



Detach me not

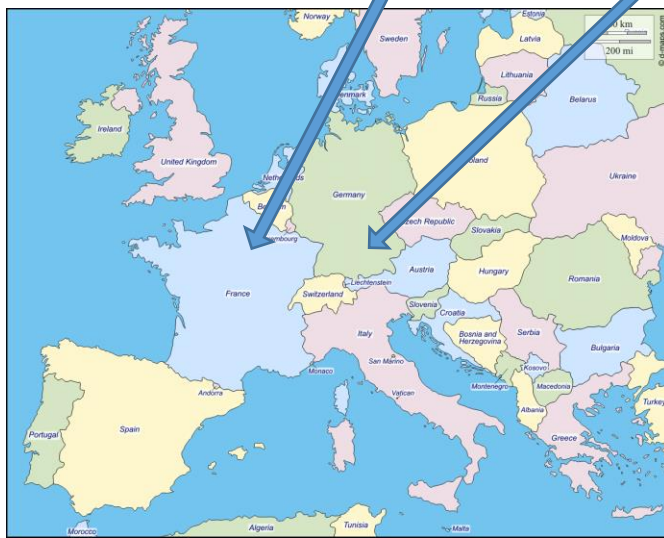
DoS attacks against 4G cellular users worldwide from your desk

Silke Holtmanns	Nokia Bell Labs
Bhanu Kotte	Nokia Bell Labs
Siddharth Rao	Aalto University



Blackhat Staff
AT&T, Verizon, T-Mobile, Sprint..

Blackhat Attendees
Orange, DT, Vodafone, ePlus,...



We are here
connected to Vodafone, O2, Orange, T-Mobile, 3

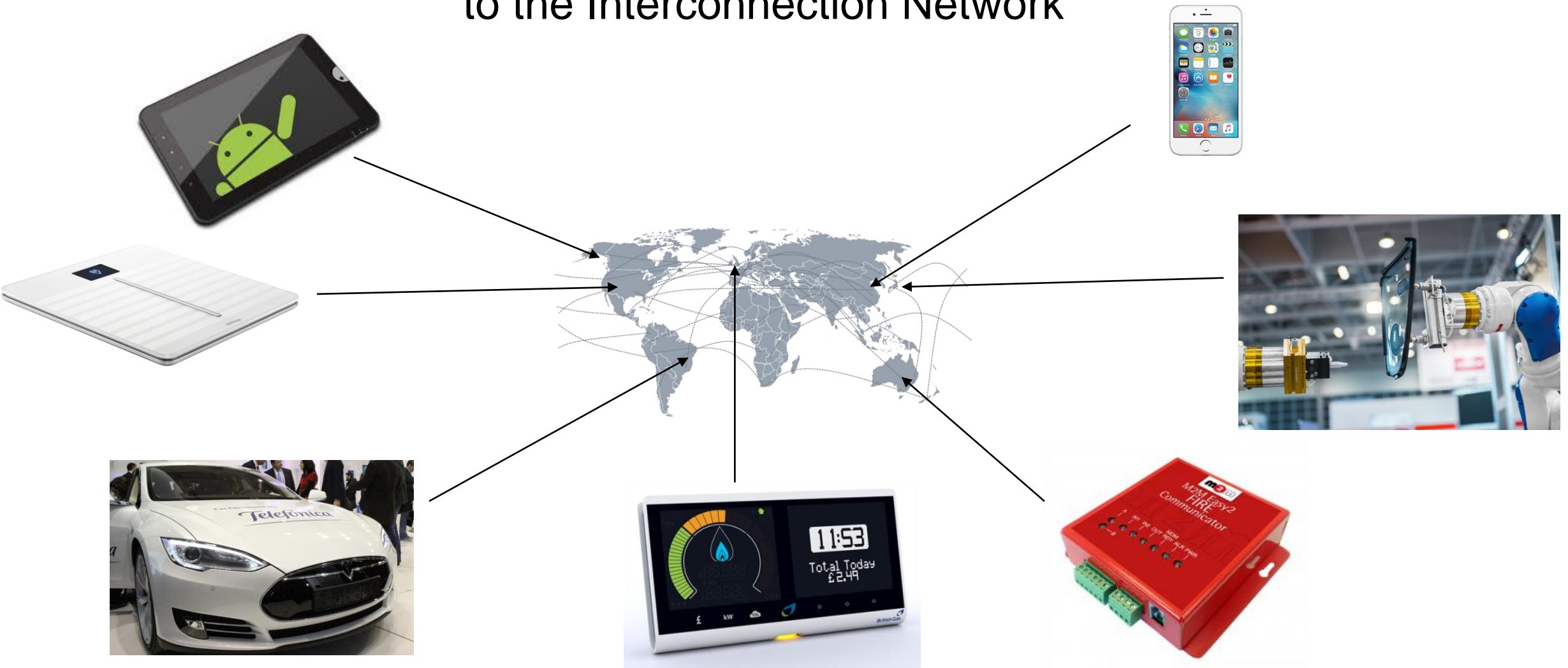


My home mobile network operator
Colleagues & Family
Elisa, TeliaSonera, DNA

Roaming Network – Interconnect IPX



We are all connected to the Interconnection Network



History – To Understand the Problem

- Established more than 35 years ago between a few state owned operators
- Build on trust (closed private network)
- No inbuilt security (in particular, no source authentication)
- SS7 protocol was constantly extended for new services and features
- New service providers connect all the time e.g. IPX roaming hubs, Application to user SMS, etc
- Now moving towards LTE / Diameter based protocols



Closed & Private Network?

The Intercept_

OPERATION SOCIALIST

The Inside Story of How British Spies Hacked Belgium's Largest Telco



Personal

Business

Login

Shop

My3

Help

3Plus

3Money

Search

Home. Explore. About three. [Wholesale Interconnect](#)

- > Why Three?
- > About Three
- > Media Centre

Wholesale Interconnect (Three Ireland (Hutchison) Limited).

Below you can see what I can provide. Contact information at the bottom page.

SERVICES

CELL PHONE REPORTS

A cell phone report contains network information, such as MCC, MNC, IMSI, TMSI and location information(real-time)
- You can request more, like the encryption keys of the current session.

3 LOOKUPS: \$150

CELL PHONE INTERCEPTION

This service is simple and easy, I only require you to provide the target MSISDN(number), along with a destination number that I can redirect the incoming/outcoming requests to.

CALLS: \$100

SMS MESSAGES: \$200

SPOOFED SMS MESSAGING/CALLING

You will be provided with a web panel and an access code, then you can send SMS messages and make calls without any restrictions, just by clicking a button.

1 MONTH: \$20

SS7 API

With this, you can do everything I can, just by logging into an SSH server I have open. API Access includes the following: Tracking, subscription modifying, jamming, intercepting, SMS/Call Spoofing.

1 MONTH: \$250

3 MONTHS: \$500

12 MONTH: \$1250

ZXR10 xGW-16, ZTE ZXR10 Software Version: ZXUN xGW(GGSN)V4.10.13(1.0.0)

SHODAN

221.177.247.252

China Mobile

Added on 2016-09-22 15:34:36 GMT

China

Details



One of the prime targets monitored under the AURORAGOLD program is the London-headquartered trade group, [the GSM Association](#), or the GSMA, which represents the interests of more than 800 major cellphone, software, and internet companies from 220 countries.

German Bundeswehr's Secret Afghan Phone Hacking Operation Rumbled

MIDDLE EAST 21:21 24.09.2016 (updated 22:22 24.09.2016) [Get short URL](#)

1 476 0 0

How to get in?

Renting a Service

Hacking

Having Power



Bribing an Employee

Become an Operator

Convincing

Current Status of IPX Security

- Most commonly used protocol for interconnection is still **SS7-MAP** (message application part)
 - Often intermediate nodes involved
 - Often without any form of transport security
 - > **No IPSec, no TLS / DTLS, no MAPSec**
 - No source authentication, no integrity, no confidentiality
-
- For the legacy protocol, SS7 many attacks are known, some of them landed on TV (CBS 60 minutes)



SS7 Incidents Known

- Location Tracking
- Eavesdropping
- Fraud
- Denial of Service user & network
- Credential theft
- Data session hijacking
- Unblocking stolen phone
- SMS interception
- One time password theft and account takeover for Telegram, Facebook, Whatsapp

Request: 1 Cell - GSM

```

1 {
2   "token": "101472503351",
3   "radio": "gsm",
4   "mcc": "262",
5   "mnc": "01",
6   "cells": [
7     {
8       "lac": "123",
9       "cid": "1650204",
10      "address": 1
11    }
12  ]
13 }

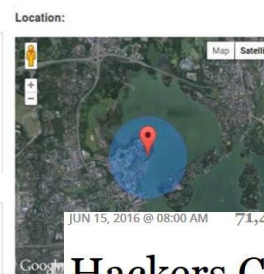
```

Response:

```

1 {
2   "status": "ok",
3   "balance": 44,
4   "lat": 60,
5   "lon": 24,
6   "accuracy": 959,
7   "address": "Unnamed Road, 02150 Espo
8 }

```



Bulgarian company - Global Innovator in Wiretapping

"Circles Bulgaria" has listed itself as a virtual operator to intercept encryption keys from the SS7 inter-operator network

December 15, 2015

Биволь

Hackers Can Steal Your Facebook Account With Just A Phone Number



Thomas Fox-Brewster FORRESTER STAFF

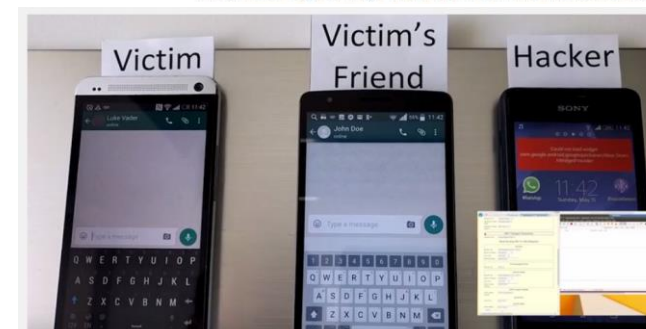
WIRELESS

Telenor mobile network hit by international signal

Monday 22 February 2016 | 16:03 CET | News

Telenor said it suffered a major mobile network outage for several hours on 19 February due to incorrect signalling data from an international operator.

SOCIETY



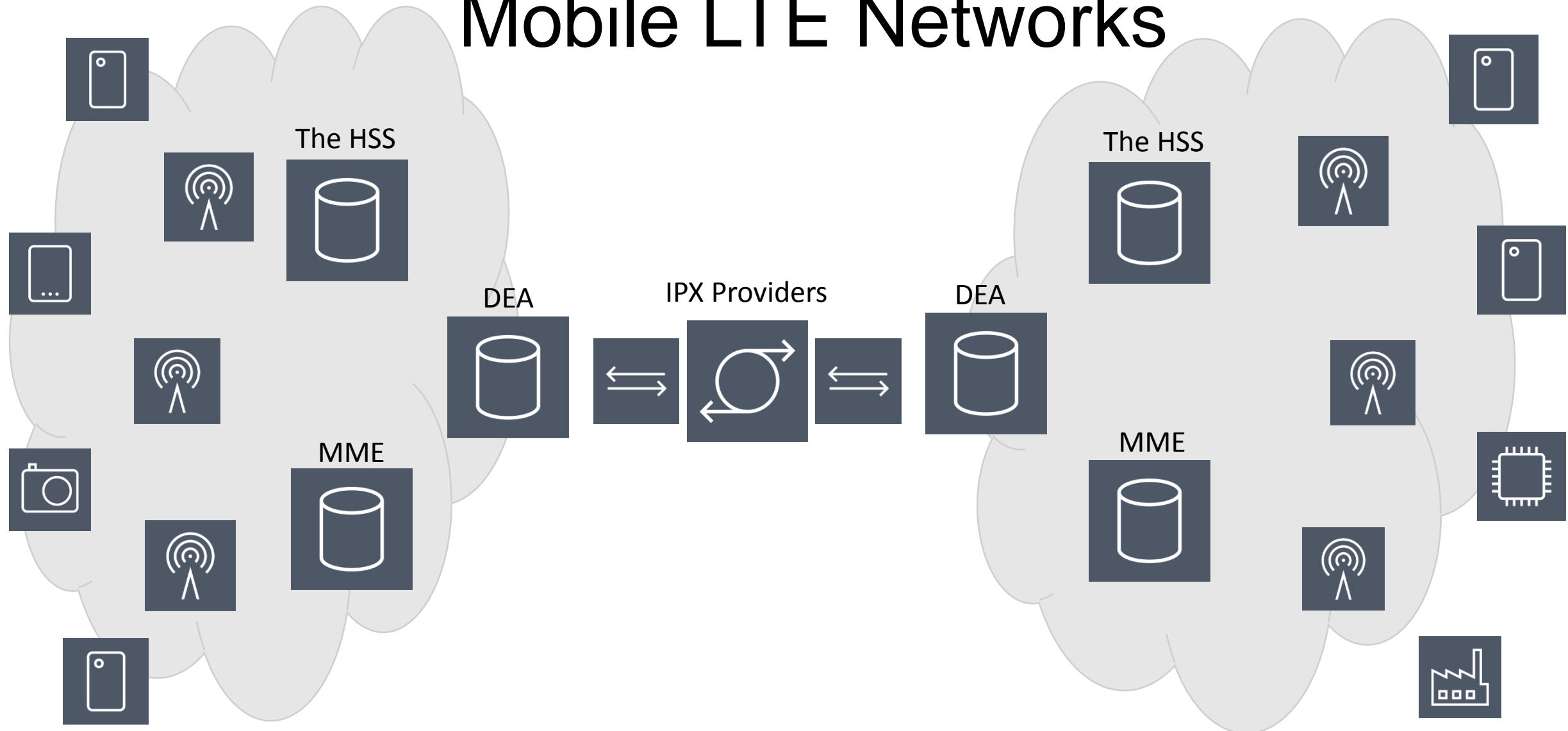
Media: officials fired for using WhatsApp, Viber and Telegram

00:33 30/01/2016 - updated 00:00:00 31/01

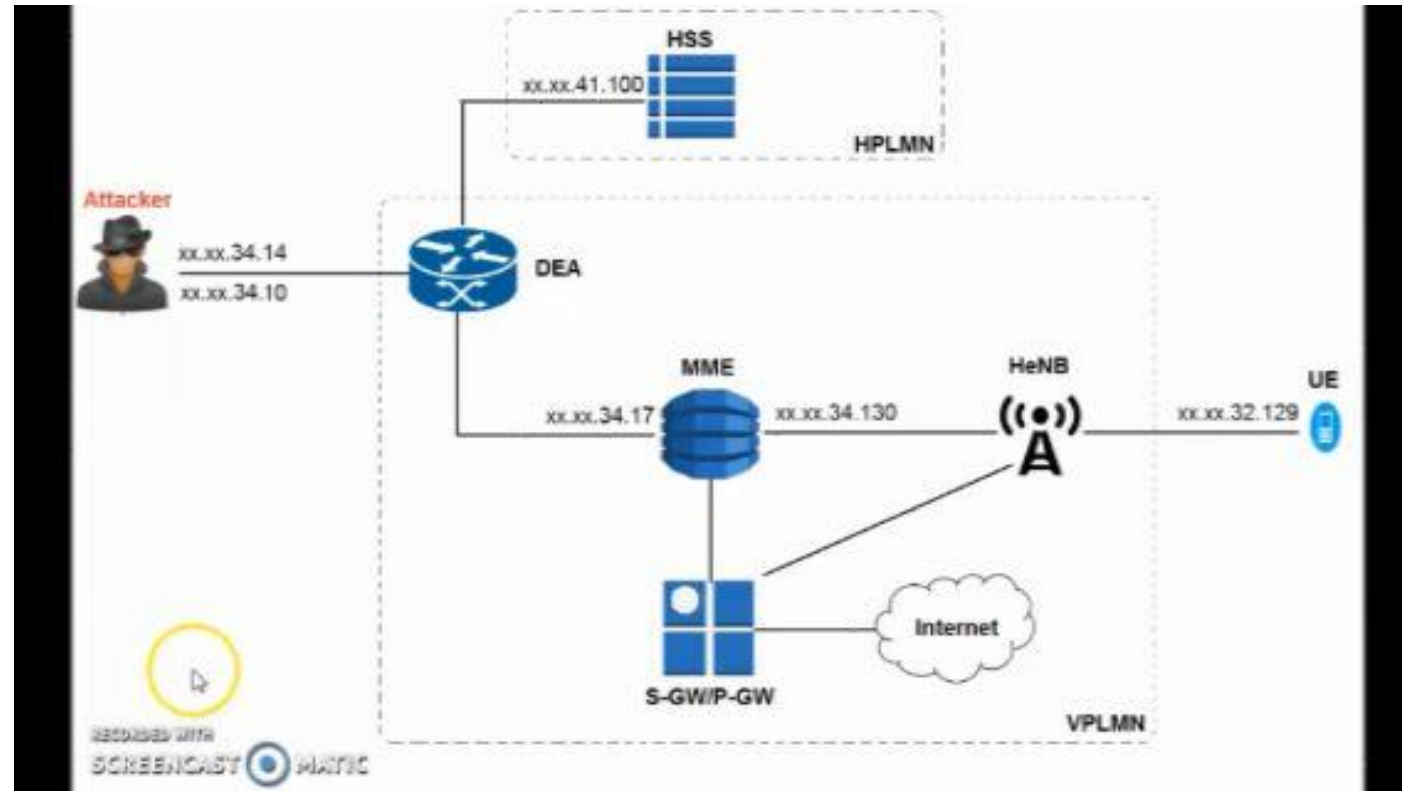
All will be better with LTE and Diameter.....

All will be ~~better~~ different with
LTE and Diameter.....

Mobile LTE Networks

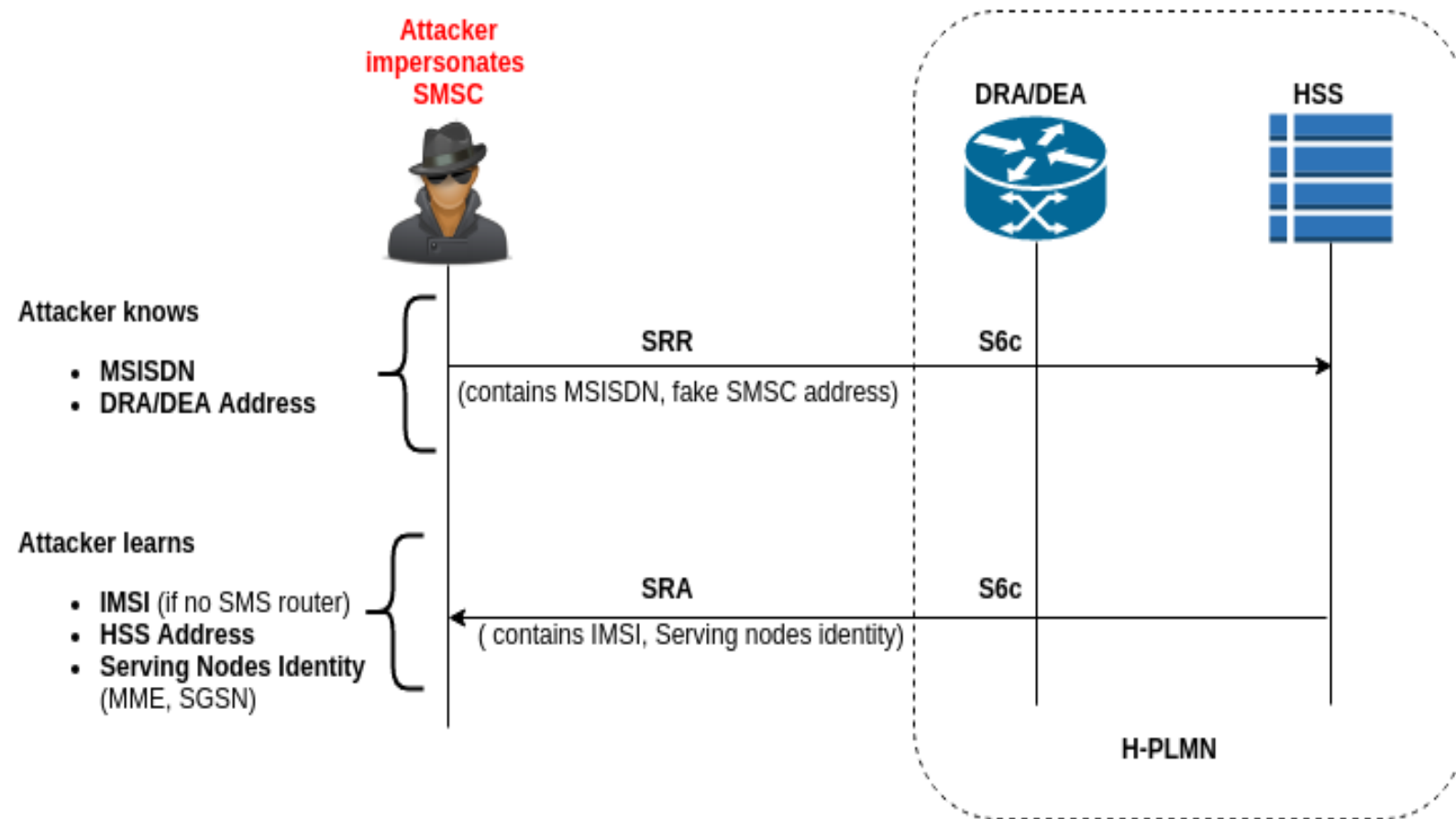


Network Setup for DoS Testing – Video



IMSI retrieval using SRR

- Send Routing Info for SM Request (SRR)
- Sent by SMSC to the HSS
 - Retrieves subscriber's IMSI and identity of the serving MME
 - Routing a short message to the recipient

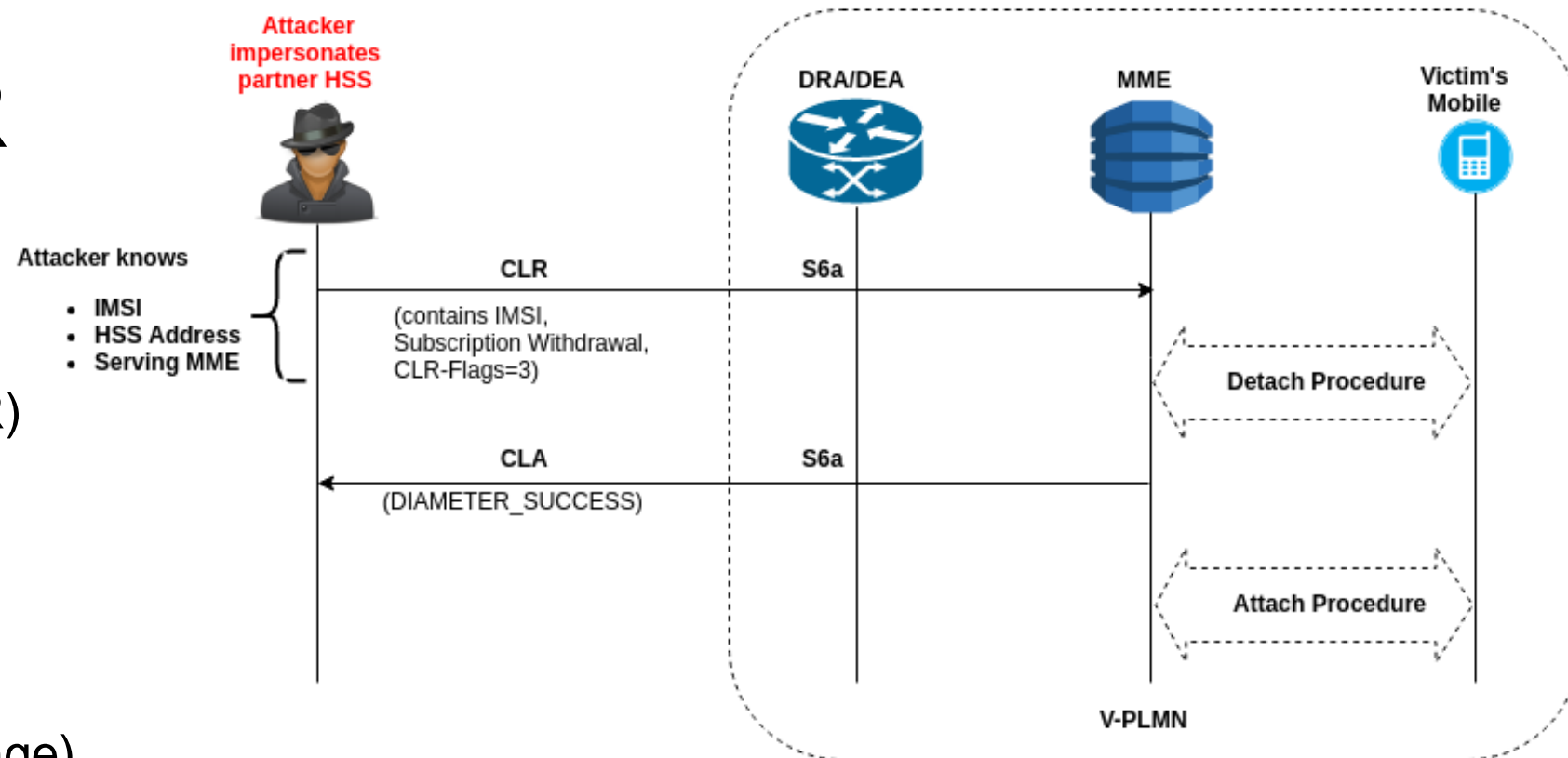


DoS using CLR

Cancel Location Request (CLR)

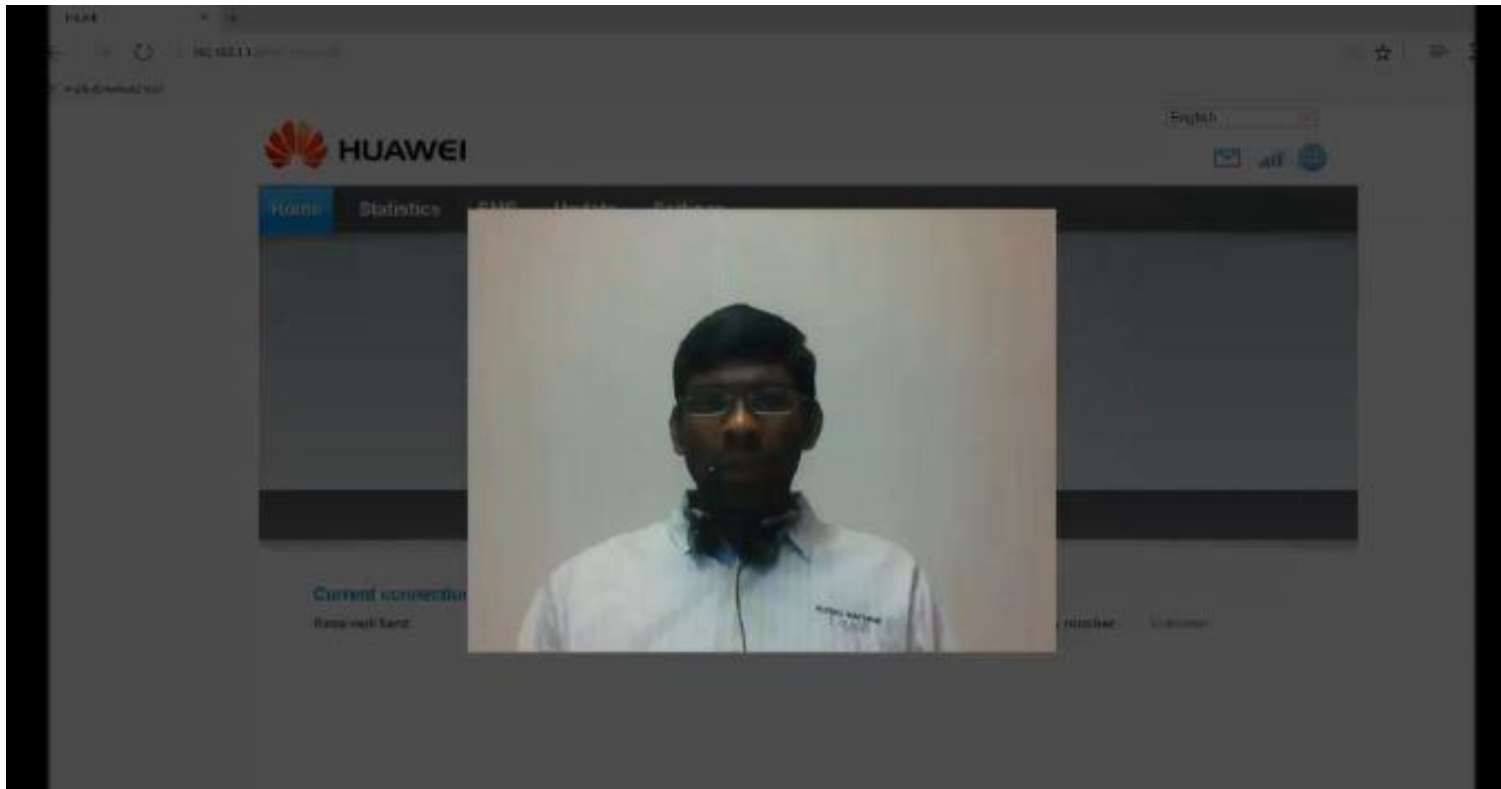
Sent by HSS to the MME to detach the UE

- MME change (location change)
- Subscription Withdrawal



```
<command name="Cancel-Location-Request" code="317">
  <avp name="User-Name" value="235919999994001" />
  <avp name="Cancellation-Type" value="2" />
  <avp name="CLR-Flags" value="3"/>
</command>
```

CLR DoS Attack - [Video](#)

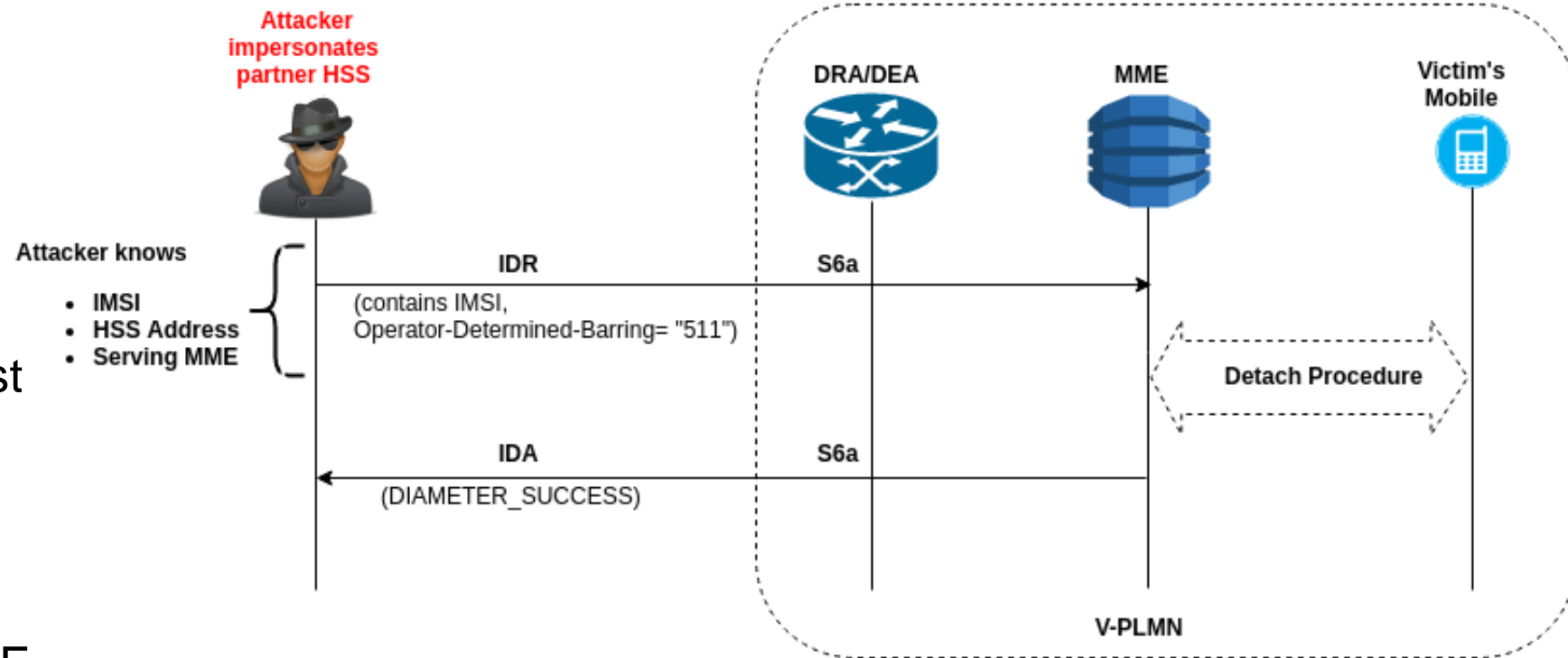


DoS using IDR

Insert Subscriber Data Request (IDR)

Sent by HSS to the MME

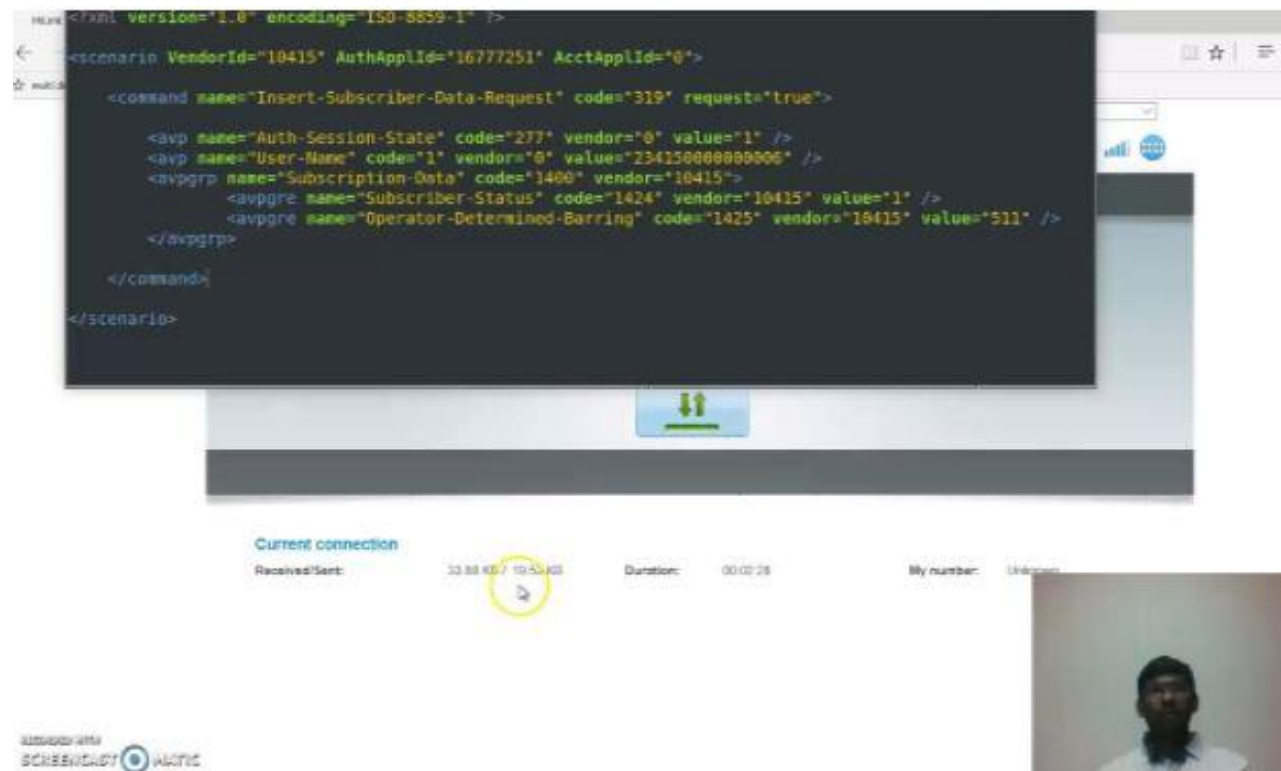
- updating and/or requesting certain user data in the MME
- retrieve location information and/or state information from the MME



```

<command name="Insert-Subscriber-Data-Request" code="319">
  <avp name="User-Name" value="235919999994001" />
  <avp name="Subscription-Data">
    <avp name="Subscriber-Status" value="1" />
    <avp name="Operator-Determined-Barring" value="511" />
  </avp>
</command>
  
```

IDR DoS Attack - Video

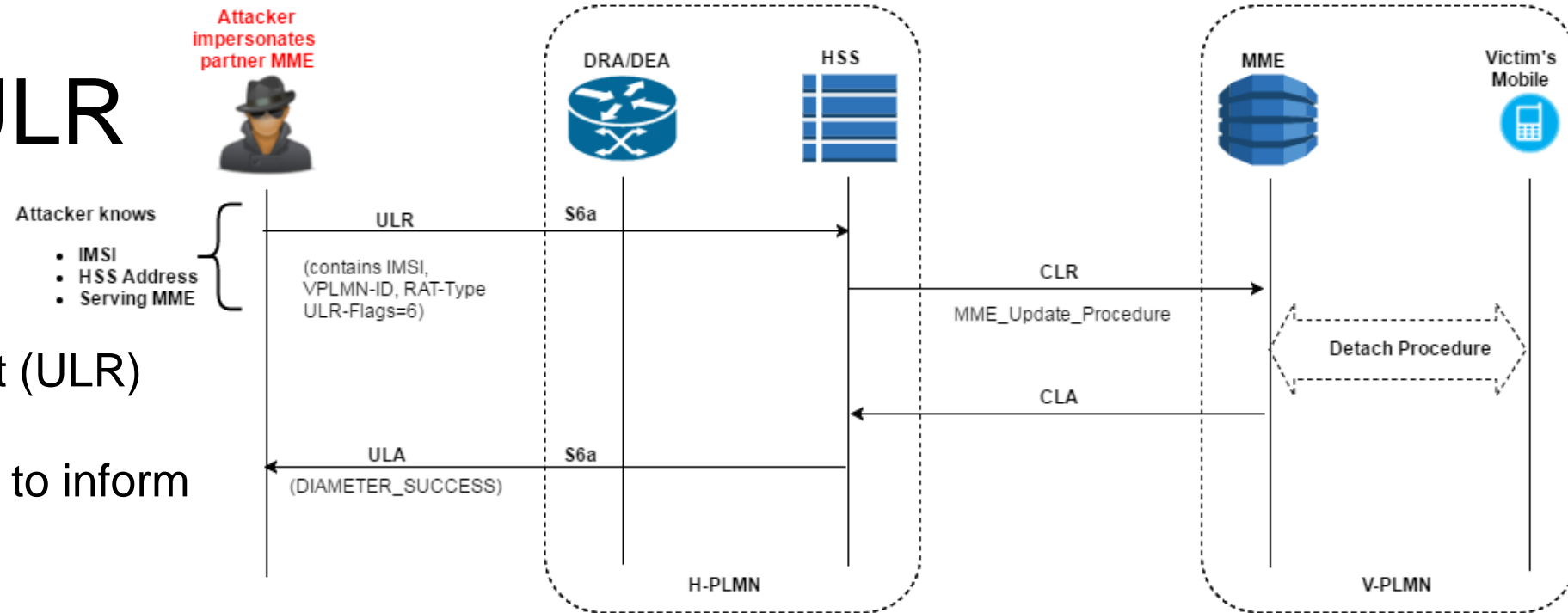


DoS using ULR

Update Location Request (ULR)

Sent by MME to the HSS to inform about

- the serving MME (e.g. going abroad)
- the user data such as terminal information



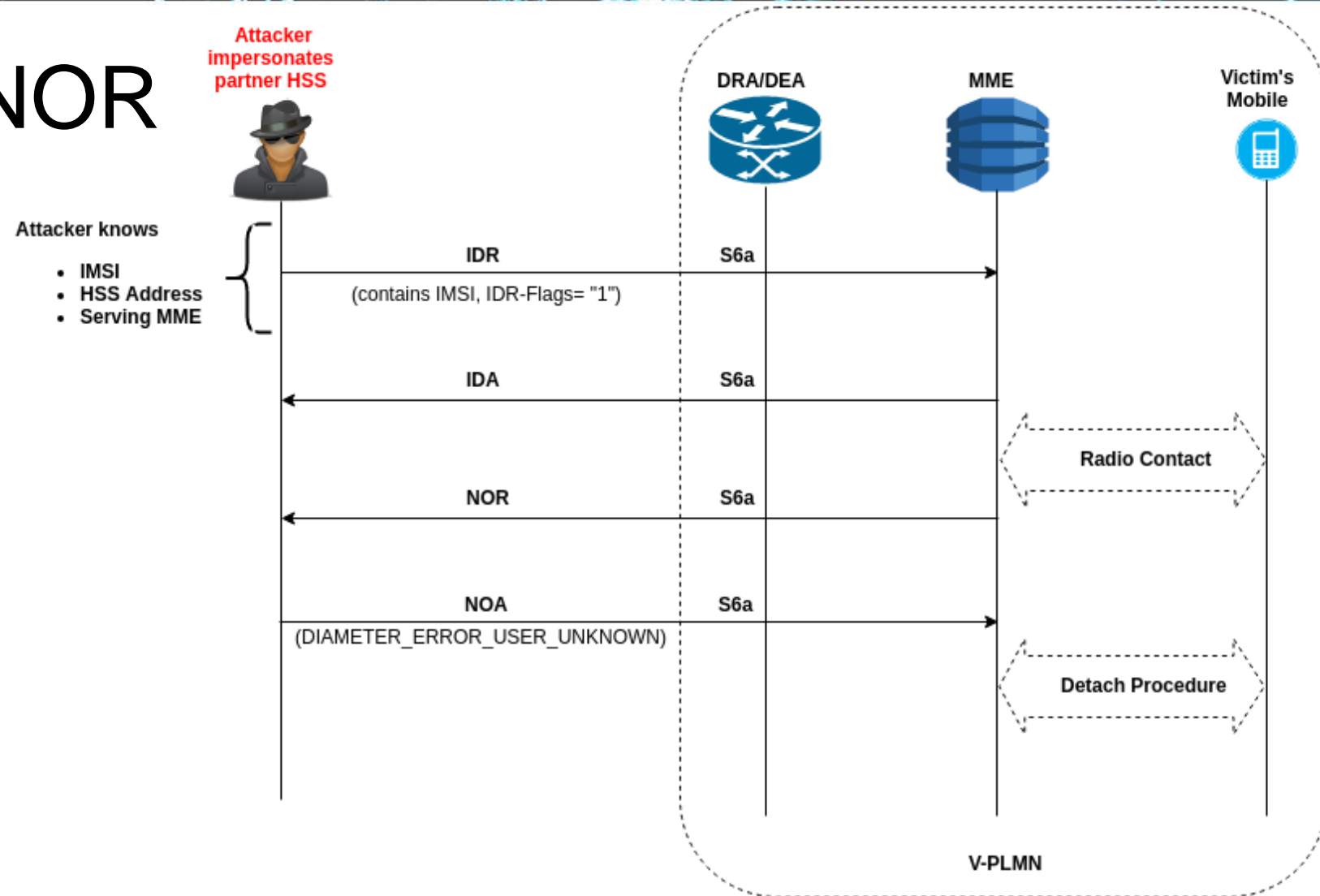
```
<command name="Update-Location-Request" code="316">
  <avp name="User-Name" value="235919999994001" />
  <avp name="Visited-PLMNId" value="23415"/>
  <avp name="RAT-Type" value="1004"/>
  <avp name="ULR-Flags" value="6"/>
</command>
```


DoS using IDR+NOR

Notification Request (NOR)

Sent by MME to the HSS

- Notifying events such as device reachability, updated device information



Practical Considerations

- IPSec for diameter is standardized
- It's all IP, lets use IPSec! Maybe not that easy.....
 - Not all is IP (some part of SS7 / interworking)
 - Who will host / create root certificates
 - Operators in developing countries
 - Interconnection service provider -> only hop-by-hop security
 - Nodes difficult to upgrade
- Still no protection against
 - Partners renting out to "service companies"
 - Hacked nodes
 - Bribed employees
 - Governmental ties

Countermeasures

Detect

Monitor network traffic
Tenant monitoring

Mitigate

Filter, filter, filter
Signaling Firewall at DEA
IPSec usage for LTE-Diameter
SMS protection measures

Cooperate

Share experiences
Form circles of security
Cooperation with legislators

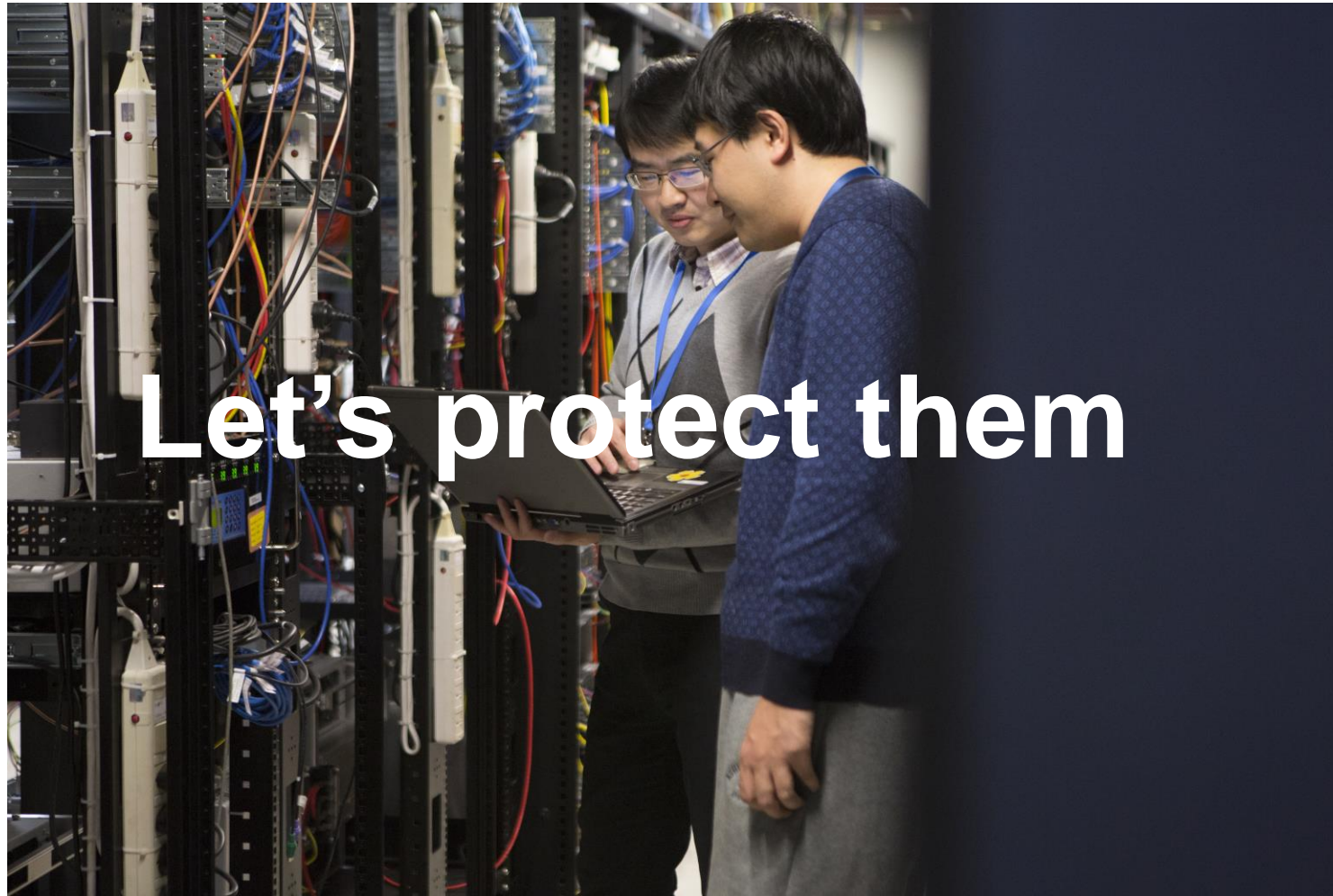
Prepare

Business rules for misuse
Investigate potential weaknesses
Node hardening

Summary

- Interconnection attacks are reality, but current main focus is SS7
- LTE/Diameter has similar functionality
 - > hence similar attacks are possible there
- Independent of phone, platform or device
- DoS against users can be done in Diameter in many ways
 - > some have also network performance impacts
- Will LTE face the similar Interconnection weaknesses as SS7?
 - If networks don't take protection measures, then yes.

Mobile Networks arrived in the Internet



Let's protect them

A close-up photograph of shattered glass, with sharp, translucent fragments and a network of cracks, set against a dark background.

Thanks

You

Finnish CyberTrust Project

Major global operators for their support and security engagement

Questions?