4G - Who is paying your cellular phone bill?

Silke Hoffmanns
Isha Singh
Nokia Bell Labs

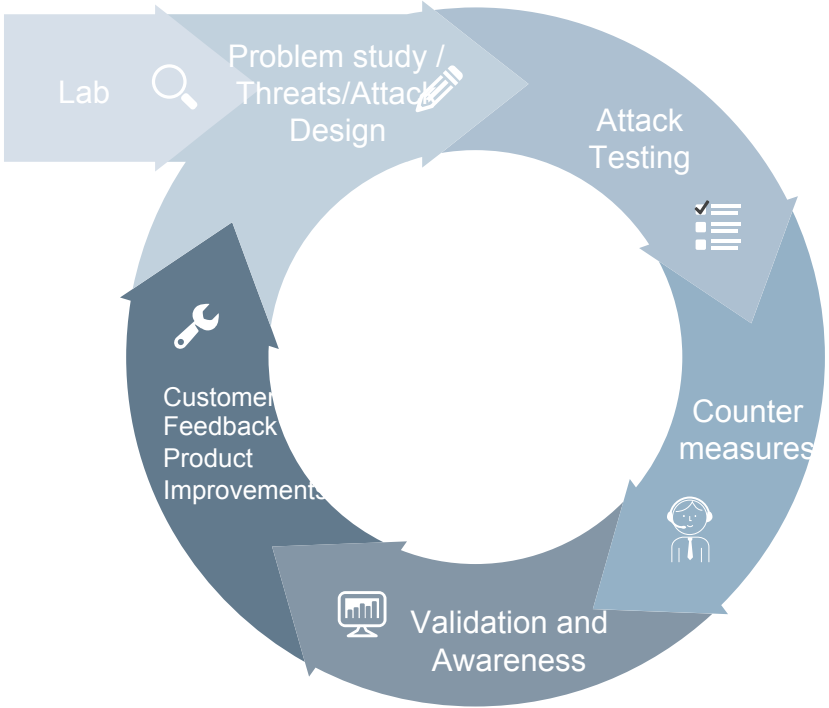
Industrial Security Research?

Nokia Bell Labs – Future Attacks and Mitigation

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

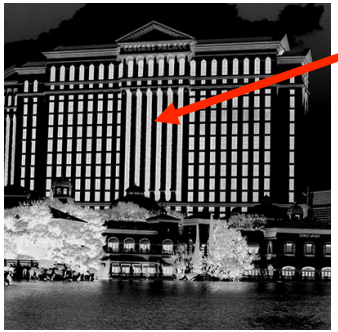
- Theoretical studies go into attack and countermeasure design
- Validation and awareness of our research by GSMA standards input and publication
- Customer feedback and test results allow us to fine-tune and optimize our countermeasures
- Research input will fit product needs and operators requests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

Bell Labs Research Lifecycle



You connect
What does actually happen?

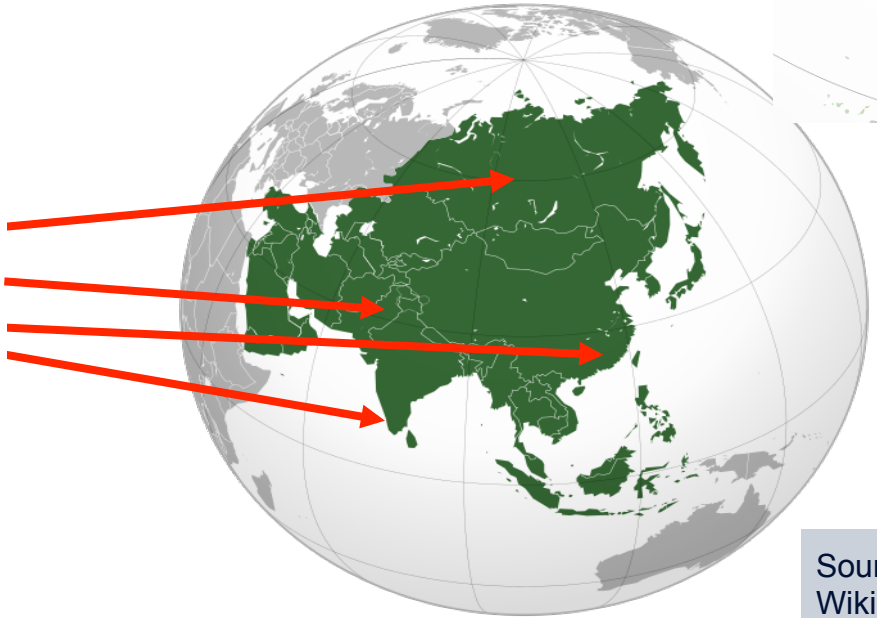
Roaming
Why should you care?



You connected to AT&T, Verizon, T-Mobile, Sprint

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

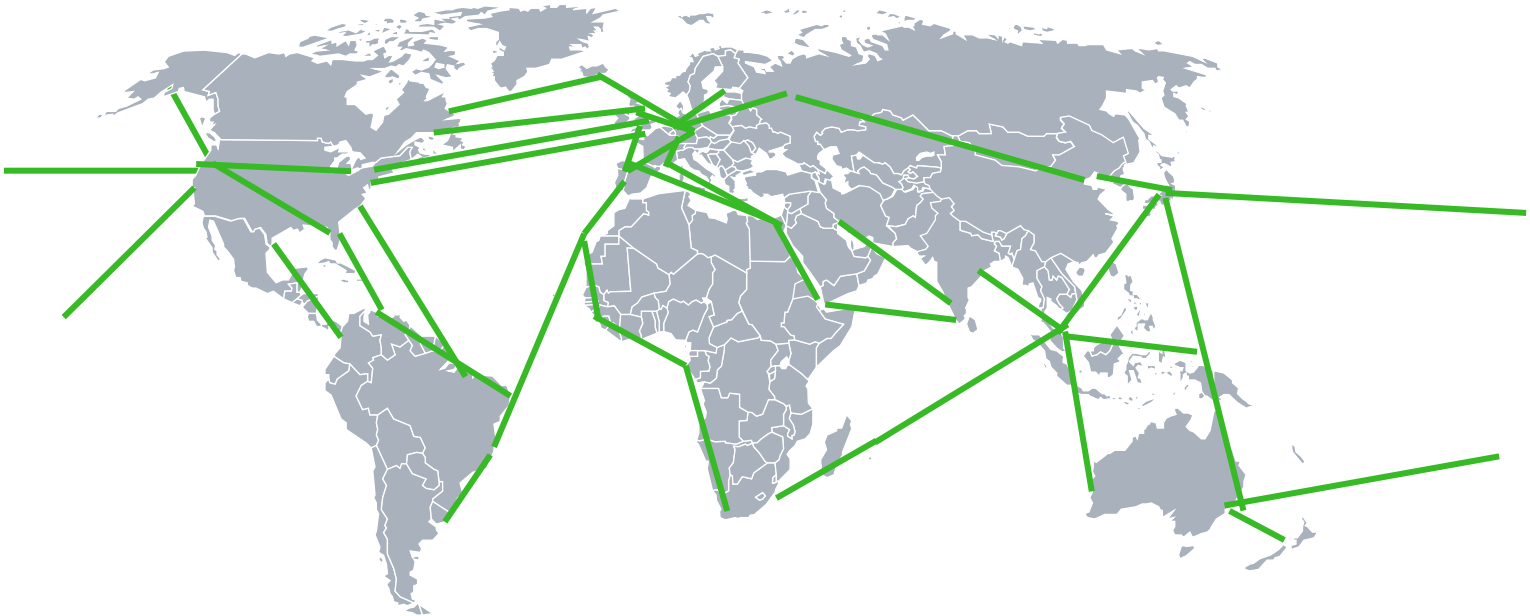
DefCon participants CMCC, Airtel, MegaFon, Telenor



Source: DefCon, National Geographics, Wikipedia

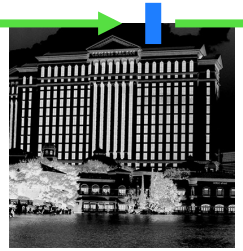
Connecting networks – The hidden private Internet

The Interconnection Network (IPX)



I switch on my phone

Las Vegas
Antenna



Core Network

Carrier / IPX

Authentication -> run to home network
Checking subscriber

Carrier / IPX

Core Network

What is this secret network?
Where does it come from?

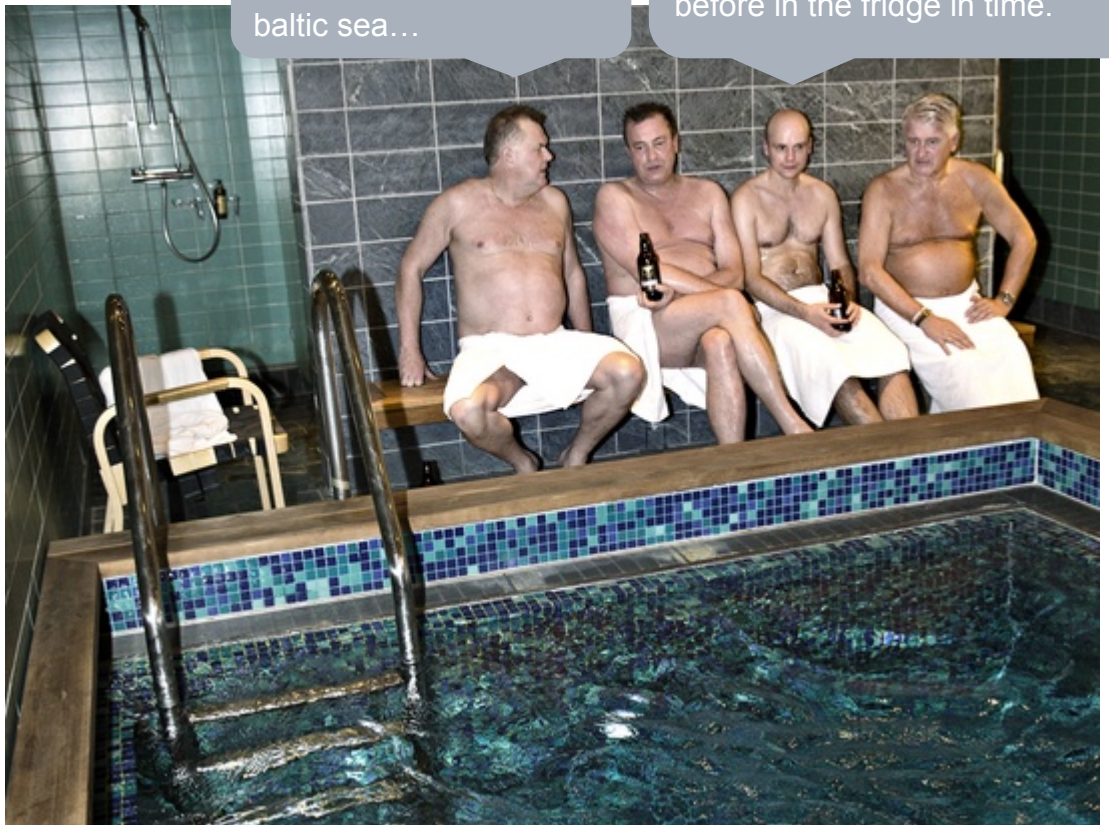
The good auld history

1981 – Nordic Operator Meeting

Bell Labs

Source: Kauppalehti.fi / Erja Lempinen

Starting of practical discusions



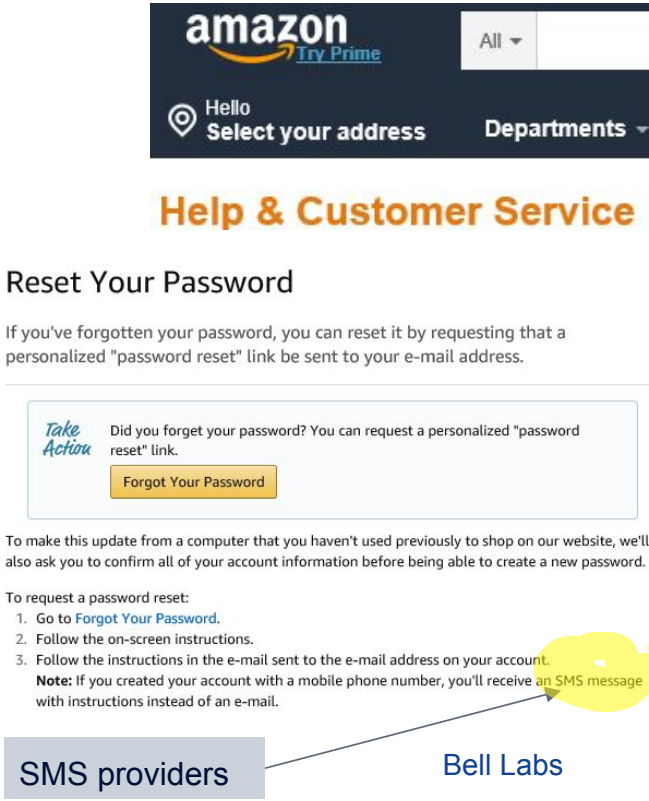
Source: Kauppalehti.fi / Erja Lempinen

The technica worked out

Source: Kauppalehti.fi / Erja Lempinen

Evolutions of IPX

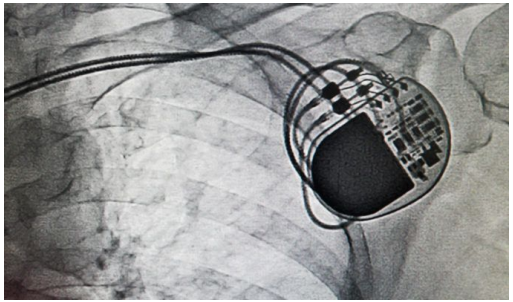
- Started with 5 Nordic operators and calls only about 35 years ago
- Now about 2000 companies connected to it
  - Mobile operators
  - Service providers (SMS aggregators, password recovery)
  - Satelite communication providers etc
- Very inhomogenous operator structure
- Networks are a mix and match
  - 2G, 2.5G, 3G, 4G and now 5G
  - Different hardware, protocols, products, releases
  - Many services voice, SMS, MMS, IMS, data, VoIP
- Network evolved, but security awareness only recently started (2014)

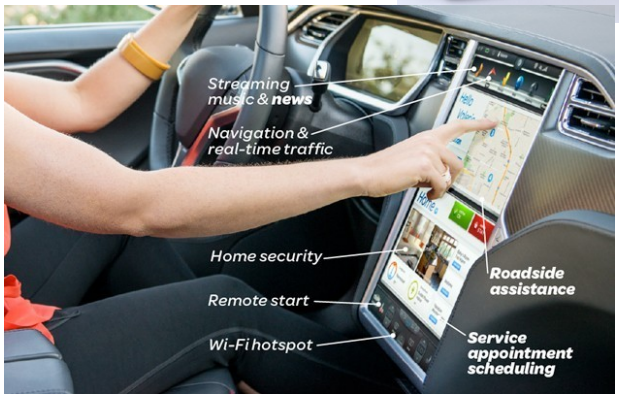


SEP – Somebody Else Problem?

Message for you…..

It is not only you that is ”reachable”



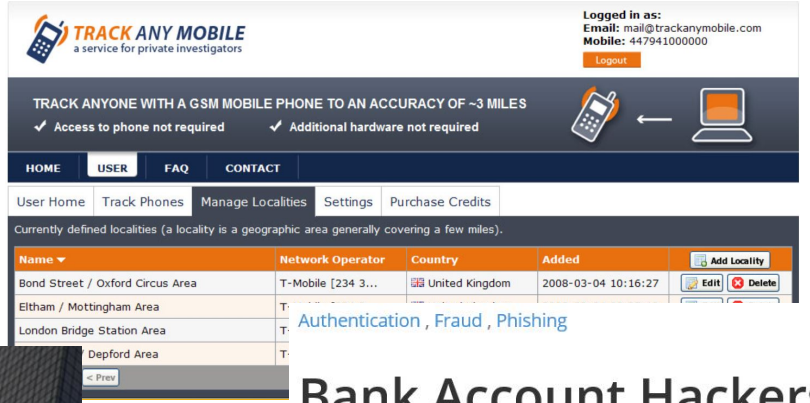


Security?

Who would hack this network

KIM ZETTER SECURITY 04.28.16 07:00 AM

THE CRITICAL HOLE AT THE HEART OF OUR CELL PHONE NETWORKS



Authentication , Fraud , Phishing

THE HILL

How the NSA could spy on a American phone — without congressional approval

Bank Account Hackers Used SS7 to Intercept Security Codes

Well-Known Signaling System 7 Protocol Flaws Exploited in Germany

erified SMS/OTP

communications with
, partners and employees are
e to interception. When SMS is
nd factor authentication (2FA)
rd recovery, it can also be
leveraged by criminals to commit fraud

03 / VA Service

Too often organizations are unaware of the exposure of current business processes to Cellular (SS7 and MITM) interception.
Vaulto offers the world's first telecom vulnerability assessment (VA) service, to

SkyLock's location finding capabilities are based on the ability to send and handle standard signaling messages (MAP messages) through the international SS7 network. This solution does not require any

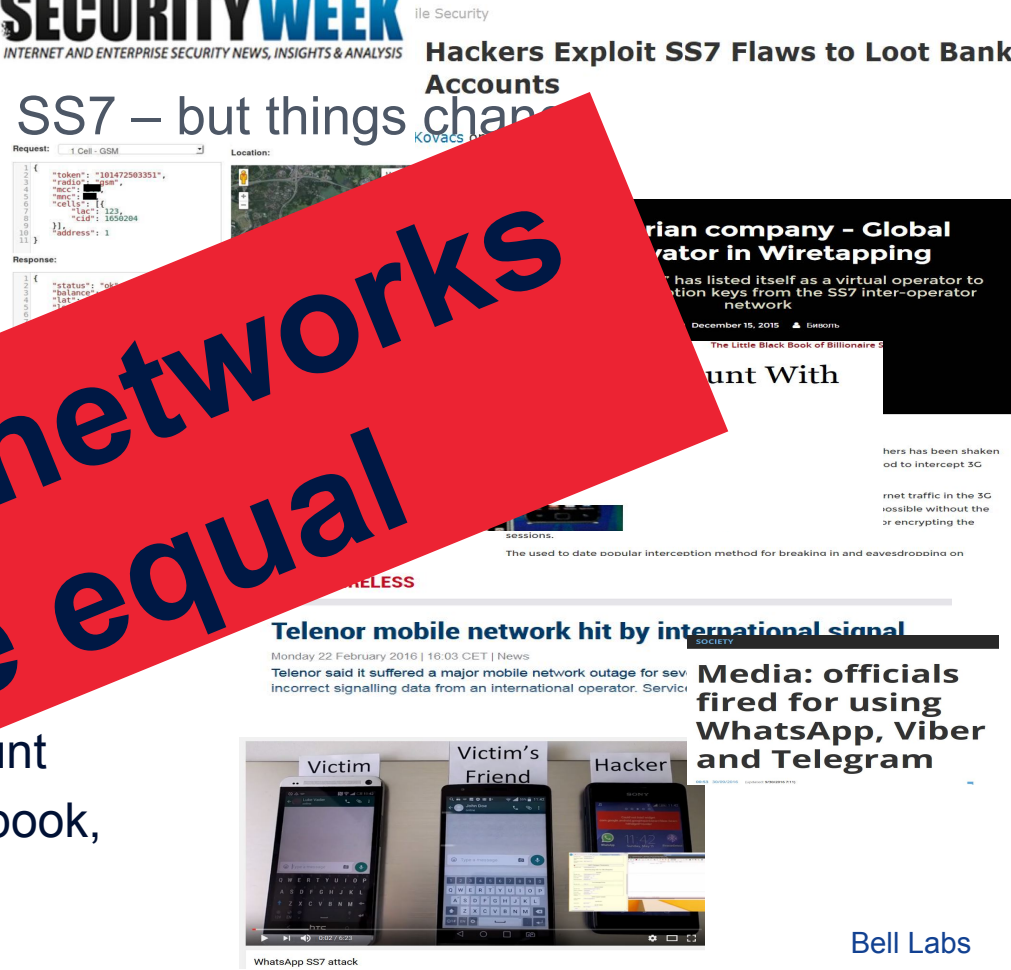
Source: wired, the intercept, Verint skylock product description, vault.co, trace any mobile, bankinfosecurity, the hill

Existing Attacks for the ”old” SS7

Most of the attacks today are still SS7 – but things chan

- Location Tracking
- Eavesdropping
- Fraud
- Denial of Service user & n
- Credential theft
- Data sessi
- Unblock
- SMS inte
- One time p ccount takeover for t gram, Facebook, Whatsapp, bitc in wallet

Not all networks are equal



Source: Security Week, The register, YouTube, wireless, wired, techworm

How do attackers get in

Rent a Service

Become an Operator

Kick in the door

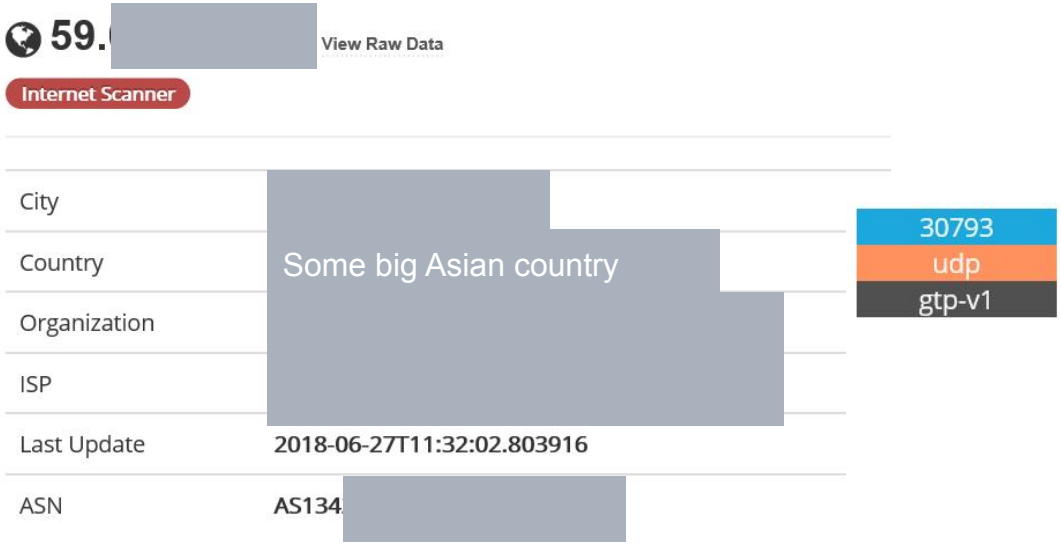
Bribing and Employee

Hack via Internet

Social Engineering

That is how they get in

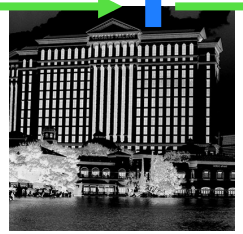
Well, of course there might be legitimate reason…maybe….



New protocol - New luck?

I switch on my phone

Las Vegas Antenna



Core Network

Carrier / IPX

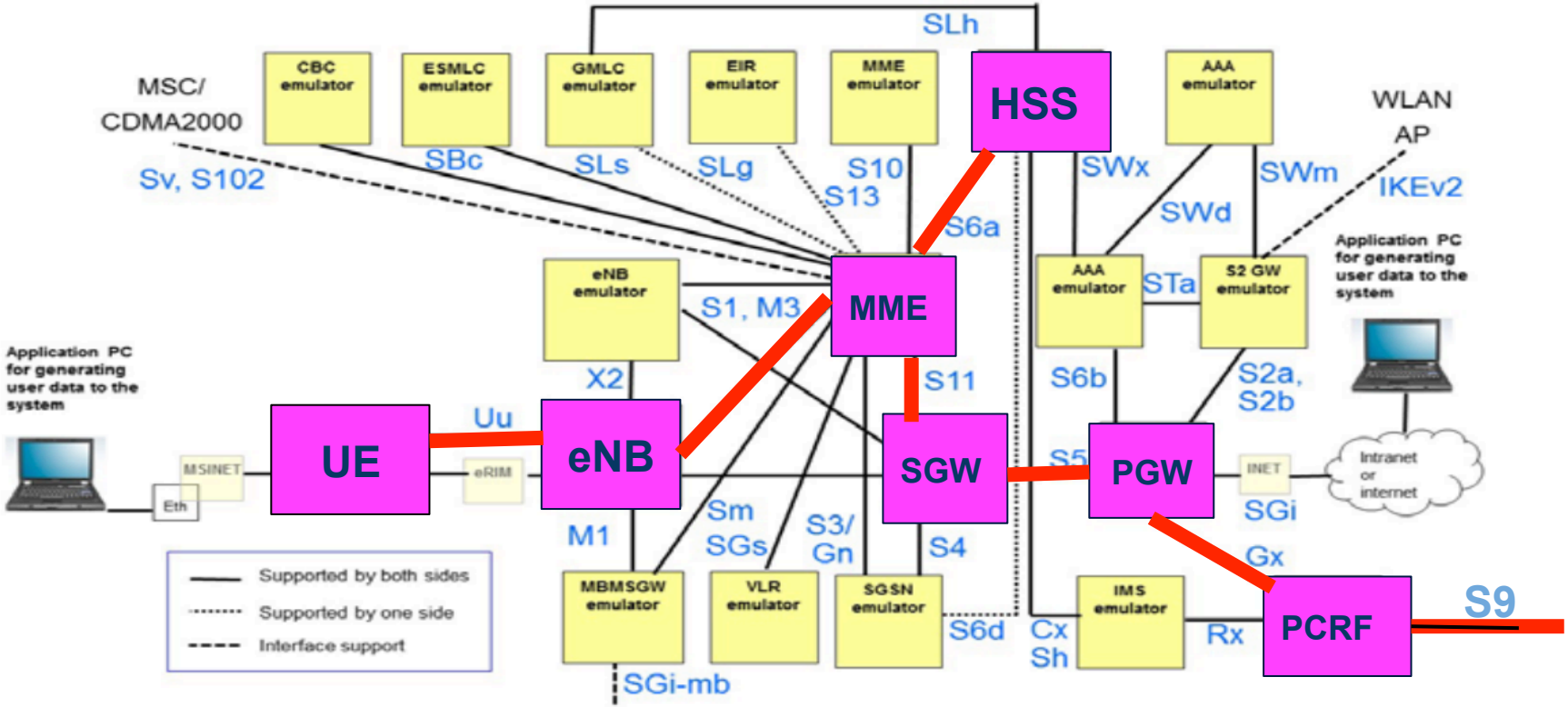
Checking subscriber:

”Hey, does she have money, and what did he pay for”
”Make sure it is really her”

Carrier / IPX

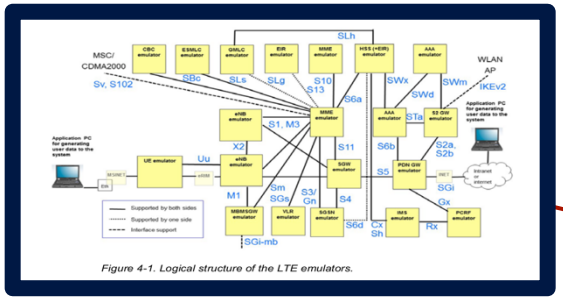
Core Network

Network used for testing of attack



LTE Emulator

Operators with connected S9 billing interface

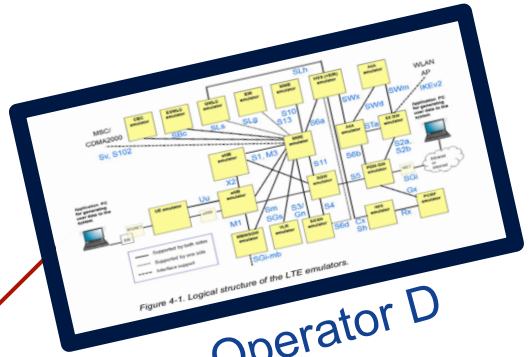


Operator A

S9

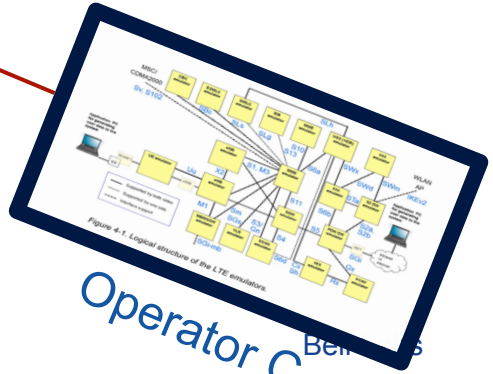
IPX

S9



Operator D

S9

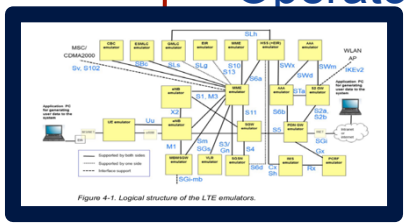


Operator C

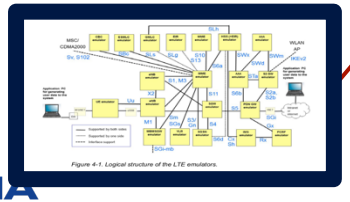
S9

S9

Operator F

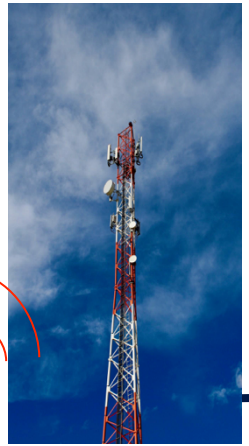


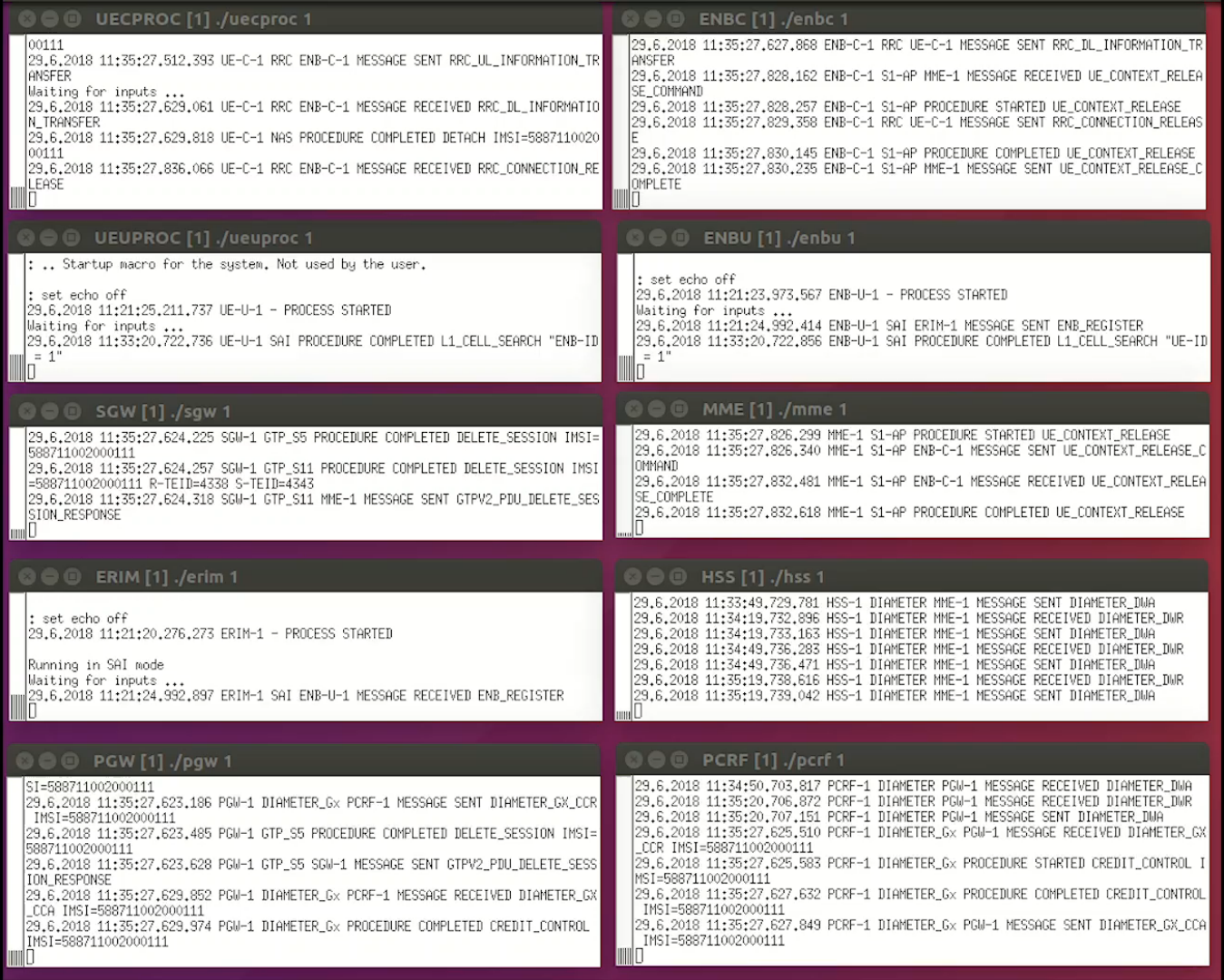
S9



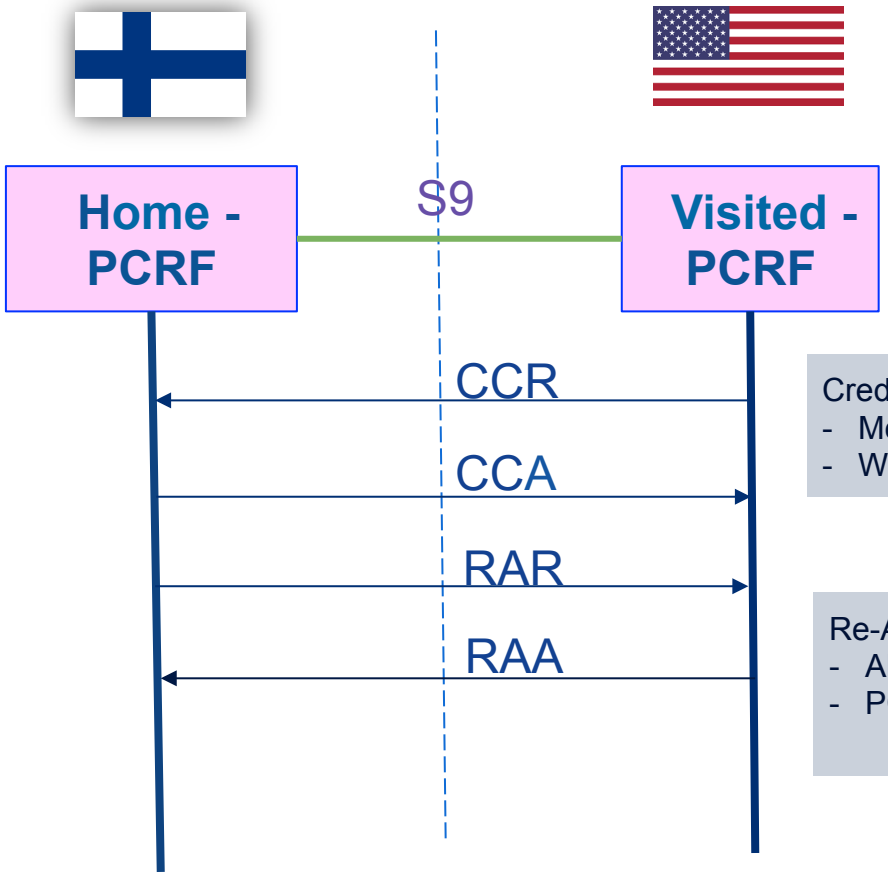
Operator B

Network Architecture (3G/4G)




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_TR
ANSFER
Waiting for inputs ...
29.6.2018 11:35:27.629.061 UE-C-1 RRC ENB-C-1 MESSAGE RECEIVED RRC_DL_INFORMATIO
N_TRANSFER
29.6.2018 11:35:27.629.818 UE-C-1 NAS PROCEDURE COMPLETED DETACH IMSI=5887110020
00111
29.6.2018 11:35:27.836.066 UE-C-1 RRC ENB-C-1 MESSAGE RECEIVED RRC_CONNECTION_RE
LEASE
ENBC [1] ./enbc 1
29.6.2018 11:35:27.627.868 ENB-C-1 RRC UE-C-1 MESSAGE SENT RRC_DL_INFORMATION_TR
ANSFER
29.6.2018 11:35:27.828.162 ENB-C-1 S1-AP MME-1 MESSAGE RECEIVED UE_CONTEXT_RELEA
SE_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_RELEAS
E
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_C
OMPLETE
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_SES
SION_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_C
OMMAND
29.6.2018 11:35:27.832.481 MME-1 S1-AP ENB-C-1 MESSAGE RECEIVED UE_CONTEXT_RELEA
SE_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_SESS
ION_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 I
MSI=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 US)



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

Diameter Routing Issue – Two Possibilities how to route…..Hop-by-Hop

Core Network

Carrier / IPX

Carrier / IPX

Core Network

Request
Orig:
FakeFin
Dest:
US_NW
Hop-by-hop
ID: 3

Answer
Orig:
US_NW
Hop-by-hop
ID: 3

Request
Orig:
FakeFin
Dest:
US_NW
Hop-by-hop
ID: 2

Answer
Orig:
US_NW
Hop-by-hop
ID: 2

Request
Orig:
FakeFin
Dest:
US_NW
Hop-by-hop
ID: 1

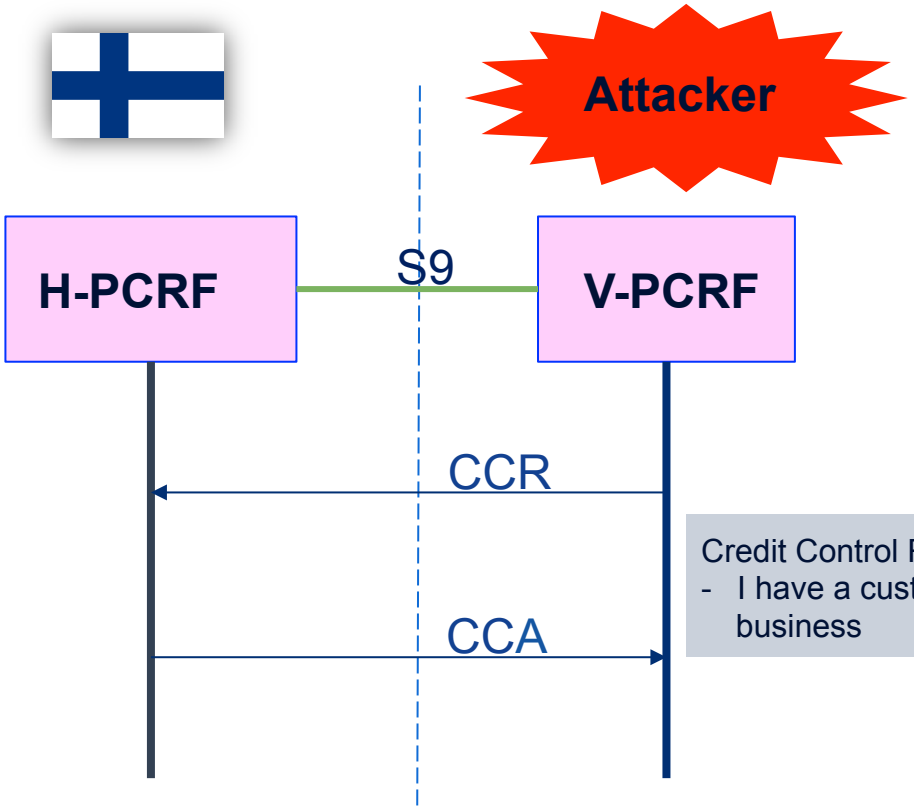
Answer
Orig:
US_NW
Hop-by-hop
ID: 1

Attacker

Attack

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

Attack scenario against finnish operator – Request PCC via CCR



Message Format:
<CC-Request> ::= < Diameter Header: 272, REQ, PXY >

< Session-Id >

{ Origin-Host }

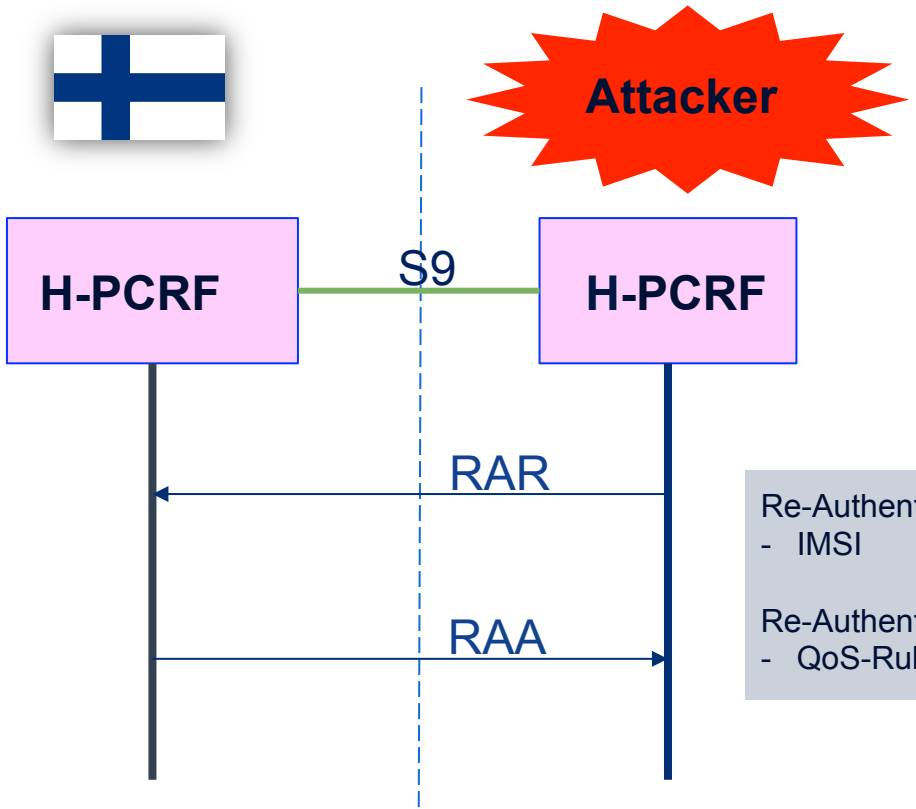
Diameter Edge Agent (DEA)

{ Origin-Realm }

Used operator

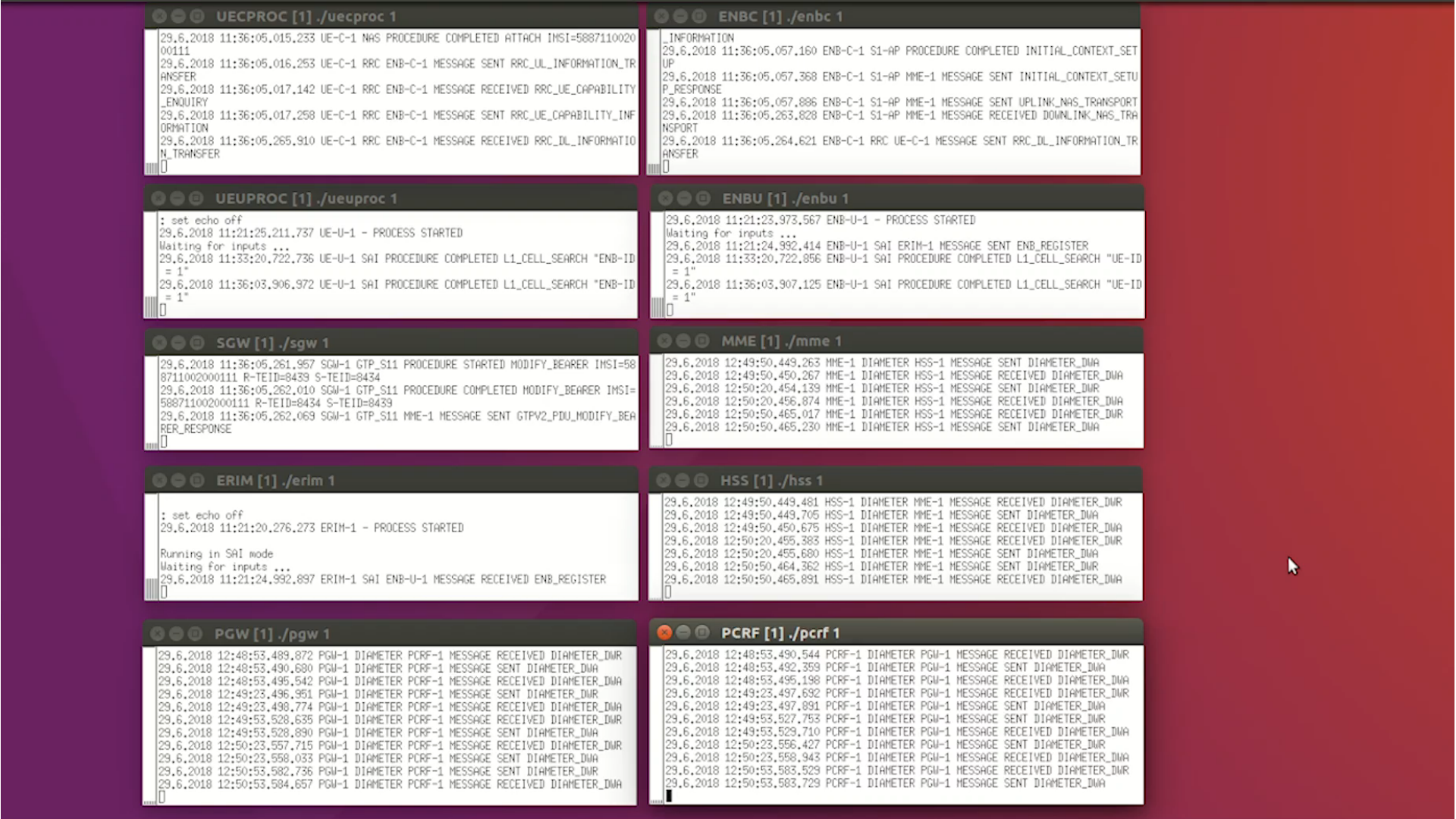
{ Destination-Realm }

Requesting PCC via RAR (posing as home network)



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 12:49:50.449.263 MME-1 DIAMETER HSS-1 MESSAGE SENT DIAMETER_DWA
29.6.2018 12:49:50.450.267 MME-1 DIAMETER HSS-1 MESSAGE RECEIVED DIAMETER_DWA
29.6.2018 12:50:20.454.139 MME-1 DIAMETER HSS-1 MESSAGE SENT DIAMETER_DWR
29.6.2018 12:50:20.456.874 MME-1 DIAMETER HSS-1 MESSAGE RECEIVED DIAMETER_DWA
29.6.2018 12:50:50.465.017 MME-1 DIAMETER HSS-1 MESSAGE RECEIVED DIAMETER_DWR
29.6.2018 12:50:50.465.230 MME-1 DIAMETER HSS-1 MESSAGE SENT 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 12:49:50.449.481 HSS-1 DIAMETER MME-1 MESSAGE RECEIVED DIAMETER_DWR
29.6.2018 12:49:50.449.705 HSS-1 DIAMETER MME-1 MESSAGE SENT DIAMETER_DWA
29.6.2018 12:49:50.450.675 HSS-1 DIAMETER MME-1 MESSAGE RECEIVED DIAMETER_DWA
29.6.2018 12:50:20.455.383 HSS-1 DIAMETER MME-1 MESSAGE RECEIVED DIAMETER_DWR
29.6.2018 12:50:20.455.680 HSS-1 DIAMETER MME-1 MESSAGE SENT DIAMETER_DWA
29.6.2018 12:50:50.464.362 HSS-1 DIAMETER MME-1 MESSAGE SENT DIAMETER_DWR
29.6.2018 12:50:50.465.891 HSS-1 DIAMETER MME-1 MESSAGE RECEIVED DIAMETER_DWA
PGW [1] ./pgw 1
29.6.2018 12:48:53.489.872 PGW-1 DIAMETER PCRF-1 MESSAGE RECEIVED DIAMETER_DWR
29.6.2018 12:48:53.490.680 PGW-1 DIAMETER PCRF-1 MESSAGE SENT DIAMETER_DWA
29.6.2018 12:48:53.495.542 PGW-1 DIAMETER PCRF-1 MESSAGE RECEIVED DIAMETER_DWA
29.6.2018 12:49:23.496.951 PGW-1 DIAMETER PCRF-1 MESSAGE SENT DIAMETER_DWR
29.6.2018 12:49:23.498.774 PGW-1 DIAMETER PCRF-1 MESSAGE RECEIVED DIAMETER_DWA
29.6.2018 12:49:53.528.635 PGW-1 DIAMETER PCRF-1 MESSAGE RECEIVED DIAMETER_DWR
29.6.2018 12:49:53.528.890 PGW-1 DIAMETER PCRF-1 MESSAGE SENT DIAMETER_DWA
29.6.2018 12:50:23.557.715 PGW-1 DIAMETER PCRF-1 MESSAGE RECEIVED DIAMETER_DWR
29.6.2018 12:50:23.558.033 PGW-1 DIAMETER PCRF-1 MESSAGE SENT DIAMETER_DWA
29.6.2018 12:50:53.582.736 PGW-1 DIAMETER PCRF-1 MESSAGE SENT DIAMETER_DWR
29.6.2018 12:50:53.584.657 PGW-1 DIAMETER PCRF-1 MESSAGE RECEIVED DIAMETER_DWA
PCRF [1] ./pcrf 1
29.6.2018 12:48:53.490.544 PCRF-1 DIAMETER PGW-1 MESSAGE RECEIVED DIAMETER_DWR
29.6.2018 12:48:53.492.359 PCRF-1 DIAMETER PGW-1 MESSAGE SENT DIAMETER_DWA
29.6.2018 12:48:53.495.198 PCRF-1 DIAMETER PGW-1 MESSAGE RECEIVED DIAMETER_DWA
29.6.2018 12:49:23.497.692 PCRF-1 DIAMETER PGW-1 MESSAGE RECEIVED DIAMETER_DWR
29.6.2018 12:49:23.497.891 PCRF-1 DIAMETER PGW-1 MESSAGE SENT DIAMETER_DWA
29.6.2018 12:49:53.527.753 PCRF-1 DIAMETER PGW-1 MESSAGE SENT DIAMETER_DWR
29.6.2018 12:49:53.529.710 PCRF-1 DIAMETER PGW-1 MESSAGE RECEIVED DIAMETER_DWA
29.6.2018 12:50:23.556.427 PCRF-1 DIAMETER PGW-1 MESSAGE SENT DIAMETER_DWR
29.6.2018 12:50:23.558.943 PCRF-1 DIAMETER PGW-1 MESSAGE RECEIVED DIAMETER_DWA
29.6.2018 12:50:53.583.529 PCRF-1 DIAMETER PGW-1 MESSAGE RECEIVED DIAMETER_DWR
29.6.2018 12:50:53.583.729 PCRF-1 DIAMETER PGW-1 MESSAGE SENT DIAMETER_DWA

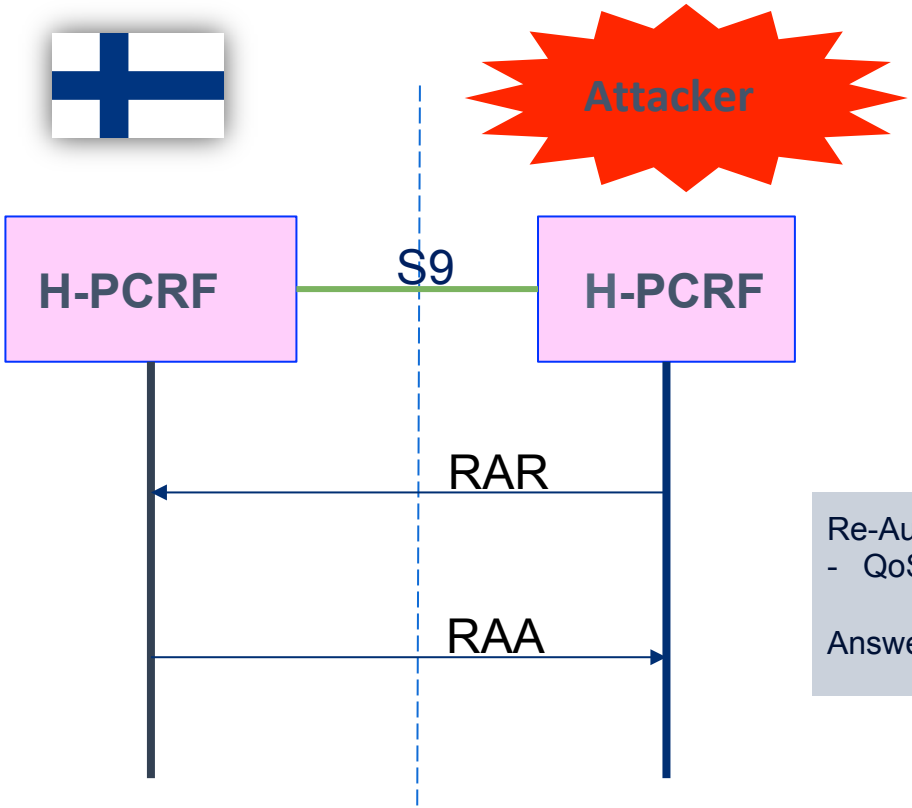
diameter

Expression...

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
```

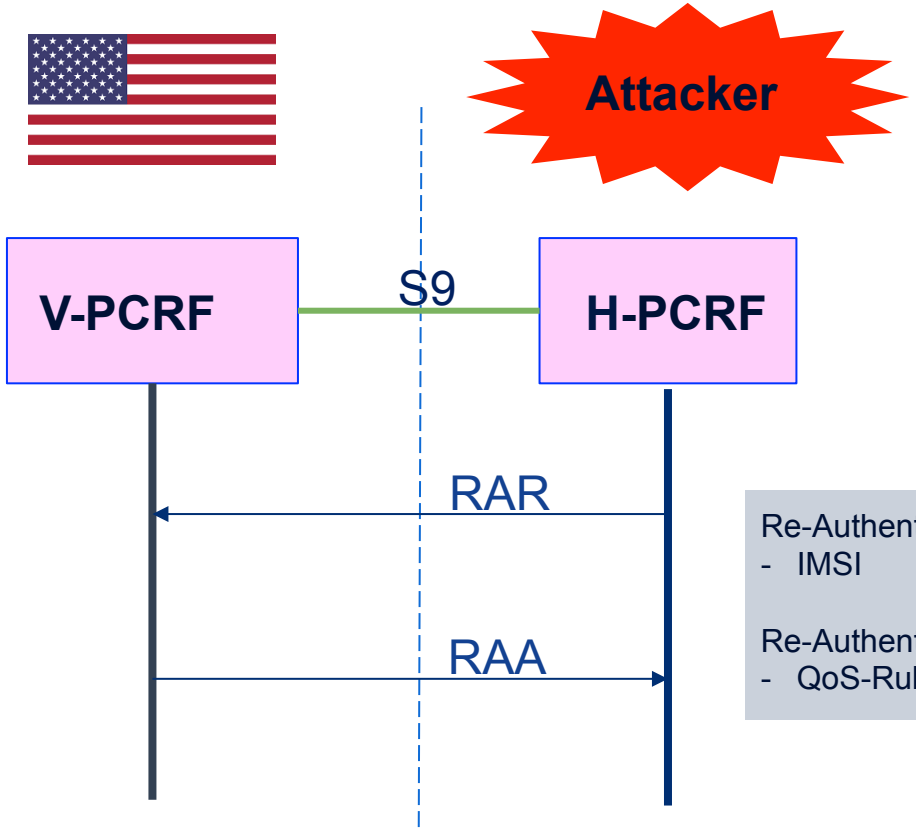
Attack Scenario 1: Putting PCC via RAR (posing as home network)



Re-Authentication Request
- QoS-Rule-Install

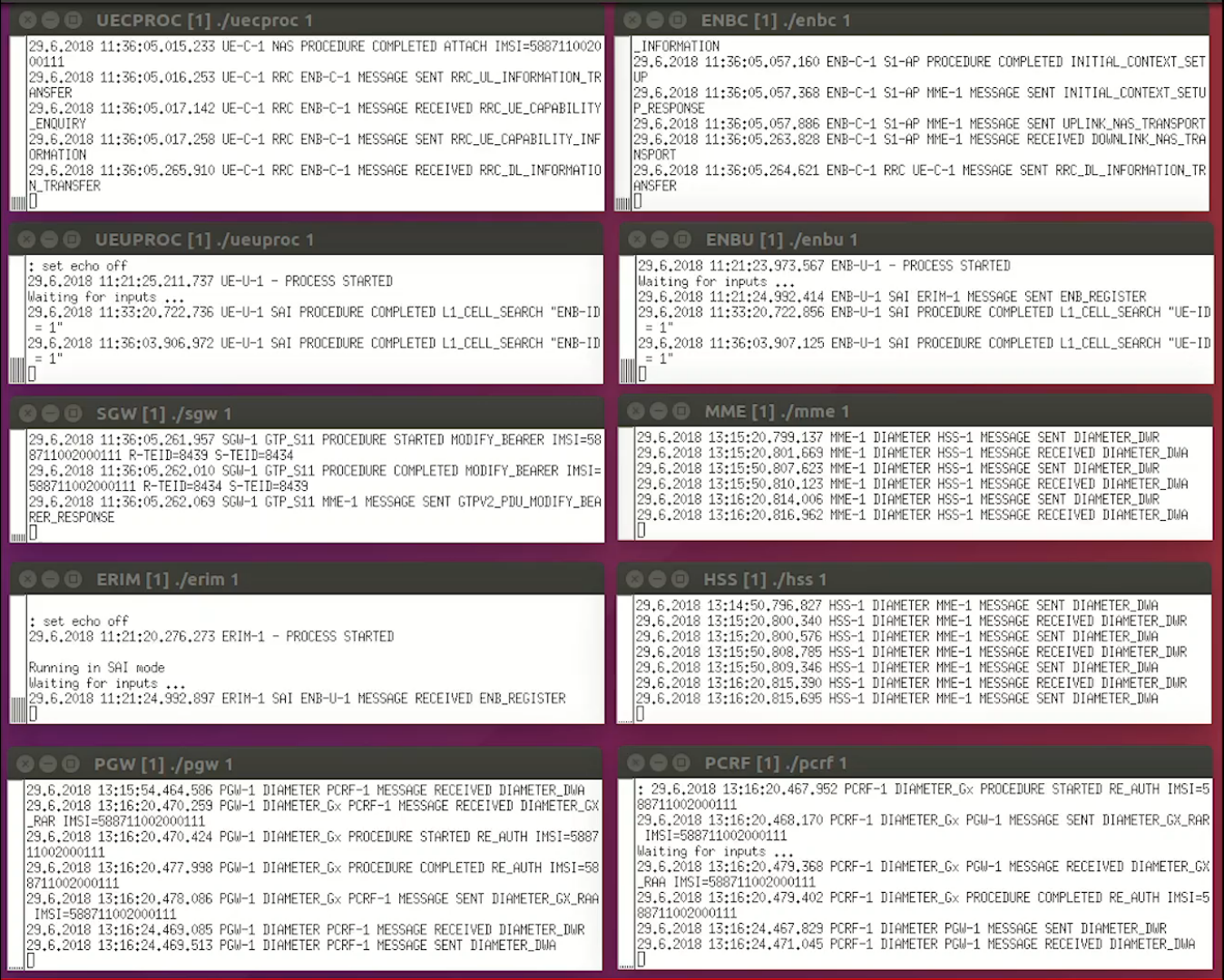
Answer does not matter

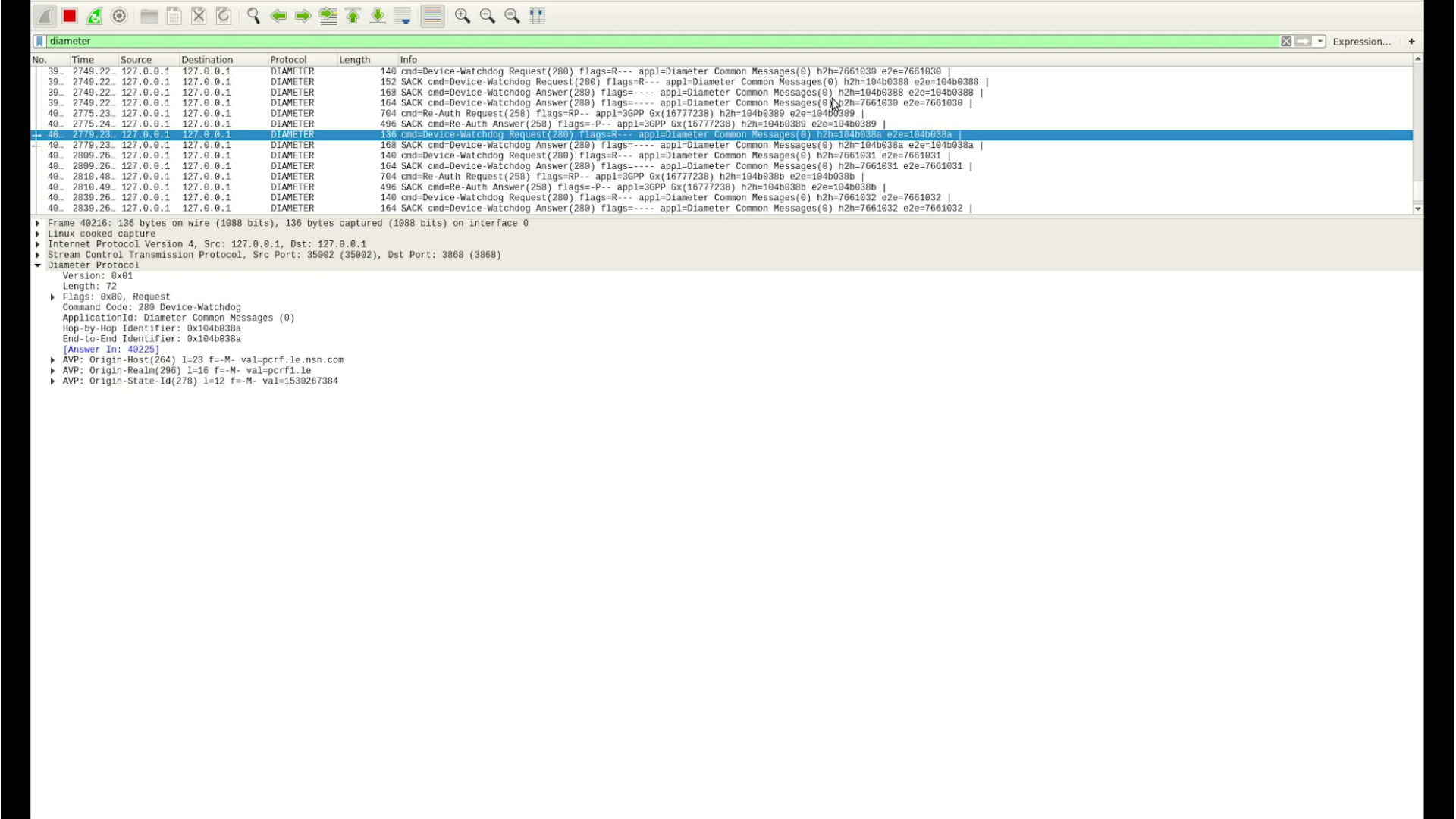
Attack Scenario 2: Putting PCC via RAR to outgoing roamer



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

Impacts

- Attacker:
  - Better services
  - Shifting the costs – Letting somebody else pay the phone bill
  - Re-selling ”opportunity”
- Users:
  - Might be billed for services he has not used (in particular company subscriptions are at risk)

- Operators:
  - Bill disputes (service desks)
  - Loss of coporate customers
  - Costs with partners that can not be charged to a user
    - IPX carriers still want to see their money

Countermeasures

Switch it off – build it from scratch?

Countermeasures

For Operators

- S9 Interface -> use IPSec with trusted partners directly
- S9 only open on need basis
- Routing via origin realm, origin host
- IMSI range – operator match
- Check not to get messages from yourself
- Logical seperation of visitors and own subscribers
- Location distance
- Fingerprint partner
- Fingerprint ”flows”

For “normal” Users

- Check your bill
- Keep an eye on the news

For “corporate” Users

- Security and network protection is something that needs to be part of a Service Layer Agreement
- It is a quality indicator, similar to bandwith and coverage

Thanks to
EU SCOTT Project for funding part of this research

Questions?

Silke.Holtmanns@nokia.com