NOKIA

Bell Labs

Interconnection Security - SS7 and Diameter

Silke Holtmanns

Nokia Bell Labs

14th November 2017

Industrial Research

Bell Lab research for signalling

Nokia Bell Labs

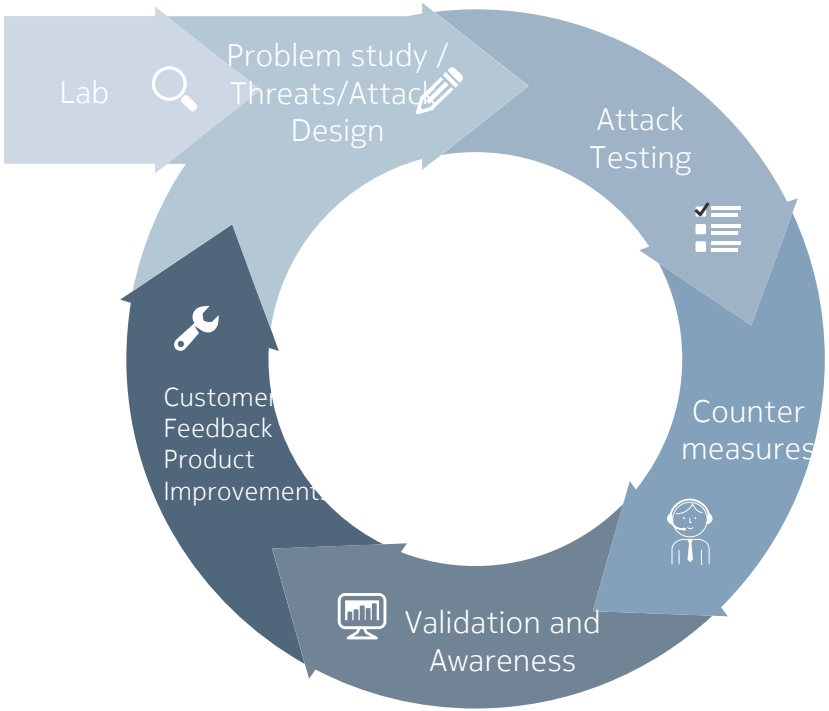
Research for technology and communication since 1925

Nokia Bell Labs – Future Attacks and Mitigation

Research that solves real problems together with our customers

- 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



Routing and Signalling Security Research in Nokia Bell Labs

Silke Holtmanns, Yoan Miche, Ian Oliver

Catching what has not been caught

Finding and mitigating signaling vulnerabilities

Telecommunication protocol security

Telco protocols meet Hackers
Two worlds move towards each other

5G Security Requests

Awareness and education on diameter security (own company, customers, legislators)

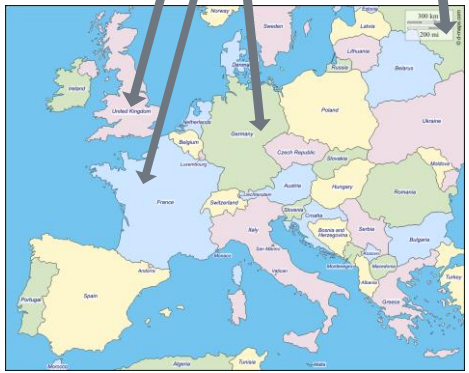
Attacks evolve, so must we

Signalling System No 7
SS7 Security

What is roaming?

We are here, somewhere
MEO, Vodafone, NOS

Meeting Attendees
Telefonica, DT, Vodafone, MTS,..

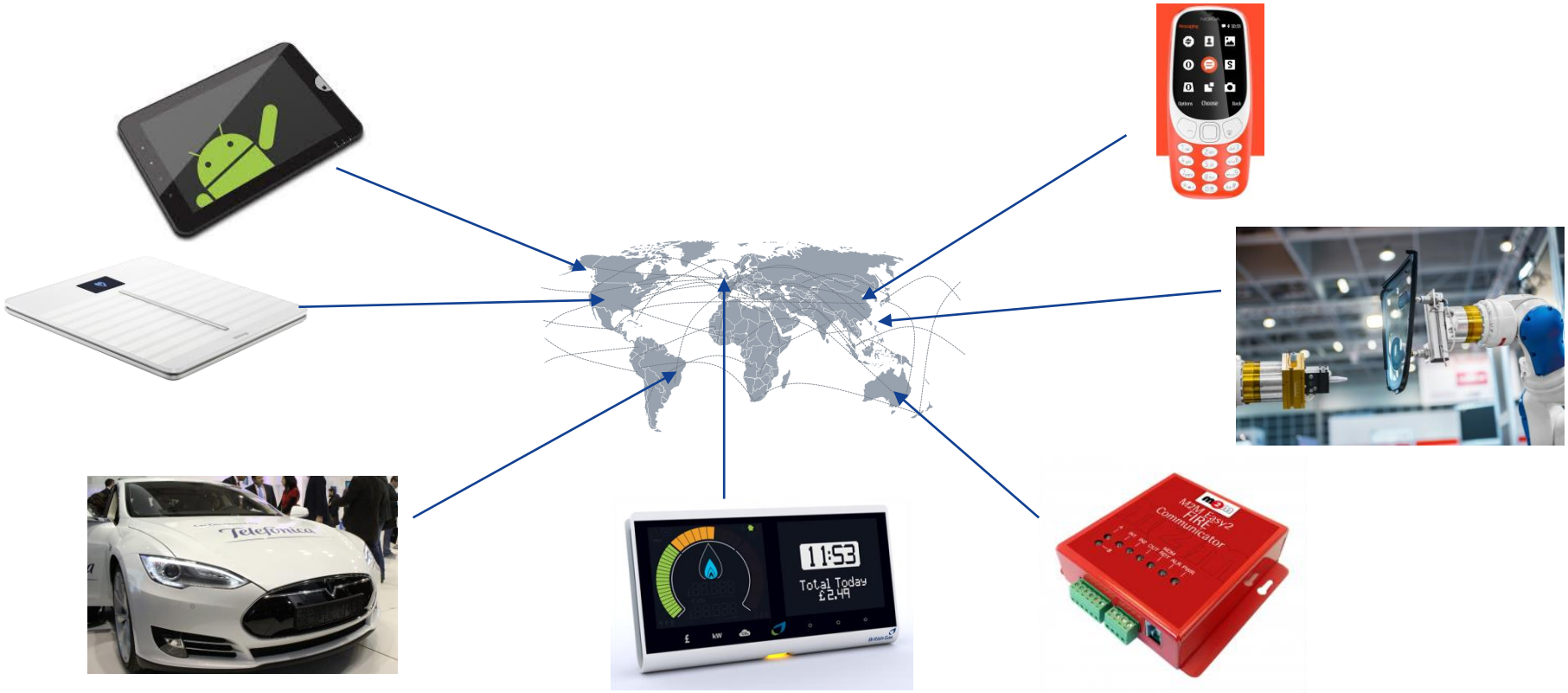


My home mobile network operator
Colleagues & Family
Elisa, TeliaSonera, DNA

Roaming Network – Interconnection Network

Not the Internet – but equally important

We are all connected to the Interconnection Network

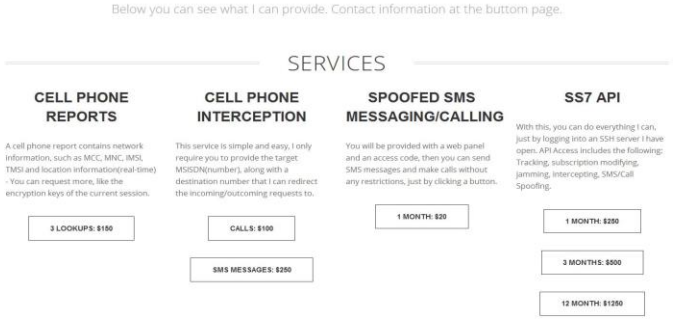


History of Interconnection Network

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 (4G/5G)

Closed & Private Network?



SHODAN

221.177.247.252
China Mobile
Added on 2016-09-22 15:34:36 GMT
China
Details

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

The Intercept_

OPERATION SOCIALIST

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

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.

Bell Labs

How the attackers get in?

Renting a Service

Hacking

Having Power

Bribing an Employee

Become an Operator

Convincing

Existing Attacks for the ”old” SS7

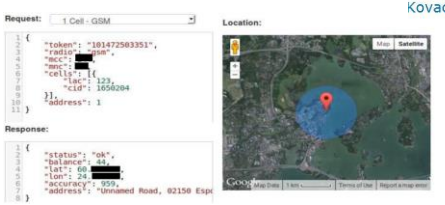
If no protection is deployed

- 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 banks, Telegram, Facebook, Whatsapp, g-mail (bitcoin)

ile Security

Hackers Exploit SS7 Flaws to Loot Bank Accounts

Kovacs on May 04, 2017



JUN 15, 2016 @ 08:00 AM 71,405 VIEWS

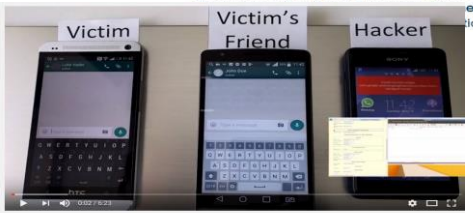
Hackers Can Steal Your Facebook Account With Just A Phone Number

Thomas Fox-Brewster, FC

WIRELESS

Telenor mobile network hit by international signal

Monday 22 February 2016 | 16:03 CET | News



WhatsApp SS7 attack

SOCIETY

Media: officials fired for using WhatsApp, Viber and Telegram

Security

Someone checked and, yup, you can still hijack Gmail, Bitcoin wallets etc via dirty SS7 tricks

Two-factor authentication by SMS? More like SOS

By John Leyden 18 Sep 2017 at 23:37 16 SHARE

Bell Labs

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

Diameter Security

All will be better with LTE and Diameter……

All will be ~~better~~ different with

LTE and Diameter……

Attacks are reality

Why should they stop? Because we have LTE??

- **Intelligence communities** see mobile networks as “all-you-can-eat-data-buffet” and 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

NOKIA

Service companies move with time and technology

International Business Times

UK | World | Business | Politics | Fintech | Technology | Science | Sport | Entertainment | Opinion | Video | Pictures

Smartphones | Cybersecurity | Innovation | Social Media | Games | Motoring

Technology | CyberSecurity

UAE recruiting 'elite task force' of cyber experts to build mass public spying system

Researcher claims he was offered $20,000 a month to help build the tool for state surveillance.

By Jason Murdock

Updated August 7, 2016 17:36 BST

IBT VIDEO

DarkMatter becomes associate member of the leading mobile operator group, GSMA

11 Jan 2017

Share

- *Membership will allow DarkMatter to interact with more than 800 telecom operators globally, as it develops end-to-end secure communications offerings*

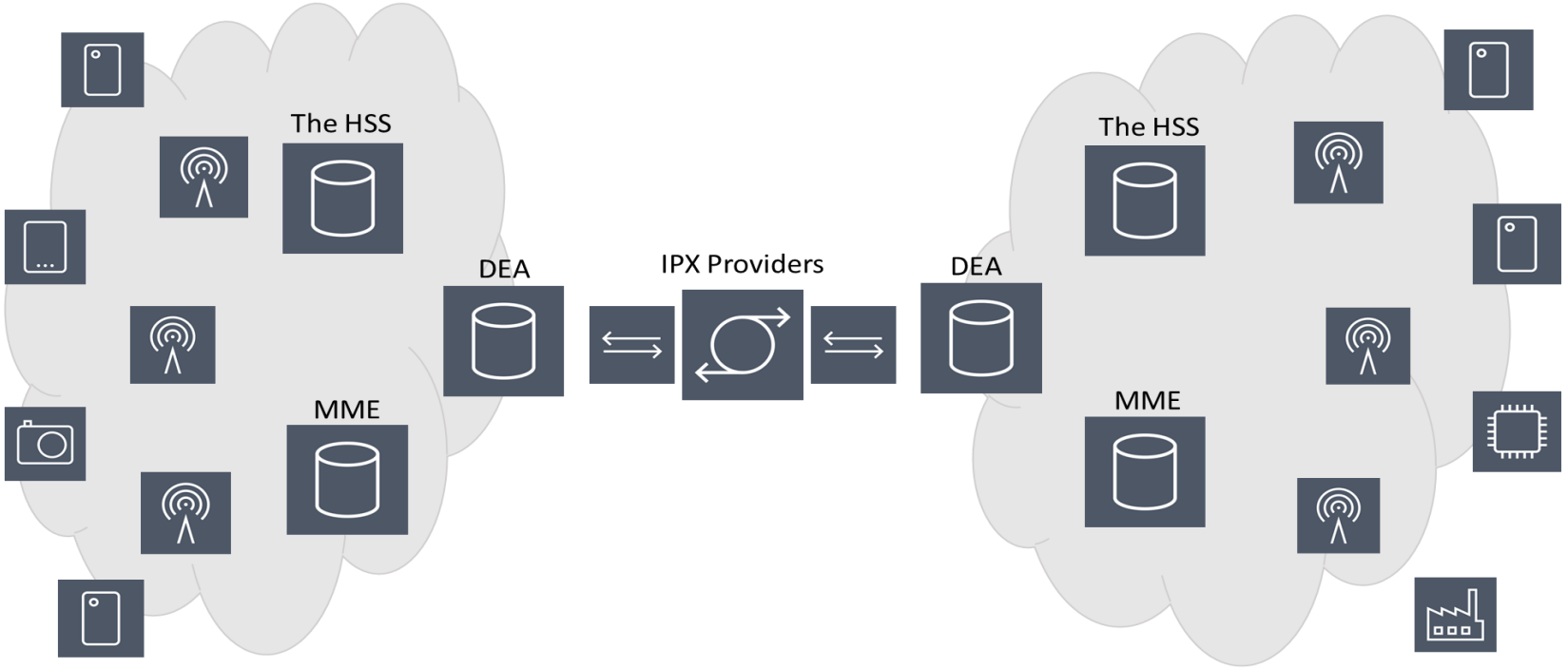
DarkMatter, the international cyber security firm headquartered in the UAE, announces it has become an Associate Member in the GSMA, the global organisation that represents the interests of the mobile telecom industry.

DarkMatter's membership will permit the firm to become active in GSMA working groups such as Fraud and Security, Web and SIM. These three groups address issues such as safeguarding SIM cards, encryption on the internet, the introduction of HTTP2, mobile malware, cloud service

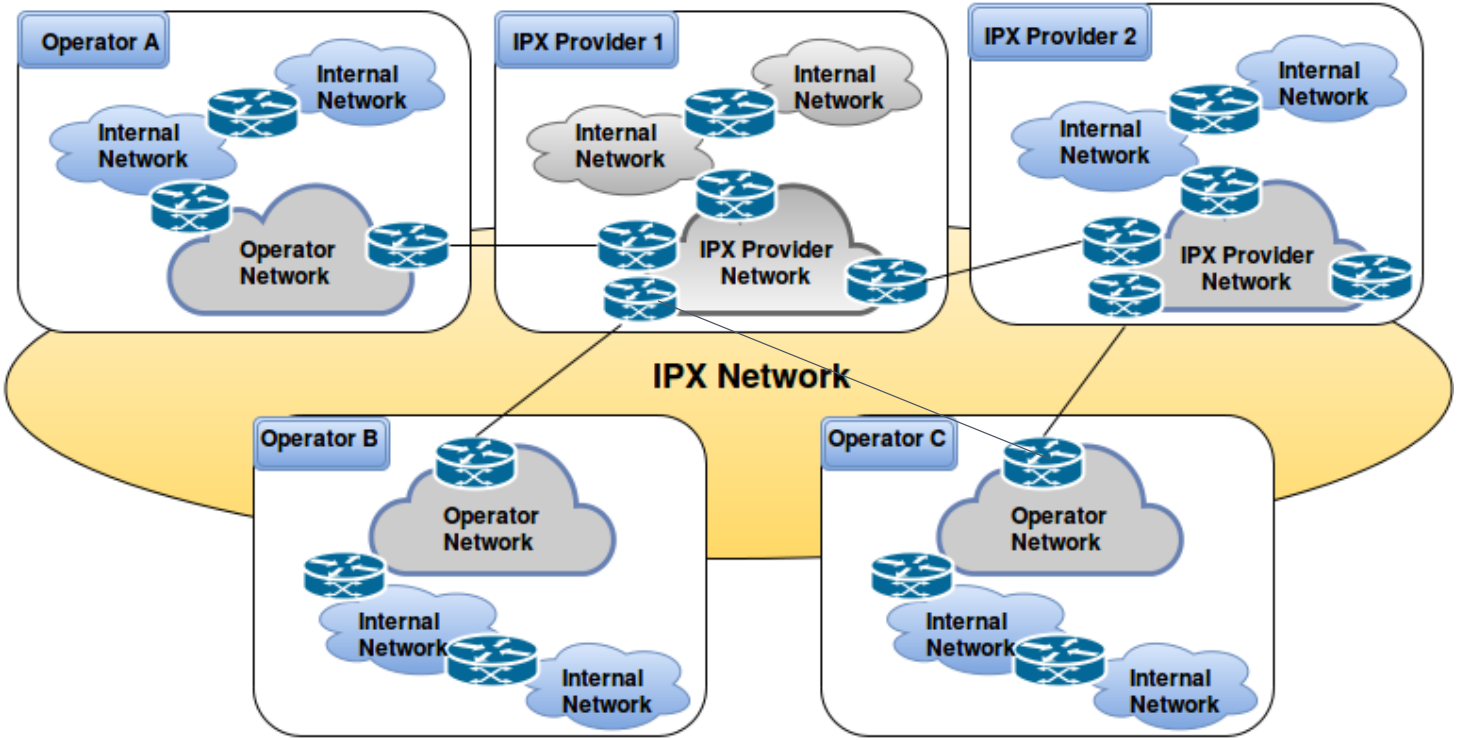
Faisal Al Bannai is Founder and CEO of

NOKIA

Two LTE Networks Connect
Connection via IPX provider



A bit more realistic….
IPX “tiny” example



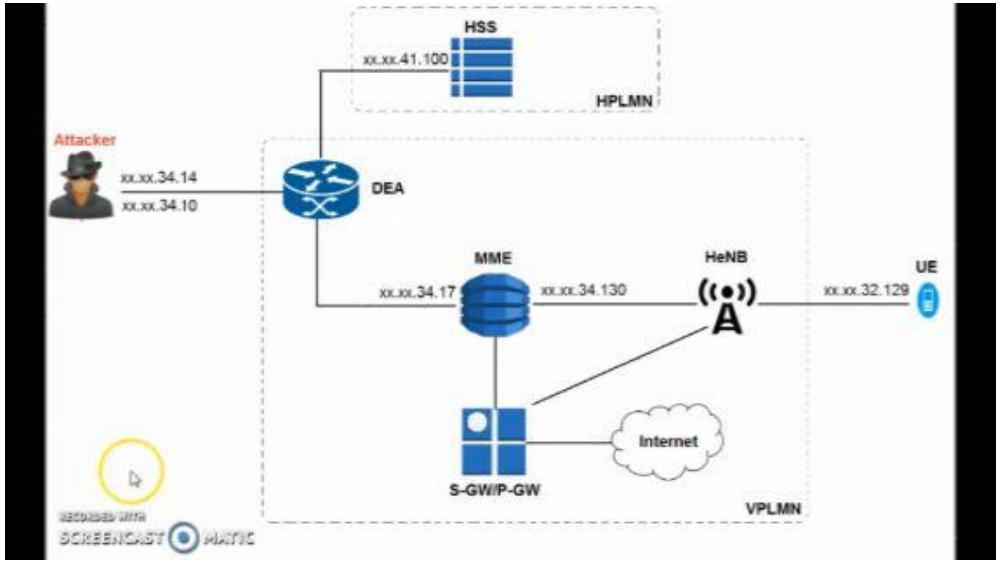
Known Diameter Attacks

- Location Tracking (NATO CyCon Conference, 2015)
- Downgrading attacks (Troopers TelcoSec 2016)
- Denial of Service & Fraud (Blackhat, 2016)
- SMS and one time password interception (IEEE ICC 2017)
- Subscriber Profile Modification (Network and System Security 2017)

To come

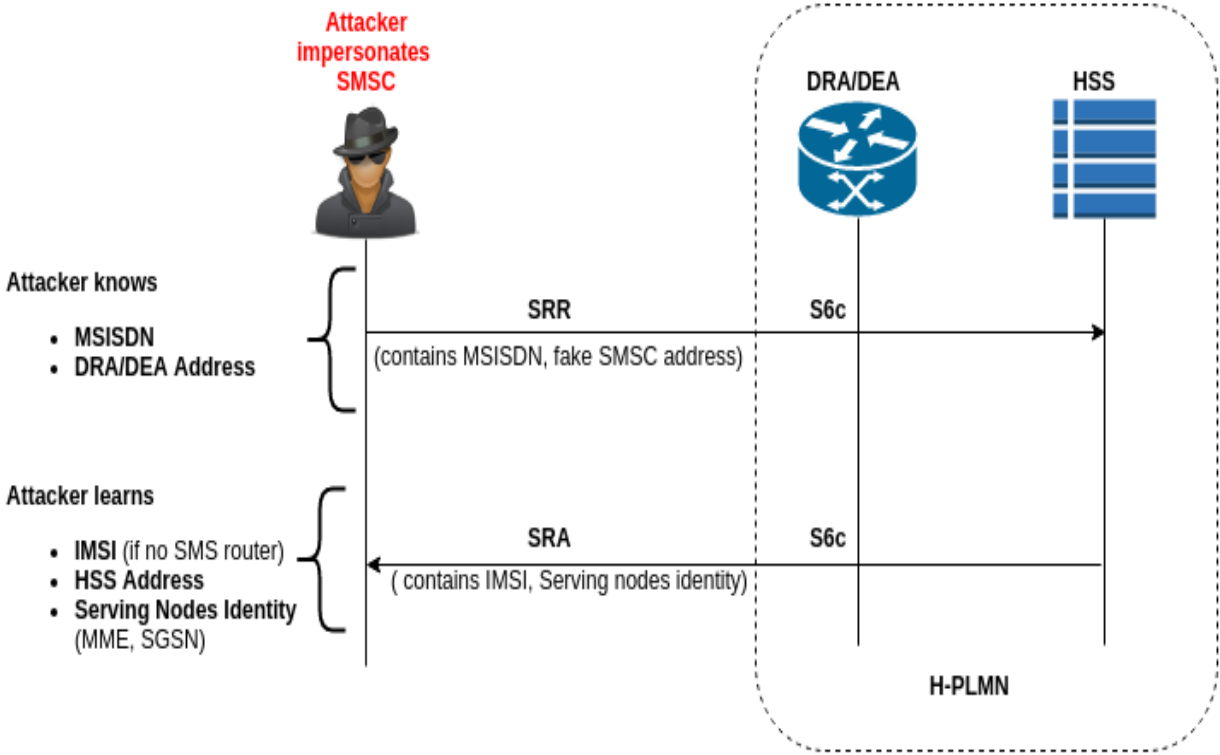
- Data interception for GPRS, LTE (potentially December 2017)

Network Setup for DoS Testing – Video



Get the IMSI 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

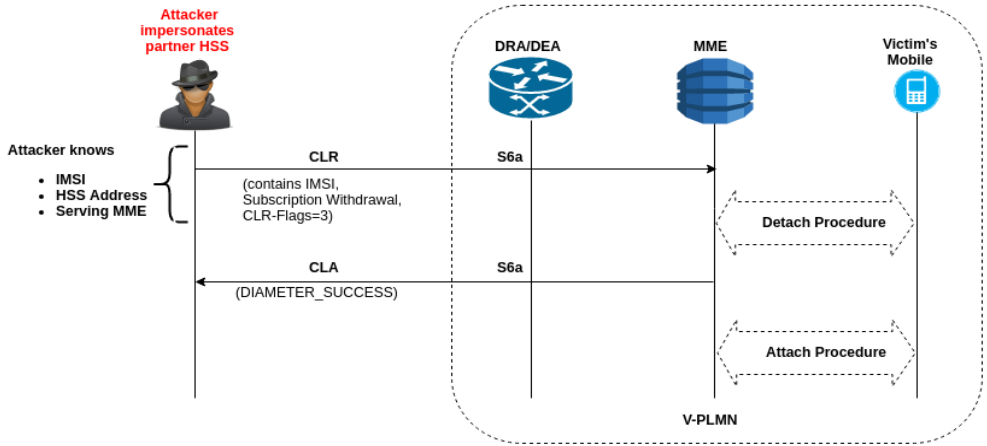


Denial of Service using CLR

Cancel Location Request (CLR)

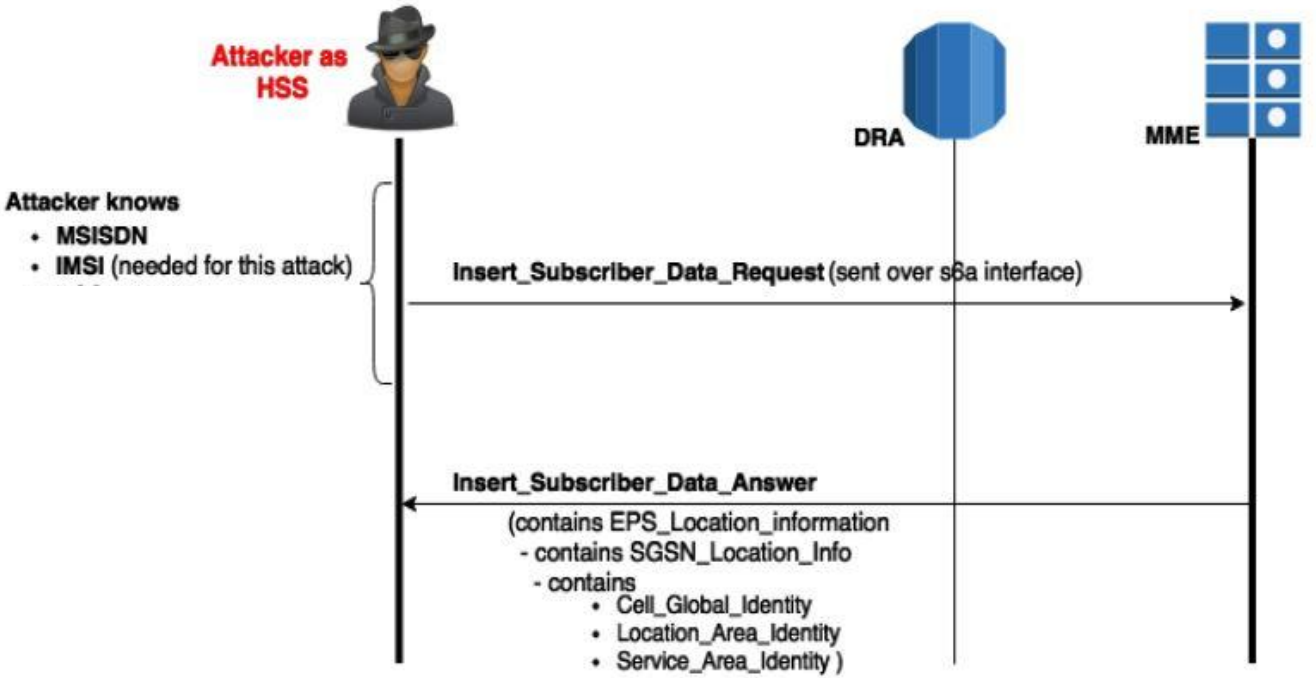
Sent by HSS to the MME to detach the UE

- MME change (location change)
- Subscription Withdrawal



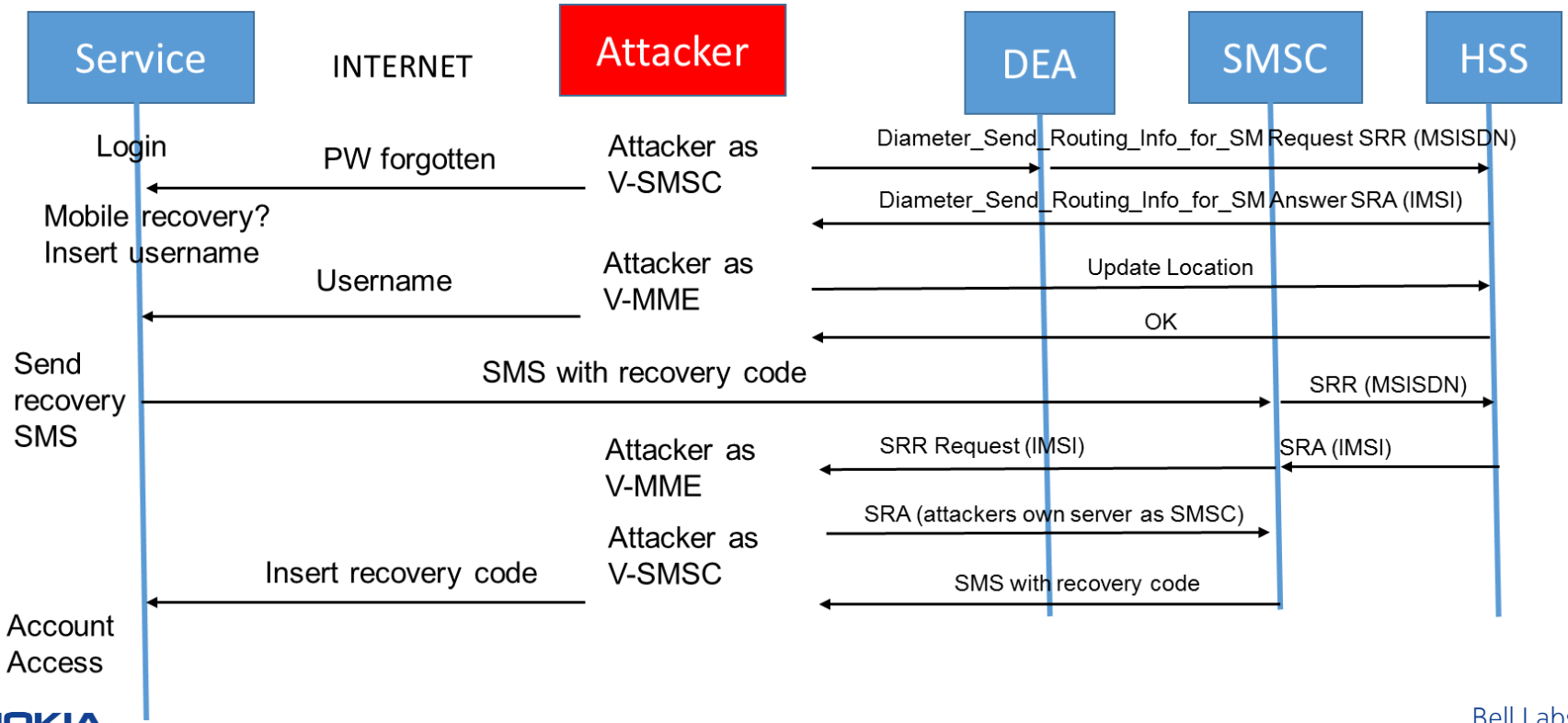

```
<command name="Cancel-Location-Request" code="317">
  <avp name="User-Name" value="235919999994001" />
  <avp name="Cancellation-Type" value="2" />
  <avp name="CLR-Flags" value="3"/>
</command>
```

IDR usage for Location Tracking

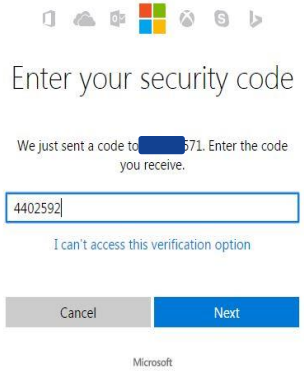


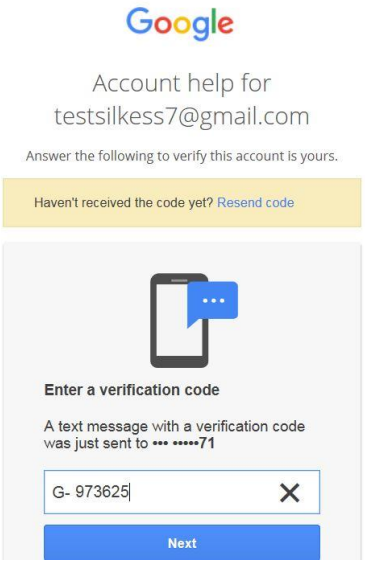
One Time Password Interception using SMS

LTE Diameter based



Services that use SMS password recovery



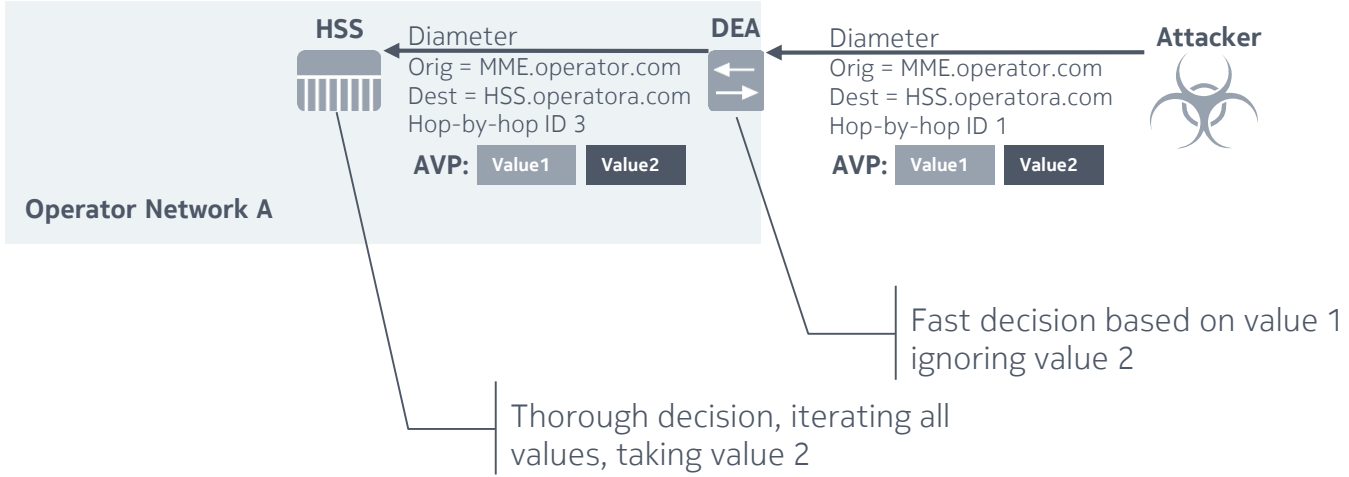


To reset your password via text from the Snapchat Login screen:

1. Tap "**Forgot Your Password?**"
2. Then select how you would like to reset your password (via text).
3. A verification code should be sent to the phone number associated with your account.
4. Enter the verification code and select "**Continue**".
5. Finally, choose and enter your new password.

Diameter Security – Old tricks come again (implementation specific)

Diameter message manipulation - Attribute Value Pair (AVP) doubling.



Diameter messages can be manipulated to contain multiple AVPs of the same kind (same AVP id) even though the specification clearly says it's illegal to do so.

IoT & Interconnection

Who are IoT B2B customers?

Public Sector

- Public Safety
- Defense
- Government Broadband
- Smart Cities/Smart Government

Energy

- Utilities
- Electricity
- Oil, Gas & Mining
- Utility Broadband

Transportation

- Railways
- Highways
- Logistics
- Aviation/Airports
- Maritime

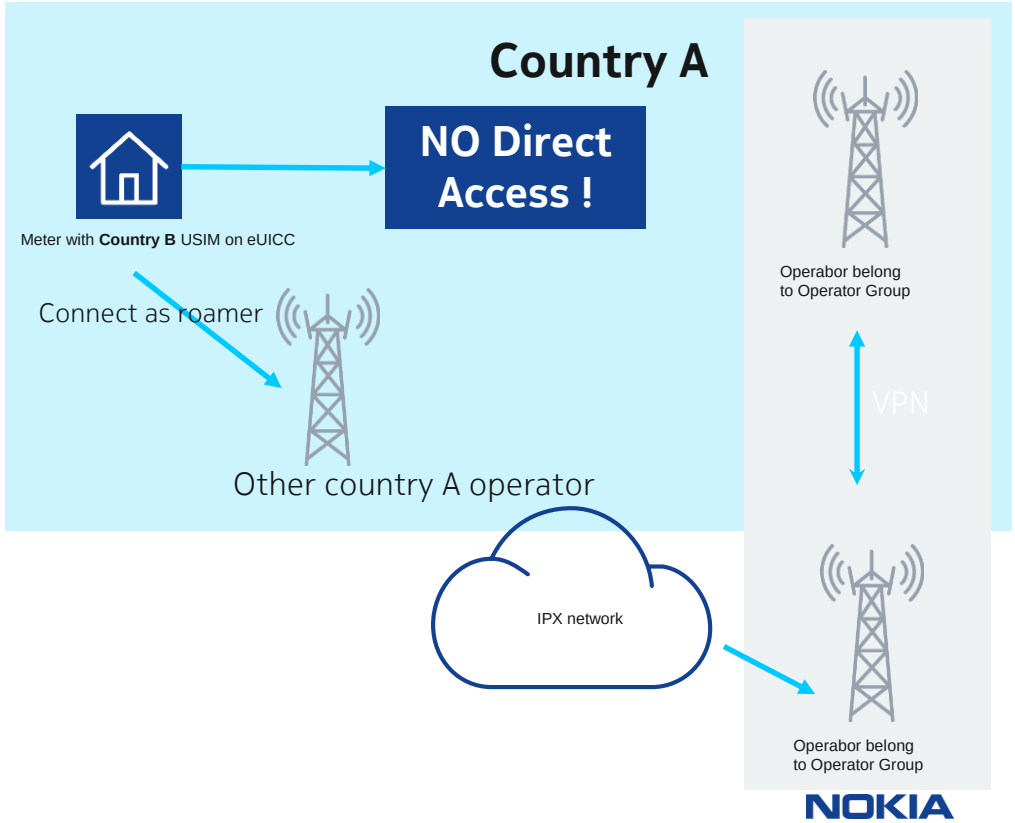
Large Enterprises

- Financial
- Healthcare
- Automotive
- Retail

There might be many roaming IoT devices

Roaming IoT devices

- Even meters, buiding sensors etc may roam (coverage reasons). In particular for global operators.
- Normal roaming e.g. cars, logistics etc
- Broker SIMs (e.g. Apple iSIM)
- Ease of production
- New business models e.g. global company wanting to have a ”harmonized” infrastructure and being supplied by one connectivity supplier
- Large amounts of same device types behaving in the consistent same

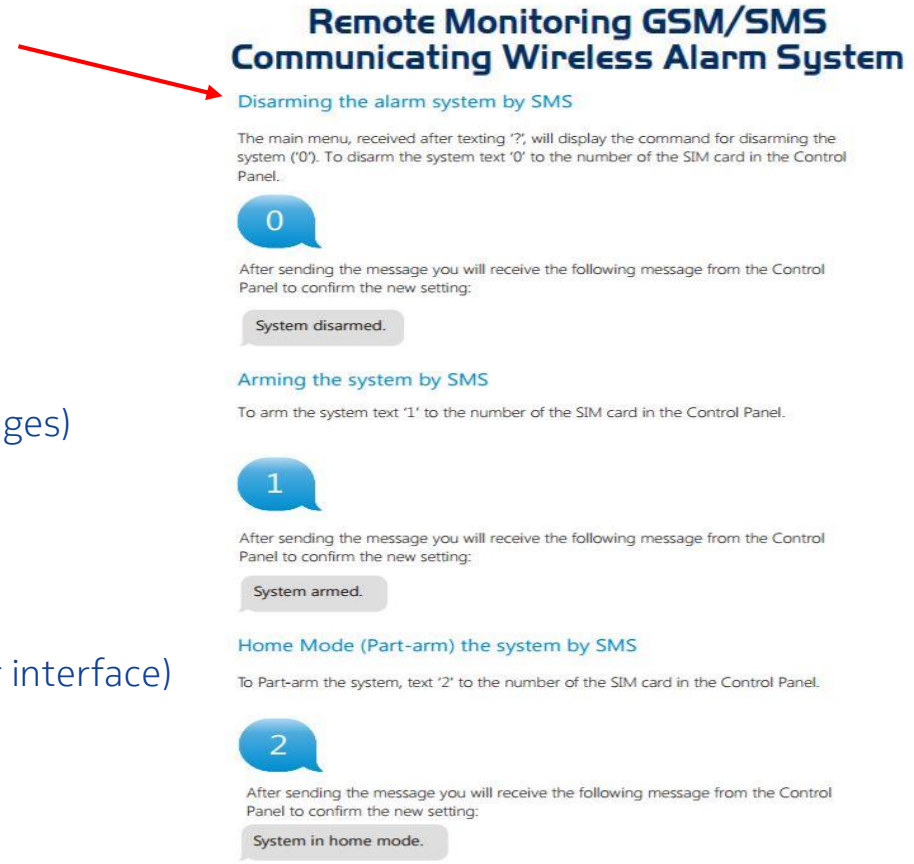


”Classical” Interconnection Risks

Affecting also IoT devices

- **Location Tracking**
- **Fraud**
- **Credential Theft**
- **SMS Attacks**
  - Interception
  - Spoofing (steering messages / reporting messages)

- **GTP data attacks**
  - Session hijacking
  - Cryptographic key theft (potentially used on air interface)

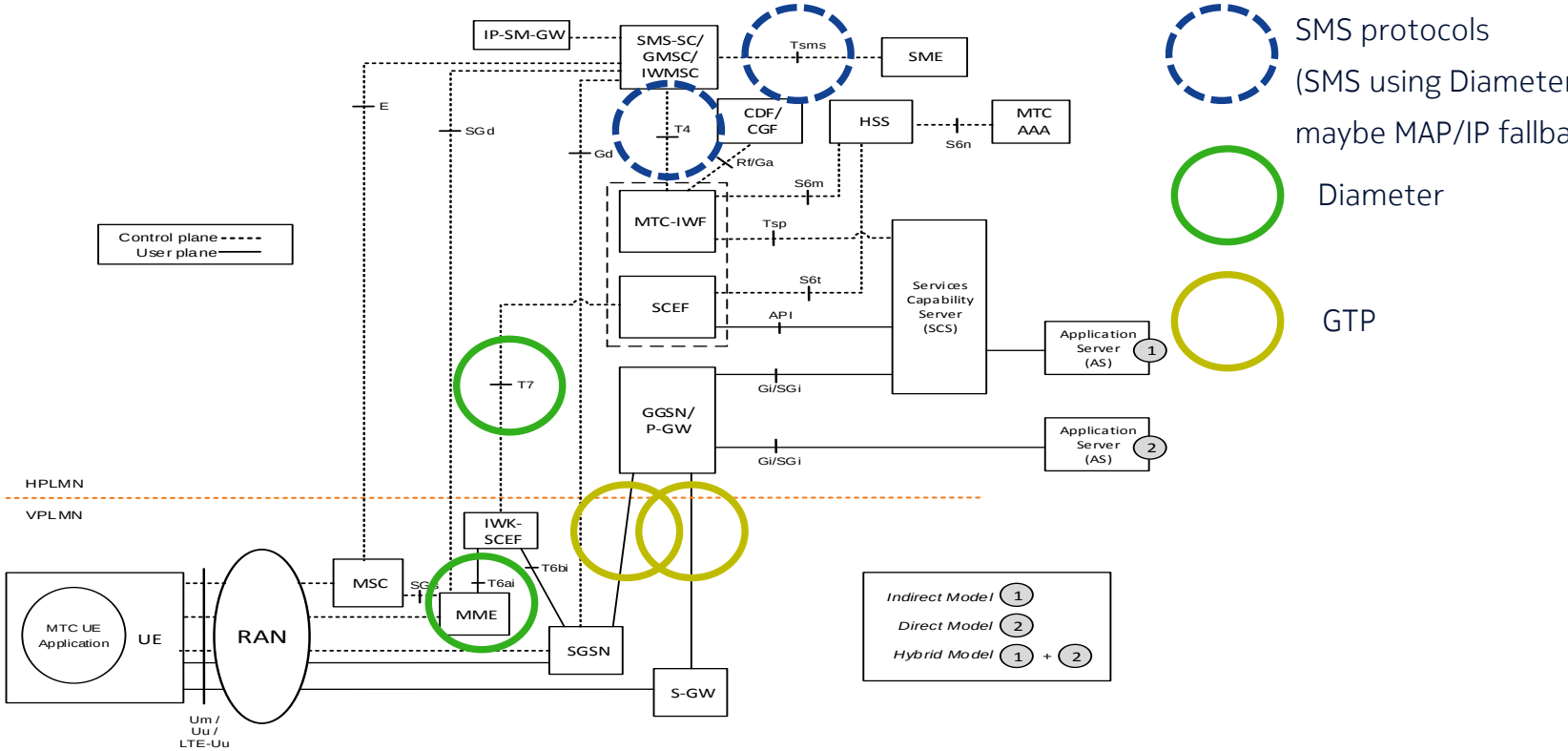


3GPP Release 14 – IoT Extensions
TS 23.682

- Trust model for new interfaces is the same as for the existing ones
  - 3GPP TS 33.210 to be used for connecting to partners
- Easy interworking and access for machine service providers
- Non-MSISDN based devices
  - External identifier (DNS resolvable)
- New nodes and interworking functions to allow seamless integration into existing networks

3GPP TS 23.682 - Protocols

Figure 4.2-1b: 3GPP Architecture for Machine-Type Communication (Roaming)



IoT and Interconnection - Summary

- **New IoT interfaces bring new risks**
  - Some risks similar to existing risks, but could be ”larger in scale”
  - Trust model need to be carefully studied when opening up new interfaces
  - Business models (i.e.coverage) may suddenly open up interfaces that were not designed for interconnection i.e. extra protection needed
- **New Security Approaches for IoT Roaming**
  - Understanding and profiling of groups of devices
  - Roaming specific aspecs for groups of IoT devices need to taken into account at network edge
  - Specific IoT group filtering capabilities needed in long run

- **Today:**
  - One subscription is roughly like another from security point of view (exception pre-paid)

Countermeasures

Let's use IPSec

Good idea, but….

- 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 for operators

Detect Monitor network traffic Penetration & re-testing Tenant monitoring	**Mitigate** Filter, filter, filter Signaling Firewall SMS Home Routing
Cooperate Share experiences (GSMA) IPSec with partners e.g. EU Cooperation with legislators	**Prepare** Follow FS.11,FS.19,FS.07 Find weak spots Node hardening/procedures

Summary

Summary

- Interconnection attacks are reality, but current main focus is SS7

  -> attackers move also with technology

- LTE/Diameter has similar functionality

  -> hence similar attacks are possible there

- Security is not part of operator core business model

  -> impacts and risks too large to ignore

- Independent of phone, platform or device

- Will LTE face the similar Interconnection weaknesses as SS7?

  -> If networks don’t take protection measures, then yes.

Questions?

Silke.Holtmanns@nokia.com