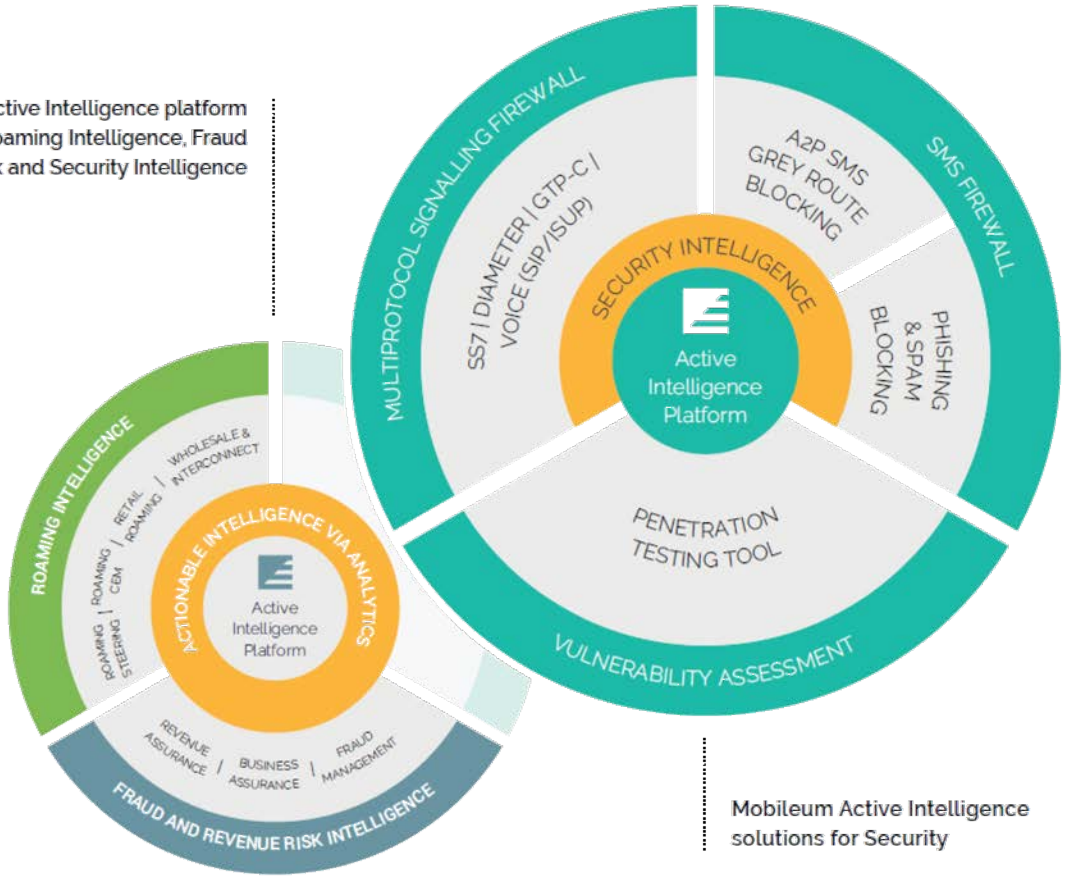
# MOBILEUM

Stephen Buck
SVP Security products

Mobileum Active Intelligence platform for Roaming Intelligence, Fraud and Revenue Risk and Security Intelligence



Mobileum Active Intelligence solutions for Security

**18**
YEARS OF GROWTH

**65%**
MARKET SHARE

**1Bn**
ROAMERS SERVED PER YEAR

**BEST SECURITY PRODUCT**
2017 & 2018

**110**
PATENTS AWARDED

**#1**
INNOVATOR OF 183 VENDORS

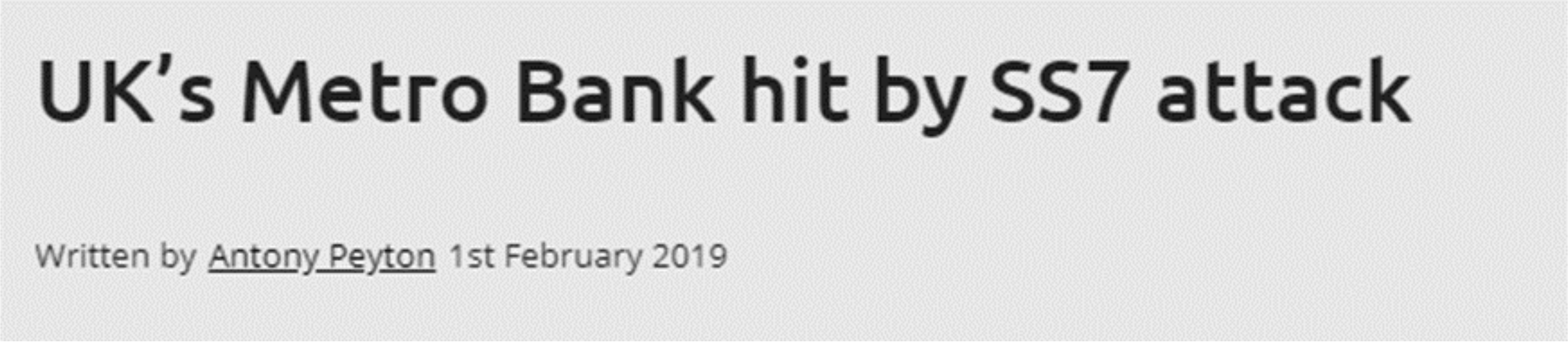
WeDo technologies
A MOBILEUM Company

MOBILEUM

# Agenda

- Examples risks and incidents - SS7, Diameter, GTP
- Solution options
- Long term solution – 5G and its impact on IPX

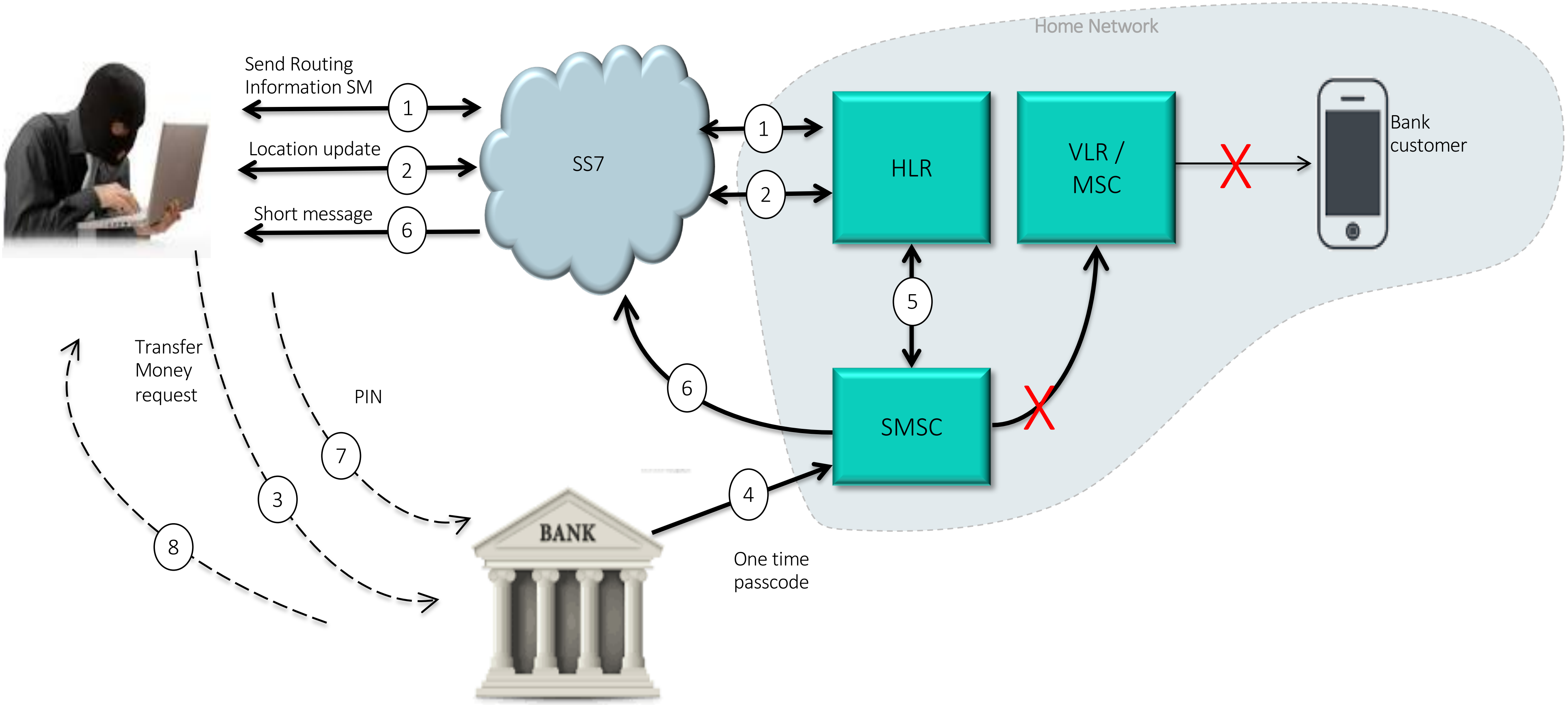
# Attacks frequent – rarely publicised



UK’s Metro Bank hit by SS7 attack

Written by Antony Peyton 1st February 2019

# SMS two factor authentication interception



# Types of attack

- The problem
  - International signalling was a trusted environment
  - No encryption or authentication
  - Easy and cheap access, stacks etc
- Attacks
  - Tracking
  - Call and text interception
  - Denial of service
  - Fraud

**GSMA documents define different categories**

- Cat 1 – Reject messages that should not be present on interconnect
- Cat 2 – Intra message checks. Check consistency. Check own subscriber.
- Cat 3 – Inter message checks. Stateful checks (e.g. location, service info, device)

# Impact

**52%**

Of consumers would leave or consider leaving their operator because of a security breach

**3rd**

Most likely reason to churn.

After price and coverage

**62%**

Of consumers would want to use 2FA less, stop using or have an alternative

**58%**

Of enterprises would leave or consider leaving their operator because of a security breach

**2nd**

Most likely reason to churn.

After price

**73%**

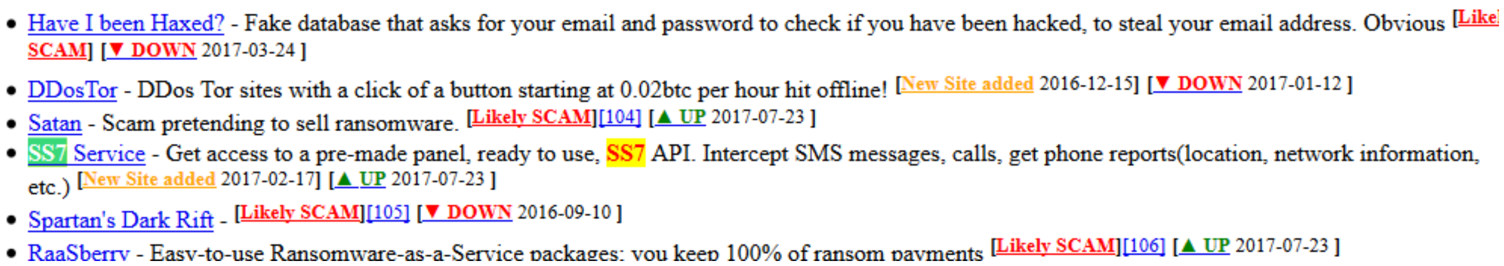
Of enterprises would want to use 2FA less, stop using or have an alternative

Source 2017 and 2018 consumer and Enterprise survey by Mobile Squared (sponsored by Mobileum/EI)

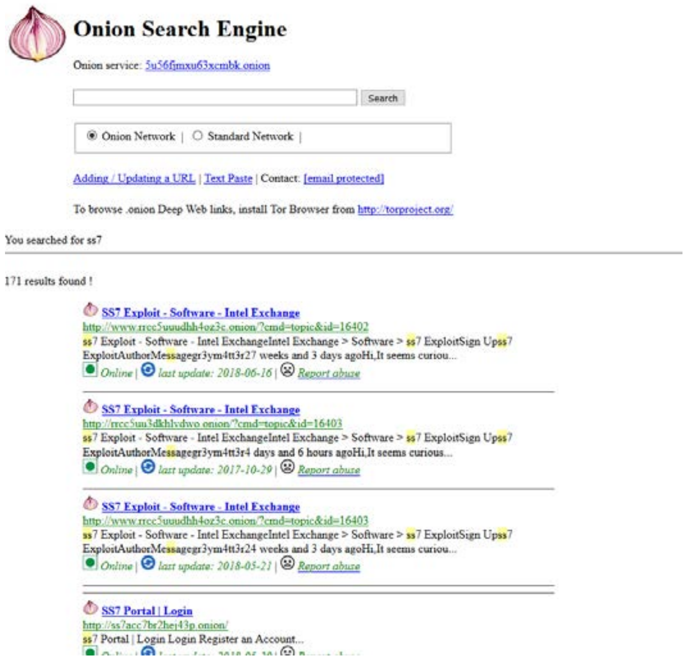
# Threat is real and happening

Not much price change on dark web for SS7 hacks in last 2 years

## Evidence of SS7 attacks



- Have I been Haxed? - Fake database that asks for your email and password to check if you have been hacked, to steal your email address. Obvious [Likely SCAM] [▼ DOWN 2017-03-24 ]
- DDosTor - DDos Tor sites with a click of a button starting at 0.02btc per hour hit offline! [New Site added 2016-12-15] [▼ DOWN 2017-01-12 ]
- Satan - Scam pretending to sell ransomware. [Likely SCAM][104] [▲ UP 2017-07-23 ]
- SS7 Service - Get access to a pre-made panel, ready to use, SS7 API. Intercept SMS messages, calls, get phone reports(location, network information, etc.) [New Site added 2017-02-17] [▲ UP 2017-07-23 ]
- Spartan's Dark Rift - [Likely SCAM][105] [▼ DOWN 2016-09-10 ]
- RaaSberry - Easy-to-use Ransomware-as-a-Service packages: you keep 100% of ransom payments [Likely SCAM][106] [▲ UP 2017-07-23 ]



**Onion Search Engine**

Onion service: 5u56fjmxu63xcmbk.onion

● Onion Network | ○ Standard Network |

Adding / Updating a URL | Text Paste | Contact: [email protected]

To browse .onion Deep Web links, install Tor Browser from http://torproject.org/

You searched for ss7

171 results found !

SS7 Exploit - Software - Intel Exchange
http://www.rrcc5uuudhh4oz3c.onion/?cmd=topic&id=16402
ss7 Exploit - Software - Intel ExchangeIntel Exchange > Software > ss7 ExploitSign Upss7 ExploitAuthorMessagegr3ym4tt3r27 weeks and 3 days agoHi,It seems curiou...
Online | last update: 2018-06-16 | Report abuse

SS7 Exploit - Software - Intel Exchange
http://rrcc5uu3dkhlvdwo.onion/?cmd=topic&id=16403
ss7 Exploit - Software - Intel ExchangeIntel Exchange > Software > ss7 ExploitSign Upss7 ExploitAuthorMessagegr3ym4tt3r4 days and 6 hours agoHi,It seems curious...
Online | last update: 2017-10-29 | Report abuse

SS7 Exploit - Software - Intel Exchange
http://www.rrcc5uuudhh4oz3c.onion/?cmd=topic&id=16403
ss7 Exploit - Software - Intel ExchangeIntel Exchange > Software > ss7 ExploitSign Upss7 ExploitAuthorMessagegr3ym4tt3r24 weeks and 3 days agoHi,It seems curiou...
Online | last update: 2018-05-21 | Report abuse

SS7 Portal | Login
http://ss7acc7br2hej43p.onion/
ss7 Portal | Login Login Register an Account...

- **14 vulnerability assessments in last 9 months – all had attacks or attempts**
- **Typically we see between 0.05% and 0.01% of signalling is "fraudulent" @ 1,000 TPS = hundreds/thousands per hour**

# Attack categorisation on SS7

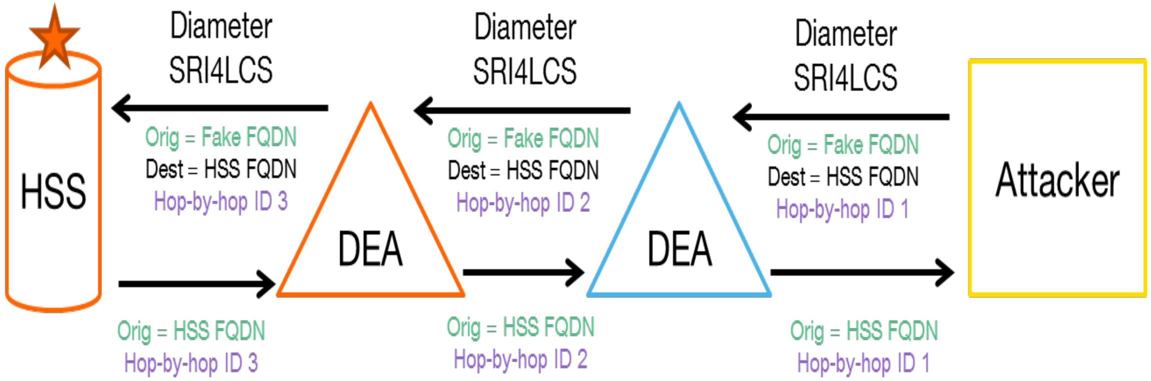
## DT results (snapshot example with permission)

| Category | % attacks | % traffic blocked | Examples |
|---|---|---|---|
| Category 1<br>(Not expected on interconnect) | 99.26% | 0.19% | SRI, Send parameters, ATI, sendIMSI, PSI, SRIforLCS |
| Category 2<br>(Inconsistency or not own subscriber) | 0.05% | 0.001% | CancelLocation, UnstructuredSS |
| Category 3<br>(Stateful checks – e.g. velocity, service key) | 0.69% | 0.01% | UpdateLocation, AuthFailureReport, ReadyforSM, PurgeMS, SAI |

- Does this imply blocking category 1 gives 99% protection ? – No!
  - Category 1 tends to be tracking, commercial services, grey routing, IMSI capture – least damaging
  - Category 2 Denial of service, diverts
  - Category 3 most damaging typically – e.g. call and text divert
- This is after removal of (many) false positives – perhaps 90% of “attacks” are false positives

# Diameter – more risk

- More scope for attacks
  - Most SS7 messages have diameter equivalents
  - Spoofing is easy
  - AVP flexibility
- Less visible real attacks today (i.e. <0.01%)
  - Category 1 – Basically zero
  - Category 2 – Very few (<0.001%)
  - Category 3 – Some (~0.001%) but many are remote SIM MiFi
- Many false positives
- Expect to see diameter threats increasing and new threats – e.g. CCR refund account
  - SS7 is ubiquitous today



# GTP threats – in (very) brief

- Scanning – network discovery (e.g. echo request)
- IMSI retrieval (e.g. ID request)
- Key and APN retrieval (e.g. context request)
- Denial of service (e.g. Delete context, restart counters (echo))
- Interception of data traffic (e.g. modify bearer, update PDP context to redirect traffic
- Fraud (e.g. modify bearer, create session for own IMSI)

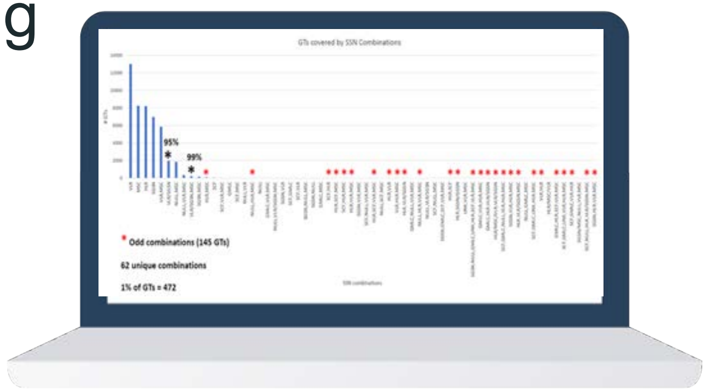
# Threat analysis – common invalid assumptions

FALSE

- The types of network equipment are quite small – therefore identifying equipment by messages is straightforward
  - ~99% sources behave as expected combinations of network equipment BUT
  - ~1.5% of sources behave uniquely (but only few are bad)

FALSE

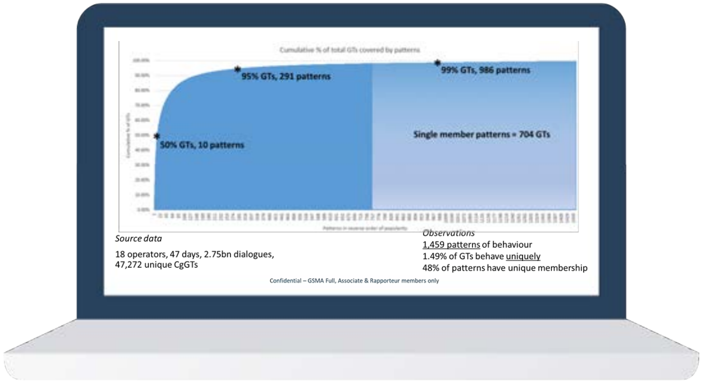
- For each operator the set of equipment is stable over time
  - ~0.5% signalling sources (GTs) are new every day (i.e. hundreds)
- To identify new threats requires big data analytics to exclude valid new sources and valid, but unusual signalling



* Odd combinations (145 GTs)

62 unique combinations

1% of GTs = 472



*Source data*

18 operators, 47 days, 2.75bn dialogues,
47,272 unique CgGTs

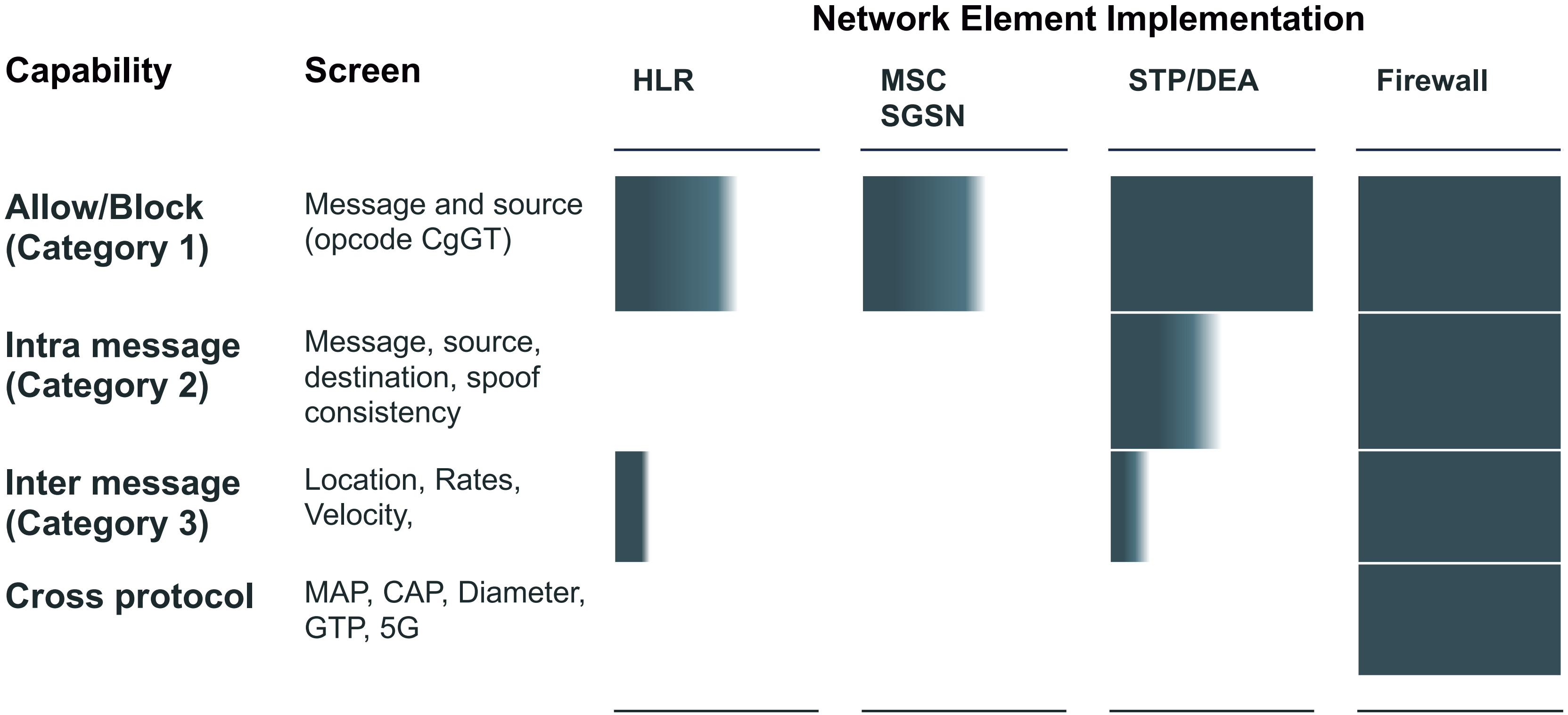
*Observations*

1,459 patterns of behaviour
1.49% of GTs behave uniquely
48% of patterns have unique membership

Confidential – GSMA Full, Associate & Rapporteur members only

# Solutions

- Home routing (protect IMSI)
- STP/DEA configuration - block messages not allowed (category 1)
- Signalling firewall(s) + analytics



| Capability | Screen | Network Element Implementation | | | |
|---|---|---|---|---|---|
| | | HLR | MSC<br>SGSN | STP/DEA | Firewall |
| **Allow/Block (Category 1)** | Message and source (opcode CgGT) | ▨ | ▨ | ■ | ■ |
| **Intra message (Category 2)** | Message, source, destination, spoof consistency | | | ▨ | ■ |
| **Inter message (Category 3)** | Location, Rates, Velocity, | ▨ | | ▨ | ■ |
| **Cross protocol** | MAP, CAP, Diameter, GTP, 5G | | | | ■ |

# Agenda

- Examples risks and incidents - SS7, Diameter, GTP
- Solution options
- Long term solution – 5G and its impact on IPX

# Protocol evolution

| 2G | 3G | 4G | 5G |
|---|---|---|---|
| Update Location | Update Location | Update Location | Update Location |
| MAP | MAP | S6a | JSON (N8/N32) |
| TCAP | TCAP | Diameter | HTTP2 |
| SCCP | SCCP | SCTP | TCP |
| MTP | SIGTRAN | IP | IP |

| | | | | |
|---|---|---|---|---|
| **Parameters** | Mostly fixed | Mostly fixed | Flexible AVPs | Free text |
| **E2E security** | Not used | Not used | Not used | TLS/JOSE |
| **Session** | TCAP dialogue | TCAP dialogue | Diameter Req/Resp (id) | Http Req/resp (id) |
| **E2E routing** | Global title | Global title | Host/realm route record | Host |

# 5G interconnect security requirements

- Encryption of message / parameters
- Signing of message

### Authentication

Who is the real sender?

### Integrity

Was the message/parameter modified ?

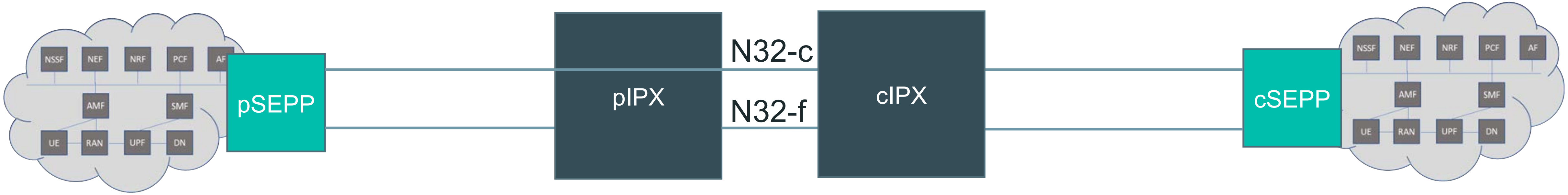
### Replay protection

Can a message be recorded and replayed

### Confidentiality

Can the message/parameter be read

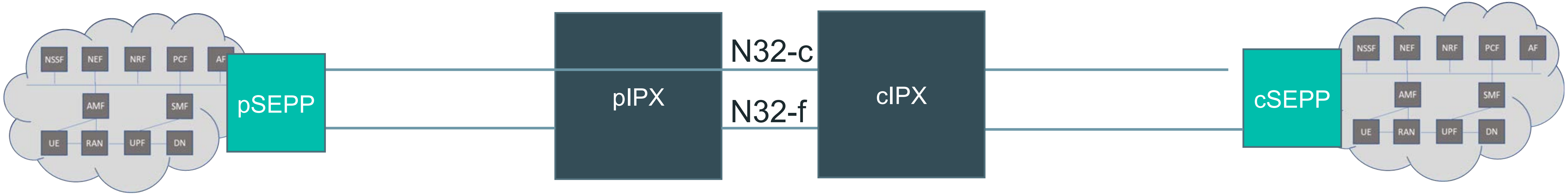
# 5G interconnect security overview



- pSEPP signs and encrypts messages
- cSEPP decrypts, reconstructs and checks signature

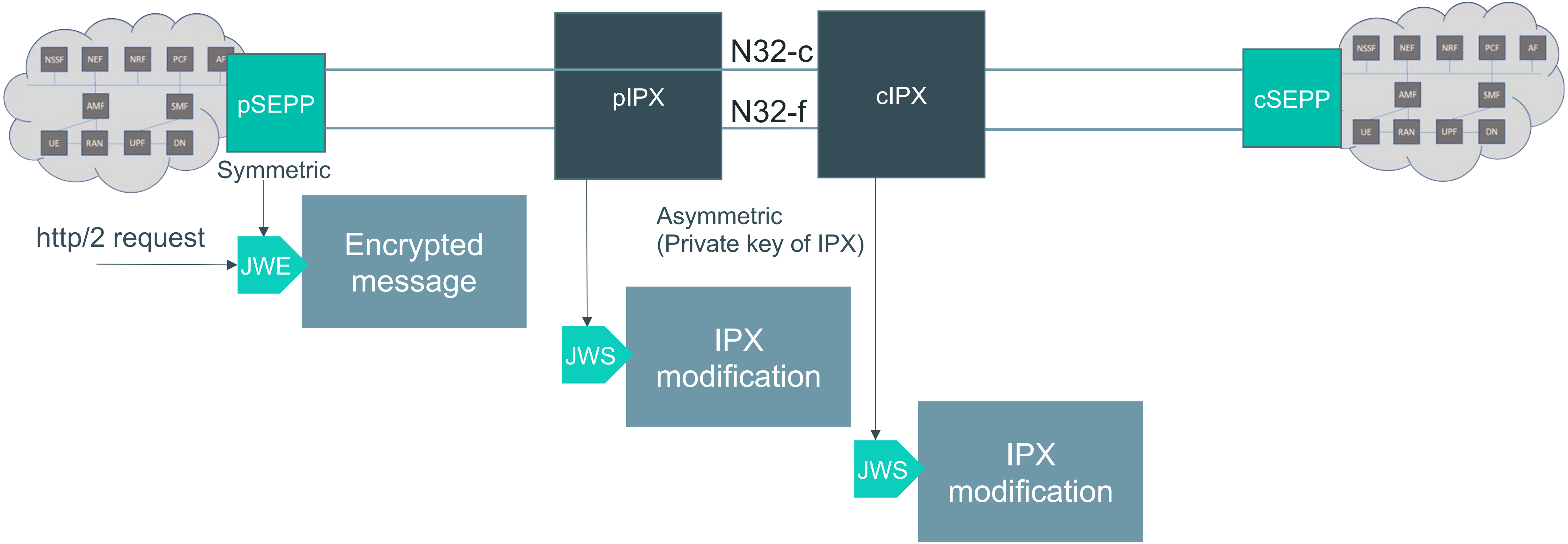
- But what about the IPX? For IPX to deliver services either:
  - SEPP needs to come from IPX and be part of trusted network domain
  - Operator and IPX need to negotiate which parameters can be seen/modified

# 5G interconnect security overview



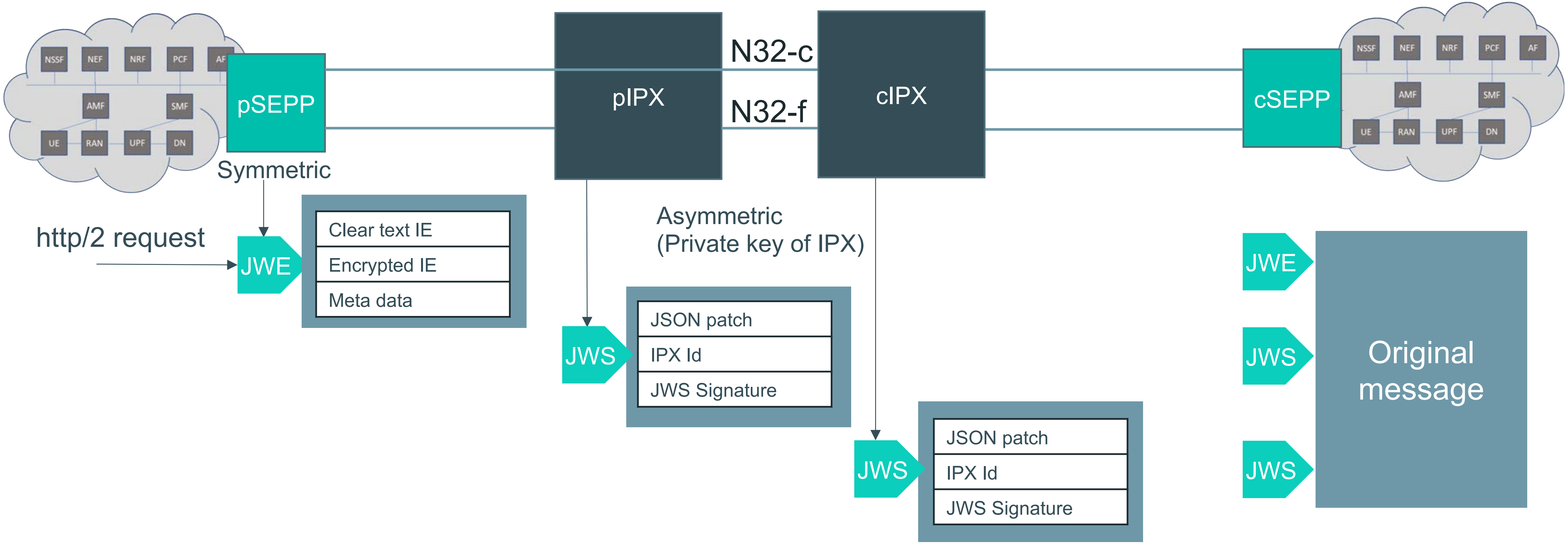
- SEPP needs to come from IPX and be part of trusted network domain

# 5G interconnect security overview



- Operator and IPX need to negotiate which parameters can be seen/modified (but expect more influence of regulators)

# 5G interconnect security overview



- Operator and IPX need to negotiate which parameters can be seen/modified (but expect more influence of regulators)

# Summary

- Significant level of attacks/risks on SS7, Diameter and GTP
- Significant risk to customers and operators brand and financial risk
- Real networks are more complex than standards imply
- This requires a signalling firewall to provide protection (and manage new sources and threats)
- 5G (and 4G retrofit) will improve protection, but should be delivered in conjunction with signalling firewall

THANK YOU