Attacking NextGen Roaming Networks

Hendrik Schmidt hschmidt@ernw.de @hendrks_
Daniel Mende dmende@ernw.de
Enno Rey erey@ernw.de @enno_insinuator

Agenda

- Technical overview
- Attacks, and a tool
- Conclusions

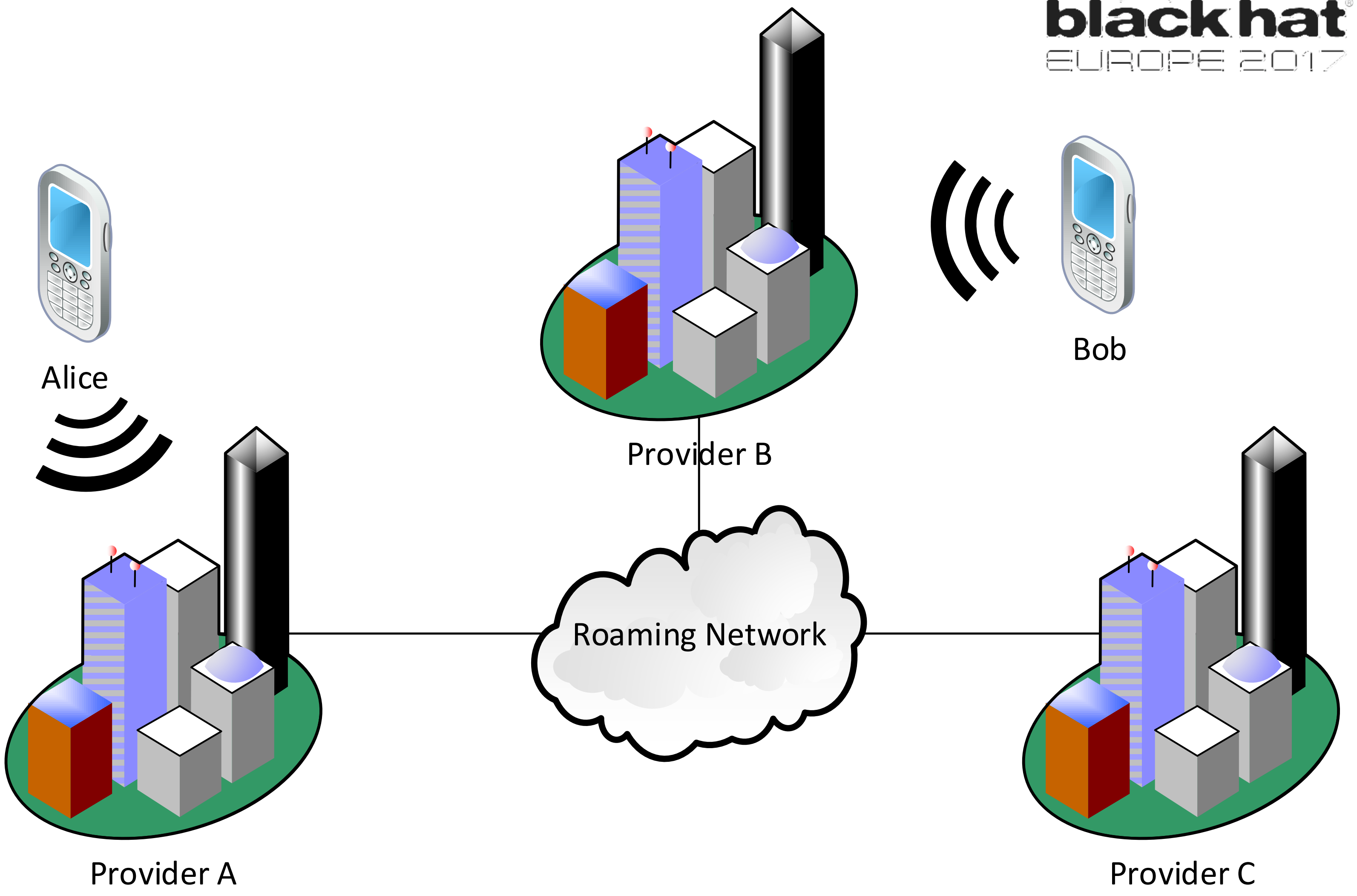
What is SS7?

- Standardized by ITU-T in 1981.
- Used for transporting signaling information between providers, including:
  - Authentication & encryption information
  - Call-setup & channel information
  - Call management / supplementary services
  - Messages

The Most Simple Situation:

Alice has a contract with Provider A

Bob has a contract with
Provider B

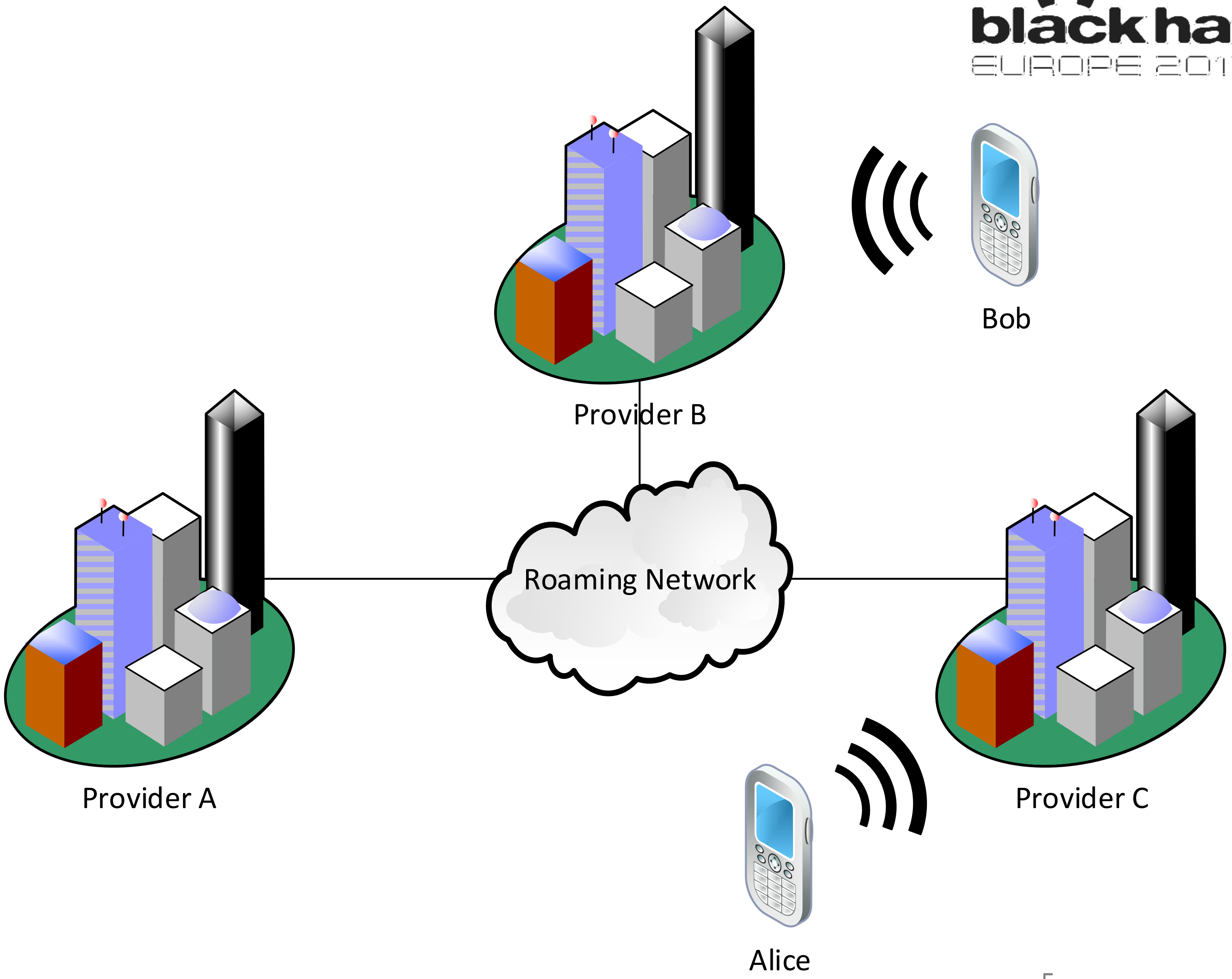


The roaming situation:

Alice has a contract with Provider A

Bob has a contract with Provider B

Alice is connected to Network of Provider C

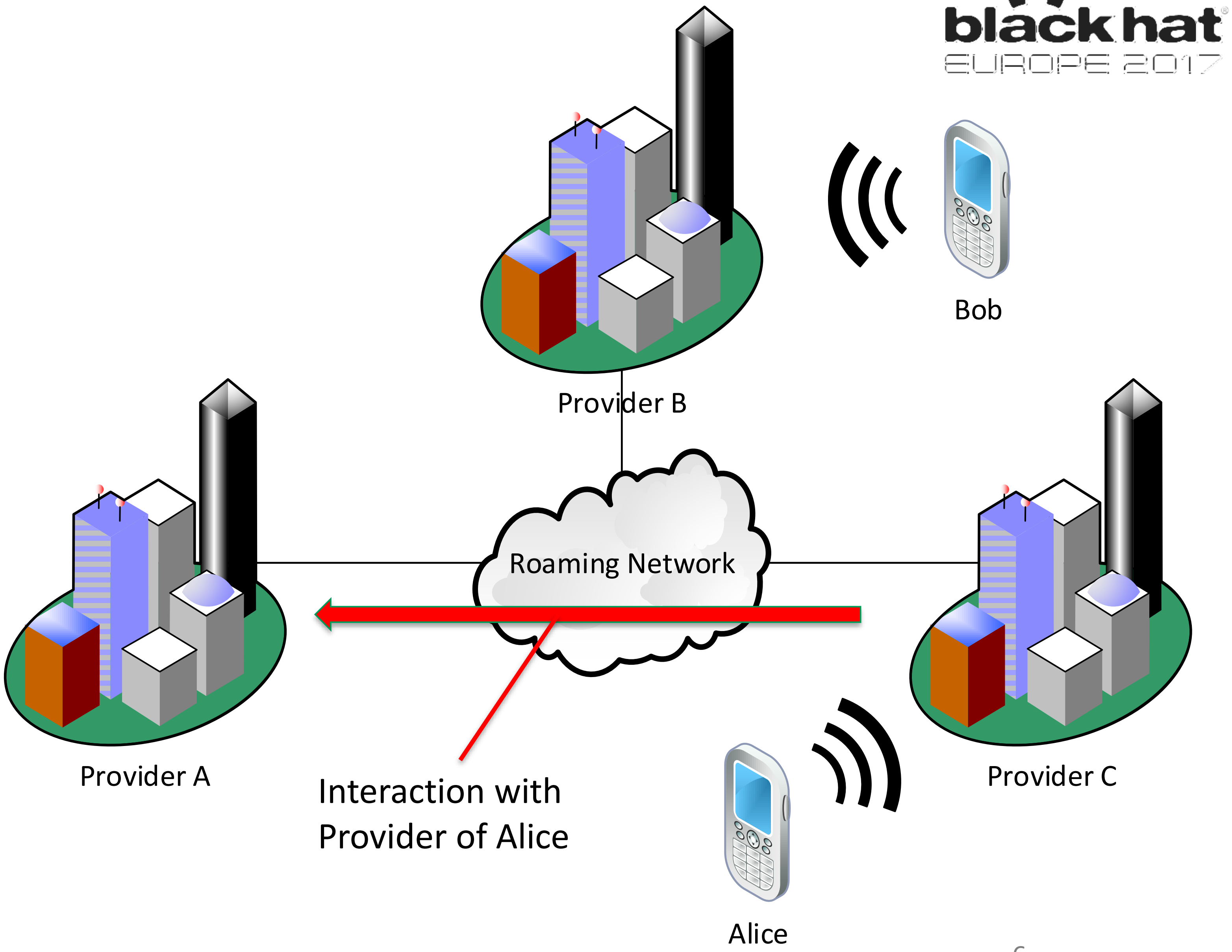


The roaming situation:

Alice has a contract with Provider A

Bob has a contract with Provider B

Alice is connected to Network of Provider C



Typical Roaming Interaction

- Retrieve authentication information
- Get encryption material
- Get routing / subscriber information
- Get and update location information of the subscriber

SS7 Weaknesses

- SS7 is built without authentication at all, as it is assumed to be used in a **trusted environment only.**

- As shown in the past at several occasions, this is not necessarily true…
  - https://berlin.ccc.de/~tobias/31c3-ss7-locate-track-manipulate.pdf
  - https://berlin.ccc.de/~tobias/25c3-locating-mobile-phones.pdf
  - https://events.ccc.de/camp/2015/Fahrplan/system/attachments/2649/original/CCCamp-SRLabs-Advanced_Interconnect_Attacks.v1.pdf

Vulnerability Classification

- SANS classified these attacks into three categories
  - *Category 1: Messages that have no legitimate use case for external exposures*
  - *Category 2: Messages that have no legitimate need to be exposed externally for the operator's own subscribers, but can be received for other operator's roaming subscribers.*
  - *Category 3: Messages that have legitimate need for external exposure*

Source: SANS Institute - The Fall of SS7 How Can the Critical Security Controls Help?

SS7-MAP Message Classification

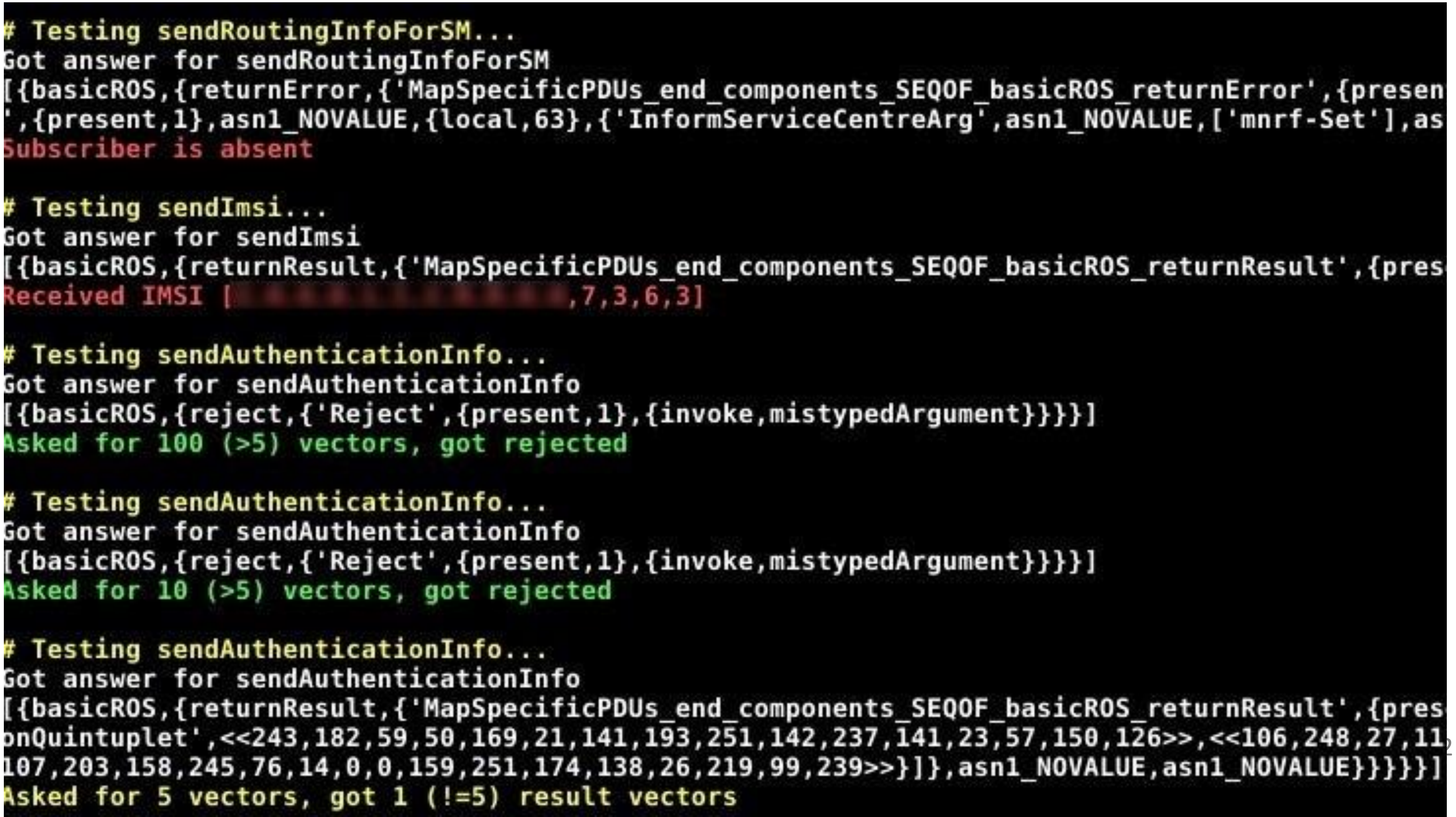
by SANS

	Attack	Category
	Interception	Category 1
Message	Interception	Category 3
sendIdentification!(SI)	Interception (Outgoing)	Category 2
registerSS – eraseSS	Interception (Incoming) Fraud	Category 3
updateLocation	Interception (SMS) Denial of Service	Category 3
processUnstructuredSS	Fraud	Category 3
insertSubscriberData	Denial of Service	Category 2
deletedSubscriberData	Denial of Service	Category 2
cancelLocation	Denial of Service	Category 3
anyTimeInterrogation	Tracking	Category 1
anyTImeModification	Tracking	Category 1
provideSubscriberInformation	Tracking	Category 2
provideSubscriberLocation	Tracking	Category 1
sendRoutingInformation (USM, ULCS)	Facilitates multiple attacks	Category 3

Tool

- ss7MAPer
  - https://github.com/ernw/ss7MAPer
  - https://insinuator.net/2016/02/ss7maper-a-ss7-pen-testing-toolkit/

- Implements probes for the different kinds of known attacks.
- Useful to check if $TELCO is vulnerable to attacks via SS7.
- Needs legitimate SS7 uplink.



```
# Testing sendRoutingInfoForSM...
Got answer for sendRoutingInfoForSM
[{basicROS,{returnError,{'MapSpecificPDUs_end_components_SEQOF_basicROS_returnError',{presen
',{present,1},asn1_NOVALUE,{local,63},{'InformServiceCentreArg',asn1_NOVALUE,['mnrf-Set'],as
Subscriber is absent

# Testing sendImsi...
Got answer for sendImsi
[{basicROS,{returnResult,{'MapSpecificPDUs_end_components_SEQOF_basicROS_returnResult',{pres
Received IMSI [[redacted],7,3,6,3]

# Testing sendAuthenticationInfo...
Got answer for sendAuthenticationInfo
[{basicROS,{reject,{'Reject',{present,1},{invoke,mistypedArgument}}}}]
Asked for 100 (>5) vectors, got rejected

# Testing sendAuthenticationInfo...
Got answer for sendAuthenticationInfo
[{basicROS,{reject,{'Reject',{present,1},{invoke,mistypedArgument}}}}]
Asked for 10 (>5) vectors, got rejected

# Testing sendAuthenticationInfo...
Got answer for sendAuthenticationInfo
[{basicROS,{returnResult,{'MapSpecificPDUs_end_components_SEQOF_basicROS_returnResult',{pres
onQuintuplet',<<243,182,59,50,169,21,141,193,251,142,237,141,23,57,150,126>>,<<106,248,27,11
107,203,158,245,76,14,0,0,159,251,174,138,26,219,99,239>>}]},asn1_NOVALUE,asn1_NOVALUE}}}}}]
Asked for 5 vectors, got 1 (!=5) result vectors
```

Roaming in 4G/LTE Networks

- Split up in Packet Data and VoIP traffic
  - All traffic in LTE is IP.
  - Diameter is mainly used as out-of-band control protocol.
  - This includes authentication purposes.

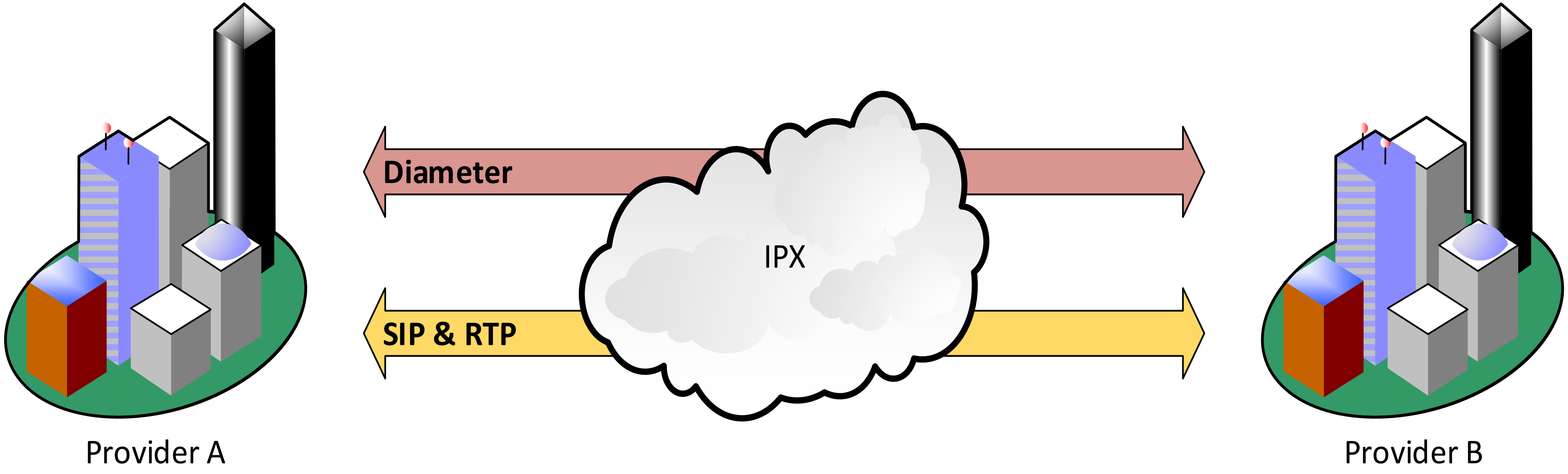
  - For VoLTE traffic there usually exists a dedicated APN ("ims").

Diameter Networks

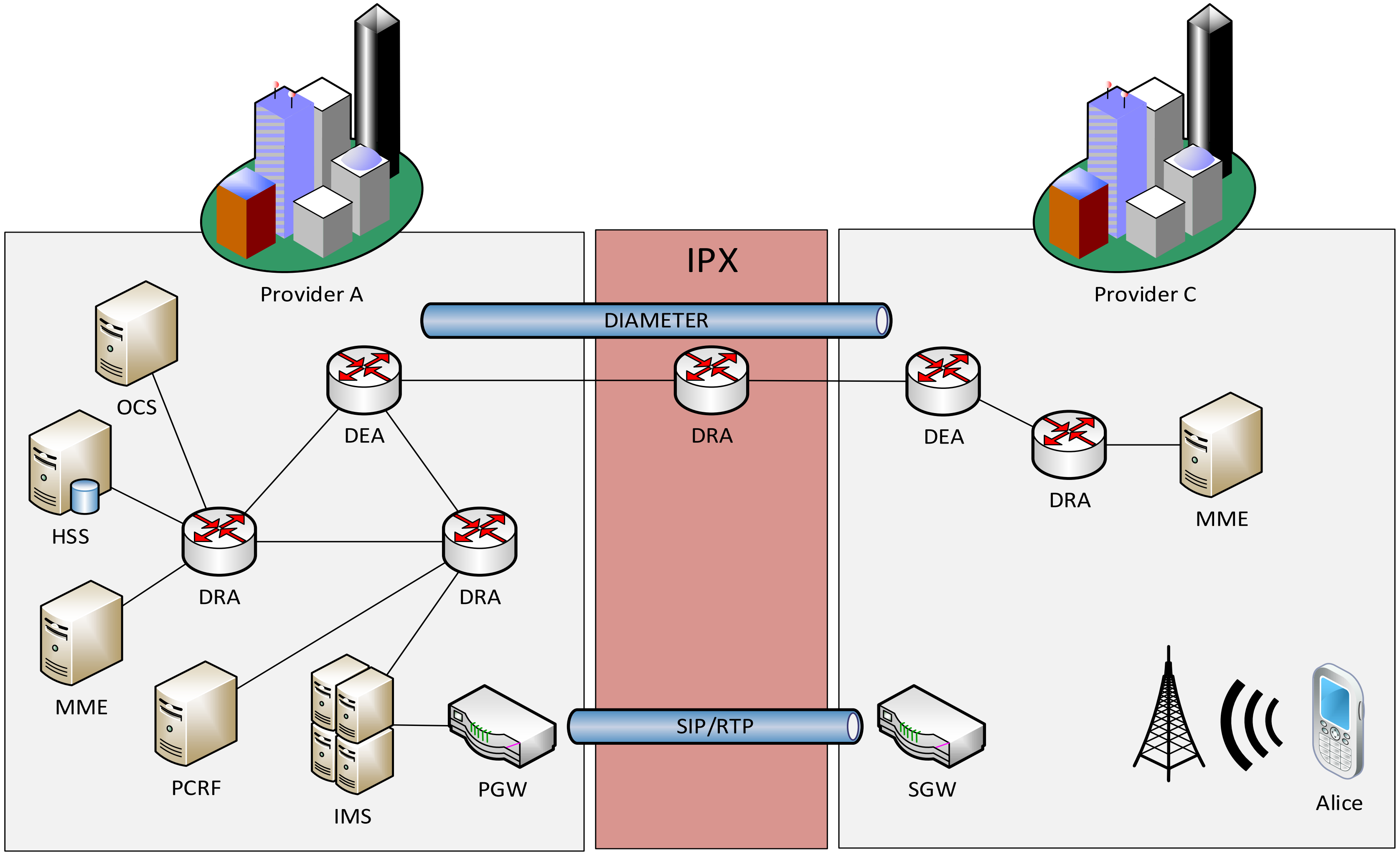
- Base Protocol is defined in RFC 6733.
- Enhanced by applications, standardized by 3GPP.

- IP Based Communication, on top of either TCP or SCTP (because yes, we are telco).
- Transporting Signaling Information, similar to SS7.

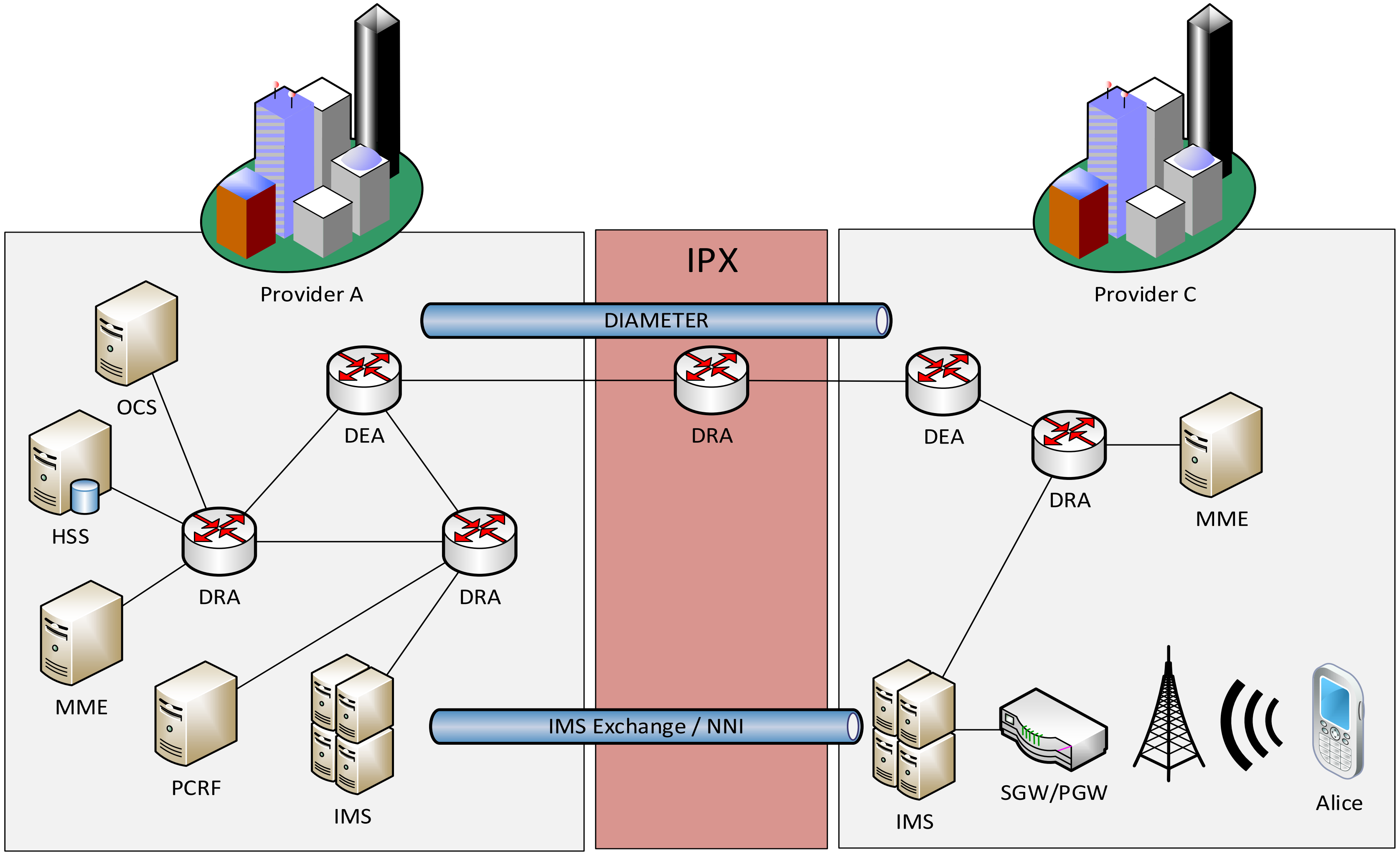
LTE Roaming



Method 1: Home Routed IMS

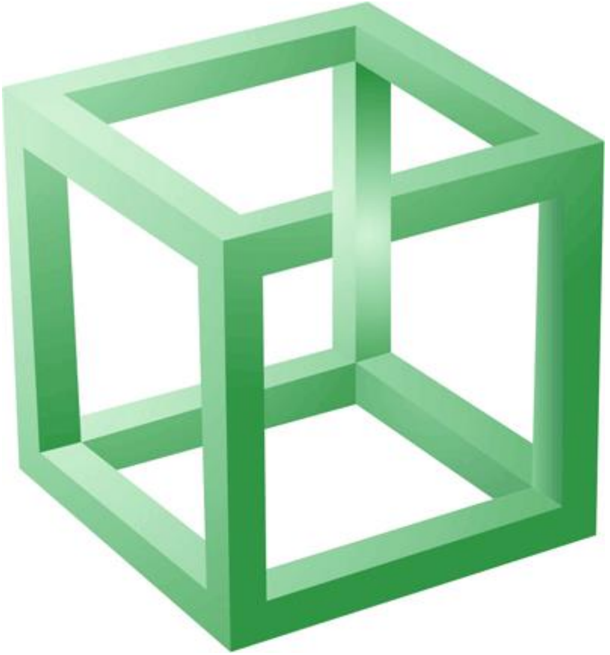


Method 2: Local Breakout



Some Diameter Interfaces

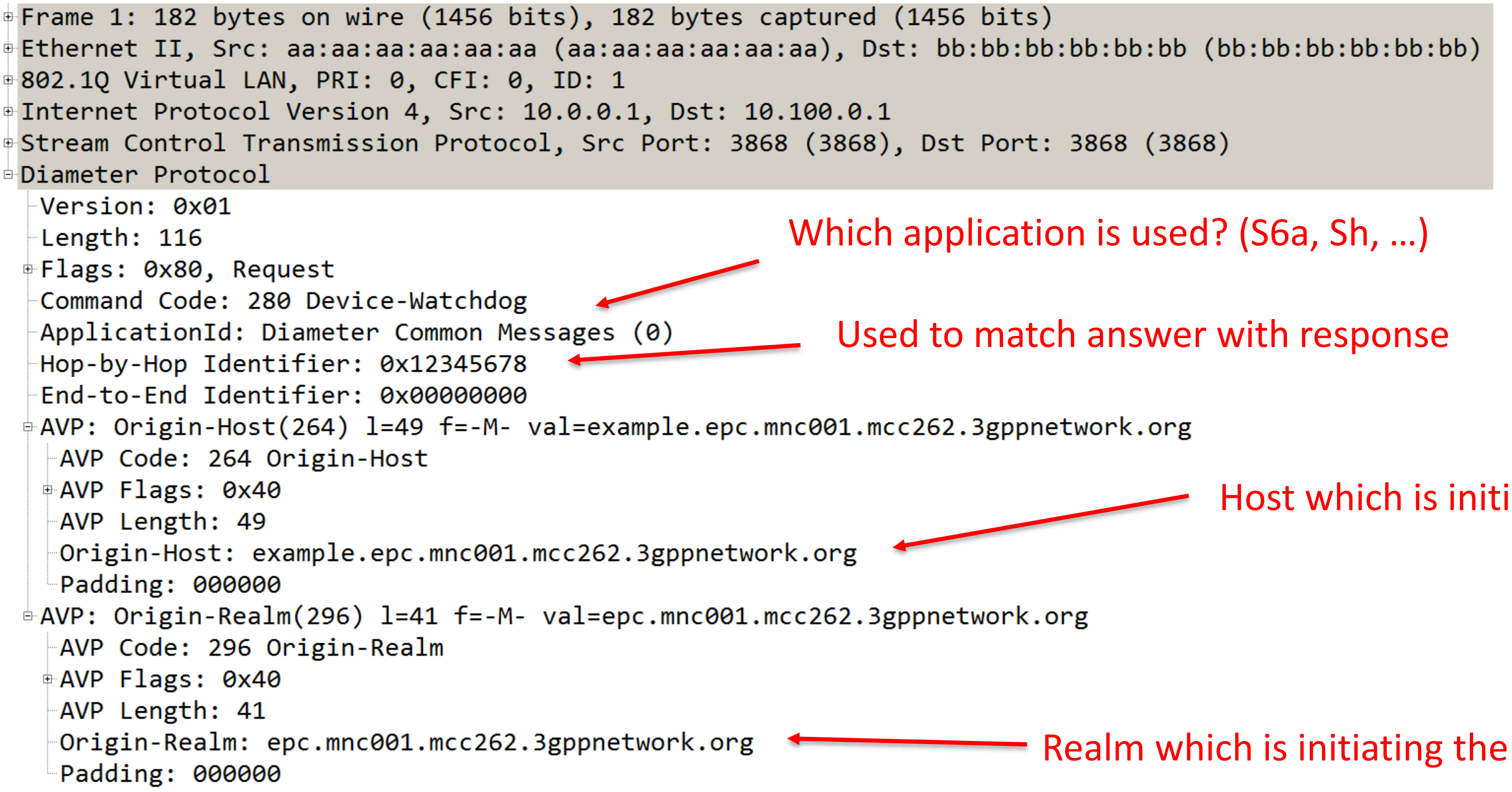
- S6a: MME <-> HSS (typical LTE Roaming)
- S6d: SGSN <-> HSS
- Cx: IMS (CSCF) <-> HSS
- Sh: IMS (AS) <-> HSS
- Zh: IMS (BSF) <-> HSS
- S9: H-PCRF <-> V-PCRF
- S13: MME <-> EIR
- and more …



Diameter – The Base Protocol

```
 0                   1                   2                   3
 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|    Version    |                 Message Length                |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
| Command Flags |                  Command Code                 |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                         Application-ID                        |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                      Hop-by-Hop Identifier                    |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                      End-to-End Identifier                    |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|  AVPs ...
+-+-+-+-+-+-+-+-+-+-+-+-+-
```

Source: RFC 6733



```
⊞Frame 1: 182 bytes on wire (1456 bits), 182 bytes captured (1456 bits)
⊞Ethernet II, Src: aa:aa:aa:aa:aa:aa (aa:aa:aa:aa:aa:aa), Dst: bb:bb:bb:bb:bb:bb (bb:bb:bb:bb:bb:bb)
⊞802.1Q Virtual LAN, PRI: 0, CFI: 0, ID: 1
⊞Internet Protocol Version 4, Src: 10.0.0.1, Dst: 10.100.0.1
⊞Stream Control Transmission Protocol, Src Port: 3868 (3868), Dst Port: 3868 (3868)
⊟Diameter Protocol
   Version: 0x01
   Length: 116
  ⊞Flags: 0x80, Request
   Command Code: 280 Device-Watchdog
   ApplicationId: Diameter Common Messages (0)
   Hop-by-Hop Identifier: 0x12345678
   End-to-End Identifier: 0x00000000
  ⊟AVP: Origin-Host(264) l=49 f=-M- val=example.epc.mnc001.mcc262.3gppnetwork.org
     AVP Code: 264 Origin-Host
    ⊞AVP Flags: 0x40
     AVP Length: 49
     Origin-Host: example.epc.mnc001.mcc262.3gppnetwork.org
     Padding: 000000
  ⊟AVP: Origin-Realm(296) l=41 f=-M- val=epc.mnc001.mcc262.3gppnetwork.org
     AVP Code: 296 Origin-Realm
    ⊞AVP Flags: 0x40
     AVP Length: 41
     Origin-Realm: epc.mnc001.mcc262.3gppnetwork.org
     Padding: 000000
```

Which application is used? (S6a, Sh, …)

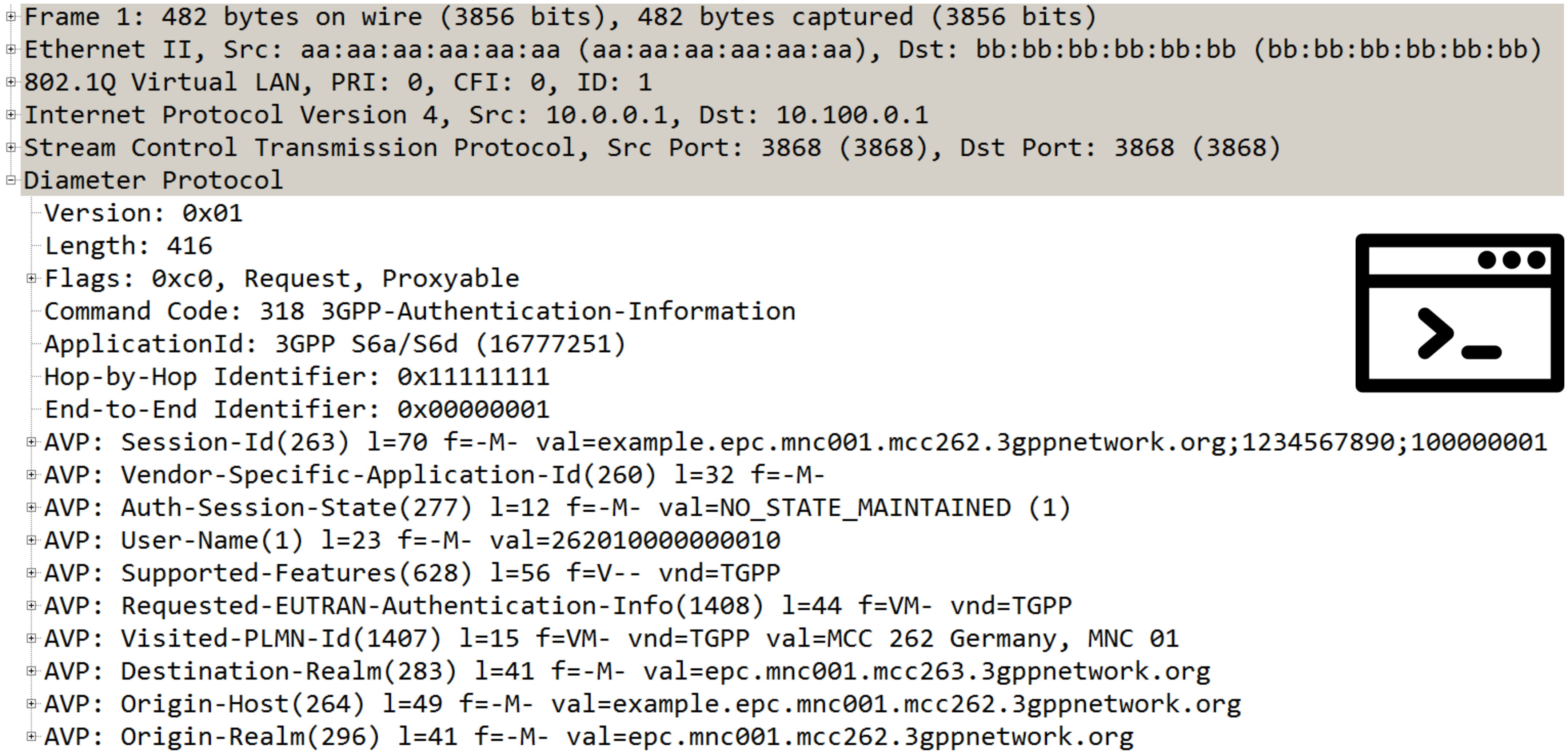
Used to match answer with response

Host which is initiating the request

Realm which is initiating the request

Diameter Messages (S6a)

- Authentication Information Request (AIR)
- Update Location Request (ULR)
- Notification Request (NOR)
- Profile Update Request (PUR)
- Insert Subscriber Data Request (IDR)
- Delete Subscriber Data Request (DSR)
- Cancel Location Request (CLR)
- Reset Request (RSR)



```
⊞ Frame 1: 482 bytes on wire (3856 bits), 482 bytes captured (3856 bits)
⊞ Ethernet II, Src: aa:aa:aa:aa:aa:aa (aa:aa:aa:aa:aa:aa), Dst: bb:bb:bb:bb:bb:bb (bb:bb:bb:bb:bb:bb)
⊞ 802.1Q Virtual LAN, PRI: 0, CFI: 0, ID: 1
⊞ Internet Protocol Version 4, Src: 10.0.0.1, Dst: 10.100.0.1
⊞ Stream Control Transmission Protocol, Src Port: 3868 (3868), Dst Port: 3868 (3868)
⊟ Diameter Protocol
    Version: 0x01
    Length: 416
  ⊞ Flags: 0xc0, Request, Proxyable
    Command Code: 318 3GPP-Authentication-Information
    ApplicationId: 3GPP S6a/S6d (16777251)
    Hop-by-Hop Identifier: 0x11111111
    End-to-End Identifier: 0x00000001
  ⊞ AVP: Session-Id(263) l=70 f=-M- val=example.epc.mnc001.mcc262.3gppnetwork.org;1234567890;100000001
  ⊞ AVP: Vendor-Specific-Application-Id(260) l=32 f=-M-
  ⊞ AVP: Auth-Session-State(277) l=12 f=-M- val=NO_STATE_MAINTAINED (1)
  ⊞ AVP: User-Name(1) l=23 f=-M- val=262010000000010
  ⊞ AVP: Supported-Features(628) l=56 f=V-- vnd=TGPP
  ⊞ AVP: Requested-EUTRAN-Authentication-Info(1408) l=44 f=VM- vnd=TGPP
  ⊞ AVP: Visited-PLMN-Id(1407) l=15 f=VM- vnd=TGPP val=MCC 262 Germany, MNC 01
  ⊞ AVP: Destination-Realm(283) l=41 f=-M- val=epc.mnc001.mcc263.3gppnetwork.org
  ⊞ AVP: Origin-Host(264) l=49 f=-M- val=example.epc.mnc001.mcc262.3gppnetwork.org
  ⊞ AVP: Origin-Realm(296) l=41 f=-M- val=epc.mnc001.mcc262.3gppnetwork.org
```

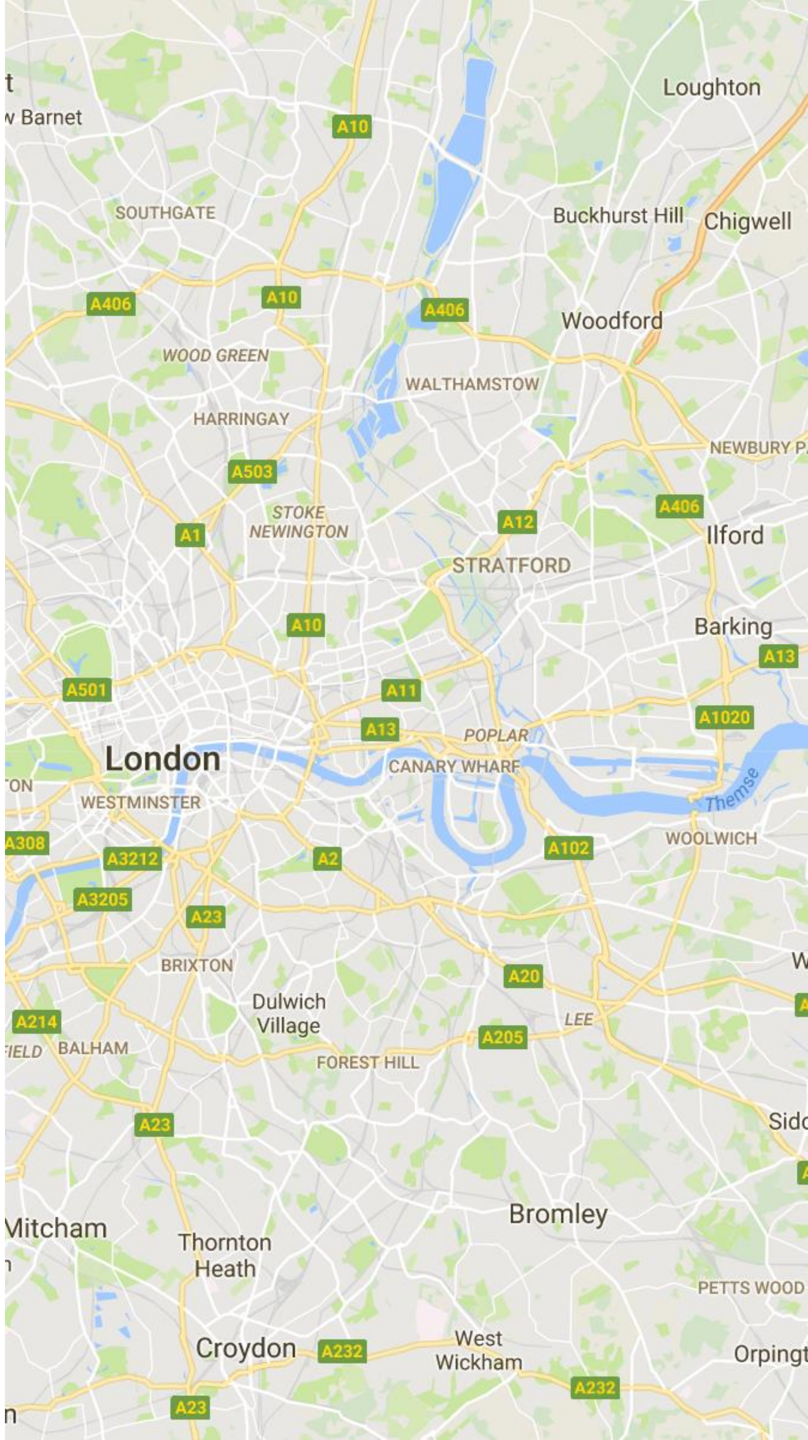
Let‘s do some Attacker Modeling

- We saw from SS7
  - Interception Attacks (Voice/Message)
  - Denial of Service
  - Fraud
  - Tracking

- Potentially also
  - Topology Information related stuff
  - Logical Errors
  - Impersonation
  - Implementation flaws

Tracking

- Yes!
- Using the IDR message, the attacker might be able to retrieve the Cell-ID of the victim.

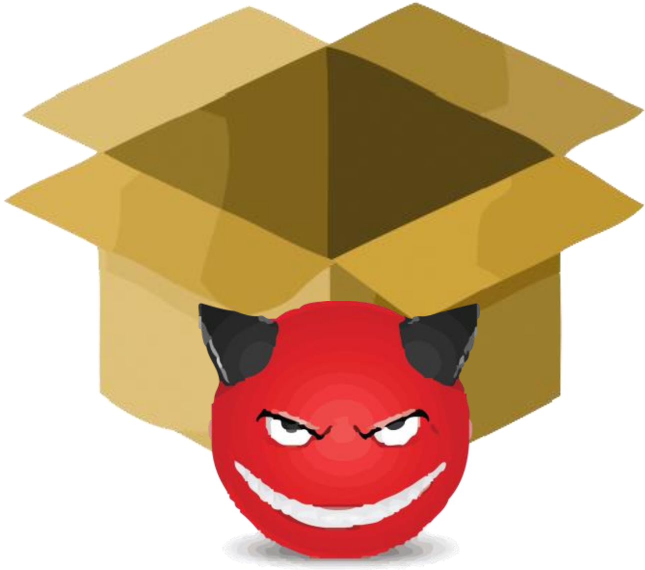


Interception Attacks

- Voice & Messages are not transmitted via Diameter.
- But: HSS holds Authentication and Encryption Material.
- User Profiles can include information as PDN-GW to be used.

That way an attacker is able to intercept a subscriber' s user data when being in a man-in-the-middle situation (e.g. via Fake-Basestation).

This also includes calls/messages!



Message/Call Interception

- Home-Routed IMS
  - Only the raw data can be intercepted. In case of additional encryption, there is less chance to get into the communication.
  - *From what we´ve seen: often VoLTE is not encrypted.*
- Local Breakout
  - Encryption keys will be retrieved via Diameter
  - Additionally, Policy and Charging information can be retrieved via S9 interface.

    → Fraud?
  - *Will most probably be used in some countries for lawful interception.*

Fraud

- In general to create charging records a couple of information from the HSS are considered (so called *Profiles*).

- Some of the information is provided by the MME or can be changed by the MME using Diameter.

- Potential messages: DSR & IDR.

Denial of Service

- Quite easy, changing responsible hosts / current UE's location and more

- Possible with: PUR, CLR, ULR, DSR

Limitations

- Usually most of the messages can only be sent by those *origin-hosts* which are currently responsible for an active UE.

- Anyhow, with the ULR message we can set ourselves to the responsible host.

Summary
(aka. let there be attacks)

Interfac e	Message	Target	Attack Type
S6a	AIR	HSS	Interception (Air)
S6a	ULR	HSS	DoS
S6a	CLR	MME	DoS
S6a	PUR	HSS	DoS
S6a	RSR	MME	DoS (Network)
S6a	IDR	MME	Tracking, Fraud, (Interception)
S6a	DSR	MME	DoS, Fraud

Topology & Topology Hiding

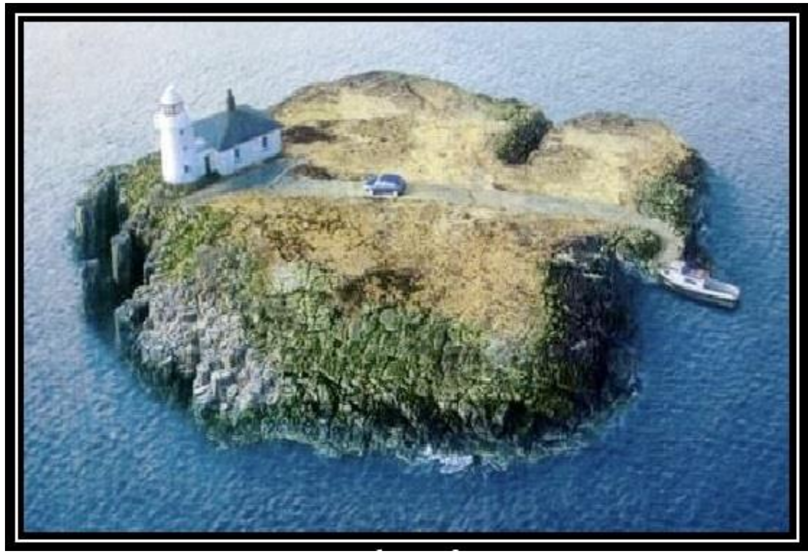
- ○ DRA routing is based on the application ID given in the Diameter messages.
- ○ IP addresses are only identifying the DRA hops.

- ○ Origin Host & Realm identifies the source
- ○ Destination Host & Realm identifies the target

→ HSS must be globally known (in case of AIR)

→ MME can be "secret" as it must only be known by the H-HSS.

→ HSS/MME usually follows a naming scheme.



Spoofing? Yes!

- Regarding to the roaming architecture
  - Only the Origin-Host is identifying the message source.

→ Origin-Hosts validation should be done at the entry point.

→ We never saw this correctly implemented as it is quite hard to deploy.

Cross-Checking of PLMNs and Identities

- A lot of messages only make sense if they are coming from a certain PLMN and are targeting a certain PLMN, e.g.
  - Provider A is asking Provider B for UE location
  - Provider B is asking Provider B for UE location
  - Provider C is asking Provider B for UE location (with Provider A as Home)

Tool!

- diameter_enum
  - Written in Python.
  - Build around libDiameter from https://github.com/thomasbhatia/pyprotosim
  - Will be released under BSD license.
  - Is able to send Diameter messages to a defined host (DRA).

Tool (cont.)

- Similar to ss7MAPer implements probe packets for (known working) attacks on Diameter roaming.
- Tries to implement all 3GPP Diameter messages and valid probes to check the targets diameter routing/firewall configuration.
- Diameter Application scanner to check which applications are available on a target system. (e.g. 3GPP Cx, 3GPP Sh, 3GPP Re, etc.)

Tool (cont.)

- Can be downloaded from https://c0decafe.de/tools/diameter_enum-v0.1.tar.bz2

- Will also be on github soon!

diameter_enum config file

```
[DEFAULT]
origin-host: vanir
origin-realm: vanir
destination-host: fd.ernw.net
destination-realm: fd.ernw.net
host-ip-address: 10.11.12.1
vendor-id: 0
product-name: denum
inband-security-id: 0

mnc: 001
mcc: 001
imsi: 0010012345678
plmnid: 12f345
msisdn: 12345678
imei: 9876543210
```

LIVE DEMO!

- Unfortunately I can't show the real stuff, as we don't have a link to IPX here)-:

Penetration Testing of Interconnect Technologies

- A standard has just been released by GSMA, called ”Guidelines for Independent Remote Security Testing“
  - Interconnect Security Testing Types
  - Responsibilities of Testers
- Mainly focusing on SS7 tests, but also includes Diameter testing requirements.
- https://www.gsma.com/aboutus/wp-content/uploads/2017/11/FS.26_v1.0.pdf

What’s in There / Recommendations

- Spoofing of Network Operator (SNO)
- Configure specific DNO/ONO/IMSI
- DoS Testing
- Separate between high-risk & low-risk messages
- Logging & Traceability
- Control of used messages
  - Messages that Extract Information
  - State-Changing or Charge-Triggering Messages
  - High-Risk Messages
- Limit of Test-Frequency
- Detection of potential Disruption

Controls from Our Perspective

- Understand Diameter applications & related message types, and their security implications.
- Establish visibility!
- Monitor for known attacks.
- Think about ways to filter/restrict interactions
  - E.g. drop messages with “internal” origin-hosts when arriving inbound at IPX.

Summary & Outlook

- SS7 ”vulnerabilities“ continue to exist in Diameter.
- Diameter is getting more and more important.

- diameter_enum gives a framework to start security testing of Diameter interfaces.
  - Some initial test cases are already included.
  - We’re working on more messages. And fuzzing :-)

There's never enough time...

THANK YOU...

...for yours!

@Enno_Insinuator

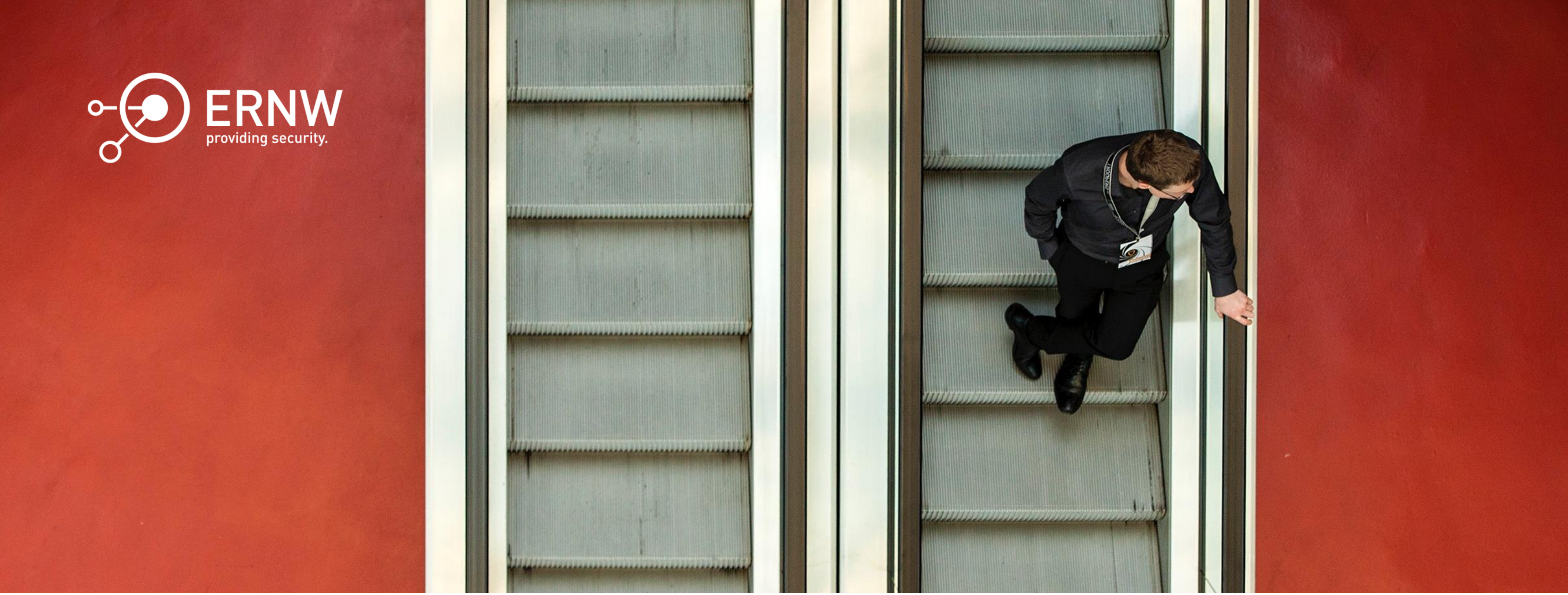
erey@ernw.de

ernw.de

insinuator.net

Slides available soon.

ERNW
providing security.



Thank you!

Any questions?

ERNW
providing security.

Sources

As indicated on slides.

Image Source:

- Icons made by Freepik from www.flaticon.com