NOKIA Bell Labs

New Attack Vectors for Mobile Core Networks

Silke Holtmanns, Isha Singh
Cyber Security Team Espoo
29.11.2018

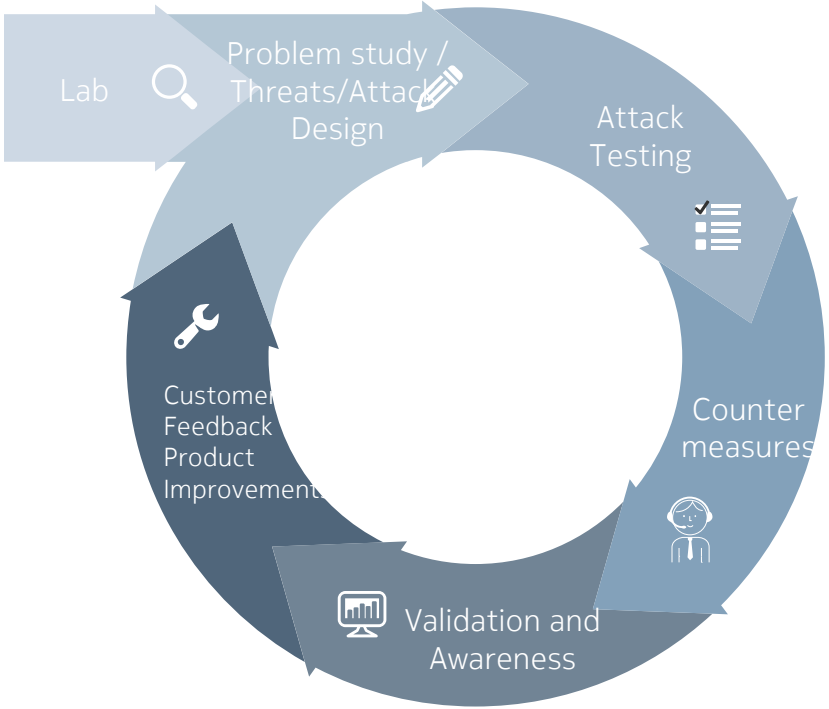
Industrial Security Research?

Nokia Bell Labs – Future Attacks and Mitigation

Research that solves real problems together with our customers and sometimes even competitors

- Theoretical studies go into attack and countermeasure design
- Validation and awareness of our research by GSMA standards input and publication
- Customer feedback and test results allow us to fine-tune and optimize our countermeasures
- Research input will fit product needs and operators requests
- Operator needs can be discovered ”live” for new research challenges and disruptive new solutions

Bell Labs Research Lifecycle

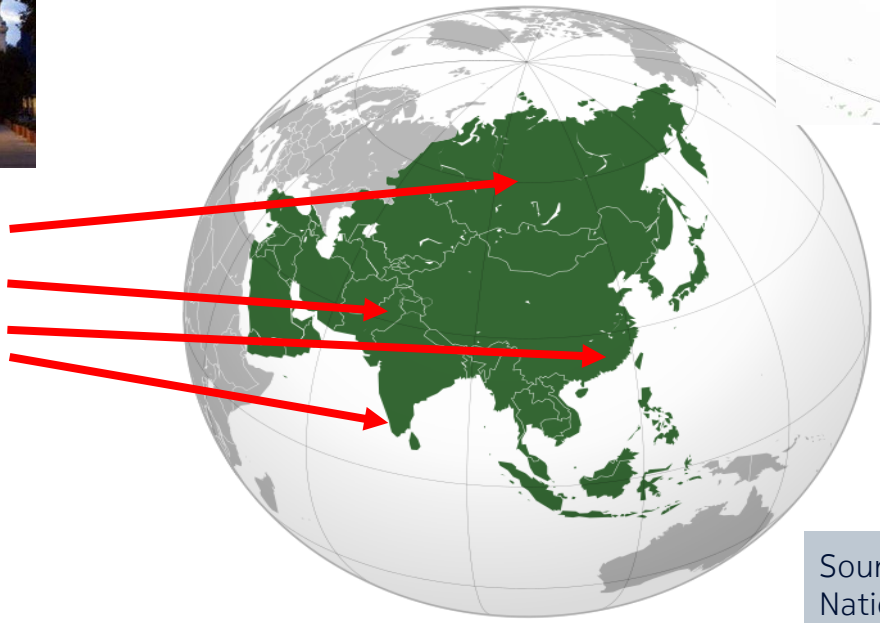


A brief history of roaming

Roaming

You connected to
3 Austria, T-Mobile, A1

DeepSec
participants
CMCC, Airtel,
MegaFon, Telenor

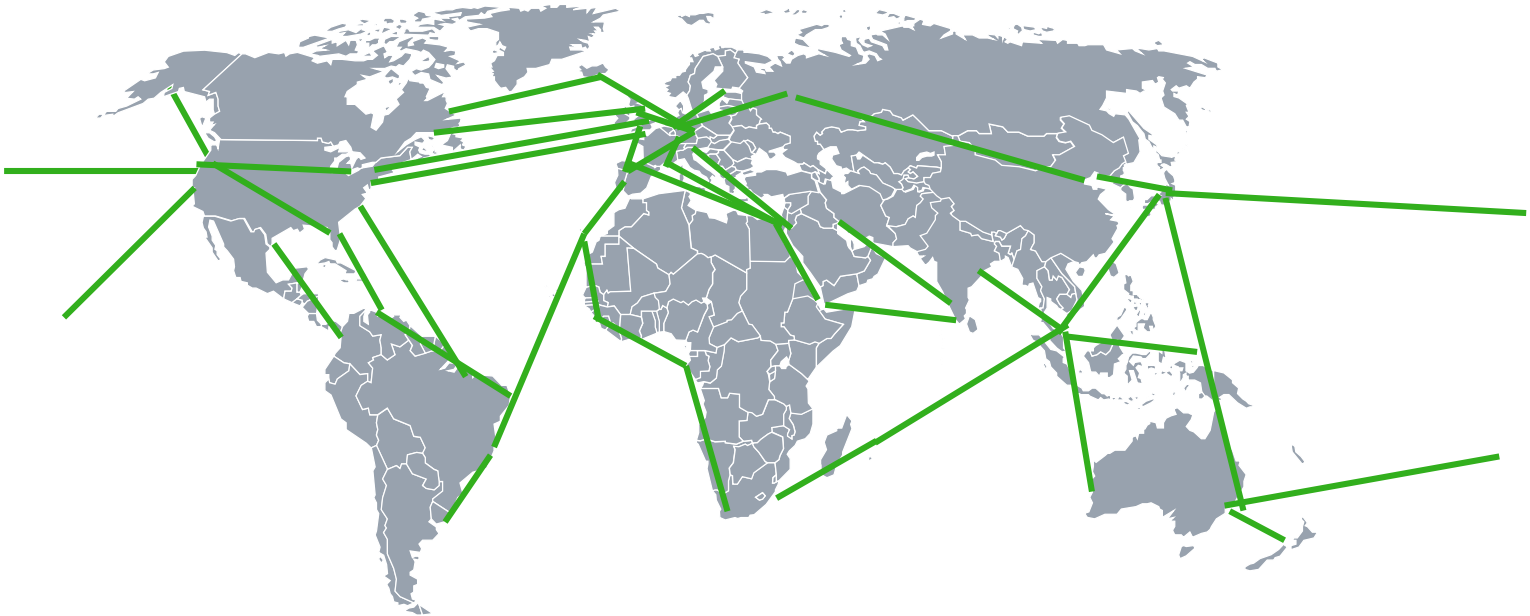


My colleagues,
friends, family
connected to DNA,
Elisa, Telia

Source: Mondial Location Finder,
National Geographics, Wikipedia

The Interconnection Network (IPX)

Connecting networks – The ”hidden private Internet”



I switch on my phone

Vienna
Antenna

Core Network

Carrier / IPX

Authentication -> run to home network
Checking subscriber

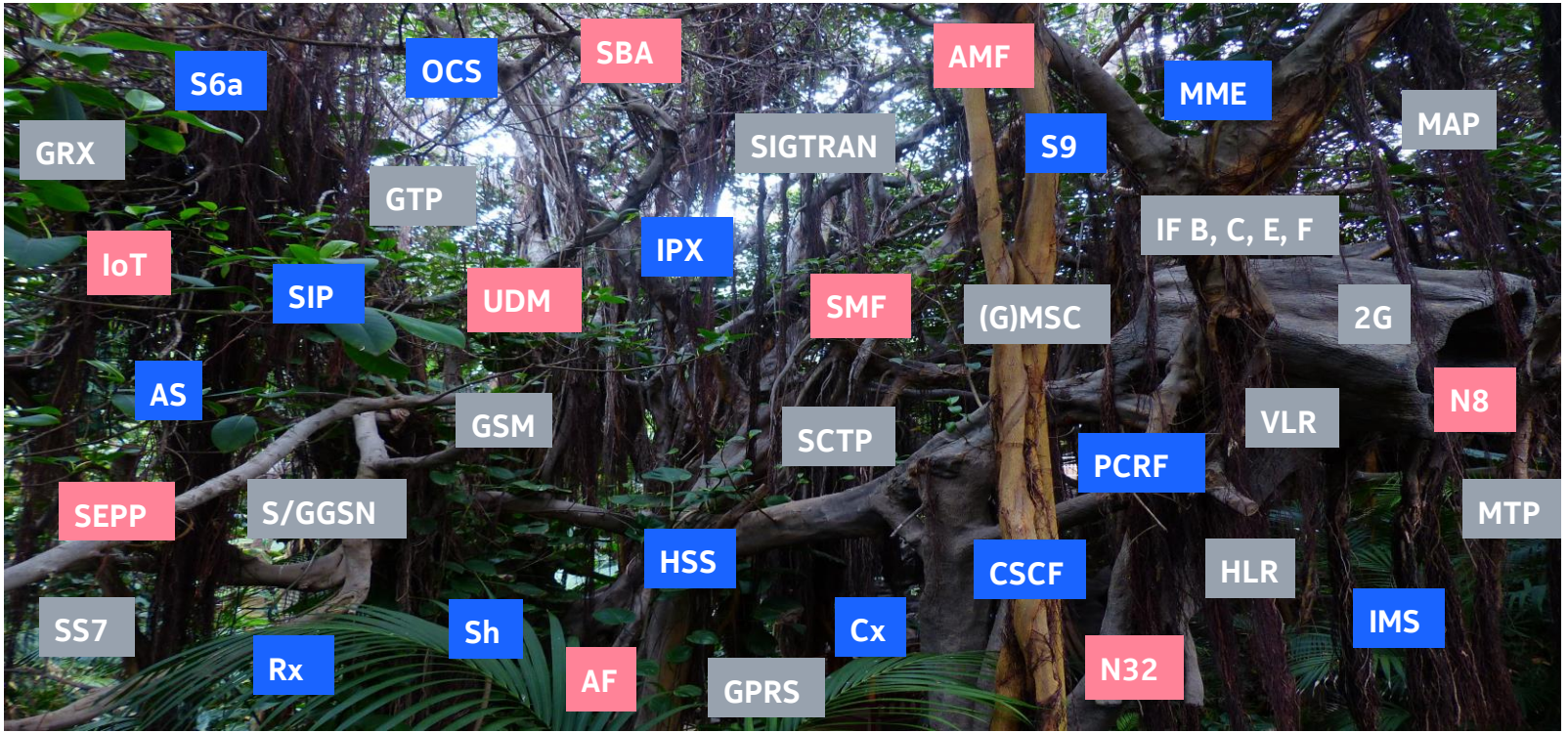
Core Network

The start of roaming
Handful of Nordic Operators




Global Mobile Phone Core Networks

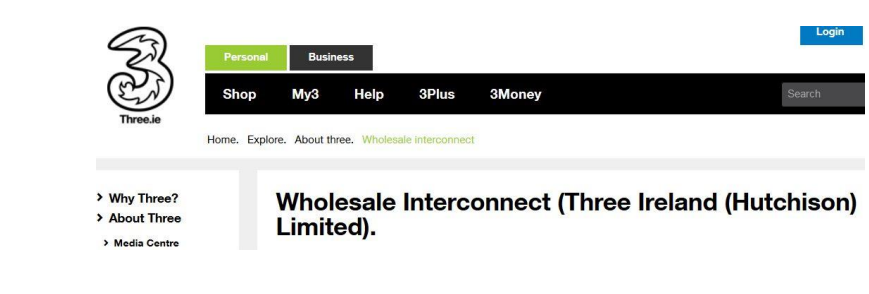
Organically grown structure – Connect them all…..



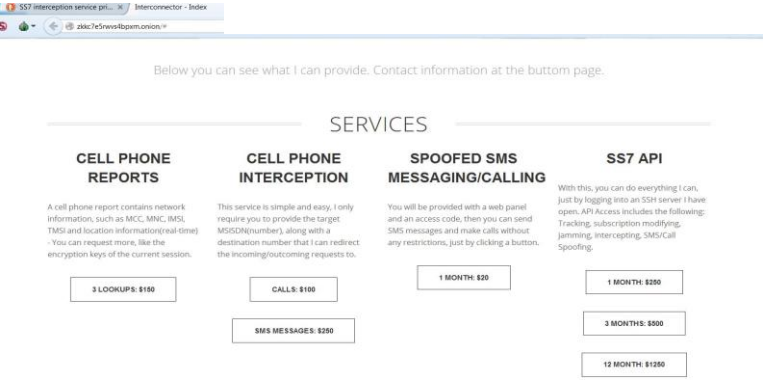
History of Interconnection Networks

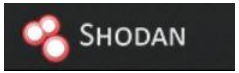
- Roaming network established more than 37 years ago between a few state owned operators
- Build on trust (closed private network)
- No inbuilt security (in particular, no source authentication)
- Nowadays about 2000 partners
- SS7 protocol stack was constantly extended for new services and features
- Now moving towards LTE/Diameter (3G/4G)
- 5G Service Based Architecture at the horizont

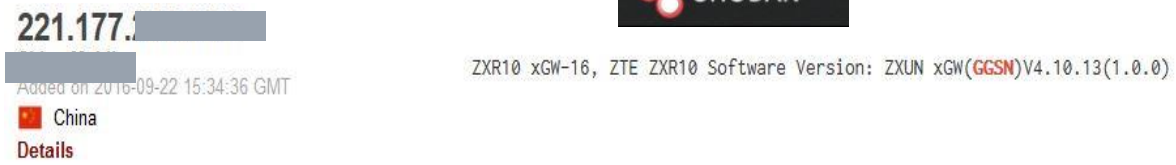
Closed & Private Network?



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







Bell Labs

How do attackers get in

Rent a Service

Become an Operator

Kick in the door

Bribing an Employee

Hack via Internet

Social Engineering

Even our ”friends & partners”

Support The Guardian | Subscribe | Search jobs | Sign in | Search

News | Opinion | Sport | Culture | Lifestyle | More

World ▸ Europe | US | Americas | Asia | Australia | Middle East | Africa | Inequality | Cities | Global developmen

GCHQ

UK refusal to cooperate with Belgian hacking inquiry condemned

Fears stance on GCHQ’s alleged hacking of Belgacom could damage diplomatic relations

Daniel Boffey *in Brussels*

Thu 25 Oct 2018
11.39 BST

GTP Internet Scanner

GPRS Transfer Protocol (GTP)

[redacted] View Raw Data

Internet Scanner

City	Shenzhen
Country	China
Organization	[redacted]
ISP	
Last Update	2018-06-27T11:32:02.803916
ASN	AS13[redacted]

30793
udp
gtp-v1

GPRS Tunneling Protocol Version: 1

```
GPRS Tunneling Protocol
Correct data length for version 1
Version: 1
Flags: XXX1 0010
Type: 2 (Echo response)
Length: 6
Data: \x0c=\x00\x00\x0e\x00
```

Protocol and Attack Evolution

Attacks are reality

Why should attackers stop? Because we have 4G or 5G?

- **Intelligence communities** use mobile networks as a way for VIP tracking and eavesdropping
- **Dark Service companies** use Interconnection to make money (fraud, SMS interception, location tracking offerings)
- **Military** uses mobile network data for target localization

The Switch

New documents show how the NSA infers relationships based on mobile location data

Intercept Implications of 4G/5G Diameter Signaling Replacing SS7

Presented by: *Dr. Jerry Lucas, President,* ***TeleStrategies*** *and a Distinguished* ***Telecom Technology Expert*** *to be announced*

As telecom service providers transition to IP based VoLTE and introduce 5G, SS7 will be replaced with diameter signaling. This session provides the technical basics of diameter, options for transitioning SS7 to diameter and the new challenges facing law enforcement.

Bell Labs

Existing Attacks for the ”old” SS7

If no protection is deployed

- Location Tracking
- Eavesdropping
- Fraud
- Denial of Service user & n
- Credential theft
- Data sessi
- Unblock
- SMS inte
- One time p ccount takeover for gram, Facebook, Whatsapp, g- (bitcoin)

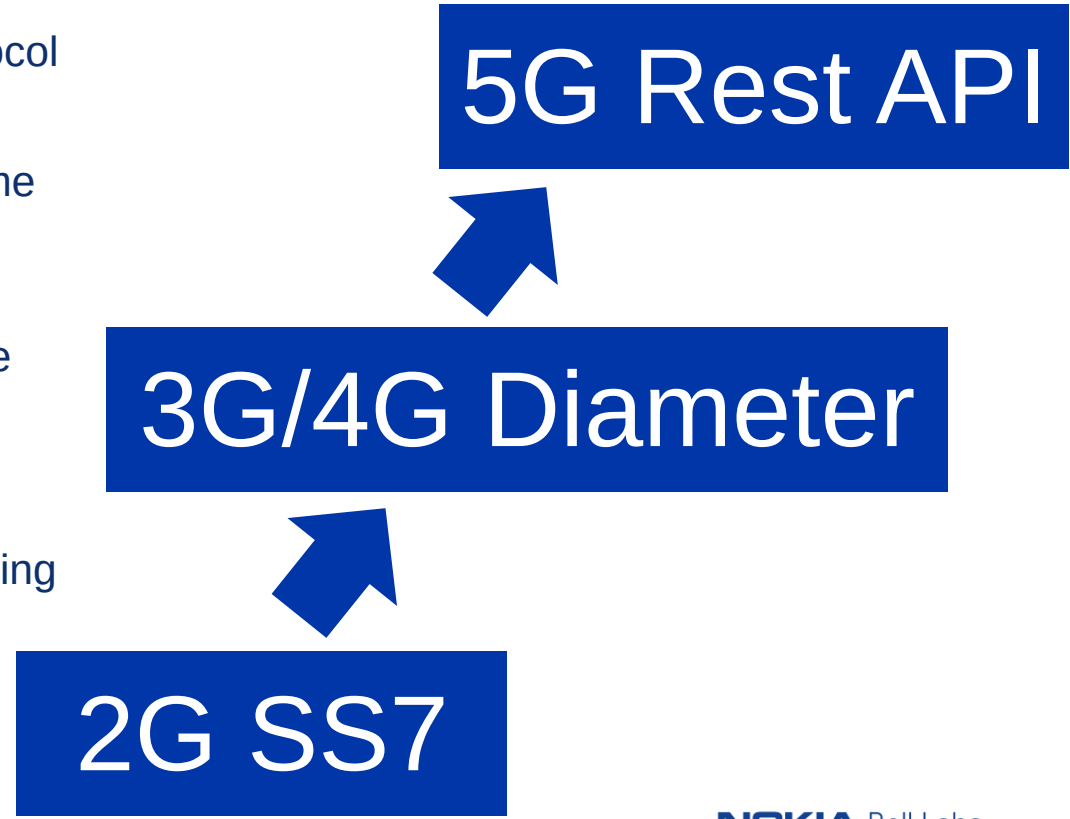
Not all networks are equal

Countermeasures (SS7)

- Standards:
  - GSMA IR.88, FS.07, FS.11
  - CVE program
- Regulations:
  - Nordic Countries, EU ENISA, US FCC
- Products:
  - SS7 ”understanding” firewalls
  - Security functionalities in Core Network nodes
- Services:
  - Telco penetration testing
- Public community
  - SS7 on github

3G/4G Diameter Based Communication Attacks

- Functionality similar to SS7, but protocol is different
- When in 2014 the SS7 attacks became known, also attention was paid to diameter
- Highest priority was SS7 as it was the most commonly used protocol
- Diameter was soon also tackled
- Countermeasures, filters and monitoring approaches exist
- Global trust problem still causing difficulties



3G/4G Diameter Based Communication

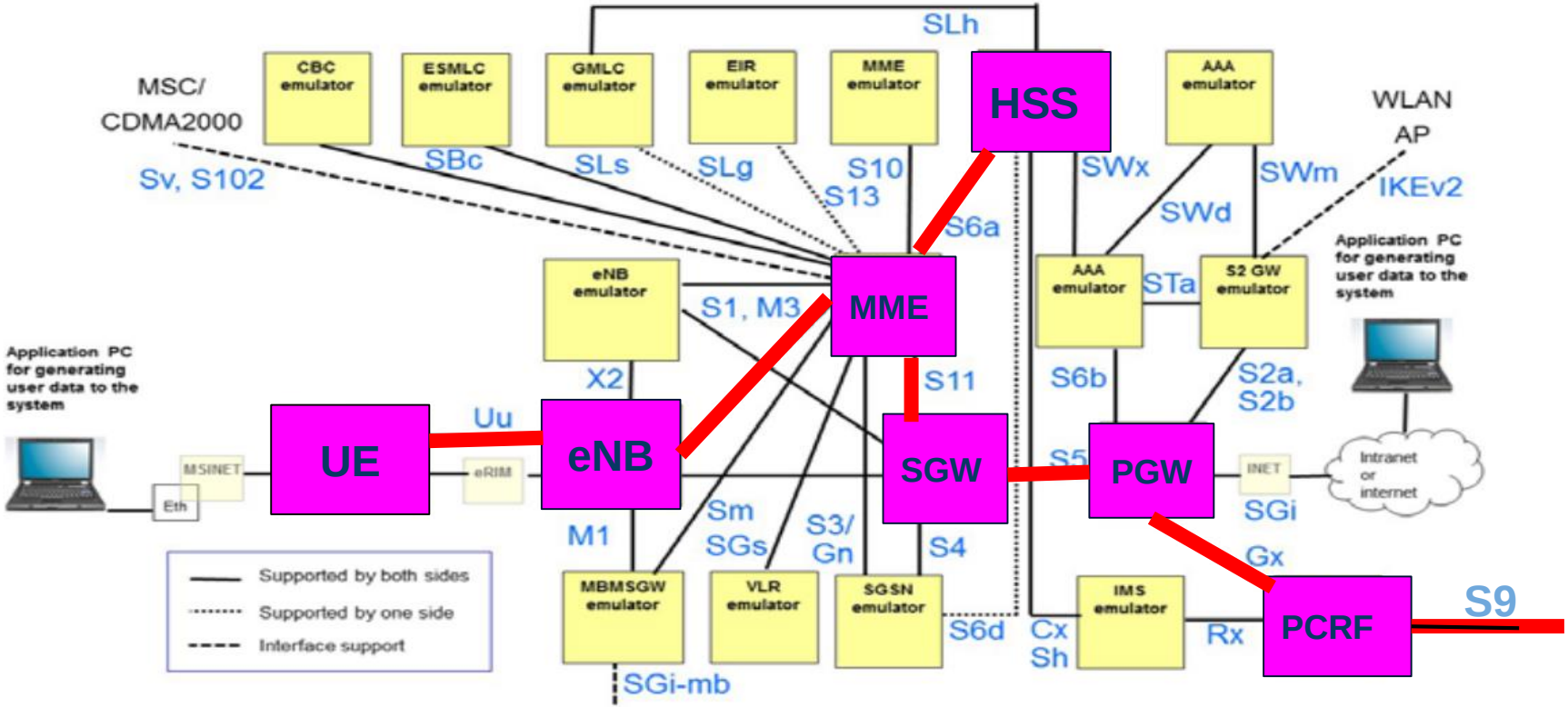
- Attacks are more ”operator specific”
  - Depend strongly on actual configuration and deployement
  - 3G/4G IPX is used by more progressive operators
- Attacks
  - Location Tracking (CyCon)
  - Fraud (DefCon)
  - Data Interception (CCC)
  - DoS of subscriber (Blackhat)

NOKIA Bell Labs

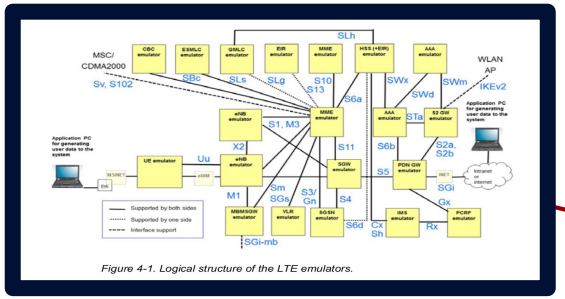
How do 3G/4G attacks work?

Example: Charging Attack

Network used for testing of attack



Operators with connected 3G/4G S9 charging interface

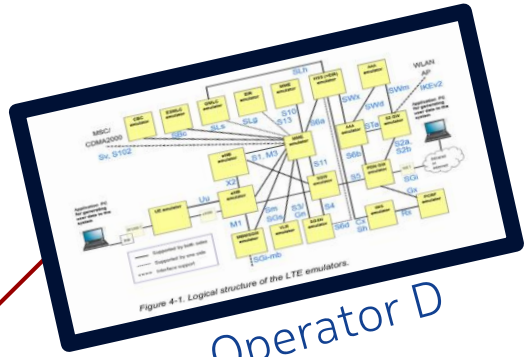


Operator A

S9

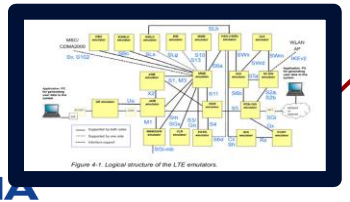
IPX

S9



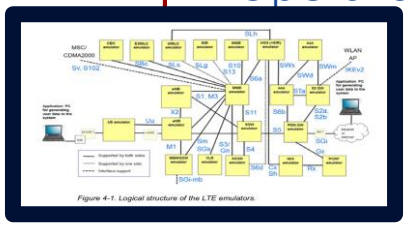
Operator D

S9



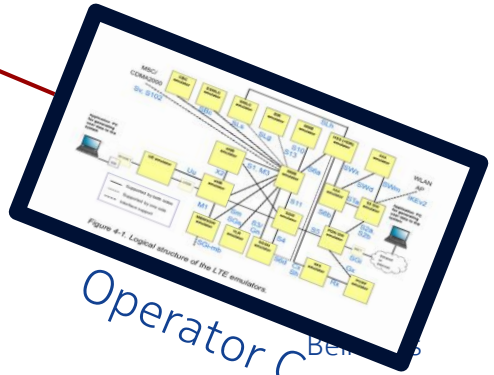
Operator B

S9

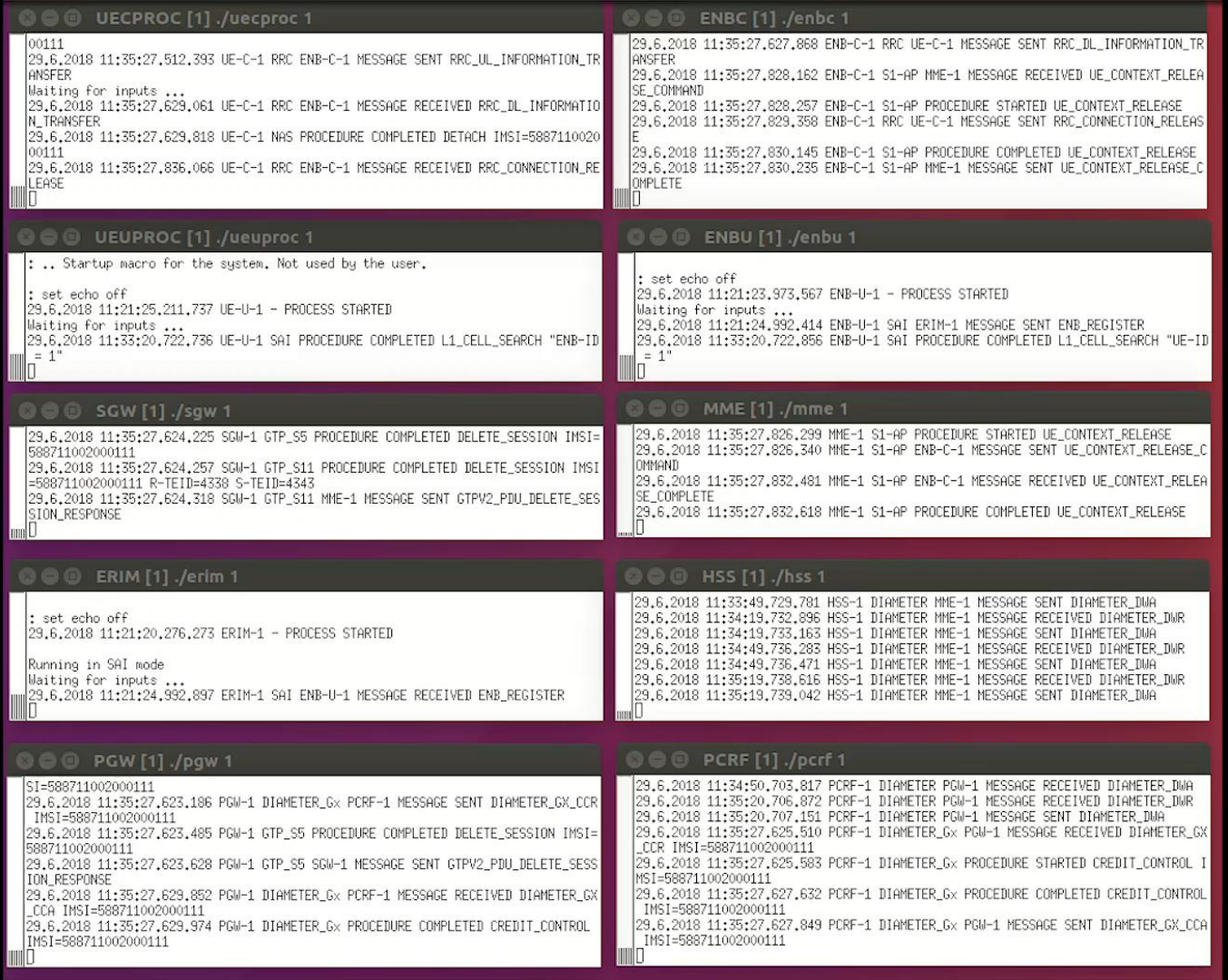


Operator F

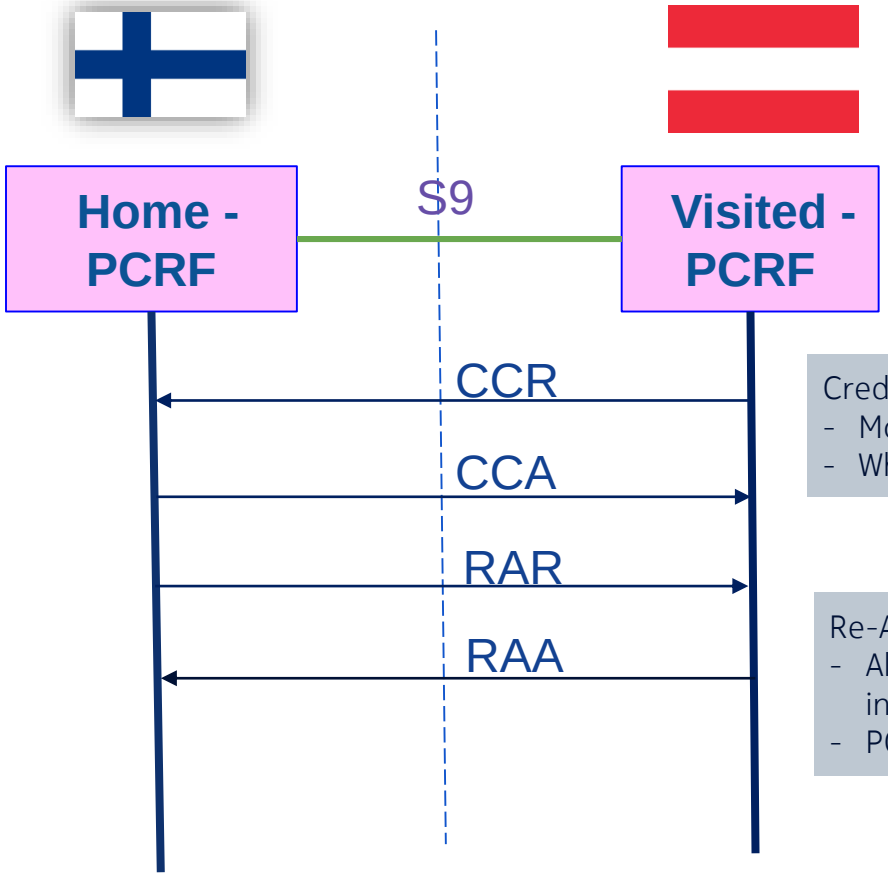
S9



Operator C


UECPROC [1] ./uecproc 1
00111
29.6.2018 11:35:27.512.393 UE-C-1 RRC ENB-C-1 MESSAGE SENT RRC_UL_INFORMATION_TRANSFER
Waiting for inputs ...
29.6.2018 11:35:27.629.061 UE-C-1 RRC ENB-C-1 MESSAGE RECEIVED RRC_DL_INFORMATION_TRANSFER
29.6.2018 11:35:27.629.818 UE-C-1 NAS PROCEDURE COMPLETED DETACH IMSI=588711002000111
29.6.2018 11:35:27.836.066 UE-C-1 RRC ENB-C-1 MESSAGE RECEIVED RRC_CONNECTION_RELEASE
ENBC [1] ./enbc 1
29.6.2018 11:35:27.627.868 ENB-C-1 RRC UE-C-1 MESSAGE SENT RRC_DL_INFORMATION_TRANSFER
29.6.2018 11:35:27.828.162 ENB-C-1 S1-AP MME-1 MESSAGE RECEIVED UE_CONTEXT_RELEASE_COMMAND
29.6.2018 11:35:27.828.257 ENB-C-1 S1-AP PROCEDURE STARTED UE_CONTEXT_RELEASE
29.6.2018 11:35:27.829.358 ENB-C-1 RRC UE-C-1 MESSAGE SENT RRC_CONNECTION_RELEASE
29.6.2018 11:35:27.830.145 ENB-C-1 S1-AP PROCEDURE COMPLETED UE_CONTEXT_RELEASE
29.6.2018 11:35:27.830.235 ENB-C-1 S1-AP MME-1 MESSAGE SENT UE_CONTEXT_RELEASE_COMPLETE
UEUPROC [1] ./ueuproc 1
: .. Startup macro for the system. Not used by the user.
: set echo off
29.6.2018 11:21:25.211.737 UE-U-1 - PROCESS STARTED
Waiting for inputs ...
29.6.2018 11:33:20.722.736 UE-U-1 SAI PROCEDURE COMPLETED L1_CELL_SEARCH "ENB-ID = 1"
ENBU [1] ./enbu 1
: set echo off
29.6.2018 11:21:23.973.567 ENB-U-1 - PROCESS STARTED
Waiting for inputs ...
29.6.2018 11:21:24.992.414 ENB-U-1 SAI ERIM-1 MESSAGE SENT ENB_REGISTER
29.6.2018 11:33:20.722.856 ENB-U-1 SAI PROCEDURE COMPLETED L1_CELL_SEARCH "UE-ID = 1"
SGW [1] ./sgw 1
29.6.2018 11:35:27.624.225 SGW-1 GTP_S5 PROCEDURE COMPLETED DELETE_SESSION IMSI=588711002000111
29.6.2018 11:35:27.624.257 SGW-1 GTP_S11 PROCEDURE COMPLETED DELETE_SESSION IMSI=588711002000111 R-TEID=4338 S-TEID=4343
29.6.2018 11:35:27.624.318 SGW-1 GTP_S11 MME-1 MESSAGE SENT GTPV2_PDU_DELETE_SESSION_RESPONSE
MME [1] ./mme 1
29.6.2018 11:35:27.826.299 MME-1 S1-AP PROCEDURE STARTED UE_CONTEXT_RELEASE
29.6.2018 11:35:27.826.340 MME-1 S1-AP ENB-C-1 MESSAGE SENT UE_CONTEXT_RELEASE_COMMAND
29.6.2018 11:35:27.832.481 MME-1 S1-AP ENB-C-1 MESSAGE RECEIVED UE_CONTEXT_RELEASE_COMPLETE
29.6.2018 11:35:27.832.618 MME-1 S1-AP PROCEDURE COMPLETED UE_CONTEXT_RELEASE
ERIM [1] ./erim 1
: set echo off
29.6.2018 11:21:20.276.273 ERIM-1 - PROCESS STARTED
Running in SAI mode
Waiting for inputs ...
29.6.2018 11:21:24.992.897 ERIM-1 SAI ENB-U-1 MESSAGE RECEIVED ENB_REGISTER
HSS [1] ./hss 1
29.6.2018 11:33:49.729.781 HSS-1 DIAMETER MME-1 MESSAGE SENT DIAMETER_DWA
29.6.2018 11:34:19.732.896 HSS-1 DIAMETER MME-1 MESSAGE RECEIVED DIAMETER_DWR
29.6.2018 11:34:19.733.163 HSS-1 DIAMETER MME-1 MESSAGE SENT DIAMETER_DWA
29.6.2018 11:34:49.736.283 HSS-1 DIAMETER MME-1 MESSAGE RECEIVED DIAMETER_DWR
29.6.2018 11:34:49.736.471 HSS-1 DIAMETER MME-1 MESSAGE SENT DIAMETER_DWA
29.6.2018 11:35:19.738.616 HSS-1 DIAMETER MME-1 MESSAGE RECEIVED DIAMETER_DWR
29.6.2018 11:35:19.739.042 HSS-1 DIAMETER MME-1 MESSAGE SENT DIAMETER_DWA
PGW [1] ./pgw 1
SI=588711002000111
29.6.2018 11:35:27.623.186 PGW-1 DIAMETER_Gx PCRF-1 MESSAGE SENT DIAMETER_GX_CCR IMSI=588711002000111
29.6.2018 11:35:27.623.485 PGW-1 GTP_S5 PROCEDURE COMPLETED DELETE_SESSION IMSI=588711002000111
29.6.2018 11:35:27.623.628 PGW-1 GTP_S5 SGW-1 MESSAGE SENT GTPV2_PDU_DELETE_SESSION_RESPONSE
29.6.2018 11:35:27.629.852 PGW-1 DIAMETER_Gx PCRF-1 MESSAGE RECEIVED DIAMETER_GX_CCA IMSI=588711002000111
29.6.2018 11:35:27.629.974 PGW-1 DIAMETER_Gx PROCEDURE COMPLETED CREDIT_CONTROL IMSI=588711002000111
PCRF [1] ./pcrf 1
29.6.2018 11:34:50.703.817 PCRF-1 DIAMETER PGW-1 MESSAGE RECEIVED DIAMETER_DWA
29.6.2018 11:35:20.706.872 PCRF-1 DIAMETER PGW-1 MESSAGE RECEIVED DIAMETER_DWR
29.6.2018 11:35:20.707.151 PCRF-1 DIAMETER PGW-1 MESSAGE SENT DIAMETER_DWA
29.6.2018 11:35:27.625.510 PCRF-1 DIAMETER_Gx PGW-1 MESSAGE RECEIVED DIAMETER_GX_CCR IMSI=588711002000111
29.6.2018 11:35:27.625.583 PCRF-1 DIAMETER_Gx PROCEDURE STARTED CREDIT_CONTROL IMSI=588711002000111
29.6.2018 11:35:27.627.632 PCRF-1 DIAMETER_Gx PROCEDURE COMPLETED CREDIT_CONTROL IMSI=588711002000111
29.6.2018 11:35:27.627.849 PCRF-1 DIAMETER_Gx PGW-1 MESSAGE SENT DIAMETER_GX_CCA IMSI=588711002000111

Normal incoming request for roaming (Fin in Austria)



Credit Control Request
- Money?
- What kind of service?

Re-Authentication Request
- All kind of control and information
- PCC management

What is a ”PCC”?

Something you all have

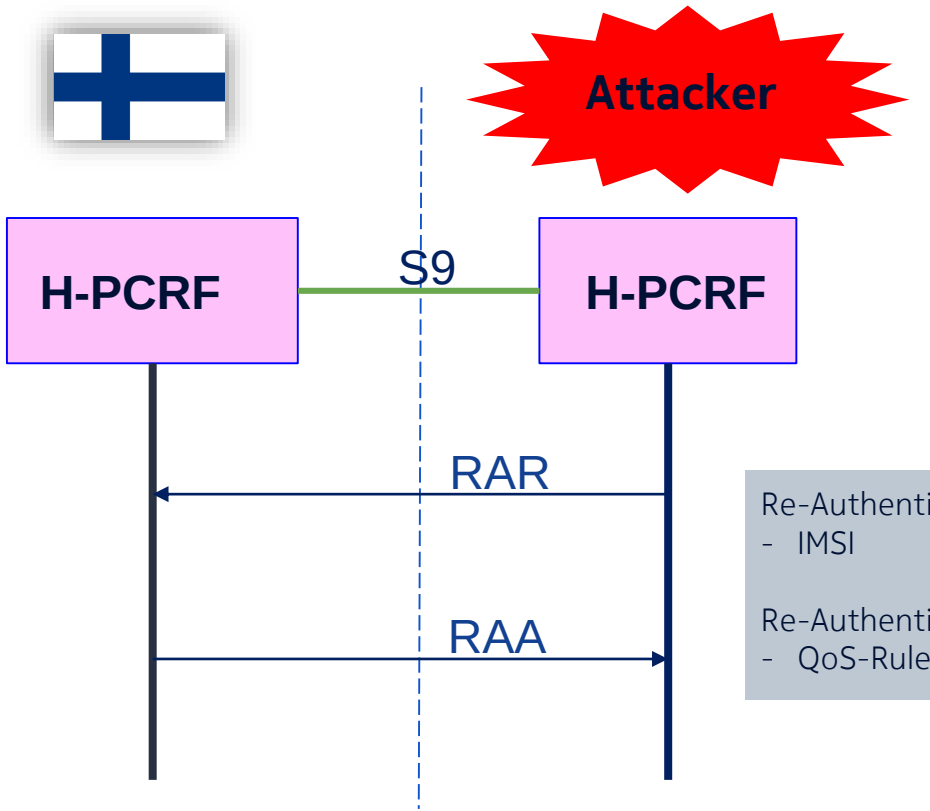
- Policy Charging Control
  - Defines everything about your subsription
  - Data type
  - Data rates
  - Whatever cellular service you can think off
- Defines how to handle you and what to grant you ”service flow filters”
- Usually identified by a string

- My own subscription is company paid and quite ”generous”
  - Perfect target for an attacker

Attack

1. Steal PCC of good subscription
2. Update cheap subscription with PCC of good subscripion

Requesting PCC via RAR (posing as home network)



Re-Authentication Request (RAR)
- IMSI

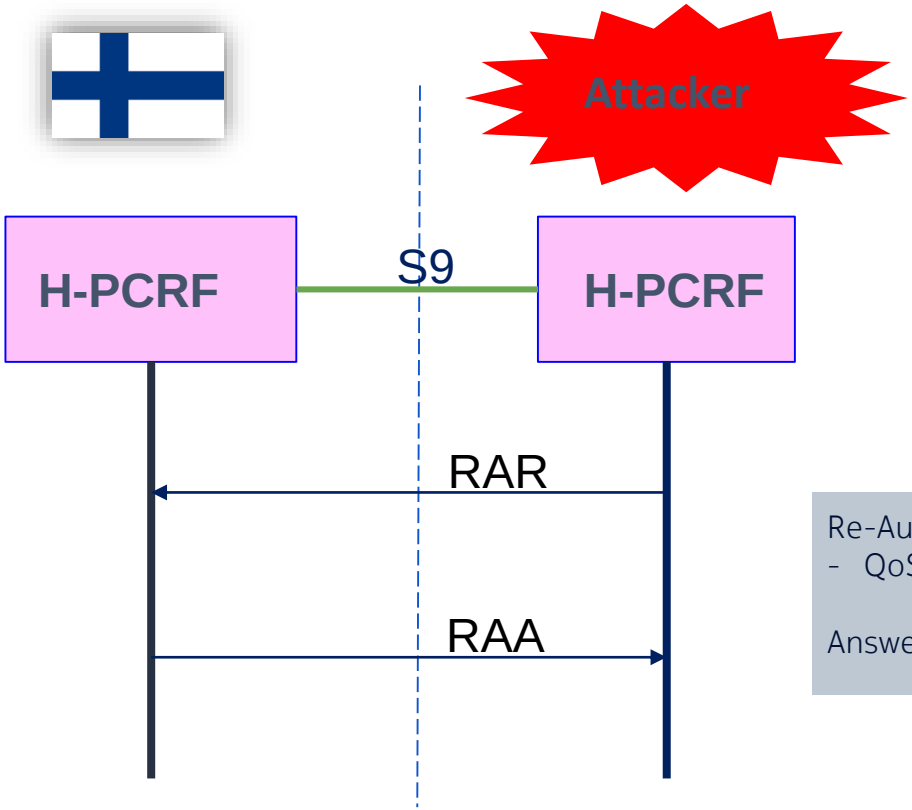
Re-Authentication Answer (RAA)
- QoS-Rule-Install AVP

diameter

No.	Time	Source	Destination	Protocol	Length	Info
365	47.5750…	127.0.0.1	127.0.0.1	DIAMETER	140	cmd=Device-Watchdog Request(280) flags=R--- appl=Diameter Common Messages(0) h2h=7660fed e2e=7660fed |
366	47.5752…	127.0.0.1	127.0.0.1	DIAMETER	152	SACK cmd=Device-Watchdog Request(280) flags=R--- appl=Diameter Common Messages(0) h2h=104b0355 e2e=104b0355 |
381	47.5761…	127.0.0.1	127.0.0.1	DIAMETER	168	SACK cmd=Device-Watchdog Answer(280) flags=---- appl=Diameter Common Messages(0) h2h=104b0355 e2e=104b0355 |
384	47.5765…	127.0.0.1	127.0.0.1	DIAMETER	164	SACK cmd=Device-Watchdog Answer(280) flags=---- appl=Diameter Common Messages(0) h2h=7660fed e2e=7660fed |
679	77.5804…	127.0.0.1	127.0.0.1	DIAMETER	140	cmd=Device-Watchdog Request(280) flags=R--- appl=Diameter Common Messages(0) h2h=7660fee e2e=7660fee |
688	77.5818…	127.0.0.1	127.0.0.1	DIAMETER	164	SACK cmd=Device-Watchdog Answer(280) flags=---- appl=Diameter Common Messages(0) h2h=7660fee e2e=7660fee |
736	81.0369…	127.0.0.1	127.0.0.1	DIAMETER	704	cmd=Re-Auth Request(258) flags=RP-- appl=3GPP Gx(16777238) h2h=104b0356 e2e=104b0356 |
745	81.0440…	127.0.0.1	127.0.0.1	DIAMETER	496	SACK cmd=Re-Auth Answer(258) flags=-P-- appl=3GPP Gx(16777238) h2h=104b0356 e2e=104b0356 |
931	107.598…	127.0.0.1	127.0.0.1	DIAMETER	140	cmd=Device-Watchdog Request(280) flags=R--- appl=Diameter Common Messages(0) h2h=7660fef e2e=7660fef |
940	107.599…	127.0.0.1	127.0.0.1	DIAMETER	164	SACK cmd=Device-Watchdog Answer(280) flags=---- appl=Diameter Common Messages(0) h2h=7660fef e2e=7660fef |
11…	137.631…	127.0.0.1	127.0.0.1	DIAMETER	136	cmd=Device-Watchdog Request(280) flags=R--- appl=Diameter Common Messages(0) h2h=104b0357 e2e=104b0357 |
11…	137.632…	127.0.0.1	127.0.0.1	DIAMETER	156	SACK cmd=Device-Watchdog Request(280) flags=R--- appl=Diameter Common Messages(0) h2h=7660ff0 e2e=7660ff0 |
12…	137.636…	127.0.0.1	127.0.0.1	DIAMETER	164	SACK cmd=Device-Watchdog Answer(280) flags=---- appl=Diameter Common Messages(0) h2h=7660ff0 e2e=7660ff0 |
12…	137.636…	127.0.0.1	127.0.0.1	DIAMETER	168	SACK cmd=Device-Watchdog Answer(280) flags=---- appl=Diameter Common Messages(0) h2h=104b0357 e2e=104b0357 |

```
▸ Frame 679: 140 bytes on wire (1120 bits), 140 bytes captured (1120 bits) on interface 0
▸ Linux cooked capture
▸ Internet Protocol Version 4, Src: 127.0.0.1, Dst: 127.0.0.1
▸ Stream Control Transmission Protocol, Src Port: 3868 (3868), Dst Port: 35002 (35002)
▾ Diameter Protocol
    Version: 0x01
    Length: 76
  ▸ Flags: 0x80, Request
    Command Code: 280 Device-Watchdog
    ApplicationId: Diameter Common Messages (0)
    Hop-by-Hop Identifier: 0x07660fee
    End-to-End Identifier: 0x07660fee
    [Answer In: 688]
  ▸ AVP: Origin-Host(264) l=22 f=-M- val=pgw.le.nsn.com
  ▸ AVP: Origin-Realm(296) l=18 f=-M- val=le.nsn.com
  ▸ AVP: Origin-State-Id(278) l=12 f=-M- val=1530264682
```

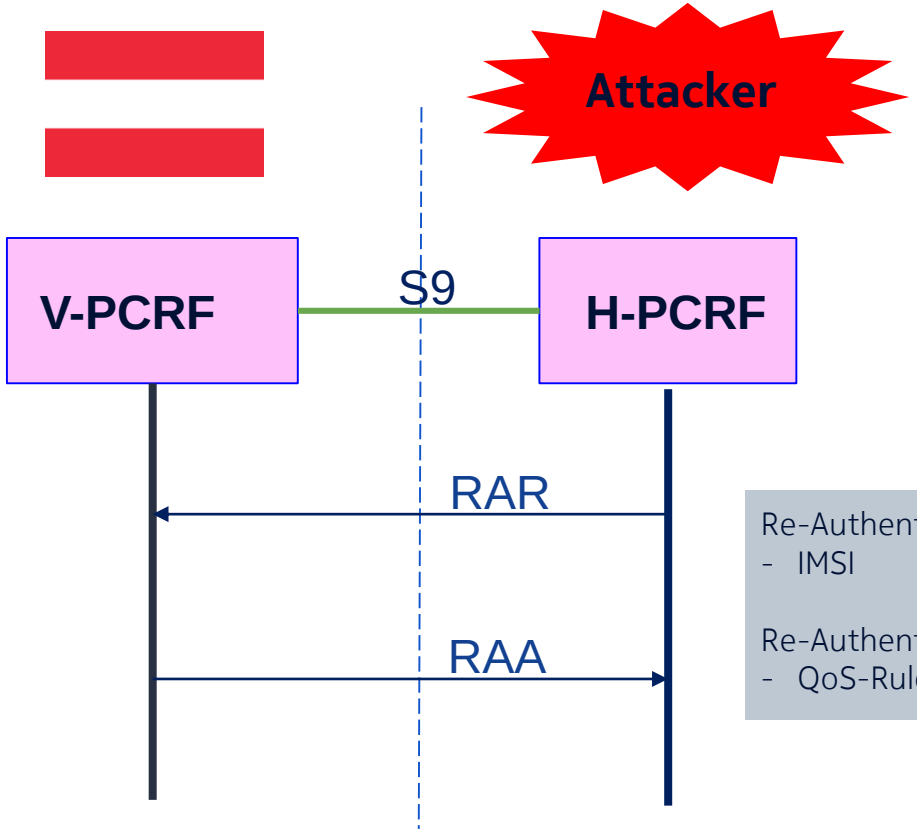
Attack Scenario 1: Putting PCC via RAR (posing as home network)



Re-Authentication Request
- QoS-Rule-Install

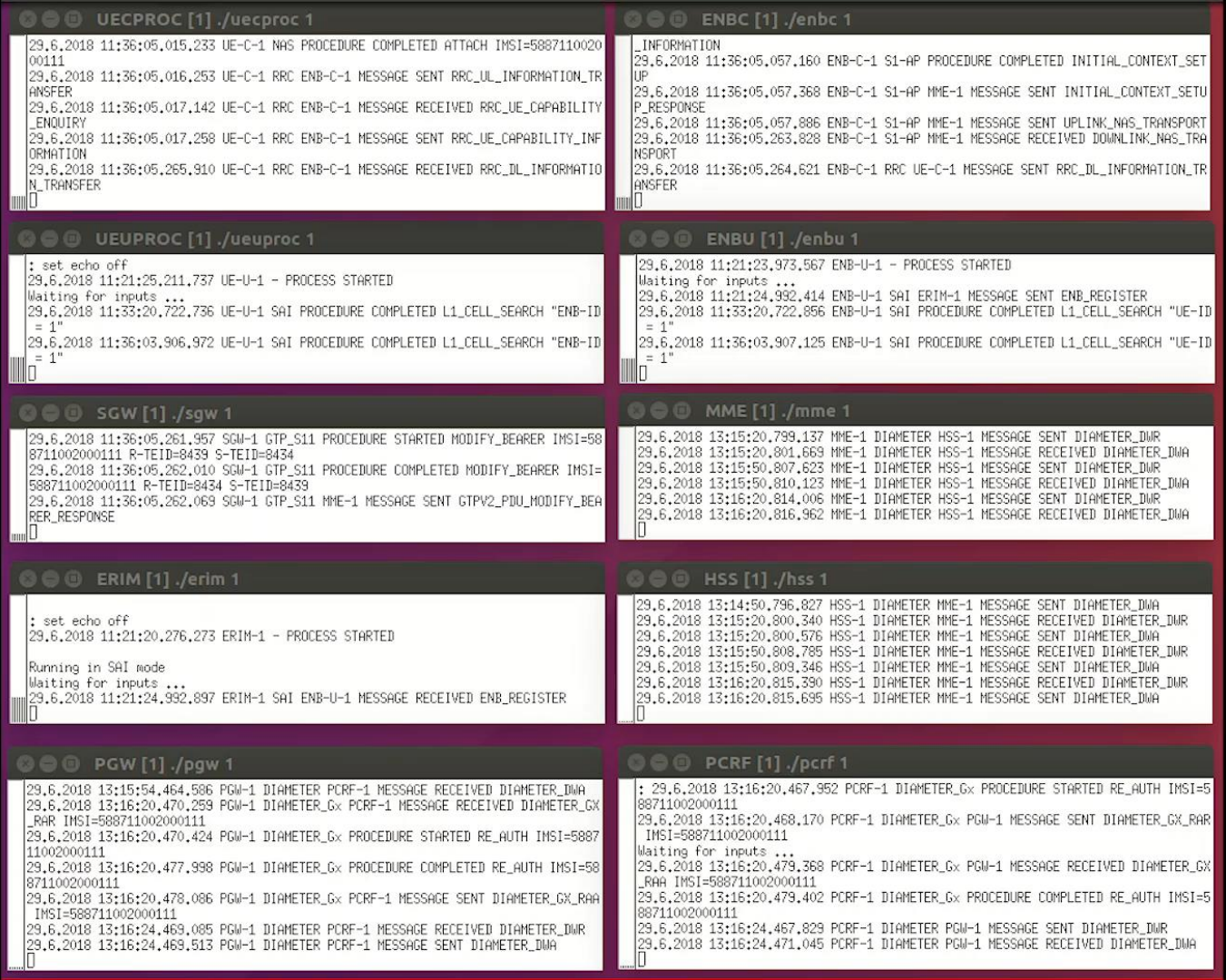
Answer does not matter

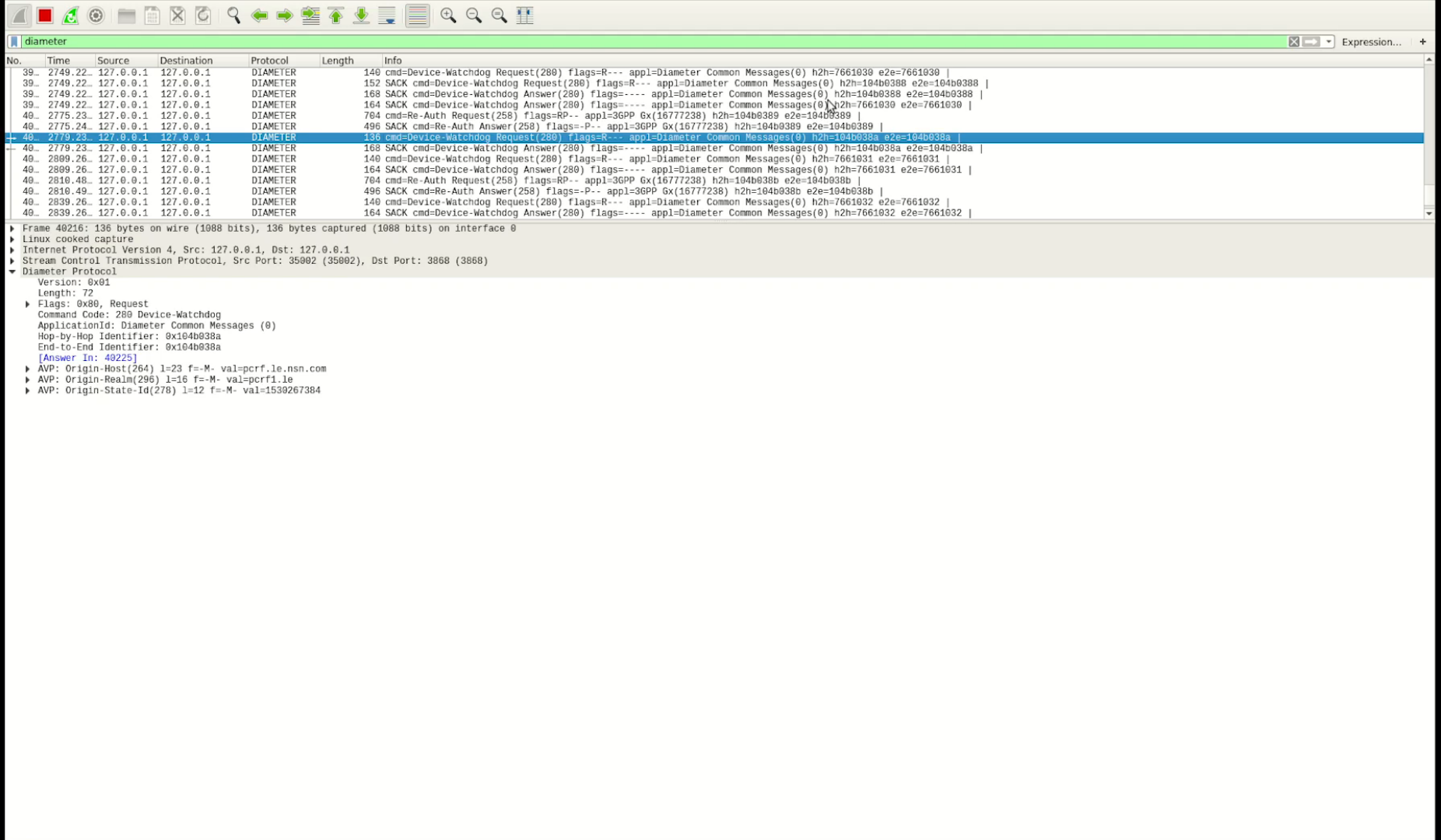
Attack Scenario 2: Putting PCC via RAR to outgoing roamer



Re-Authentication Request (RAR)
- IMSI

Re-Authentication Answer (RAA)
- QoS-Rule-Install AVP


UECPROC [1] ./uecproc 1
29.6.2018 11:36:05.015.233 UE-C-1 NAS PROCEDURE COMPLETED ATTACH IMSI=588711002000111
29.6.2018 11:36:05.016.253 UE-C-1 RRC ENB-C-1 MESSAGE SENT RRC_UL_INFORMATION_TRANSFER
29.6.2018 11:36:05.017.142 UE-C-1 RRC ENB-C-1 MESSAGE RECEIVED RRC_UE_CAPABILITY_ENQUIRY
29.6.2018 11:36:05.017.258 UE-C-1 RRC ENB-C-1 MESSAGE SENT RRC_UE_CAPABILITY_INFORMATION
29.6.2018 11:36:05.265.910 UE-C-1 RRC ENB-C-1 MESSAGE RECEIVED RRC_DL_INFORMATION_TRANSFER
ENBC [1] ./enbc 1
_INFORMATION
29.6.2018 11:36:05.057.160 ENB-C-1 S1-AP PROCEDURE COMPLETED INITIAL_CONTEXT_SETUP
29.6.2018 11:36:05.057.368 ENB-C-1 S1-AP MME-1 MESSAGE SENT INITIAL_CONTEXT_SETUP_RESPONSE
29.6.2018 11:36:05.057.886 ENB-C-1 S1-AP MME-1 MESSAGE SENT UPLINK_NAS_TRANSPORT
29.6.2018 11:36:05.263.828 ENB-C-1 S1-AP MME-1 MESSAGE RECEIVED DOWNLINK_NAS_TRANSPORT
29.6.2018 11:36:05.264.621 ENB-C-1 RRC UE-C-1 MESSAGE SENT RRC_DL_INFORMATION_TRANSFER
UEUPROC [1] ./ueuproc 1
: set echo off
29.6.2018 11:21:25.211.737 UE-U-1 - PROCESS STARTED
Waiting for inputs ...
29.6.2018 11:33:20.722.736 UE-U-1 SAI PROCEDURE COMPLETED L1_CELL_SEARCH "ENB-ID = 1"
29.6.2018 11:36:03.906.972 UE-U-1 SAI PROCEDURE COMPLETED L1_CELL_SEARCH "ENB-ID = 1"
ENBU [1] ./enbu 1
29.6.2018 11:21:23.973.567 ENB-U-1 - PROCESS STARTED
Waiting for inputs ...
29.6.2018 11:21:24.992.414 ENB-U-1 SAI ERIM-1 MESSAGE SENT ENB_REGISTER
29.6.2018 11:33:20.722.856 ENB-U-1 SAI PROCEDURE COMPLETED L1_CELL_SEARCH "UE-ID = 1"
29.6.2018 11:36:03.907.125 ENB-U-1 SAI PROCEDURE COMPLETED L1_CELL_SEARCH "UE-ID = 1"
SGW [1] ./sgw 1
29.6.2018 11:36:05.261.957 SGW-1 GTP_S11 PROCEDURE STARTED MODIFY_BEARER IMSI=588711002000111 R-TEID=8439 S-TEID=8434
29.6.2018 11:36:05.262.010 SGW-1 GTP_S11 PROCEDURE COMPLETED MODIFY_BEARER IMSI=588711002000111 R-TEID=8434 S-TEID=8439
29.6.2018 11:36:05.262.069 SGW-1 GTP_S11 MME-1 MESSAGE SENT GTPV2_PDU_MODIFY_BEARER_RESPONSE
MME [1] ./mme 1
29.6.2018 13:15:20.799.137 MME-1 DIAMETER HSS-1 MESSAGE SENT DIAMETER_DWR
29.6.2018 13:15:20.801.669 MME-1 DIAMETER HSS-1 MESSAGE RECEIVED DIAMETER_DWA
29.6.2018 13:15:50.807.623 MME-1 DIAMETER HSS-1 MESSAGE SENT DIAMETER_DWR
29.6.2018 13:15:50.810.123 MME-1 DIAMETER HSS-1 MESSAGE RECEIVED DIAMETER_DWA
29.6.2018 13:16:20.814.006 MME-1 DIAMETER HSS-1 MESSAGE SENT DIAMETER_DWR
29.6.2018 13:16:20.816.962 MME-1 DIAMETER HSS-1 MESSAGE RECEIVED DIAMETER_DWA
ERIM [1] ./erim 1
: set echo off
29.6.2018 11:21:20.276.273 ERIM-1 - PROCESS STARTED
Running in SAI mode
Waiting for inputs ...
29.6.2018 11:21:24.992.897 ERIM-1 SAI ENB-U-1 MESSAGE RECEIVED ENB_REGISTER
HSS [1] ./hss 1
29.6.2018 13:14:50.796.827 HSS-1 DIAMETER MME-1 MESSAGE SENT DIAMETER_DWA
29.6.2018 13:15:20.800.340 HSS-1 DIAMETER MME-1 MESSAGE RECEIVED DIAMETER_DWR
29.6.2018 13:15:20.800.576 HSS-1 DIAMETER MME-1 MESSAGE SENT DIAMETER_DWA
29.6.2018 13:15:50.808.785 HSS-1 DIAMETER MME-1 MESSAGE RECEIVED DIAMETER_DWR
29.6.2018 13:15:50.809.346 HSS-1 DIAMETER MME-1 MESSAGE SENT DIAMETER_DWA
29.6.2018 13:16:20.815.390 HSS-1 DIAMETER MME-1 MESSAGE RECEIVED DIAMETER_DWR
29.6.2018 13:16:20.815.695 HSS-1 DIAMETER MME-1 MESSAGE SENT DIAMETER_DWA
PGW [1] ./pgw 1
29.6.2018 13:15:54.464.586 PGW-1 DIAMETER PCRF-1 MESSAGE RECEIVED DIAMETER_DWA
29.6.2018 13:16:20.470.259 PGW-1 DIAMETER_Gx PCRF-1 MESSAGE RECEIVED DIAMETER_GX_RAR IMSI=588711002000111
29.6.2018 13:16:20.470.424 PGW-1 DIAMETER_Gx PROCEDURE STARTED RE_AUTH IMSI=588711002000111
29.6.2018 13:16:20.477.998 PGW-1 DIAMETER_Gx PROCEDURE COMPLETED RE_AUTH IMSI=588711002000111
29.6.2018 13:16:20.478.086 PGW-1 DIAMETER_Gx PCRF-1 MESSAGE SENT DIAMETER_GX_RAA IMSI=588711002000111
29.6.2018 13:16:24.469.085 PGW-1 DIAMETER PCRF-1 MESSAGE RECEIVED DIAMETER_DWR
29.6.2018 13:16:24.469.513 PGW-1 DIAMETER PCRF-1 MESSAGE SENT DIAMETER_DWA
PCRF [1] ./pcrf 1
: 29.6.2018 13:16:20.467.952 PCRF-1 DIAMETER_Gx PROCEDURE STARTED RE_AUTH IMSI=588711002000111
29.6.2018 13:16:20.468.170 PCRF-1 DIAMETER_Gx PGW-1 MESSAGE SENT DIAMETER_GX_RAR IMSI=588711002000111
Waiting for inputs ...
29.6.2018 13:16:20.479.368 PCRF-1 DIAMETER_Gx PGW-1 MESSAGE RECEIVED DIAMETER_GX_RAA IMSI=588711002000111
29.6.2018 13:16:20.479.402 PCRF-1 DIAMETER_Gx PROCEDURE COMPLETED RE_AUTH IMSI=588711002000111
29.6.2018 13:16:24.467.829 PCRF-1 DIAMETER PGW-1 MESSAGE SENT DIAMETER_DWR
29.6.2018 13:16:24.471.045 PCRF-1 DIAMETER PGW-1 MESSAGE RECEIVED DIAMETER_DWA


diameter
Expression...
No. Time Source Destination Protocol Length Info
39… 2749.22… 127.0.0.1 127.0.0.1 DIAMETER 140 cmd=Device-Watchdog Request(280) flags=R--- appl=Diameter Common Messages(0) h2h=7661030 e2e=7661030 |
39… 2749.22… 127.0.0.1 127.0.0.1 DIAMETER 152 SACK cmd=Device-Watchdog Request(280) flags=R--- appl=Diameter Common Messages(0) h2h=104b0388 e2e=104b0388 |
39… 2749.22… 127.0.0.1 127.0.0.1 DIAMETER 168 SACK cmd=Device-Watchdog Answer(280) flags=---- appl=Diameter Common Messages(0) h2h=104b0388 e2e=104b0388 |
39… 2749.22… 127.0.0.1 127.0.0.1 DIAMETER 164 SACK cmd=Device-Watchdog Answer(280) flags=---- appl=Diameter Common Messages(0) h2h=7661030 e2e=7661030 |
40… 2775.23… 127.0.0.1 127.0.0.1 DIAMETER 704 cmd=Re-Auth Request(258) flags=RP-- appl=3GPP Gx(16777238) h2h=104b0389 e2e=104b0389 |
40… 2775.24… 127.0.0.1 127.0.0.1 DIAMETER 496 SACK cmd=Re-Auth Answer(258) flags=-P-- appl=3GPP Gx(16777238) h2h=104b0389 e2e=104b0389 |
40… 2779.23… 127.0.0.1 127.0.0.1 DIAMETER 136 cmd=Device-Watchdog Request(280) flags=R--- appl=Diameter Common Messages(0) h2h=104b038a e2e=104b038a |
40… 2779.23… 127.0.0.1 127.0.0.1 DIAMETER 168 SACK cmd=Device-Watchdog Answer(280) flags=---- appl=Diameter Common Messages(0) h2h=104b038a e2e=104b038a |
40… 2809.26… 127.0.0.1 127.0.0.1 DIAMETER 140 cmd=Device-Watchdog Request(280) flags=R--- appl=Diameter Common Messages(0) h2h=7661031 e2e=7661031 |
40… 2809.26… 127.0.0.1 127.0.0.1 DIAMETER 164 SACK cmd=Device-Watchdog Answer(280) flags=---- appl=Diameter Common Messages(0) h2h=7661031 e2e=7661031 |
40… 2810.48… 127.0.0.1 127.0.0.1 DIAMETER 704 cmd=Re-Auth Request(258) flags=RP-- appl=3GPP Gx(16777238) h2h=104b038b e2e=104b038b |
40… 2810.49… 127.0.0.1 127.0.0.1 DIAMETER 496 SACK cmd=Re-Auth Answer(258) flags=-P-- appl=3GPP Gx(16777238) h2h=104b038b e2e=104b038b |
40… 2839.26… 127.0.0.1 127.0.0.1 DIAMETER 140 cmd=Device-Watchdog Request(280) flags=R--- appl=Diameter Common Messages(0) h2h=7661032 e2e=7661032 |
40… 2839.26… 127.0.0.1 127.0.0.1 DIAMETER 164 SACK cmd=Device-Watchdog Answer(280) flags=---- appl=Diameter Common Messages(0) h2h=7661032 e2e=7661032 |
Frame 40216: 136 bytes on wire (1088 bits), 136 bytes captured (1088 bits) on interface 0
Linux cooked capture
Internet Protocol Version 4, Src: 127.0.0.1, Dst: 127.0.0.1
Stream Control Transmission Protocol, Src Port: 35002 (35002), Dst Port: 3868 (3868)
Diameter Protocol
Version: 0x01
Length: 72
Flags: 0x80, Request
Command Code: 280 Device-Watchdog
ApplicationId: Diameter Common Messages (0)
Hop-by-Hop Identifier: 0x104b038a
End-to-End Identifier: 0x104b038a
[Answer In: 40225]
AVP: Origin-Host(264) l=23 f=-M- val=pcrf.le.nsn.com
AVP: Origin-Realm(296) l=16 f=-M- val=pcrf1.le
AVP: Origin-State-Id(278) l=12 f=-M- val=1530267384

Before and After

:RaaChargingRuleBaseName1_1	rulebasename-11
:RaaChargingRuleBaseName1_2	rulebasename-12
:RaaChargingRuleBaseName2_1	rulebasename-21
:RaaChargingRuleBaseName2_2	rulebasename-22
:RaaChargingRuleName1_1	\7063632d31
:RaaChargingRuleName1_2	\7063632d32
:RaaChargingRuleName2_1	\7063632d33
:RaaChargingRuleName2_2	\7063632d34

:RaaChargingRuleBaseName1_1	rulebasename-11
:RaaChargingRuleBaseName1_2	rulebasename-12
:RaaChargingRuleBaseName2_1	rulebasename-21
:RaaChargingRuleBaseName2_2	rulebasename-22
:RaaChargingRuleName1_1	\7063632d31
:RaaChargingRuleName1_2	\7063632d31
:RaaChargingRuleName2_1	\7063632d31
:RaaChargingRuleName2_2	\7063632d31

Countermeasures for 2G/3G/4G (reality is never easy….)

Detect Monitor network traffic Penetration & re-testing Tenant monitoring	**Mitigate** GSMA IR88,FS.11,FS.19,FS.07 Signaling & IP Firewall SMS Home Routing
Cooperate Share experiences (GSMA) Business rules / contracts Cooperation with legislators	**Prepare** Budget, policies & plans Layered / Zoned Security Node hardening/procedures

What about 5G Core Network?

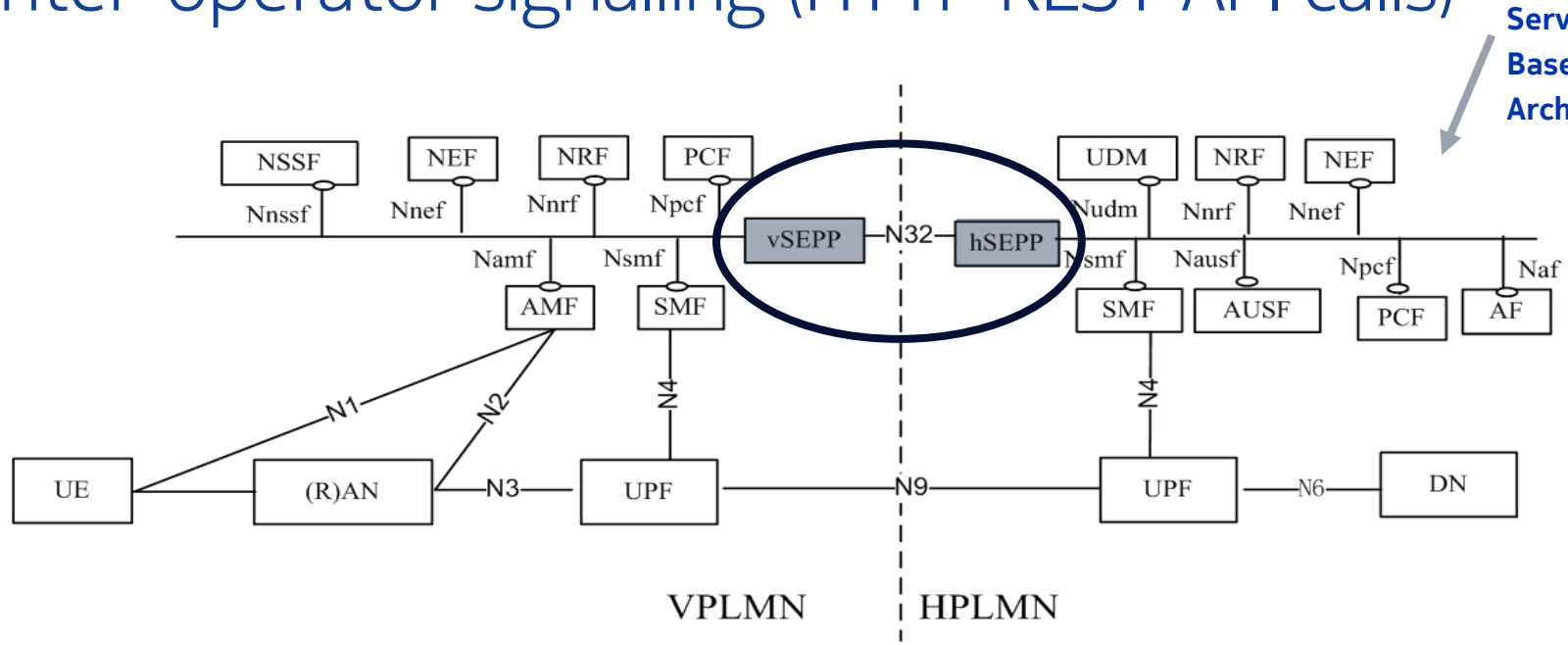
Work ahead

Security is a road

- 5G protects user privacy on the air interface
  - Various protections against false base stations
- Unified security standards also for non-cellular access
- 5G Standards have introduced a new security proxy for roaming
- Security functionalities can now be virtualized
- Steering of roaming can be used to guide users to the best partners

- **Security is more then standards & functions!**

Inter-operator signalling (HTTP REST API calls)

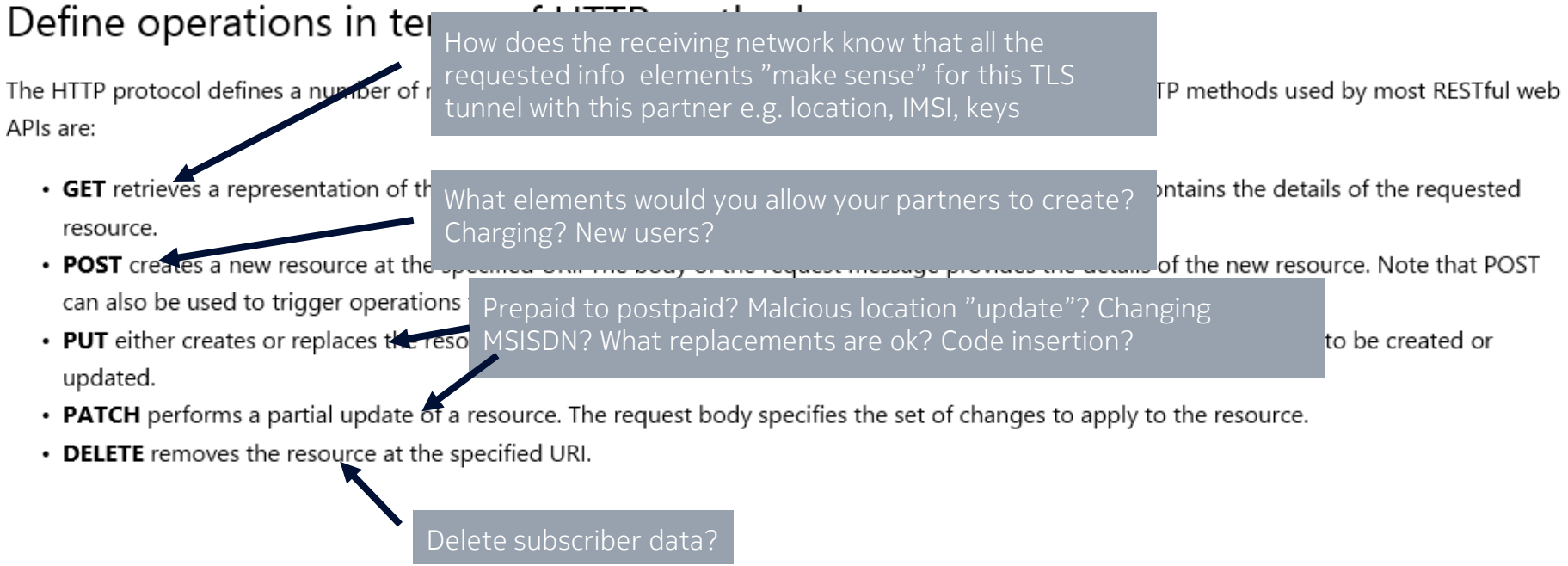


- A SEPP is a non-transparent proxy on the roaming, inter-PLMN interfaces.
- A SEPP validates, modifies, and protects every HTTP packet sent between two roaming partners' SBA Network Functions (NFs).

SEPP: Security Edge Protection Proxy

38

REST API – Authentication vs Authorization?



Who is allowed to do what?
Security requires configurations & policies!

Rogue partner node

Talking to your main database

Is doing ”something”

Each NF Service Consumer accessing the UDR, via Nudr, shall be able to add, modify, update or delete only the data it is authorised to change. This authorisation shall be performed by the UDR on a per data set and NF service consumer basis and potentially on a per UE, subscription granularity.

And you have to check in the node, if he is allowed to do that

The following data in the UDR sets exposed via Nudr to the respective NF service consumer and stored shall be standardized:

Fraud? Location tracking?

- Subscription Data,

Fraud?

- Policy Data,

Data interception?

- Structured Data for exposure,
- Application data: Packet Flow Descriptions (PFDs) for application detection and AF request information for multiple UEs, as defined in clause 5.6.7.

Rest API – Vulnerabilities are "known"

Welcome to the Internet

There are **164** CVE entries that match your search.

Name	Description
CVE-2018-9843	The REST API in CyberArk Password Vault Web Access before 9.9.5 and 10.x before 10.1 allows remote attackers to execute arbitrary code via a serialized .NET object in an Authorization HTTP header.
CVE-2018-8849	Medtronic N'Vision Clinician Programmer 8840 N'Vision Clinician Programmer, all versions, and 8870 N'Vision removable Application Card, all versions does not encrypt PII and P
CVE-2018-7272	The REST APIs in ForgeRock AM before 5.5.0 include SSOToken IDs as part of the URL, which allows attackers to obtain sensitive information by finding an ID value in a log file.
CVE-2018-5955	An issue was discovered in GitStack through 2.3.10. User controlled input is not sufficiently filtered, allowing an unauthenticated attacker to add a user to the server via the user
CVE-2018-5261	An issue was discovered in Flexense DiskBoss 8.8.16 and earlier. Due to the usage of plaintext information from the handshake as input for the encryption key used for the encr disclose sensitive information, such as the authentication credentials, to any man-in-the-middle (MITM) listener.
CVE-2018-1327	The Apache Struts REST Plugin is using XStream library which is vulnerable and allow perform a DoS attack when using a malicious request with specially crafted XML payload. Upgrade to the Apache Struts version 2.5 switch to an optional Jackson XML handler as described here http://struts.apache.org/plugins/rest/#custom-contenttypehandlers. Another option is to implement a custom XML handler based on the Jackson XML hand Apache Struts 2.5.16.
CVE-2018-1291	Apache Fineract 1.0.0, 0.6.0-incubating, 0.5.0-incubating, 0.4.0-incubating exposes different REST end points to query domain specific entities with a Query Parameter 'orderBy' which are appended directly with SQL statements. A hacker/user can inject/draft the 'orderBy' query parameter by way of the "order" param in such a way to read/update the data for which he doesn't have authorization.
CVE-2018-1289	In Apache Fineract versions 1.0.0, 0.6.0-incubating, 0.5.0-incubating, 0.4.0-incubating, the system exposes different REST end points to query domain specific entities with a Query Parameter 'orderBy' and 'sortOrder' which are appended directly with SQL statements. A hacker/user can inject/draft the 'orderBy' and 'sortOrder' query parameter in such a way to read/update the data for which he doesn't have authorization.
CVE-2018-1274	Spring Data Commons, versions 1.13 to 1.13.10, 2.0 to 2.0.5, and older unsupported versions, contain a property path parser vulnerability caused by unlimited resource allocation. An unauthenticated remote malicious user (or attacker) can issue requests against Spring Data REST endpoints or endpoints using property path parsing which can cause a denial of service (CPU and memory consumption).
CVE-2018-1273	Spring Data Commons, versions prior to 1.13 to 1.13.10, 2.0 to 2.0.5, and older unsupported versions, contain a property binder vulnerability caused by improper neutralization of special elements. An unauthenticated remote malicious user (or attacker) can supply specially crafted request parameters against Spring Data REST backed HTTP resources or using Spring Data's projection-based request payload binding hat can lead to a remote code execution attack.
CVE-2018-1086	pcs before versions 0.9.164 and 0.10 is vulnerable to a debug parameter r service did not properly remove the pcs debug argument from the /run_pcs query, possibly disclosing sensitive information. A remote attacker with a valid token could use this flaw to ele
CVE-2018-1079	pcs before version 0.9.164 and 0.10 is vulnerable to a privilege escalation e REST interface of the pcsd service did not properly sanitize the file name from the /remote/put_file query. If the /etc/booth directory exists, an authenticated attacker with write permi es with arbitrary data outside of the /etc/booth directory, in the context of the pcsd process.
CVE-2018-10732	The REST API in Dataiku DSS before 4.2.3 allows remote attackers to obtain sensitive information (i.e., determine if a username is valid) because of profile pictures visibility.
CVE-2018-0245	A vulnerability in the REST API of Cisco 5500 and 8500 Series Wireless LAN Controller (WLC) Software could allow an unauthenticated, remote attacker to view system information that under normal circumstances should be prohibited. The vulnerability is due to incomplete input and validation checking mechanisms in the REST API URL request. An attacker could exploit this vulnerability by sending a malicious URL to the REST API. If successful, an exploit could allow the attacker to view sensitive system information. Cisco Bug IDs: CSCvg89442.
CVE-2018-0195	A vulnerability in the Cisco IOS XE Software REST API could allow an authenticated, remote attacker to bypass API authorization checks and use the API to perform privileged actions on an affected device. The vulnerability is due to insufficient authorization checks for requests that are sent to the REST API of the affected software. An attacker could exploit this vulnerability by sending a malicious request to an affected device via the REST API. A successful exploit could allow the attacker to selectively bypass authorization checks for the REST API of the affected software and use the API to perform privileged actions on an affected device. Cisco Bug IDs: CSCuz56428.
CVE-2018-0089	A vulnerability in the Policy and Charging Rules Function (PCRF) of the Cisco Policy Suite (CPS) could allow an unauthenticated, remote attacker to access sensitive data. The attacker c nduct additional reconnaissance attacks. The attacker would also have to have access to the internal VLAN where CPS is deployed. The vulnerability is due to incorrect permissions of certain system file g sensitive data that is at rest. An attacker could exploit the vulnerability by using certain tools available on the internal network interface to request and view system files. An exploit could allow the at rmation about the application. Cisco Bug IDs: CSCvf77666.

Remote code execution

Data stealing, authorization fail

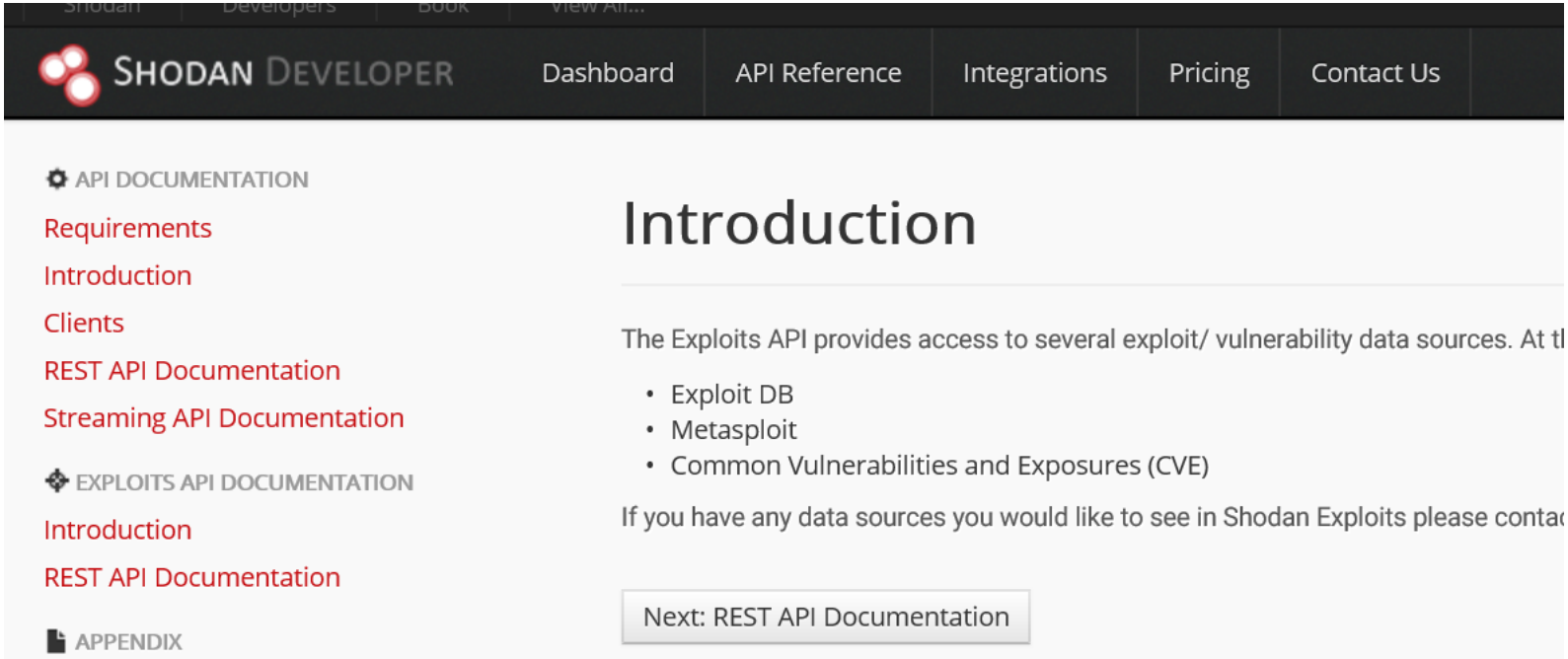
DoS

DoS Network? Priviledge escalation

Fraud, data theft

NOKIA Bell Labs

Will the vulnerable nodes be found?
Not will, only when and how fast is the question



Pay attention to little details - configurations…..

36.81.253.247

City	**Krembangan Selatan**
Country	**Indonesia**
Organization	
ISP	
Last Update	**2018-06-01T06:31:29.820574**
ASN	**AS7713**

Ports

1883 8081

Services

1883 tcp mqtt

```
MQTT Connection Code: 0

Topics:
/mne/alarm
```

8081 tcp https-simple-new

```
HTTP/1.0 200 OK
Content-Type: application/jso
Content-Length: 35
Access-Control-Allow-Origin: *
Access-Control-Allow-Headers: Content-Type,Authorization
Access-Control-Allow-Methods: GET,PUT,POST,DELETE,OPTIONS
Server: Werkzeug/0.11.2 Python/2.7.14
Date: Fri, 01 Jun 2018 06:30:45 GMT

{
    "info": "PUSPA-KS RestApi"
}
```

the requested resource allows sharing with every origin. This basically means that any site can send an request and access the server's response

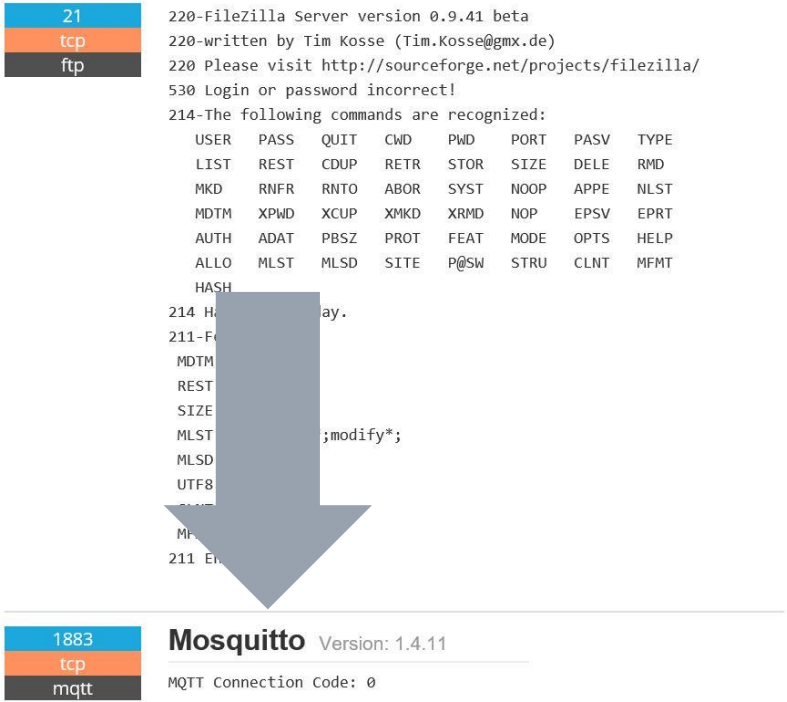
Supports info pulling, info putting and deletion

That is the software + version they use

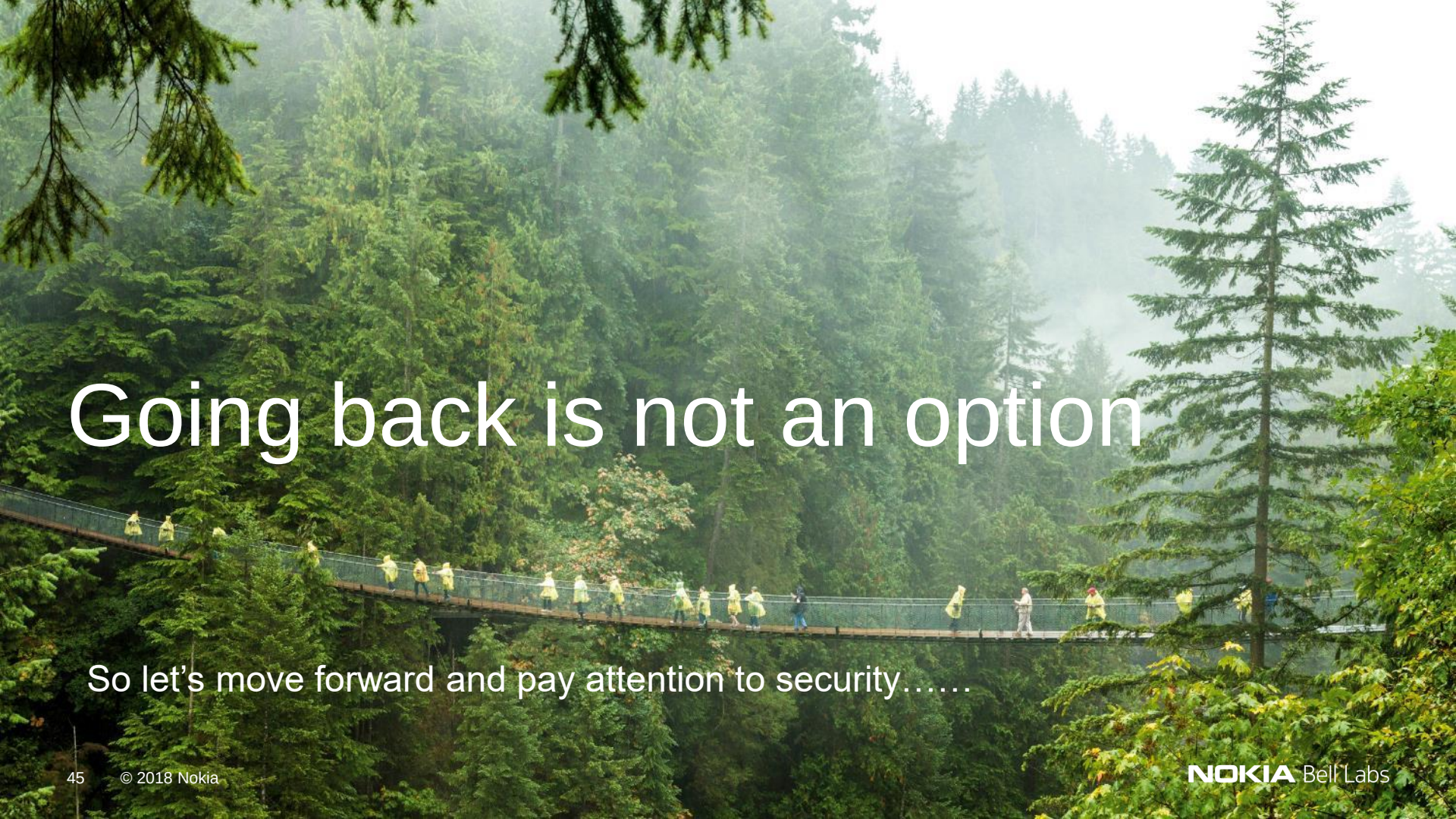
They support RestAPI

Somebody paid attention to the details
But not the right persons….

ISP	[redacted]
Last Update	2018-06-12T18:28:43.543584
ASN	AS7713



NOKIA Bell Labs



Going back is not an option

So let’s move forward and pay attention to security……

Security is a road 5G – To Do List

- Production Security Testing
  - Software composition sec analysis
  - Code sec review
  - Port scanning / vuln scan
  - Web app / OWASP sec scan
  - Robustness testing (fuzzy)
  - DoS testing

- Preparedness
  - Incident response plans
  - Network segmentation and zoning (FWs)
  - Patching plan / contract with vendor
  - Keep up to date (GSMA)

- Deployment & Operation
  - Authorization internally
  - Authorization settings with partners
    - Who is allowed to send what messages / recevie what information (conversion contracts -> access control)
  - Clean ”IT” housekeeping
    - Internal / external DNS
    - Separation of roamers and own
    - Only the right ports / interfaces open
- Validation & Lifecycle
  - PenTesting to see if things really hold (regularly as things change)
  - Algorithm retirement
  - Deployment change, when things change (employee leaves company, partner contract ends etc)

Thanks to
EU SCOTT Project for funding part of this research

Silke.Holtmanns@nokia.com

Let’s go swimming
Questions…

NOKIA