5G Security Research at Nokia Bell Labs

• Peter Schneider
• ICT SICS Security Day, 11-05-2016
Agenda

• NGMN as a source of 5G security requirements
• 5G Security Vision
• TrustCom15: Further steps “Towards 5G Security”
• 5G-PPP projects - 5G NORMA
• 3GPP next generation security
• Elements of a 5G security architecture / 5G security research topics
• Examples: network slicing, network based anomaly detection, security orchestration
NGMN Alliance – An important source of views and recommendations

“5G Whitepaper”, Version 1.0, 17-February-2015:
• “enhanced performance is expected to be provided along ... with the capability to, among others, ensure security and trust, identity, and privacy”
• Mentions various requirements for improved security compared to 4G (→ next slide)
Quotations from the NGMN “5G Whitepaper”

• “5G should be designed to provide more options beyond node-to-node and end-to-end security available in today’s mobile systems”
• “design of security solutions (e.g. key exchange/derivation protocols upon handover or when interworking with other RATs) should provide better secrecy than 4G”
• “Specific security design for use cases which require extremely low latency (including the latency of initiating communications)”
• “Improve resilience and availability of the network against signalling based threats, including overload”
• “Improve system robustness against smart jamming attacks of the radio signals and channels”
• “Improve security of 5G small cell nodes”

➢ Substantial security requirements!
“5G Whitepaper”, Version 1.0, 17-February-2015:
• “enhanced performance is expected to be provided along ... with the capability to, among others, **ensure security and trust, identity, and privacy**”
• Mentions various requirements for improved security compared to 4G

NGMN 5G Security Group:
• “does not make requirements, just recommendations”
• Recommendations concerning improvements of the access network, DoS protection (has been sent to 3GPP)
• Document on network slicing security, approval pending
• To come: Mobile edge computing, low latency, consistent user experience
5G Security Vision

Supreme built-in security
Flexible security mechanisms
Automation

New use cases
New threats
New networking paradigms
Changing ecosystem
Growing need for flexibility
Growing need for dependability

Sound security concepts must be built into the 5G architecture right from the start!
5G Security Vision – a slightly deeper look

**Higher level of security**
- Increased robustness against cyber attacks
- Enhanced privacy
- Security assurance

**Higher flexibility in the selection of security mechanisms**
- Alternative identification and authentication procedures
- User plane encryption and integrity protection optional to use
- Adjust security mechanisms per network slice

**Higher degree of security automation**
- Holistic security orchestration and management
- Self-adaptive, intelligent security controls

---

Proven network security concepts

- Standardized e.g. 3GPP LTE security
- Non-standardized e.g. traffic separation, security zones, secure OAM

Secure software and platforms
IEEE-TrustCom-15: Further steps “Towards 5G Security”

The “1st IEEE International Workshop on 5G Security”, organized by people from Nokia T&I Research, now Nokia Bell Labs

• Overall 5G security views of vendors - on this level not controversial
• Further presentations on security topics relevant for future networks

From https://research.comnet.aalto.fi/Trustcom2015/index.html
Security requirements

Building on LTE security

Potential 5G security mechanisms

- User and Device Identity Confidentiality
- Mutual authentication and key agreement
- Security between terminal and network
- Security on network interfaces
- Security visibility and configurability
- Platform security
- Protection against DoS attacks

Implication of NFV and SDN
Example: Security between mobile and network and on network interfaces

### LTE
- Access stratum security
- Backhaul link security
- Non access stratum signaling security

- eNB
- MME
- HSS
- PCRF
- Serv.-GW
- PDN-GW
- IMS / Operator services
- Internet

### 5G ?
- 5G remote radio head
- 5G-NB
- Local NFV platform
- Aggregation cloud
- Central cloud
- Internet
5G PPP

• “The 5G PPP will deliver solutions, architectures, technologies and standards for the ubiquitous next generation communication infrastructures of the coming decade.”
  From https://5g-ppp.eu/

• 5G PPP Security Working Group: Various projects have shown interest
  - 5G-ENSURE (initiator), 5G NORMA, 5G-SPEED, 5GEX, CHARISMA, COGNET, SELFNET, SESAME, VIRTUWIND

• 5G NORMA: A NOvel Radio Multiservice adaptive network Architecture for the 5G era → Combining architecture and security work
5G NORMA Consortium

5G NORMA in a nutshell
EU funded R&D project within 5GPPP Initiative, aiming on building consensus on E2E mobile network architecture and rapid implementation

Duration
July 1st, 2015 – Dec 31st, 2017 (30 months)

Project Coordinator
Simone Redana, Nokia

Connect to 5G NORMA
Webpage: https://5gnorma.5g-ppp.eu/
Twitter: 5G NORMA project @5G_NORMA
5GPPP: https://5g-ppp.eu/

Contact 5G NORMA
5G-NORMA-Contact@5g-ppp.eu
5 x 5G NORMA Innovations

1. Software Defined Mobile network Control (SDMC) applies SDN principles to mobile network

2. Adaptive (de)composition and allocation of mobile network functions (c-plane and u-plane) between network and edge cloud that depends on the service and deployment

3. Joint optimization of mobile access/core network functions when located together in the network or edge cloud

4. Multi-service- and context-aware adaptation of network functions to support a variety of services and corresponding QoE/QoS requirements

5. Mobile Network Multi-tenancy to support on-demand allocation of edge and network cloud resources in a fully multi-tenant environment

Source: 5G NORMA Consortium
## 5G NORMA Security

<table>
<thead>
<tr>
<th>5G NORMA Feature</th>
<th>Related Security</th>
</tr>
</thead>
<tbody>
<tr>
<td>NFV environments for core and RAN functions</td>
<td>NFV security (for central and distributed NFV environments)</td>
</tr>
<tr>
<td>Software Defined Mobile Network Control (SDMC)</td>
<td>SDN security, specialized for SDMC</td>
</tr>
<tr>
<td>Mobile network multi-tenancy</td>
<td>Tenant isolation, network slicing security</td>
</tr>
<tr>
<td>Multi-service awareness</td>
<td>Flexible security approach, e.g. choice of crypto-algorithms</td>
</tr>
<tr>
<td>Adaptive allocation of functions, joint optimization of RAN and core</td>
<td>Flexible security approach, e.g. support for flexible allocation of security functions</td>
</tr>
</tbody>
</table>
5G NORMA: Radio Interface Security Termination Functions

- **Bare Metal RAN Equipment**
  - Low Layer Functions
  - Secure Environment
    - Radio Interface Security Termination Function
    - Backhaul Link Security Termination Function
  - Other RAN Functions
  - Secure Radio Interface
  - Secure Backhaul Link

- **UE**
  - Secure Radio Interface
  - Physically Exposed Entities

- **Secure Cloud**
  - Other RAN Function
  - Secure Communication in the Cloud
  - Other Core Function
  - Backhaul Link Security Termination Function

- **Radio Interface Security Termination Function**

- **Other Core Function**
3GPP (3rd Generation Partnership Project)

- **SA1 – Services (➔ requirements):**
  - “SMARTER” Technical Report TR 22.891
  - Four dedicated TRs on Massive Internet of Things (mIoT), Critical Communications (CriC), Enhanced Mobile Broadband (eMBB), Network Operation (NEO)
  - An overview of security requirements in these reports is given by a current SA3 contribution (S3-160458)

- **SA2 – Architecture: Study ongoing (TR 23.799)**
  (includes an authentication framework as a topic to be investigated)

- **SA3 – Security: see next slide**

- Security appears also in the work of RAN groups
3GPP SA 3

- SA3 – Security: Study agreed, skeleton of TR 33.899 exists, security “key issues” as well as solutions to be investigated
  - ~60 contributions to SA3 Meeting #83 (this week), proposing various security areas
  - and a lot of key issues, partly already with solutions
LTE Security Aspects – A more detailed view

More security aspects: Mobility (key separation in handovers), Home eNB, Relay Node, non-3GPP access, dual connectivity (LTE, LTE/WiFi), proximity services (incl. device-to-device communication), security assurance methods, ...
Elements of a 5G Security Architecture → Research Topics

- Authentication/authorization, key agreement
  - EPS-AKA, EAP-AKA', EAP-xyz, others?

- Security negotiation, key hierarchy
  - Enhanced C-plane robustness
  - Enhanced subscriber privacy

- C/U-plane security
  - Crypto algorithms
  - Protocol layer for sec.
  - Physical layer sec.
  - Jamming Protection

- 5G remote radio head

- Local NFV platform

- Aggregation cloud

- Central cloud

- Security negotiation, key hierarchy
  - Enhanced C-plane robustness
  - Enhanced subscriber privacy

- NFV security

- Network slicing security

- Security assurance for NFV environments

- Security management and orchestration

- Self-adaptive, intelligent security controls

- Subscriber Id, Device Id, credentials
  - (e/i)UICC, other security modules

- Security awareness and control

- Crypto algorithms

- Protocol layer for sec.

- Physical layer sec.

- Jamming Protection

19 © Nokia Solutions and Networks 2016
Network Slicing Security

NGMN
- (Sub-)network slice blueprint/instance
- Sharing subnetwork slice instances
- Security considerations

Network slicing discussed in Research Projects, in 3GPP (SA1, SA2, SA3)

The obvious basic security requirement: Isolation!
Should be provided in the cloud by cloud security mechanisms.

Are we OK? Maybe not. Don’t know how to hack a hypervisor? Take a tutorial!
(https://www.troopers.de/events/troopers15/293_exploiting_hypervisors/)

➢ “Participants will learn about the [...] security pitfalls of these platforms and will analyze and exploit three recent vulnerabilities in these hypervisors”
Holistic Security Management and Orchestration

Virtual Infrastructure Manager
- Openstack
- VMware (vCenter, vCloud)

Data Center Hardware
- Compute
- Storage
- Network (SDN)

Security Orchestrator
- Trust Management
- Hardening
- Network Protection
- Data Protection

Design (policies and topology)
Automation (policies, compliance validation)

ETSI NFV Reference Architecture
- NFVO (Network Service Lifecycle)
- VNF Manager (VNF Lifecycle)
- VNF Manager
- VNF
- KVM
- VMware (ESXi)
- Security Functions

Security Orchestration
- PSF
- Data Protection
- Network Protection
- Hardening
- Trust Management

Security Functions
- Design (policies and topology)
- Automation (policies, compliance validation)

Virtual Infrastructure Manager
- Security Features
- Security Features

ETSI NFV Reference Architecture
- NFVO (Network Service Lifecycle)
- VNF Manager (VNF Lifecycle)
- VNF
- KVM
- VMware (ESXi)
- Security Functions

Security Orchestration
- PSF
- Data Protection
- Network Protection
- Hardening
- Trust Management

Security Functions
- Design (policies and topology)
- Automation (policies, compliance validation)
Example: Network based Anomaly Detection for IoT

Managed corporate IoT networks
- Known network architecture
- Known device types

Dashboard for IoT and end user devices
Uses device profiles and Telco data for detection and automated mitigation
Detailed real-time information about infected devices

---

Radio
Core

Security Insight (Dashboard)
Malware intelligence DB
Action Engine (automated actions)
Correlation of traffic

Sense
Analyze

Decide
Securing 5G networks is a multi-faceted, interesting and challenging task!

Questions?