ETSI Security Week 2020 goes virtual!

Deploying 5G Securely
5G Deployment

Presented by: Marcus Wong Futurewei
Silke Holtmanns, AdaptiveMobile Security
Pieter Veenstra, Net Number
<table>
<thead>
<tr>
<th>Date</th>
<th>Time</th>
<th>Session</th>
</tr>
</thead>
<tbody>
<tr>
<td>Monday 8 June</td>
<td>3pm</td>
<td><strong>5G Deployment</strong></td>
</tr>
<tr>
<td>Tuesday 9 June</td>
<td>3pm CET</td>
<td>SSP: The New Smart Secure Platform - A High Level Introduction</td>
</tr>
<tr>
<td></td>
<td>4.45pm</td>
<td>SSP: The New Smart Secure Platform - The Technical Realisation</td>
</tr>
<tr>
<td>Wednesday 10 June</td>
<td>10.30am</td>
<td>Insight into the First Steps of the Cybersecurity Act Reality</td>
</tr>
<tr>
<td>Thursday 11 June</td>
<td>10.00am</td>
<td>Consumer IoT Security Standards</td>
</tr>
<tr>
<td></td>
<td>11.30am</td>
<td>Consumer IoT Security – Certification Schemes</td>
</tr>
<tr>
<td>Monday 15 June</td>
<td>3pm</td>
<td><strong>5G Security for Verticals</strong></td>
</tr>
<tr>
<td>Tuesday 16 June</td>
<td></td>
<td><strong>5G Security Evolution</strong></td>
</tr>
<tr>
<td>Wednesday 17 June</td>
<td>10.30am</td>
<td><strong>5G Network Certification</strong></td>
</tr>
<tr>
<td>Thursday 18 June</td>
<td>10.00am</td>
<td>Security Challenges and Regulatory Aspects</td>
</tr>
<tr>
<td>Friday 19 June</td>
<td>10.30am</td>
<td>Industry Applications and Use Cases for Advance Cryptography</td>
</tr>
</tbody>
</table>

**Deployment 5G Securely**

Cybersecurity Act – one year on

Smart Secure Platform

Even more advanced Cryptography

scheduled in CEST
5G Deployment
Moderated by Marcus Wong, Futurewei

✔ Secure Core Network Migration
   Silke Holtmanns, AdaptiveMobile Security

✔ GSMA Investigation on 5G Security – Tracking Security Open Issues
   Pieter Veenstra, Net Number
5G Deployment Status

Mobile 5G is now commercially available from 46 operators in 24 markets worldwide; 79 operators across a further 39 markets have announced plans to launch mobile services.*

*As of January 2020
5G Deployment Status

3x: Non-Standalone/LTE-Assisted (EN-DC)

7x: Non-Standalone/NR-Assisted (NGEN-DC)

2: Standalone NR

EPC (4G)

LTE

MA 5G IC

LTE

NR

5G core

NR
Resistance is futile

3G/4G Core + 5G Core = Operational Network

Point-to-point + Service Based Architecture = Support for legacy
Attackers think differently

- 2G attack
- 3G/4G attack
- 5G attack

Attacker

SS7 FW
Diameter FW
SEPP
Subscriber Database
Policy & Charging
Data Session Handling
Mobility Handling

Policy & Charging
Data Session Handling
Mobility Handling
Subscriber Database
SEPP
Diameter FW
SS7 FW
Attacker
IPX Ecosystem

- Value Added Service Provider
- MNO1 4G
- Home Network
- Interconnection Network (IPX)
- Partners and potential message paths
- Roaming Hub
- MNO2 5G SA
- MNO3 2G-3G
- Visited Networks

MNO4 5G NSA

Partners and potential message paths
Migration Scenario 1 – Mobility Migration (HR)

- Normal Outbound Roaming Scenario
  - Home routed traffic is assumed
- Home Network has a 5G core with support for “4G legacy”
- Visited partner network has 4G and 5G RAN with dual core
  - User plane traffic is routed via home-network
- User starts a browsing session in his vacation
Migration Scenario 2 – 4G Supported Non-3GPP Access

• Outbound roaming scenario
• Usage of “legacy” 4G-based Non-3GPP access at a partner
• Home network supports legacy
• Traffic is home-routed
• Architecture for interworking between 4G ePDG/EPC and 5GS
Interworking between ePDG/EPC and 5GS

3GPP AAA Server

HSS + UDM

PGW_C + SMF

SWx

S6b

Fine tuned Diameter FW

Fine tuned GTP-C FW

User Plane protection

HOMENETWORK

N8

N10

N16

N24

N9

N4

N11

N15

N3

N2

N1

VISITED NETWORK

3GPP AAA Proxy

ePDG

vSMF

vPCF

UPF

PGW_U + vPF

3GPP AAA Proxy

Fine tuned Diameter FW

Fine tuned GTP-C FW

User Plane protection

SEPP

N24

N16

N10

N8

NG-RAN

AMF

© Copyright 2020 All rights Reserved.
Migration Scenario 3: Subscriber Database Migration

- 4G User Data Repository (UDR) in place
- HSS used to support 4G “legacy” core
- 5G Unified Data Management (UDM) “frontend” in place
- 5G User Data Repository (UDR) “frontend” in place
- Addressing of HSS using a REST API Nhss
IMS integration to 5G SBA

Service Based Architecture (SBA)

Sh, Cx

Gm

5G System

IMS Domain
Migration Threats – Countermeasures – Your toolbox

- SS7 attacks
- Diameter attacks
- 5G attacks
- New attack vectors & changing attacks
- Bad configuration / operation
- GTP attacks
- Bad user traffic
- Bad security quality

- SS7 Firewall (incl. CAMEL)
- Diameter Signaling FW
- SEPP
- Threat intelligence, update service & research
- Regular pentesting / scanning
- GTP-C Firewall
- GTP-U traffic scanner
- 3GPP & GSMA SCAS
Conclusion

- **Migration plans for core network need to consider:**
  - Make a plan on interfaces and what protocols they support
  - Each protocol needs its own protection
    - Some existing firewall can be adjusted
  - Correlate attacks to see if attacks use a toolbox
  - Assume that your defenses are breached at some point and prepare for “containing” the attack

- **Dynamic evolution with the migration**
  - How are you partner evolving?
  - Fine tune security along with their evolution
  - Threat intelligence and evolution to counter attacks immediately
More details?

16.6.2020
White Paper & Webinar


Silke.Holtmanns@adaptivemobile.com
Presenter: Pieter Veenstra, Net Number
GSMA Investigation on 5G Security – Tracking Security Open Issues
GSMA INVESTIGATION
5G SECURITY

Tracking Security Open Issues

Pieter Veenstra
NetNumber - Senior Manager Product Development
GSMA – FASG RIFS Chair
http://www.linkedin.com/in/pkveenstra
SESSION OVERVIEW

• Snapshot NetNumber

• GSMA investigation 5G Security

• Why is 5G Security needed?

• What changes with 5G Security?

• When does 5G become safer than LTE?

• Take-Aways

• Best Practices
NetNumber Snapshot

Unique Software Platform TITAN
Enables Network Transformation, reduces CAPEX, OPEX and Time to Market

Solutions from 2G – 5G, Private LTE IoT/M2M

Our Customer Segments

Mobile Network Operators
Fixed Line Operators
Cloud
IoT / M2M
Cable
Enterprise, Govt, Utilities, Satellite

Changing Future of Telco Networks
Eliminate latency, Simplify signaling core, Bundled apps, Data

Main offices in Boston, Frankfurt, Prague & Warsaw
220 Employees
Presence in 22+ countries
Founded 1999

Trusted by 200+ global customers

February 2020 Finalist
“Best Mobile Authentication & Security Solution”

June 2019 Winner,
“Best Network Security Technology”
Customer and Partner Snapshot

16 out of 20 largest Global Telcos and 18 IPX carriers use NetNumber TITAN
Investigation 5G Security

Tracking Security Open Issues

GSMA Activity
• Initiative kicked-off end 2017 in FSAG
• Overview with guidelines in PRD FS.40

Purpose
• Collect 5G security open issues relevant to GSMA members
• Per issue sketch of context and problem
• Track per issue if resolved in standards or to be covered by GSMA guidelines

Scope
• Initial focus issues in 3GPP Release 15
• Where applicable listing refinements and open issues in 3GPP Release 16
Why is 5G Security needed?

NetNumber as a Trusted Advisor
Why is 5G Security needed?

- High trust as 5G will become a critical asset with the digital transformation of our society and industry

- Stricter information privacy rules and data protection legislation (EU GDPR)

- Mandatory encryption of all information transfer as 5G networks are built with layered and virtualized technologies

- Considering the limitations of SS7 and risks for our customers, we won’t survive another network generation without operator-to-operator security

GDPR = General Data Protection Regulation
The earlier 2G/3G and 4G/LTE mobile networks ...
... but the 5G Core network will look very different

Source GSMA: 5G status update
What changes with 5G Security?

NetNumber as a Trusted Advisor
Secure by Design

5G standards development has adopted ‘Secure by Design’ principles, leading to:

- Use of Mutual Authentication
  - Confirming sender and receiver have an established trust and the end-to-end relationship is secured
- A presumed “open” network
  - Removing any assumption of safety from overlaid product(s) or process(es)
- An acknowledgment that all links could be tapped
  - Mandating encryption of inter/intra-network traffic, ensuring the encrypted information is worthless when intercepted

 Paradigm shift to existing Telco practices as this requires mandatory encryption of inter/intra-network and privacy sensitive information under all circumstances!
Subscriber Protection

5G improves confidentiality and integrity of user and device data:

• Providing confidentiality of the initial non-access stratum (NAS) messages between the device and the network

• Introducing home control, preventing various roaming fraud types

• Supporting unified authentication across other access network types

• Introducing user plane integrity checking

• Enhancing privacy protection with the use anchor keys

Increased subscriber privacy and data protection
False base station (Stingray phone tracker) prevention
Authentication confirmation added to combat fraud
Equivalent high security offered via WiFi and alike networks
Network Slicing

End-to-End Isolation in RAN, TN, and CN of slices in a 5G network

Aspects are still under discussion how this end-to-end isolation can be guaranteed under all circumstances!
Network Protection

Signaling Data Integrity

• The inter-PLMN interface is a sensitive interface, operators are responsible to protect their (user) assets, mandatory

• Attention on attacks & privacy concerns (like GDPR) will grow over time with the next steps of the digital transformation

New IT signaling protocol stack

• Taking advantage of high-performance computer resources and best practices in data centers and internet technology

• Avoiding another network generation with telecom specific signaling issues
When does 5G become safer than LTE?

NetNumber as a Trusted Advisor
Tomorrow’s 5G service with 5G Security as designed

With 5G devices controlled by a 5G Core via both 5G radio and LTE radio

The comprehensive 5G Security enhancements only work if the 5G enabled mobile device is controlled by a 5G Core!

5G UE = 5G mobile device
RAN = Radio Access Network

5G UE
RAN
Core

LTE

5G
Tomorrow’s 5G roaming with 5G Security as designed

With 5G devices controlled by a 5G Core via both 5G radio and LTE radio

The comprehensive 5G Security enhancements only work if the 5G enabled mobile device is controlled by a 5G Core and if you connect to a 5G Core network when travelling!

5G UE = 5G mobile device
RAN = Radio Access Network
VPMN = Visited Public Mobile Network
HPMN = Home Public Mobile Network
5G SA = 5G Stand-Alone Architecture
But today’s 5G service still works with LTE Security

With 5G devices controlled by an LTE Core via both 5G radio and LTE radio

Today’s 5G services are mainly with only 5G radio networks and re-use of the existing investments in LTE Core networks by which no advantage can be made of 5G Security

5G UE = 5G mobile device
RAN = Radio Access Network
VPMN = Visited Public Mobile Network
HPMN = Home Public Mobile Network
5G NSA = 5G Non-Stand-Alone Architecture
Coexistence with legacy mobile generations

The rollout of 5G will take years

- 1.8 billion 5G connections in 2025 with developed Asia and the US in the lead
- North America 48% and global coverage 20.1% in 2025

Interworking with legacy Signaling

- SS7 and Diameter are known for their security vulnerabilities
- Mobile roaming is a global eco-system with about 800 mobile operators
Protection Capability per Signaling Type

5G NSA scenario

HTTP/2
5G SA scenario

HTTP/2

Confidentiality Protection (Encryption) on top of Authentication and Integrity Protection

DESS Phase 1

Authentication and Integrity Protection (Digital Signature)

No Protection

An integrated SS7 / Diameter signaling firewall also protects 5G users
TAKE-AWAYS

NetNumber as a Trusted Advisor
TAKE-AWAYS

The digital transformation of our society and industry need the advanced 5G Security

but

5G is still LTE Security without implementation of a 5G Core

Roaming traffic is a dangerous backdoor and needs very comprehensive firewalls
BEST PRACTICES
NetNumber as a Trusted Advisor
BEST PRACTICES

Carriers should deploy 5G including 5G Core control

Reuse of existing LTE radio but with 5G Core control

Roaming traffic protected with an integrated SS7 and Diameter Firewall
Questions & Answers
Upcoming webinars in the thread Deployment 5G Securely:

10 June, 3pm: 5G Security for Verticals
16 June, 3pm: 5G Security Evolution
18 June, 10am: Security Challenges and Regulatory Aspects
Thank you for joining this webinar!

Find the full ‘ETSI Security Week 2020 goes virtual’ programme at

www.etsi.org/etsisecurityweek