

# TIDS: A Framework for Detecting Threats in Telecom Networks

Alexandre De Oliveira - Cu D. Nguyen  
Hack.lu 2017



# Who we are

- POST Luxembourg – Main Telco operator in Luxembourg
  - Critical infrastructure for the country
  - Hosting large number of sensitive customers
- Alexandre De Oliveira
  - Telecom security researcher
  - Hiking enthusiast
- Cu D. Nguyen, Ph.D. in computer science
  - Machine learning
  - Secure software engineering



# Why We are here ?

- Enhance visibility possibilities of telecom operators
- Defend against who ?
- Fraudsters, Criminals, States

ULIN

Ultimate Interception

ULIN – Product Description

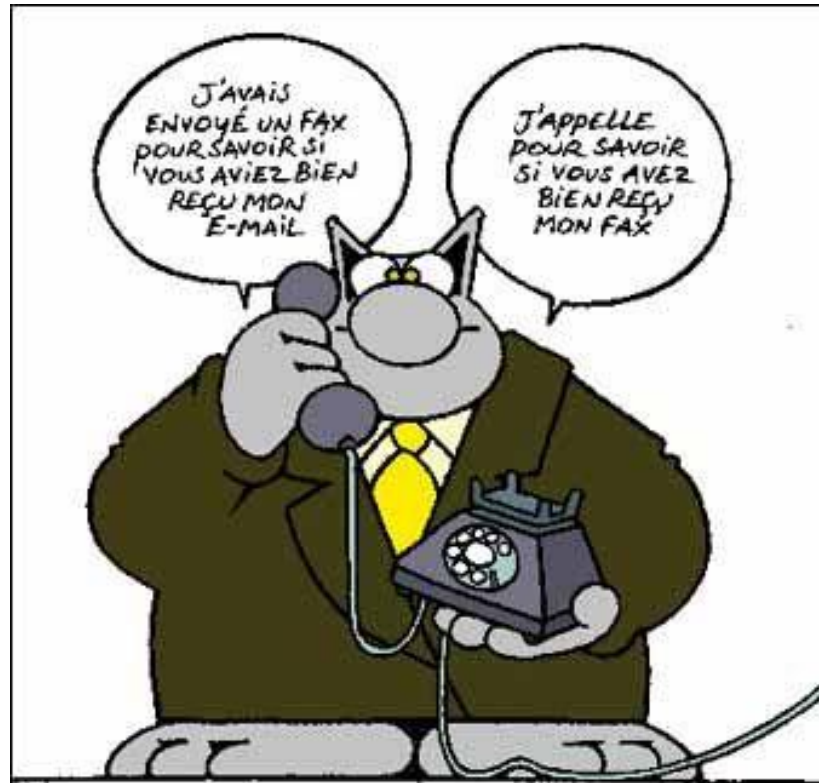
**ability**

Version 1.2  
09 / May / 2016




For \$20M, These Israeli Hackers Will Spy On Any Phone On The Planet

# Actual stack of technologies



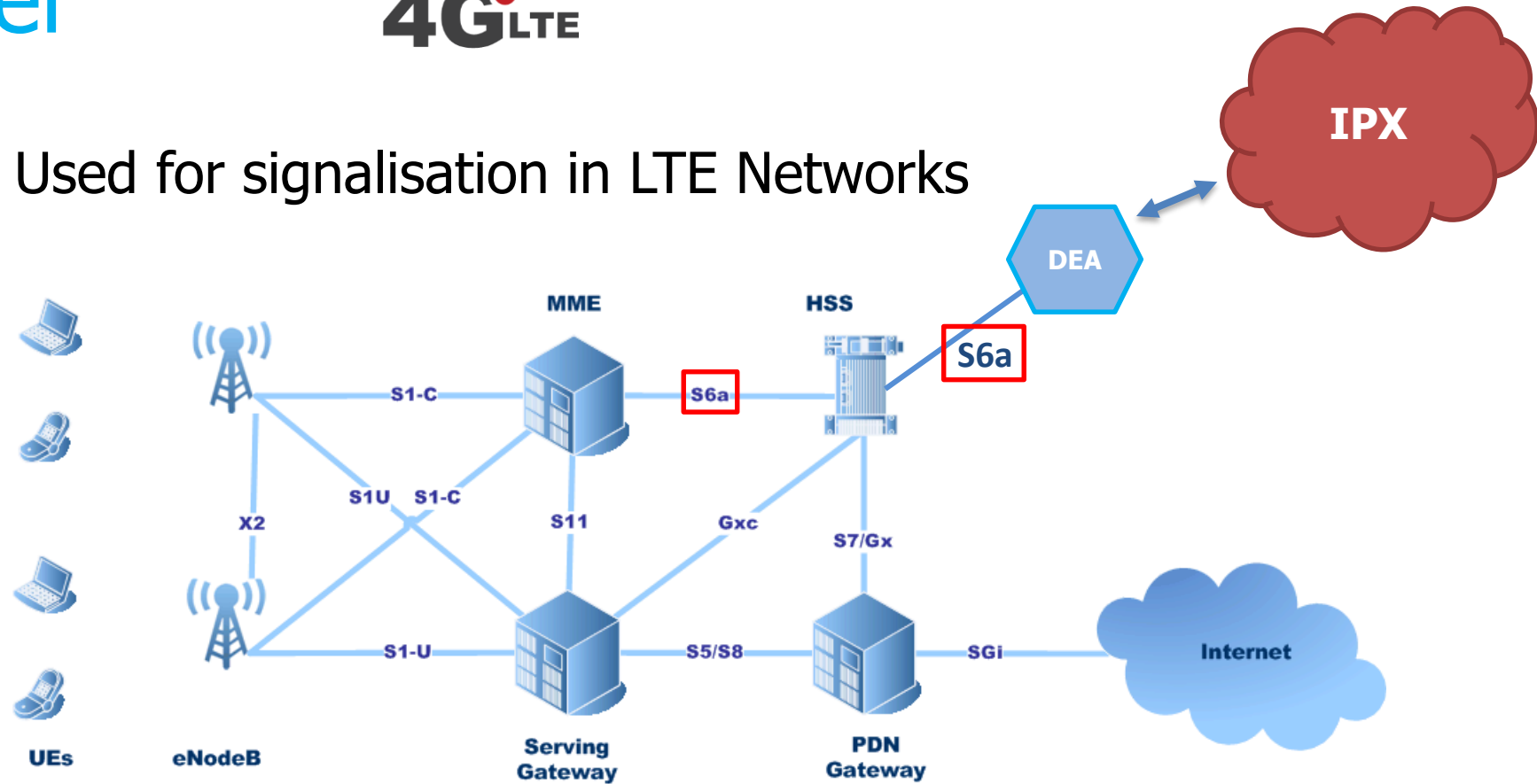
# TIDS global coverage

- Monitoring signaling networks for:
    - Frauds (Call and SMS)
    - Location tracking
    - Interceptions Call & SMS
    - Infrastructure attacks
  - Technologies covered:
    - SS7 (2G/3G)
    - GTP (2G/3G/4G)
    - Diameter (4G)
  - Infrastructure is composed of proto decoders and Splunk
- 

# Diameter



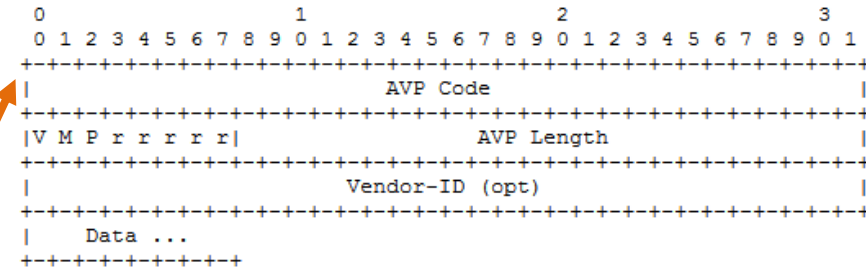
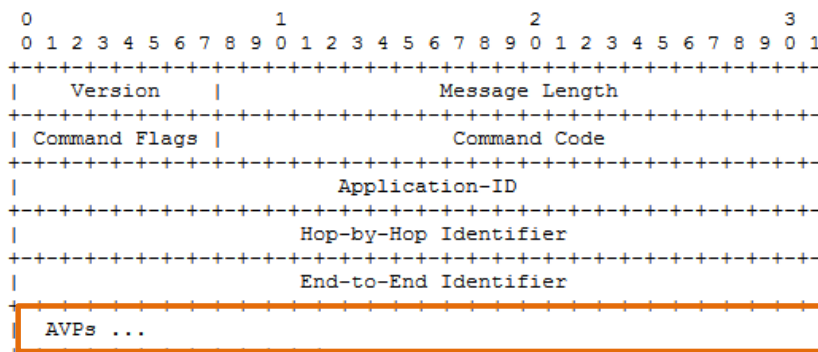
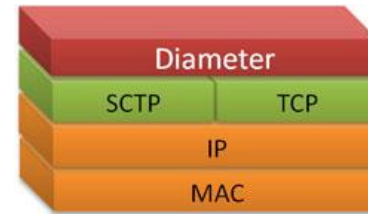
- Used for signalling in LTE Networks



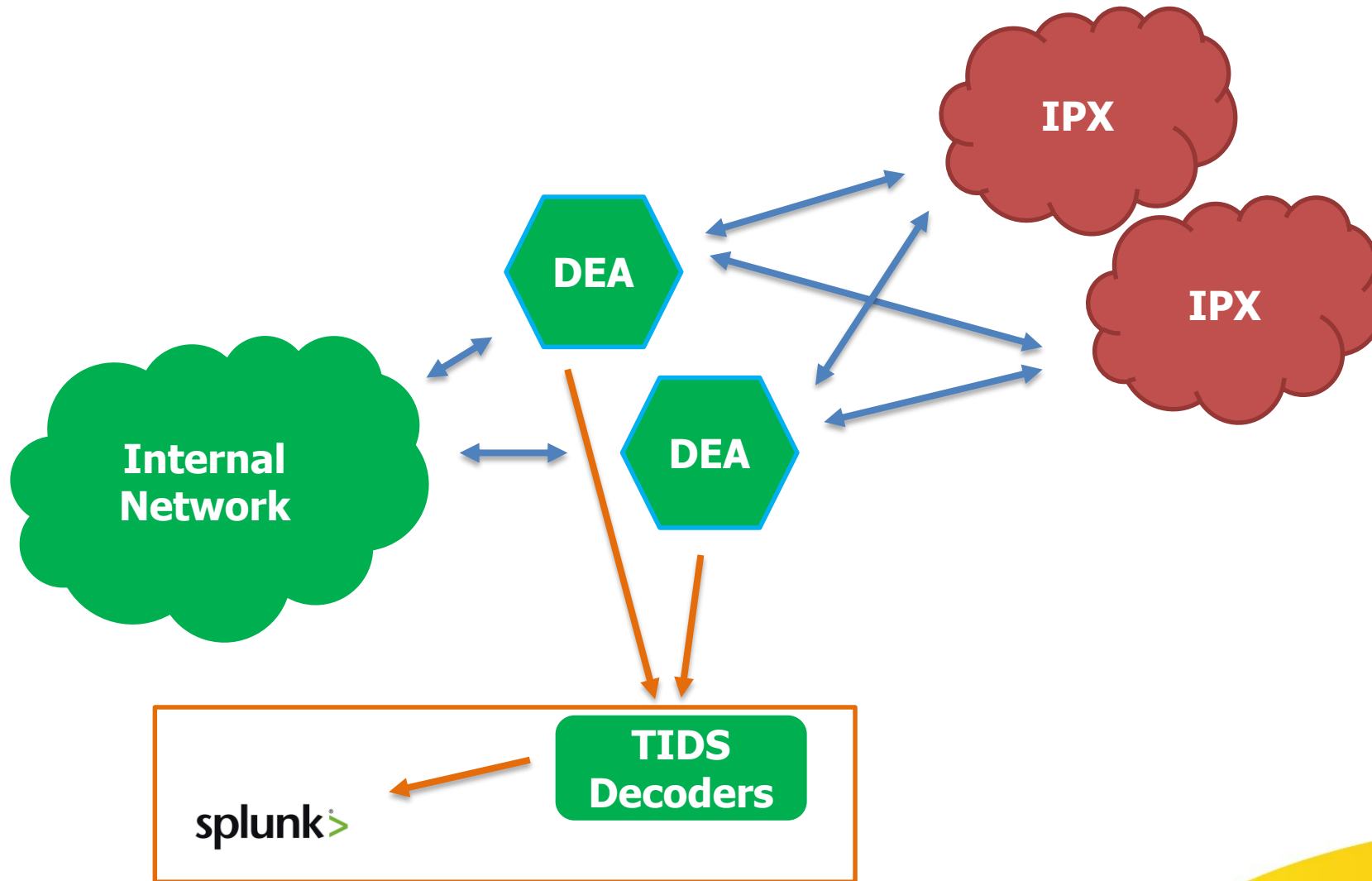
- IPX: IP exchange – Diameter Roaming network

# 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 possibilities




# Diameter Monitoring - Actual setup



TIDS Framework



# TIDS – Telecom IDS Diameter

- Parsing diameter traffic, extracting fields, exporting on JSON format
  - Two types of information extracted
    - All messages for data analytics in Splunk and realtime analysis
    - Detectors such as Location tracking, Spoofing, unwanted Application-Id
  - Minimize « intelligence » efforts on decoder – not stateful
  - Splunk is used to do stateful / correlation intelligence
- 

# Why building it

## *Le principe de précaution*

*Devise Shadok :*

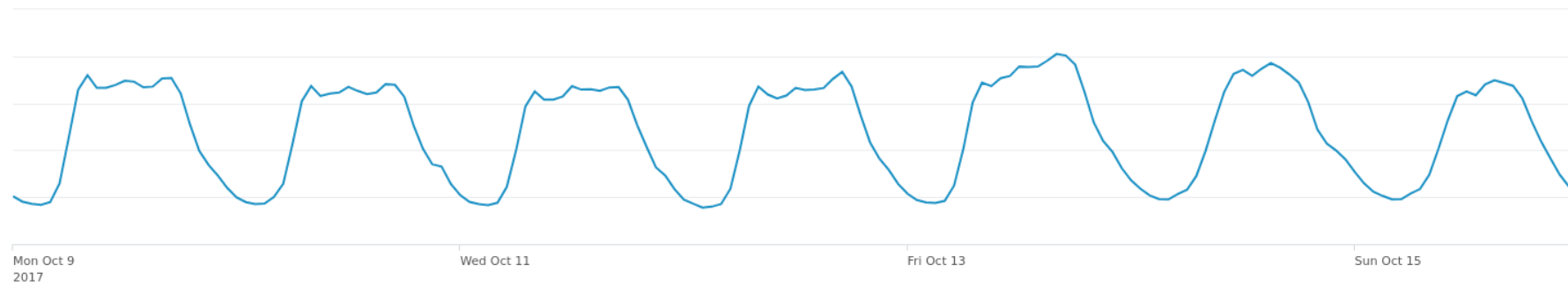


IL VAUT MIEUX POMPER MEME S'IL NE SE PASSE  
RIEN QUE RISQUER QU'IL SE PASSE QUELQUE CHOSE  
DE PIRE EN NE POMPANT PAS.

# Actual Diameter issues

Interface	Diameter Message	Target	Attack goal	Risk
S6a	ULR	HSS	Sub DoS	Yellow
S6a	CLR	MME	Sub DoS	Yellow
S6a	PUR	HSS	Sub DoS	Yellow
S6a	RSR	MME	Network DoS	Red
S6a	IDR	MME	Fraud (Profile injection)	Red
S6a	IDR	MME	Tracking	Red
S6a	*	*	Spoofing	Red
S6a	*	*	Scanning	Yellow
SLh	RIR	HSS	Tracking / Info gath	Grey
SLg	PLR	MME	Tracking	Grey
Sh	UDR	HSS	Tracking	Grey
S6c	SRR	HSS	Info gathering	Grey
S9 (S9/Rx)	CCR / RAR	PCRF	Fraud ?	Grey
S6m	SIR	HSS	Info gathering	Grey

# Who is in my network ?



# Monitored issues

Interface	Diameter Message	Target	Attack goal
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
S6a	*	*	Spoofing
S6a	*	*	Scanning

*Not monitored for inbound roamers*

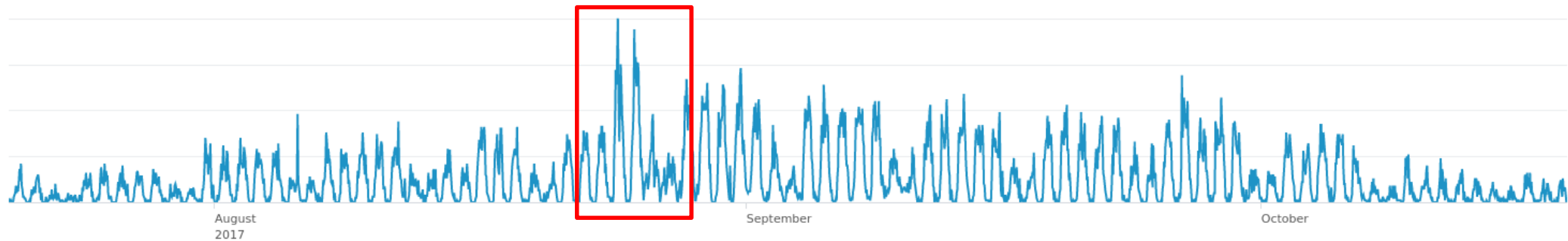
# IDR – Location tracking

- Mainly operators asking for location of their subscribers
- Not so common on the network ~150 messages per day
- Luxembourg as a lot of international interesting roamers

```
▼ IDR Flags: 0x0000002e
  0000 0000 0000 0000 0000 000. = Spare bit(s): 0x00000000
  .... ..0 = P-CSCF Restoration Request: Not set
  0... .... = RAT-Type Requested: Not set
  .0.. .... = Remove SMS Registration: Not set
  ..1. .... = Local Time Zone Request: Set
  ...0 .... = Current Location Request: Not set
  .... 1... = EPS Location Information Request: Set
  .... .1.. = EPS User State Request: Set
  .... ..1. = T-ADS Data Request: Set
  .... ...0 = UE Reachability Request: Not set
```

# IDR – Location tracking

- Three months of statistics
- During some events, periods, more IDR Loc are received...



## Top 10 Values

		%	
8887	58.242%		
5093	26.374%		
7126	6.593%		

# More targetted Subscribers

1day stat

Values	Count	%	
4148	59	53.153%	
4149	52	46.847%	

Top 10 Values	Count	%	
7520	99	41.597%	
0343	85	35.714%	
1773	5	2.101%	
1636	4	1.681%	
0305	3	1.26%	
2768	3	1.26%	
3779	3	1.26%	
3178	3	1.26%	
6361	3	1.26%	
3534	2	0.84%	

Values	Count	%	
724	13	76.47%	
243	2	11.765%	
736	1	5.882%	
878	1	5.882%	



# Who can love you so much...

- Constant IDR loc requests at fixed timings

3/3/17 4:02:33.000 PM	45093",	log/syslog	detector = diameter_idr_loc	host = diameter-monitor	imsi = 45093	time = 1488553353
3/3/17 1:02:33.000 PM	45093",		detector = diameter_idr_loc	host = diameter-monitor	imsi = 45093	time = 1488542553
3/3/17 11:05:02.000 AM	45093",		detector = diameter_idr_loc	host = diameter-monitor	imsi = 45093	time = 1488535502
3/3/17 10:02:33.000 AM	45093",		detector = diameter_idr_loc	host = diameter-monitor	imsi = 45093	time = 1488531753
3/3/17 9:02:33.000 AM	45093",		detector = diameter_idr_loc	host = diameter-monitor	imsi = 45093	time = 1488528153
3/3/17 8:02:33.000 AM	45093",		detector = diameter_idr_loc	host = diameter-monitor	imsi = 45093	time = 1488524553

# Passively fingerprint vendors

- Diameter Session-id

## Diameter RFC 6733

The Session-Id MUST begin with the sender's identity encoded in the DiameterIdentity type (see Section 4.3.1). The remainder of the Session-Id is delimited by a ";" character, and it MAY be any sequence that the client can guarantee to be eternally unique; however, the following format is recommended, (square brackets [] indicate an optional element):

<DiameterIdentity>;<high 32 bits>;<low 32 bits>[;<optional value>]

```
▼ Diameter Protocol
  Version: 0x01
  Length: 620
  ▶ Flags: 0xc0, Request, Proxyable
  Command Code: 316 3GPP-Update-Location
  ApplicationId: 3GPP S6a/S6d (16777251)
  Hop-by-Hop Identifier: 0x[redacted]41
  End-to-End Identifier: 0x[redacted]aa
  ▶ AVP: Session-Id(263) l=117 f=-M- val=[redacted].mnc001.mcc270.3gppnetwork.org;153[redacted]531;262[redacted]098;1.7;425[redacted]59
  ▶ AVP: Auth-Session-State(277) l=12 f=-M- val=NO_STATE_MAINTAINED (1)
  ▶ AVP: Origin-Host(264) l=82 f=-M- val=[redacted].epc.mnc001.mcc270.3gppnetwork.org
  ▶ AVP: Origin-Realm(296) l=41 f=-M- val=epc.mnc001.mcc270.3gppnetwork.org
  ▶ AVP: Destination-Realm(283) l=41 f=-M- val=epc.mnc010.mcc206.3gppnetwork.org
  ▶ AVP: User-Name(1) l=23 f=-M- val=[redacted]548
  ▶ AVP: RAT-Type(1032) l=16 f=VM- vnd=TGPP val=EUTRAN (1004)
  ▶ AVP: ULR-Flags(1405) l=16 f=VM- vnd=TGPP val=3
  ▶ AVP: Visited-PLMN-Id(1407) l=15 f=VM- vnd=TGPP val=MCC 270 Luxembourg, MNC 01 P&T Luxembourg
```

# Session-id vendor patterns

RFC: <DiameterIdentity>;<highint32bit>;<lowint32bits>[;<optional value>]

- Ericsson

<DiameterIdentity>;<highint32bit>;<lowint32bit>;[0-9].[0-99];<int32bit>

- Huawei

<DiameterIdentity>;0;<highint32bit>;<lowint32bit>

- ZTE

<DiameterIdentity>;<highint32bit>;<lowint32bit>;<int32bit>

- Nokia

<DiameterIdentity>;<highint32bit>;<lowint32bit>



# I'm also monitoring your network

- How could we do it passively ?
- S6a Reset



## 5.2.4 Fault Recovery Procedures

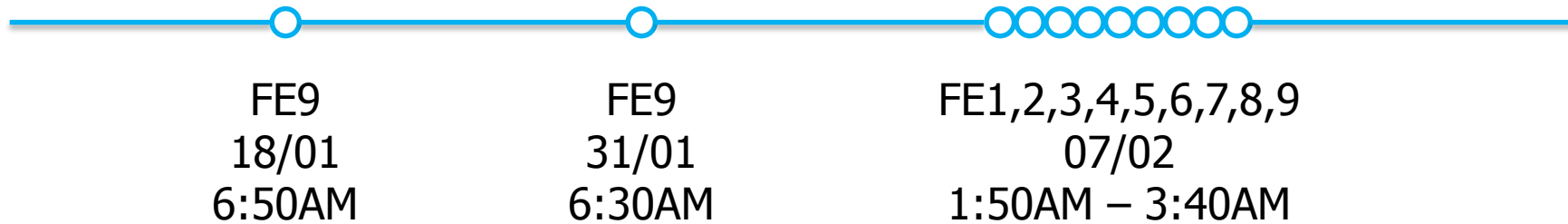
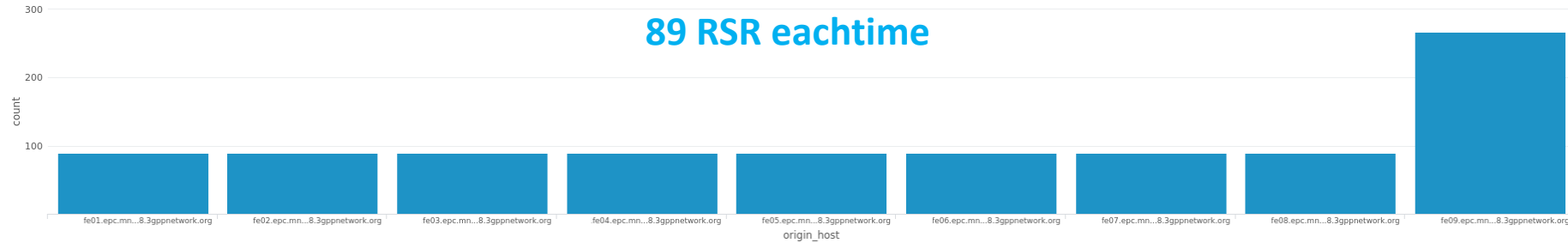
### 5.2.4.1 Reset

#### 5.2.4.1.1 General

The Reset Procedure shall be used by the HSS, after a restart, to indicate to the MME and to the SGSN that a failure has occurred.

- Could appear when HSS crashed, got upgraded
- Often leaking BackEnd HSS internal host instead of normal FE or LB one.

# S6a Reset – Upgrade in progress



# Spoofing – Topology hiding

- Usually misconfiguration
- Found several spoofing of realm – never on host
- Never on host – topology hiding ?
  - Random host outside of my network
  - Impossible to directly reach real internal hosts
- IDR location with direct host target – trying to bypass topology hiding



# Monitoring traffic rerouting



- AVP Route-Record
  - Loop detection if Network Element see itself in the Record
  - Path authorisation, check in the taken path respects the agreements
- Using it to detect rerouting of traffic over the Network

```
▶ AVP: Route-Record(282) l=51 f=-M- val=[REDACTED].3gppnetwork.org
▶ AVP: Route-Record(282) l=45 f=-M- val=[REDACTED].3gppnetwork.org
▶ AVP: Route-Record(282) l=49 f=-M- val=[REDACTED].3gppnetwork.org
▶ AVP: Route-Record(282) l=42 f=-M- val=[REDACTED].orange-multimedia.net
▶ AVP: Route-Record(282) l=46 f=-M- val=[REDACTED].orange-multimedia.net
▶ AVP: Route-Record(282) l=35 f=-M- val=[REDACTED].dtag.grx
```

# Behavior Analytics – Call SPAM

- Robot call, to callback premium numbers
- Logs based on MSS CDR's
- Call frauds detection with 5-10 min delay on Splunk
- Behavior analytics on the last 7 days
- Automatic blocking is in progress

_time	callingPartyNumber	count
2017-10-17 14:45:00	8003f	6904
2017-10-17 14:30:00	8003f	6041
2017-10-17 15:00:00	8003f	1388
2017-10-17 13:45:00	8003f	1277
2017-10-17 15:15:00	8003f	1250
2017-10-18 13:15:00	0640f	568
2017-10-17 14:15:00	8003f	556
2017-10-17 15:30:00	40326	407
2017-10-17 14:30:00	40326	396
2017-10-18 12:45:00	0640f	381
2017-10-17 14:00:00	8003f	326
2017-10-17 17:00:00	40326	326
2017-10-17 14:45:00	40326	310
2017-10-16 20:00:00	40326	303
2017-10-16 18:15:00	40326	277
2017-10-16 19:00:00	40326	277
2017-10-18 13:00:00	0640f	267
2017-10-18 11:30:00	40326	260
2017-10-18 12:30:00	40326	259
2017-10-16 21:00:00	40326	255



# Advanced Data Analytics on Telecom Data

- Advanced data analytics: treating data to gain knowledge
- Why now?
  - Maturity of hardware, machine learning researches, and tools
  - Capability to collect and store large amount of data
  - Business strategy changing toward data-driven
- Why on Telecom Data?
  - Daily fraudulent activities (mass malicious SMSs, call frauds...) impacting providers and their customers
  - Massive amount of data -> need effective automation!



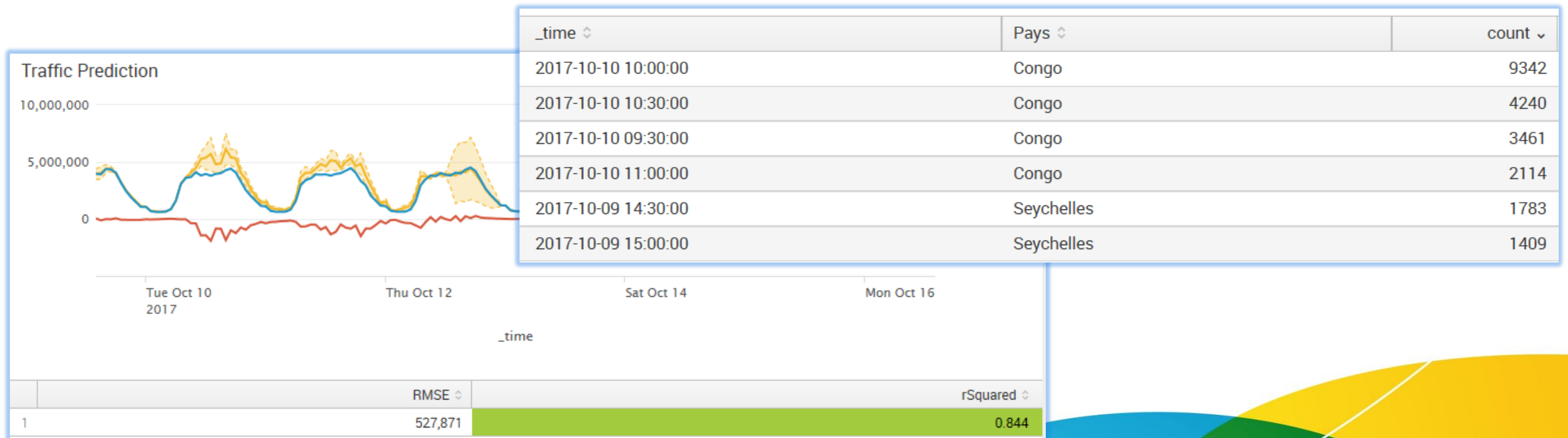
# Regulation, data, and beyond

- Regulation and customer privacy are extremely important!
  - Filtering from source
  - Anonymization and daily auditing report
- Collect live and batch data (call, sms, data) in to Splunk
  - From Diameter
  - From other equipment
- Develop advanced analytics on top of Splunk
  - Using prediction to detect anomalies
  - Using unsupervised machine learning methods to detect frauds



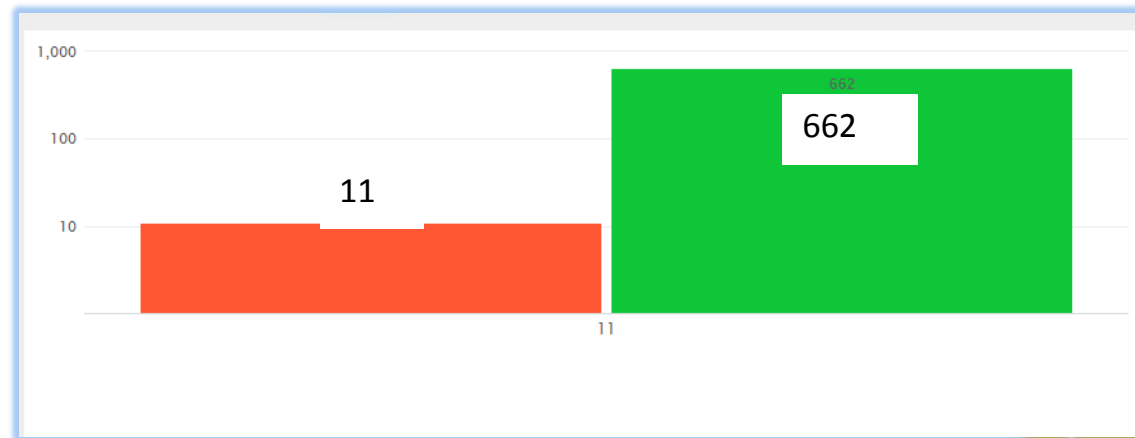
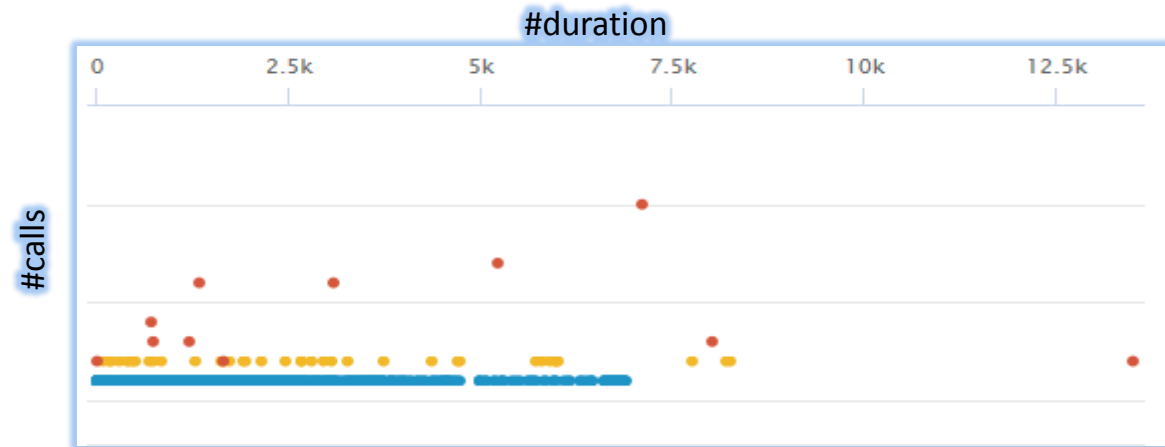
# Predicting the present to detect anomalies

- Dealing with time series data
- Based on past data, predict what we expect to see
- Then, compare with what actually happens



# Clustering data to detect outliers

- Multi-dimensional data
- Process data based on some attributes (#calls, frequency, duration, geo location, diversity)
- Able to detect relevant outliers
- Not yet super-duper sophistication, yet encouraging
- More to come!



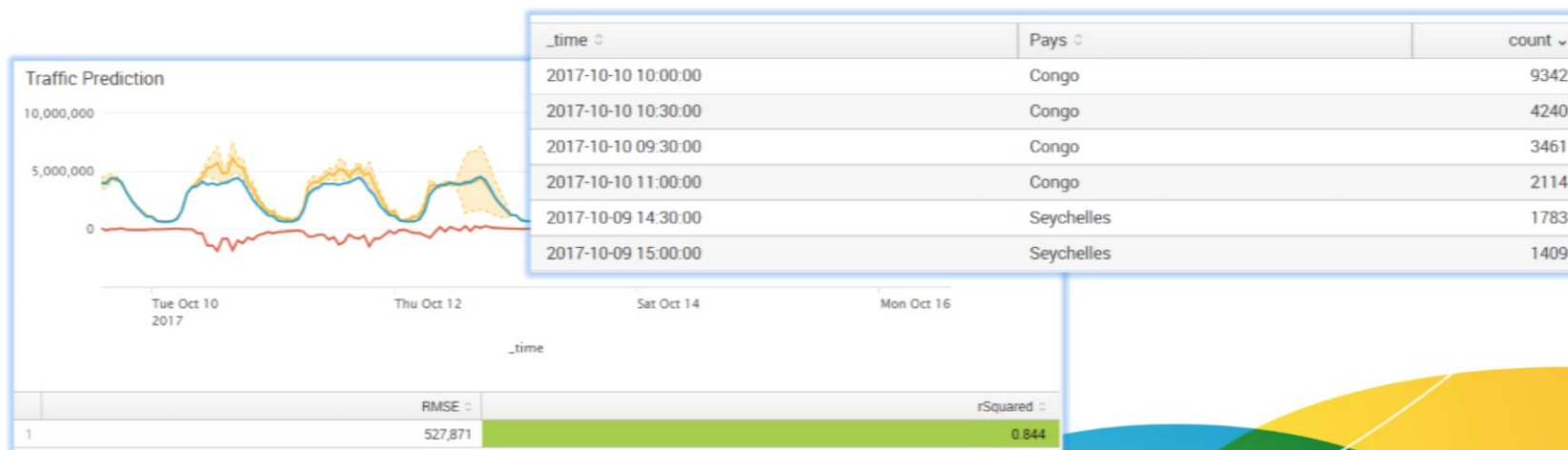
# Summary

## Diameter Monitoring



## Predicting the present to detect anomalies

- Dealing with time series data
- Based on past data, predict what we expect to see
- Then, compare with what actually happens



splunk>

Decoders

TIDS Framework

# Questions ?

Alexandre De Oliveira

[alexandre.deoliveira@post.lu](mailto:alexandre.deoliveira@post.lu)

Cu D. Nguyen

[duycu.nguyen@post.lu](mailto:duycu.nguyen@post.lu)



**KEEP  
CALM**

IT'S

**ALMOST  
THE WEEKEND**