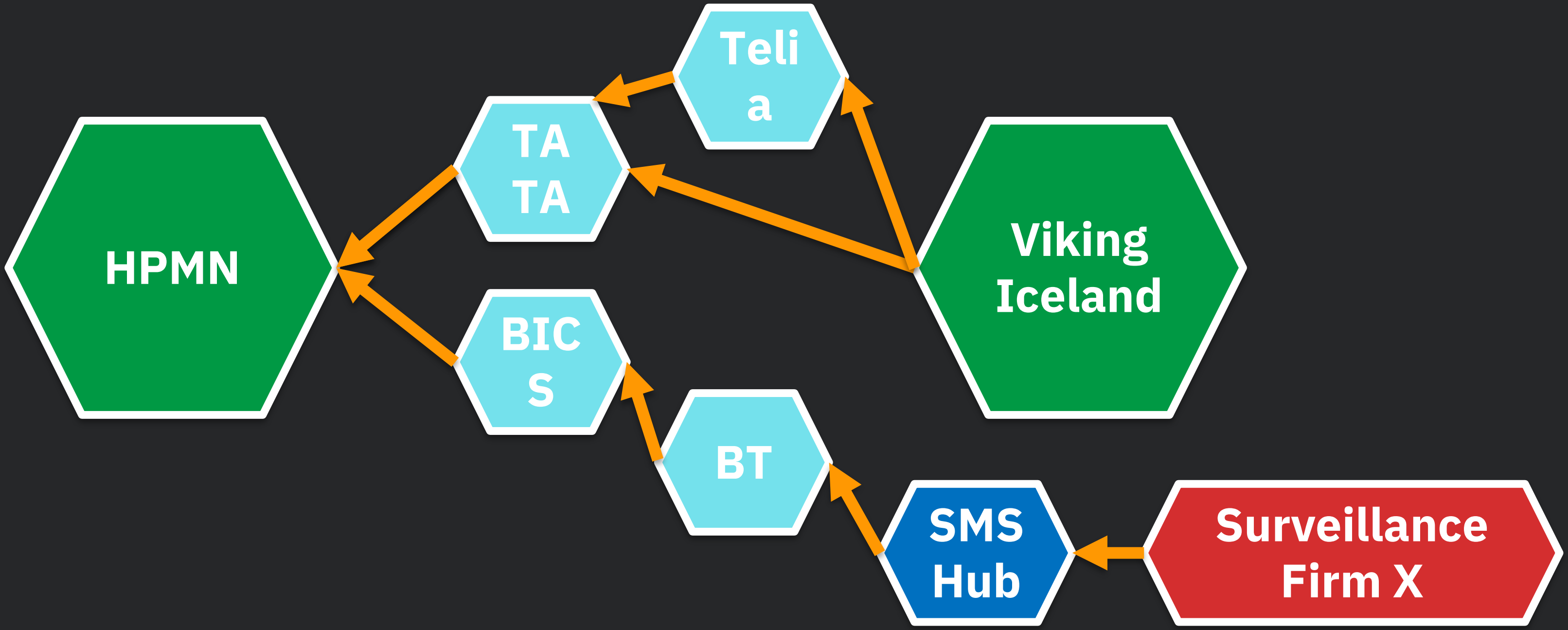
Typical adversaries:

- State (ranging from State-sponsored or State-coordinated to State-rogue activity)
- Criminal (Bank Fraud)
- Unethical or financially strained networks (abuse of steering, roaming feeds, or other fraud scenarios)

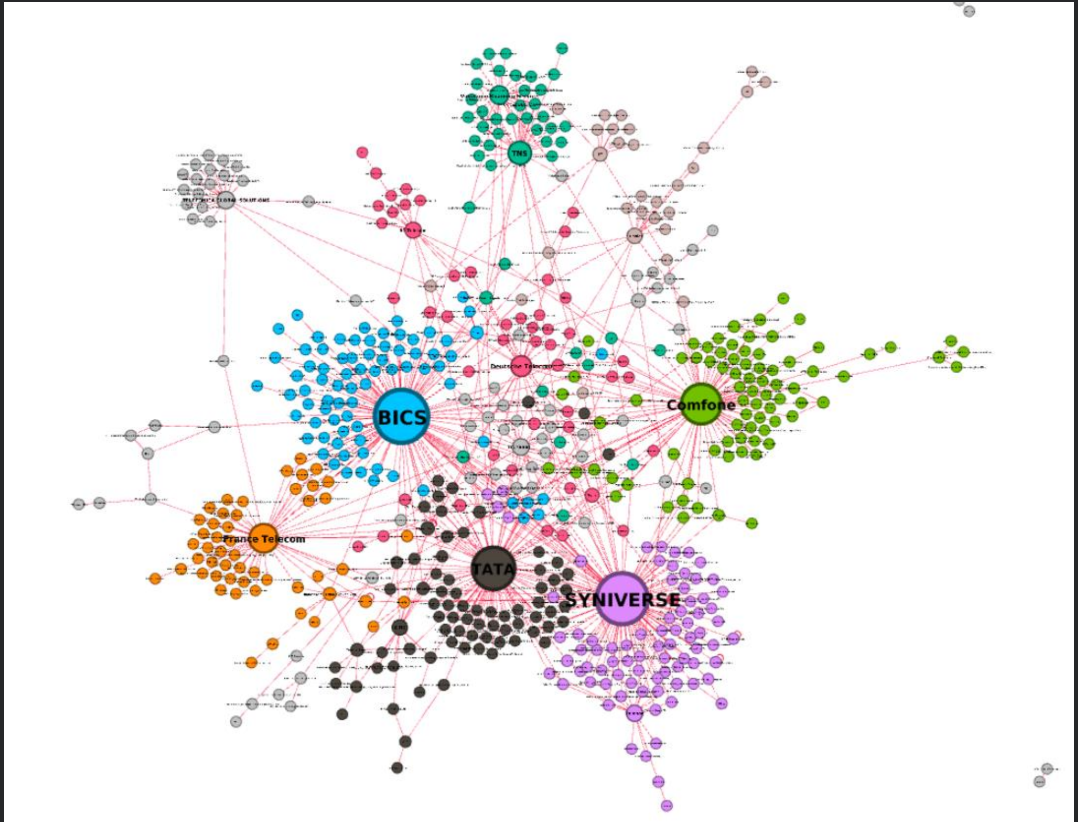
How can we know who is ultimately behind an attack?

Tracing Challenges

The origin of signalling arriving at the DNO (destination network operator) may not be obvious based on the SCCP CgPA.



SCCP Inter-carrier Map



AdaptiveMobile
Security