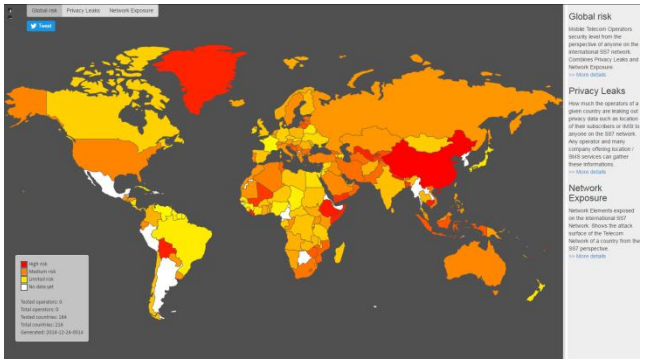
Assaulting IPX Diameter roaming network

Alexandre De Oliveira

15/03/2016

Whoami

- Telecom security curious
- Red Team at POST Luxembourg
- Previously P1 Security



- SS7map projet during 31C3 with Laurent Ghigonis
- Worldwide SS7 attacks with Pierre-Olivier Vauboin

HITB GSEC

HITBSecConf
AMSTERDAM // MALAYSIA

eico
a new dawn

Why diameter security ?

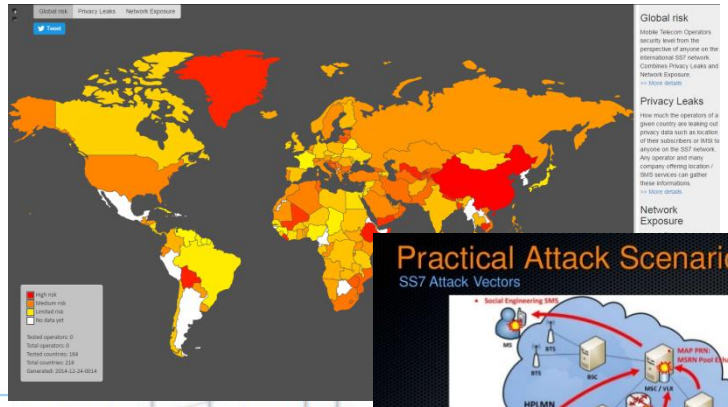
- SS7 security was a **disaster**

SS7: Locate. Track. Manipulate.

You have a remote-controlled tracking device in your pocket

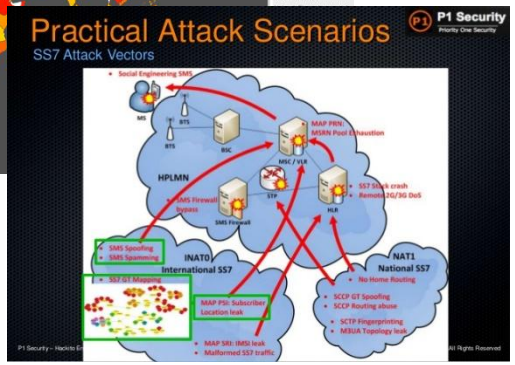
Invasive phone tracking: New SS7 research blows the lid off mobile security

Hacker conference Chaos Communication Congress 31c3 is under way in Hamburg, Germany right now where three SS7 talks have revealed the ease of invasive cell phone surveillance.



- Scoping session conducted – main focus to be on enabling CNE access to **BELGACOM GRX Operator**
- **Ultimate Goal – enable CNE access to BELGACOM Core GRX Routers from which we can undertake MiTM operations against targets roaming using Smart Phones.**
- Secondary focus – breadth of knowledge on GRX Operators
- Operations Manager assigned, team assembles

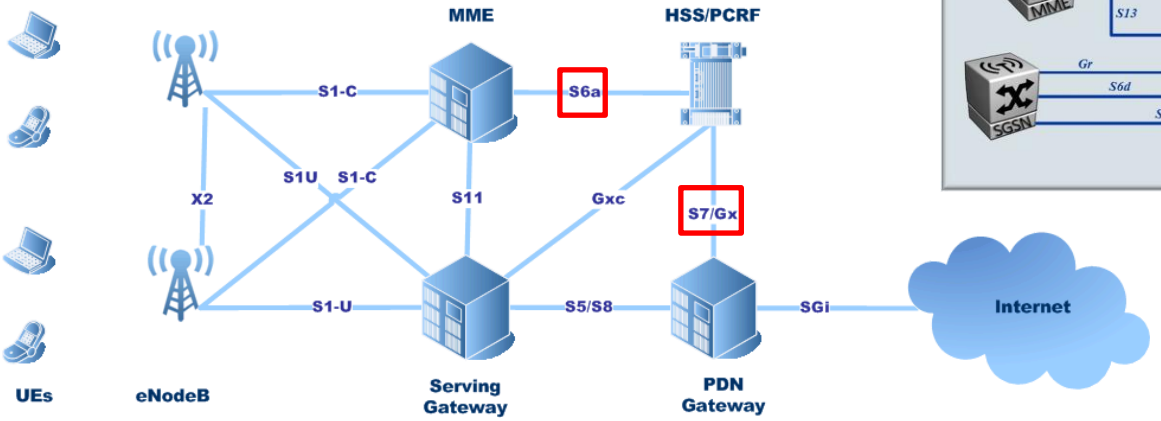
bics
a belgacom company

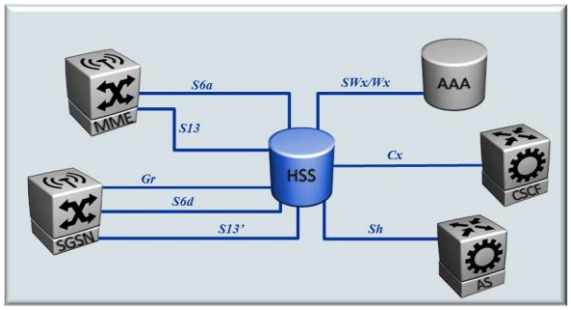


- And about Diameter ?

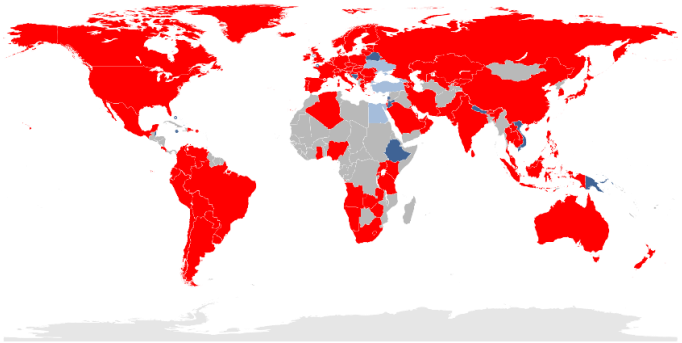
Diameter

- Used for signalisation in LTE Networks





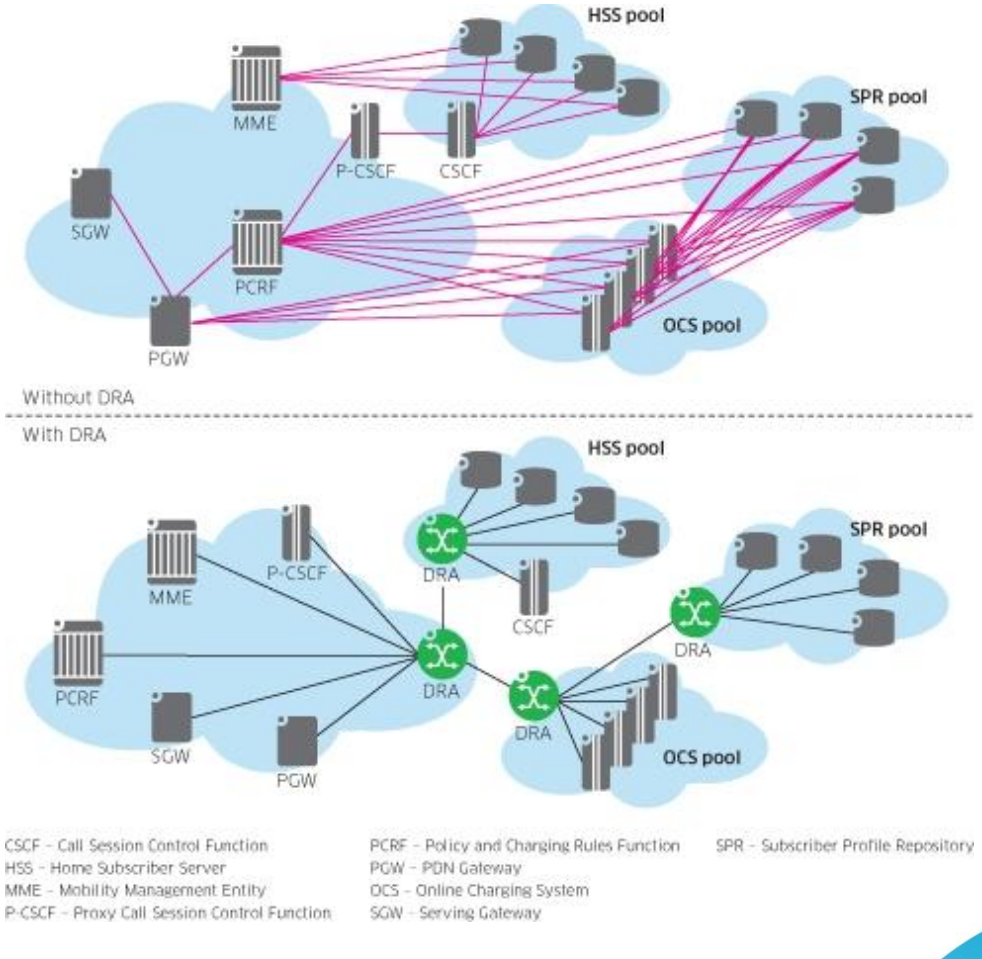
- Worldwide deployment
  - Roaming available



- IPX: IP exchange – Diameter Roaming network

Diameter architecture possibilities

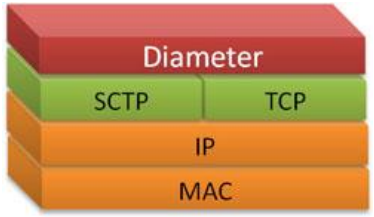
- Mesh vs Routed networks
- Real networks are mixed



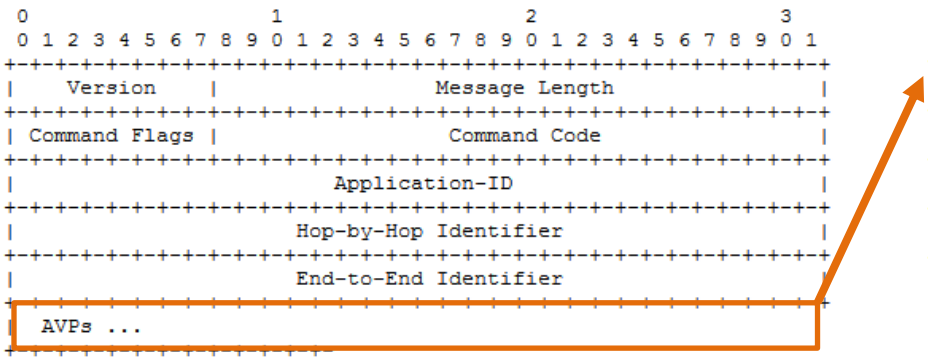
- Hard to maintain
- Filtering is complexe
- Impossible for huge networks
- Segmentation by default

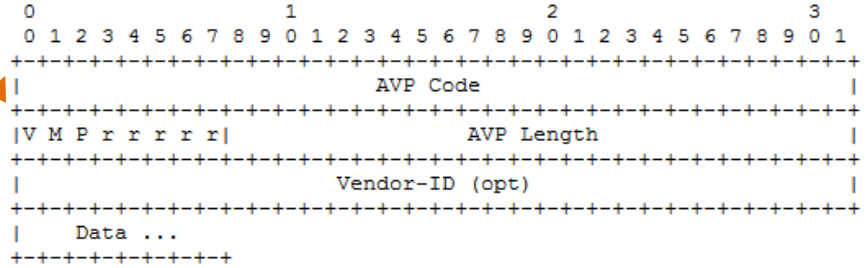
- Easier to maintain
- Filtering is centralized (DEA/DRA)
- Cost of DEA/DRA
- Routing is « Open » by default

Diameter in telecom world



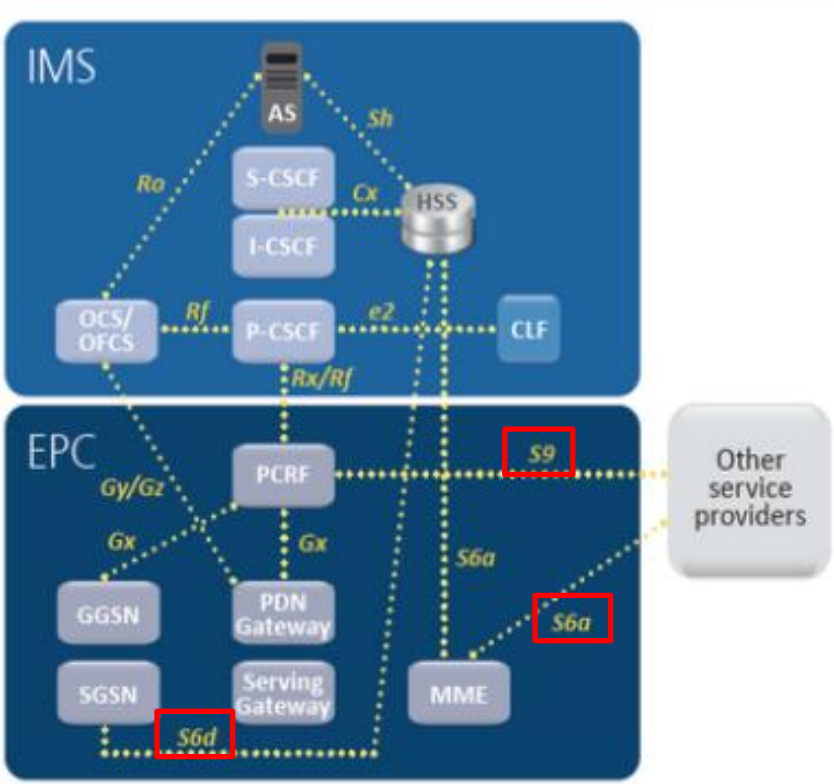
- IP based, over SCTP/3868
- Authentication, Authorization, and Accounting protocol and more
- Base defined by RFC 6733 & Telecom AVPs defined by 3GPP
- Diameter AVP allows infinity of possiblities

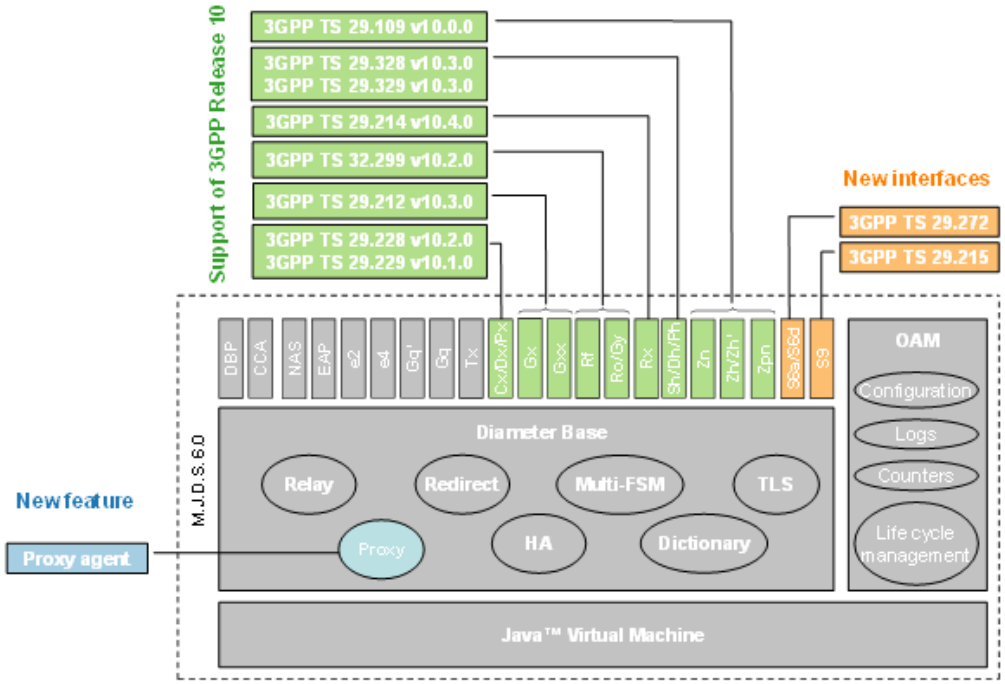




Interfaces / Applications / AVPs

- Infinity of Diameter applications & AVPs to be defined





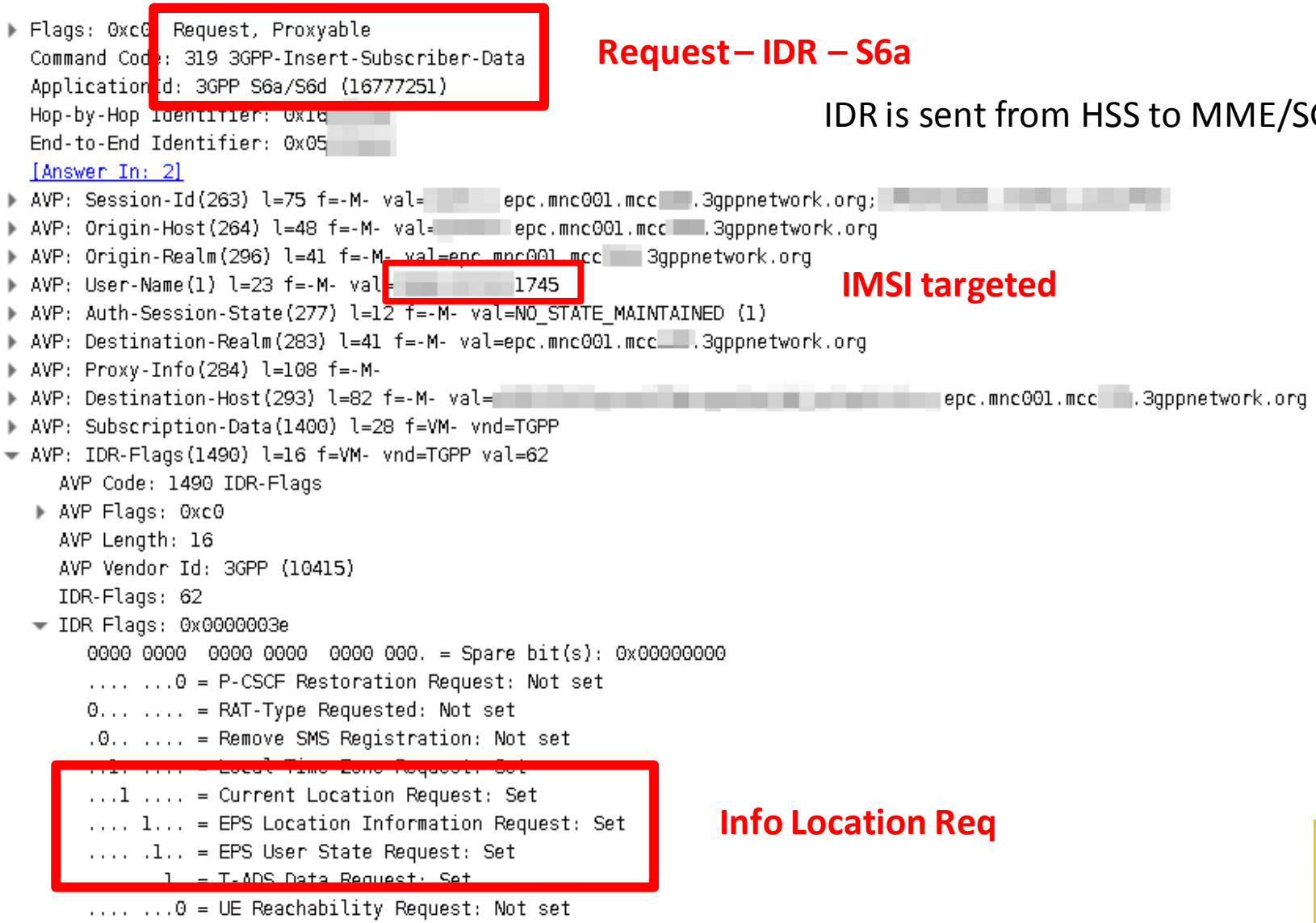
- S6a/S6d for HSS/MME/SGSN roaming
- S9 for inter PCRF roaming

Gathering information on IPX

- Operator giving to much info in **IR.21** :
  - 106 MME
  - 70 HSS
  - 18 DSC -> Ericsson DEA/DRA
  - 70 DEA
  - 8 M2M HSS
  - 146 IPX DNS
  - Etc…
- Send **automatic routed** (IMSI) messages : AIR !
  - Get **HSS host** & **naming pattern** !
- Send any diameter messages to a random host destination to the network
- Request the **IPX DNS** !

Tracking via Diameter S6a

Insert subscriber Data Request - IDR



Request – IDR – S6a

IDR is sent from HSS to MME/SGSN

IMSI targeted

Info Location Req

Insert subscriber Data Answer - IDA

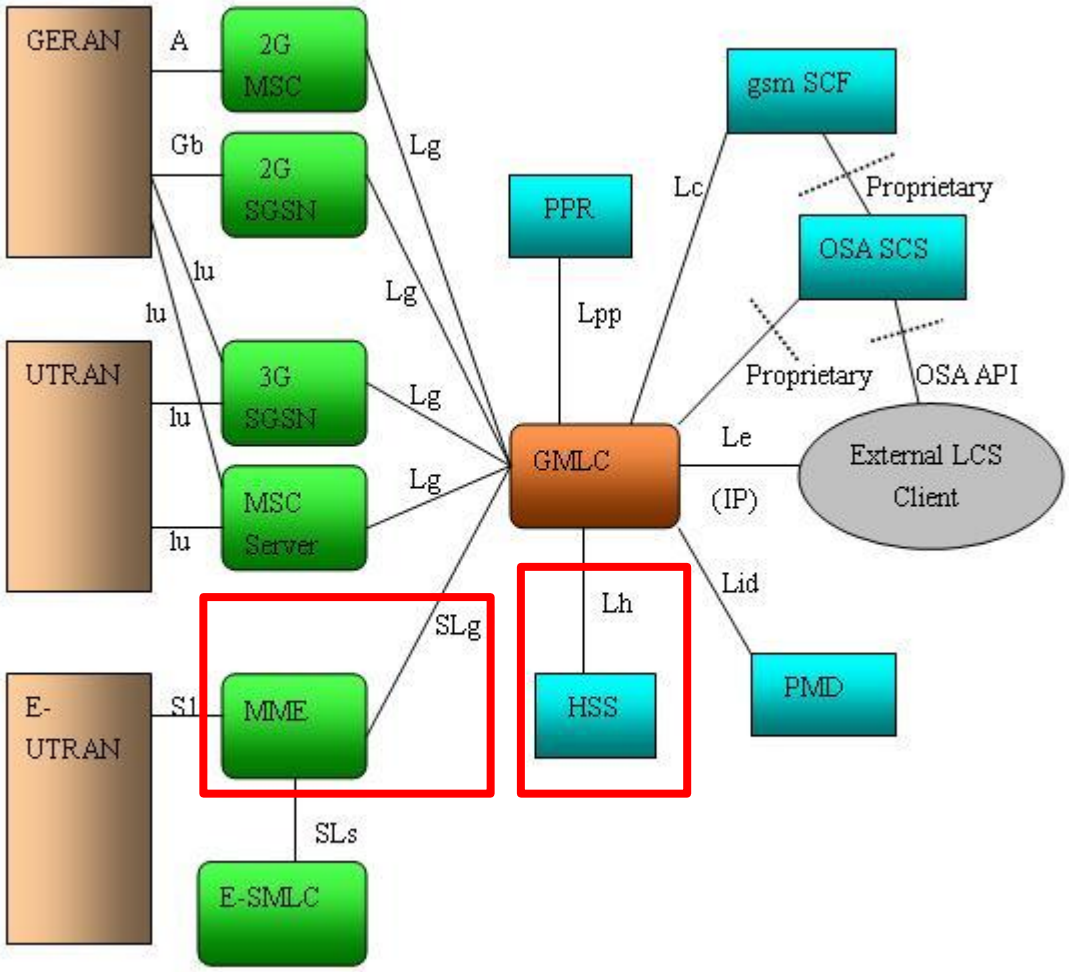
```
▼ AVP: EPS-Location-Information(1496) l=64 f=V-- vnd=TGPP
    AVP Code: 1496 EPS-Location-Information
  ▶ AVP Flags: 0x80
    AVP Length: 64
    AVP Vendor Id: 3GPP (10415)
  ▼ EPS-Location-Information:
    ▼ AVP: MME-Location-Information(1600) l=52 f=V-- vnd=TGPP
        AVP Code: 1600 MME-Location-Information
      ▶ AVP Flags: 0x80
        AVP Length: 52
        AVP Vendor Id: 3GPP (10415)
      ▼ MME-Location-Information:
        ▼ AVP: E-UTRAN-Cell-Global-Identity(1602) l=19 f=V-- vnd=TGPP val=72
            AVP Code: 1602 E-UTRAN-Cell-Global-Identity
          ▶ AVP Flags: 0x80
            AVP Length: 19
            AVP Vendor Id: 3GPP (10415)
            E-UTRAN-Cell-Global-Identity: 72
            Padding: 00
        ▼ AVP: Tracking-Area-Identity(1603) l=17 f=V-- vnd=TGPP val=72
            AVP Code: 1603 Tracking-Area-Identity
          ▶ AVP Flags: 0x80
            AVP Length: 17
            AVP Vendor Id: 3GPP (10415)
            Tracking-Area-Identity: 72
            Padding: 000000
```

Cell-ID

Tracking Area

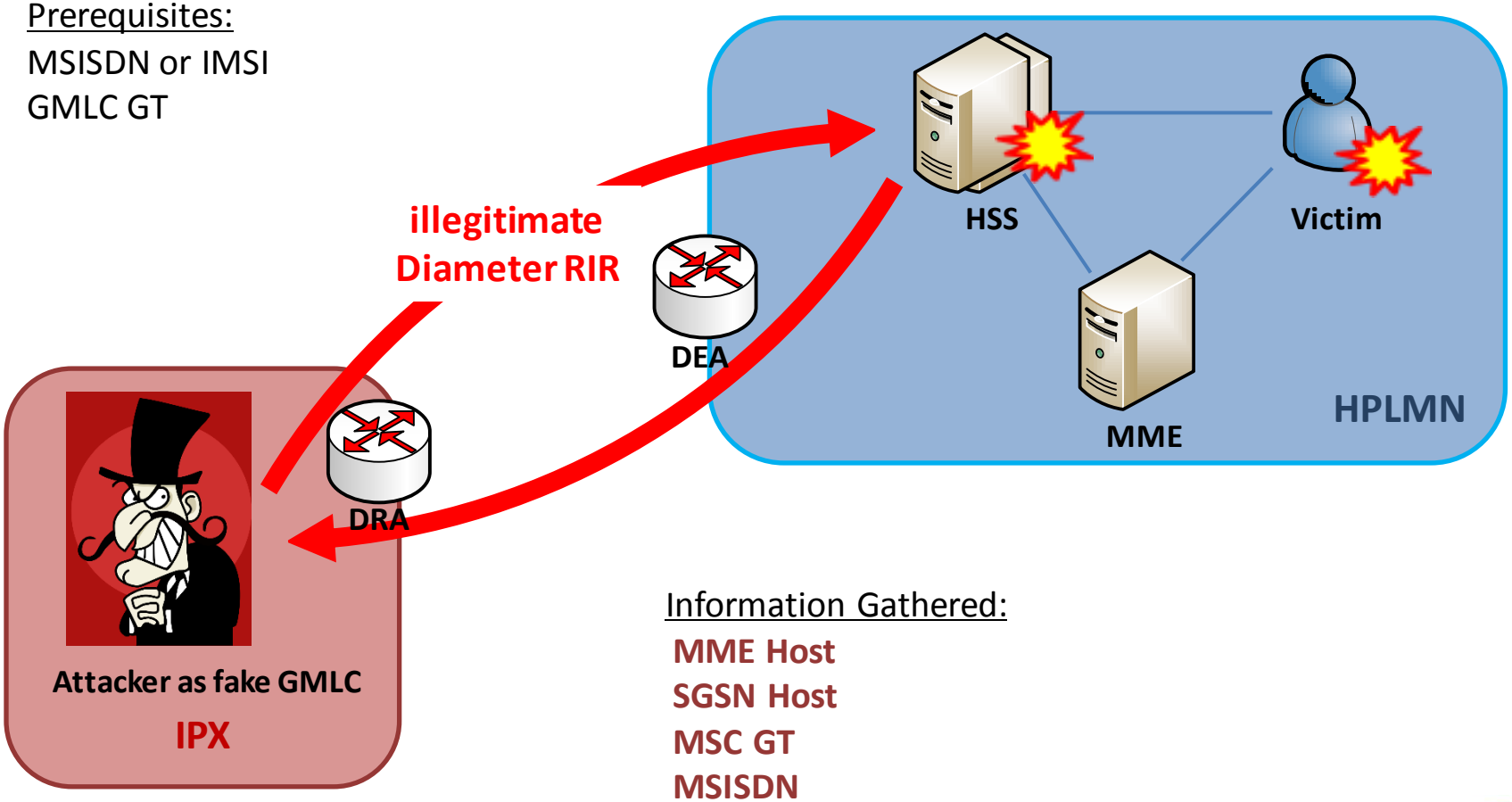
Also get current state ATTACHED / DETACHED / …

Using governmental tracking



SLh – RIR Routing Info Request

Prerequisites:
MSISDN or IMSI
GMLC GT

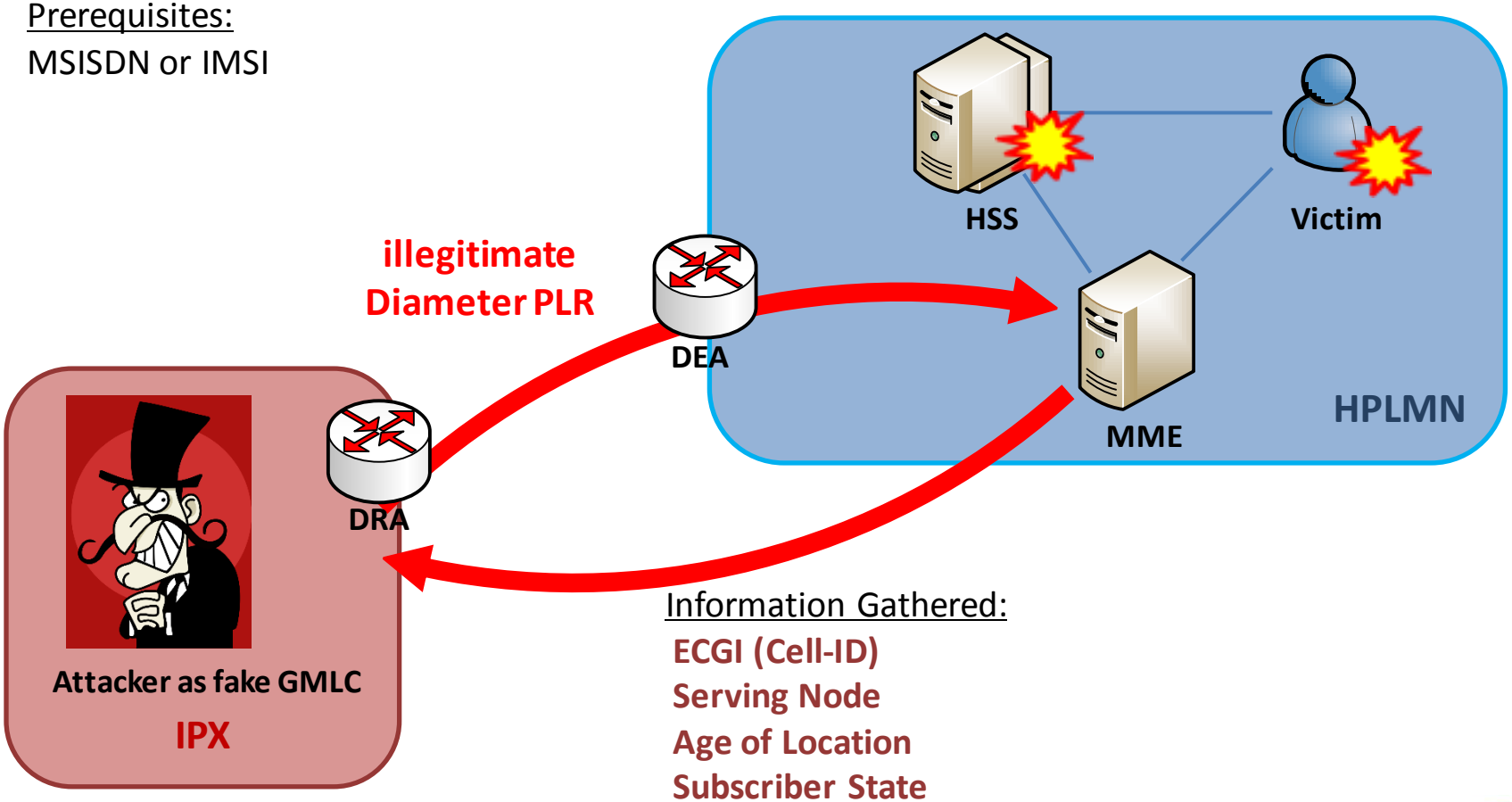


Information Gathered:

- MME Host
- SGSN Host
- MSC GT
- MSISDN

SLg – PLR Provide Location Request

Prerequisites:
MSISDN or IMSI

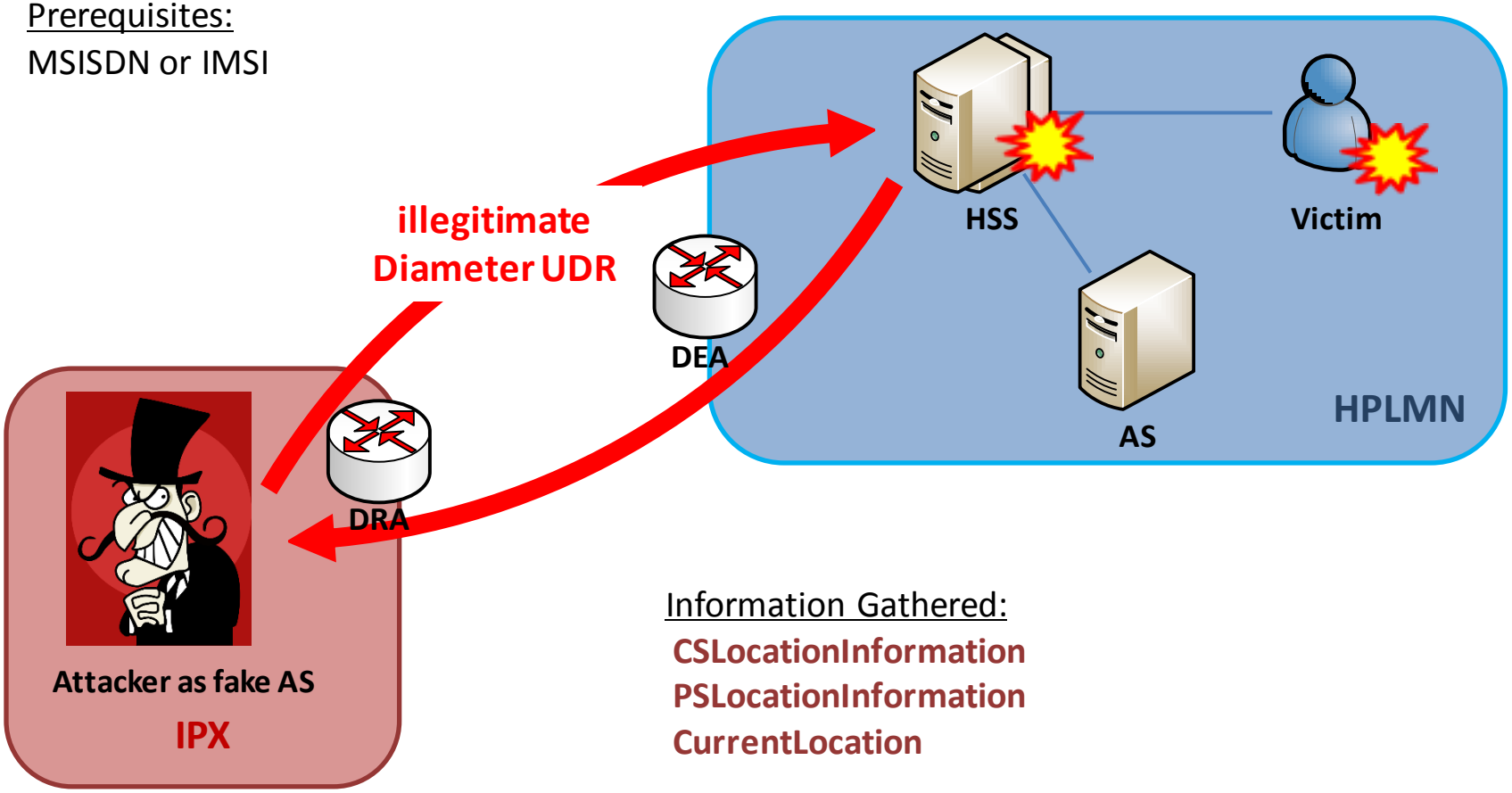


Information Gathered:

- ECGI (Cell-ID)
- Serving Node
- Age of Location
- Subscriber State
- Positionning Data

Tracking in IMS – Sh UDR

Prerequisites:
MSISDN or IMSI



Information Gathered:

CSLocationInformation
PSLocationInformation
CurrentLocation

S6c – Diameter SRR (SRISM)

- Introduced released 11 – MME / SMS-IWMSC / SMS-GMSC
- SS7 as already SRISM in SMS call-flow
- Protections implemented in SS7 with **SMS-FW** and **Home Routing** in SS7/SIGTRAN

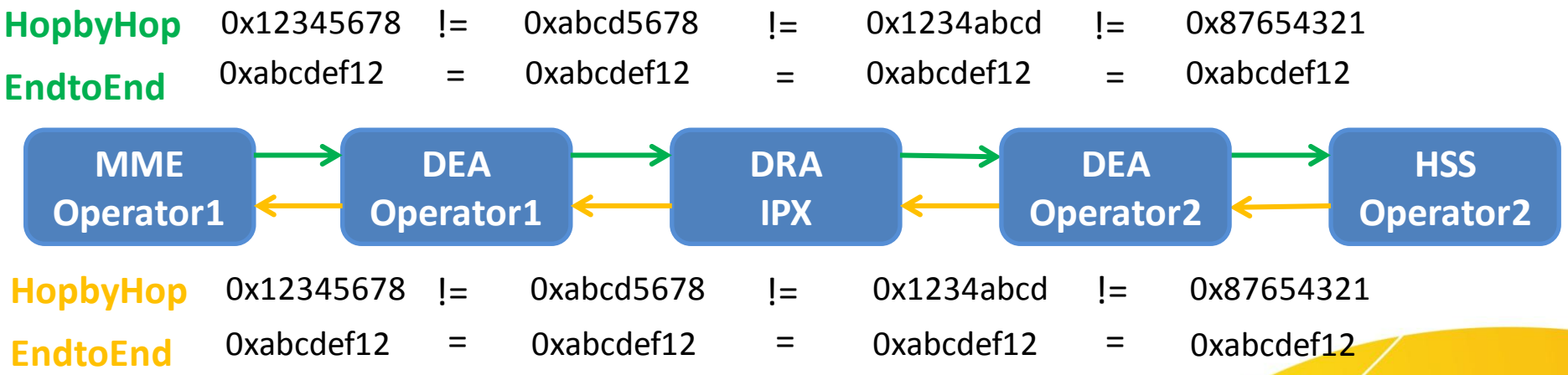
- Same protections for Diameter SRR (SRISM) ?

S6a - Denial of Service

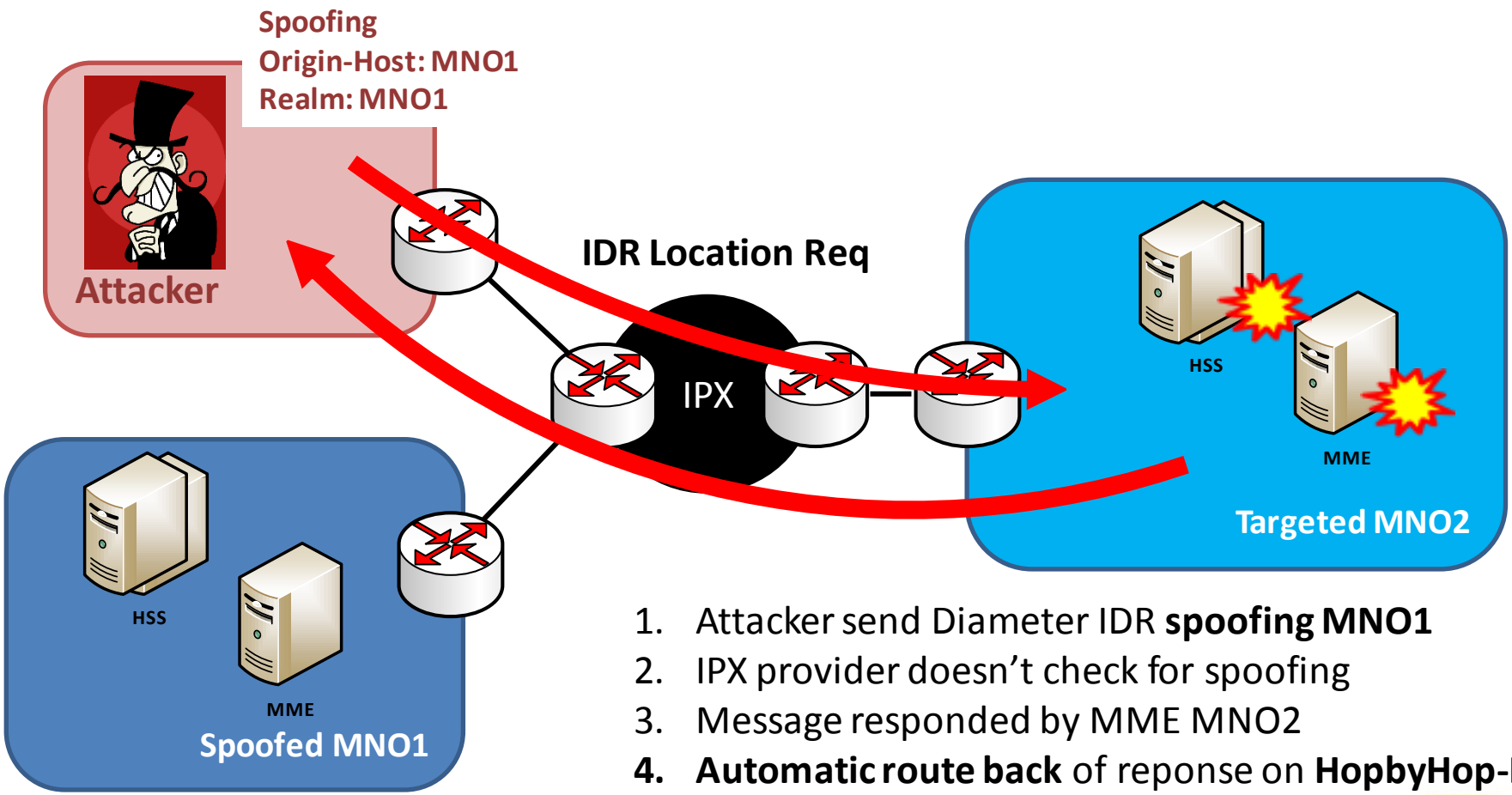
- S6a RSR – Reset Request
  - Sending RSR to MMEs after a HSS reboot/outage
  - MME is sending back information about requested subscribers
  - Signalisation DoS of the entire network by overloading HSS
- S6a CLR – Cancel Location Request
  - Need to know IMSI & MME-Host
  - Instant DoS - Remove the subscriber from the MME
- S6a ULR – Update Location Request
  - Need to know IMSI & HSS-Host
  - Instant DoS – Subscriber relocation on fake MME
- S6a PUR
  - Need to know IMSI & MME/SGSN Host
  - Instant DoS – Subscriber MME reference removed from HSS

Routing on the diameter network

- **Hop-by-Hop Id**: Unique between two routing peers (DEA/DRA), allows matching between request and response
- **End-to-End Id**: Unique on the complete packet path. Used to detect duplicates.
- **Request** routed on Destination Host & Realm OR IMSI (AIR)
- **Response** routed back with HopbyHop & DEA/DRA interface



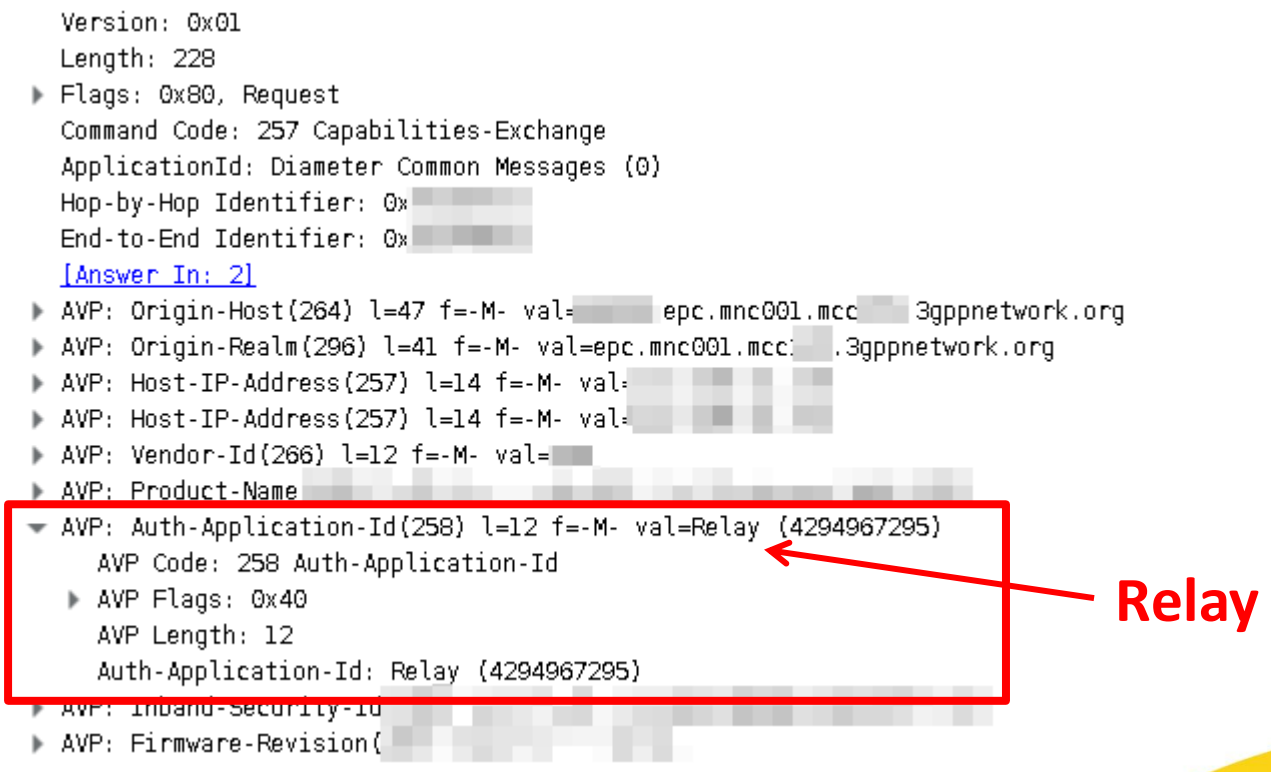
Diameter as spoofing friendly protocol



1. Attacker send Diameter IDR **spoofing MNO1**
2. IPX provider doesn't check for spoofing
3. Message responded by MME MNO2
4. **Automatic route back** of reponse on **HopbyHop-Id**
5. Spoofed packet returns to the attacker with subscriber location data

Basic mistakes on MNO DEA

- Auth-Application-Id as « Relay » will route packets
- No filtering, just route and forward.



Avoiding the unwanted

- In CER negociation be explicit in the Application-ID
- Avoid messages from any other application to be accepted

```
Version: 0x01
Length: 176
▸ Flags: 0x80, Request
Command Code: 257 Capabilities-Exchange
ApplicationId: Diameter Common Messages (0)
Hop-by-Hop Identifier: 0x
End-to-End Identifier: 0x
[Answer In: 10480]
▸ AVP: Product-Name(269) l=11 f=--- val
▸ AVP: Origin-State-Id(278) l=12 f=-M- val=0
▸ AVP: Host-IP-Address(257) l=14 f=--- val=
▸ AVP: Vendor-Id(266) l=12 f=--- val=
▸ AVP: Supported-Vendor-Id(265) l=12 f=-M- val=
▾ AVP: Auth-Application-Id(258) l=12 f=-M- val=3GPP S6a/S6d (16777251)
    AVP Code: 258 Auth-Application-Id
  ▸ AVP Flags: 0x40
    AVP Length: 12
    Auth-Application-Id: 3GPP S6a/S6d (16777251)
▸ AVP: Vendor-Specific-Application-Id(260) l=32 f=---
▸ AVP: Origin-Realm(296) l=18 f=-M- val
▸ AVP: Origin-Host(264) l=25 f=-M- val=
```

S6a only

Avoiding the unwanted

- Check CER/CEA on each network elements / interface
- CER/CEA sent must have a specified Application-Id
  - No Relay or Proxy
- Not specified in CER/CEA Application-Id received should be dropped
- Reduce possible attack surface
- Avoid a lot of attacks possible with routing abuses
  - e.g. DEA configured as Relay
  - HSS misconfiguration

Detecting attacks on your network

- How to do it ?
- Do I have equipment to do monitoring it in my network ?
  - YES
- Security monitoring ?
  - YES, just need to explore possiblities !
- Should I go for new equipment ?
  - Use what you have in your network !!!
- Operators have plenty of solutions but they don’t know it

How to quick and easy

- Using pcap trace, easy for IPX
- Simple wireshark / tshark rules

Internal Spoofing: tshark -r input_file.pcap -Y '(diameter.Origin-Host matches ".epc.mncXXX.mccXXX.3gppnetwork.org$") && diameter.flags.request == 1 && ip.src != YOUR_DEA_IP_RANGE/24' -w spoofing_attacks.pcap

Non S6a: tshark -r input_file.pcap -Y '!(diameter.applicationId == 16777251) && diameter && !(diameter.cmd.code == 280)' -w non_S6a_packets.pcap

- Ok it's not real time, but gives good visibility !

Developping a Diameter IDS

- Started to develop it at POST Luxembourg / using Splunk for easy & quick stats and research
- Still in beta, but monitoring actively IPX interconnextion
- Will be published on github.com soon… ☺
- Already detecting interesting behaviors such as
  - IDR location attacks
  - IDR bruteforce on IMSIs
  - Non S6a messages received…
- But also helping to report network misconfigurations !

IDR location request + IMSI bruteforce

IMSI **Origin-Host** **Dest-Host** **Message Type : IDR**

90 % of IDR traffic with UNKNOWN_USER responses

Green: IDR Request
Orange: UNKNOWN USER
Yellow: VALID USER

SS7 vs Diameter security

Recap

Interface	Diameter message	Target	Attack type
S6a	ULR	HSS	Sub DoS
S6a	CLR	MME	Sub DoS
S6a	PUR	HSS	Sub DoS
S6a	RSR	MME	Network DoS
S6a	IDR	MME	Fraud (Profile Injection)
S6a	IDR	MME	Tracking
SLh	RIR	HSS	Tracking / Info gath
SLg	PLR	MME	Tracking
Sh	UDR	HSS	Tracking
S6c	SRR	HSS	Info gathering
S9 (S9/Rx)	CCR / RAR	PCRF	Fraud ?
S6m	SIR	HSS	Info gathering ?

Don’t forget IR.21, IPX DNS, AIR, Route Record for info gathering

Recommendations

- Do NOT set DEA as relay, be explicit in declared applications
- Set explicit Application-Id on CER for all equipments
- Do NOT connect everything to DEA, prefer direct connectivity
  - HSS / MME with GMLC
  - PCEF, OCS, OFCS with PCRF
- Filter for IDR with location request targetting your subscribers
- Filter for spoofing of internal Host/Realm on DEA
- Drop any diameter messages that should not come from international
- There are remediations for spoofing, IPX providers will need to do their job
- Monitoring is the way ☺

Thanks

- POST Luxembourg
  - Core Mobile teams & CSE CyberSecurity team
- Pierre-Olivier Vauboin
- Laurent Ghigonis
- TROOPERS Organizers for such great event ☺

Questions ?

Thank you

alexandre.deoliveira@post.lu