

5G Security Overview

overview based on global experience

Faris Al-Katib – Lead Security Consultant – NOKIA Security

June 2019

What is 5G?

5G is the next generation mobile broadband

enhanced Mobile Broadband



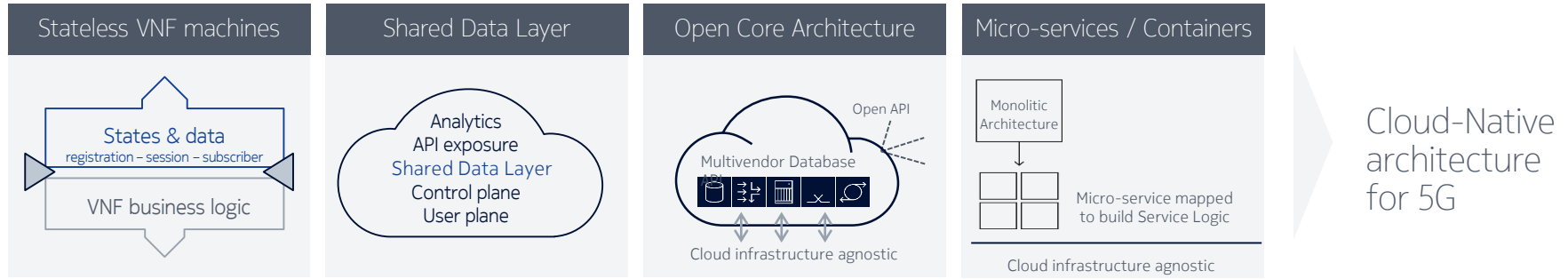
massive Machine Type
Communications

Ultra Reliable Low
Latency
Communications

NOKIA

How?

Nokia 5G Cloud-Native Core strategic direction



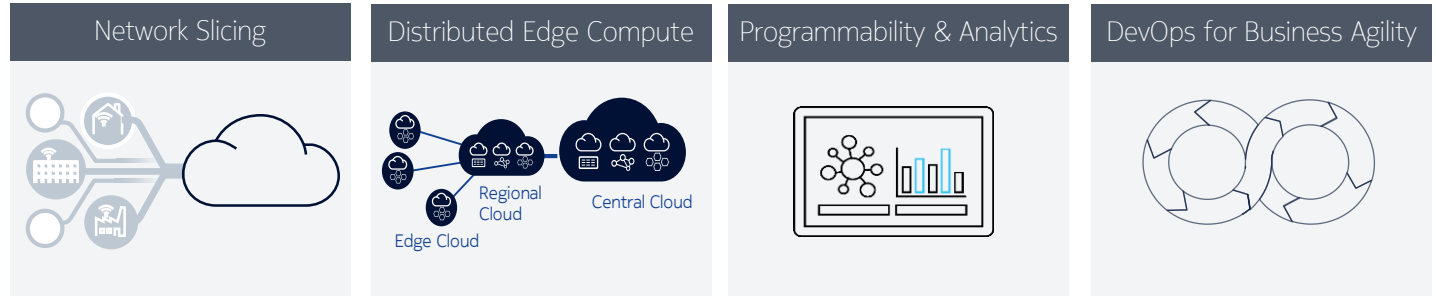
Cloud Technology Drivers

for Nokia Products and Solution

Business Transformation Drivers

for Operators to monetize cloud investment

Automated
Operation &
Cloud Agility



Key 5G Security Challenges

Fall all IP Service-Based Architecture

(increase network openness (API's), Increased complexity of trust relationships)

High traffic volumes with extreme diversity of devices

Automation, Orchestration & distributed cloud networks

(radio core, telco core, connectivity to private and public cloud)

5G Security

Evolving Threats

Massive increase in scale and complexity (ATP attacks, DDoS ... etc.)

Digital Time & new business models (Slicing)

Protection of control, user, data, management plane

Cyber attack strategy advancement demands a different approach

Cyber criminals are now using automation and artificial intelligence to attack companies and networks more efficiently. They're also exploiting an attack surface that's growing as companies embrace cloud, Internet of Things (IoT) and 5G technologies.

End-to-end security
for digital networks
and operations

Analytics that correlates
data from networks, devices
and cloud to spot anomalies

Automate security for
business processes,
regulations and policies

...to protect assets and interests:

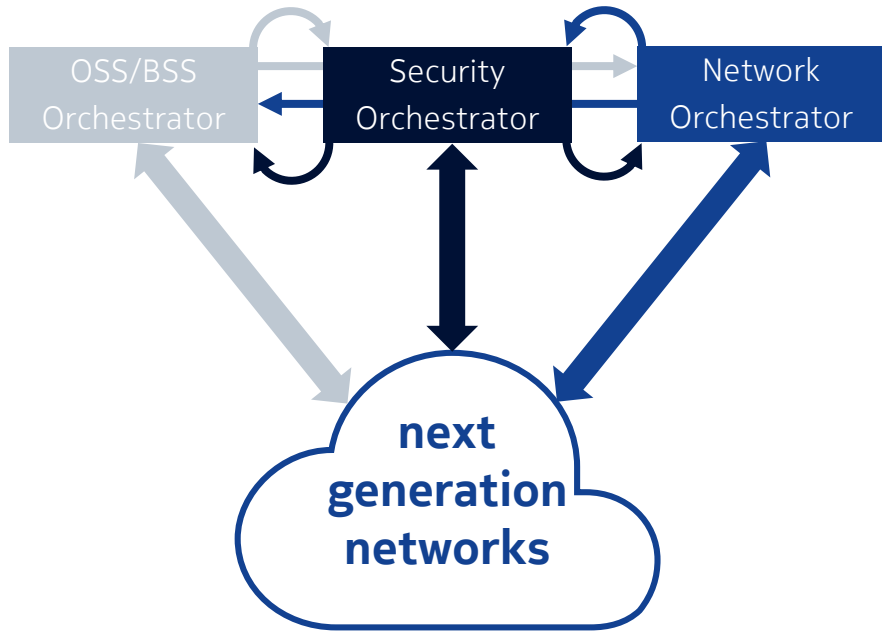
SOAR

Security **O**rchestration **A**nalytics and **R**esponse



NOKIA SOAR

Security Orchestration (SOAR)



ETSI Group Specification (GS) NVF Security 001-0013

- There are 3 orchestrators in the network
- They are parallel to each other each one with a unique task
- All of them together achieve the automation and orchestration task ensuring security lifecycle management

These 3 orchestrator interact with each other and with the network to achieve the objectives

Still, standards only define high level ideas, guidelines and methodologies they do not explain how to achieve objectives. We will have to define the techniques, processes and tools to fulfill our objectives.

Securing next generation Telco

SOAR - Security Orchestration, Analytics and Response

Automation of all security controls, security mentoring, correlation of events,
Automated Incident detection and automated security response



Securing cloud infrastructure

- Automated policy management
- While List policy enforcement
- Telco Security Zoning
- Roaming Security
- DNS Security
- Radio Access Security
- VNF/Container security

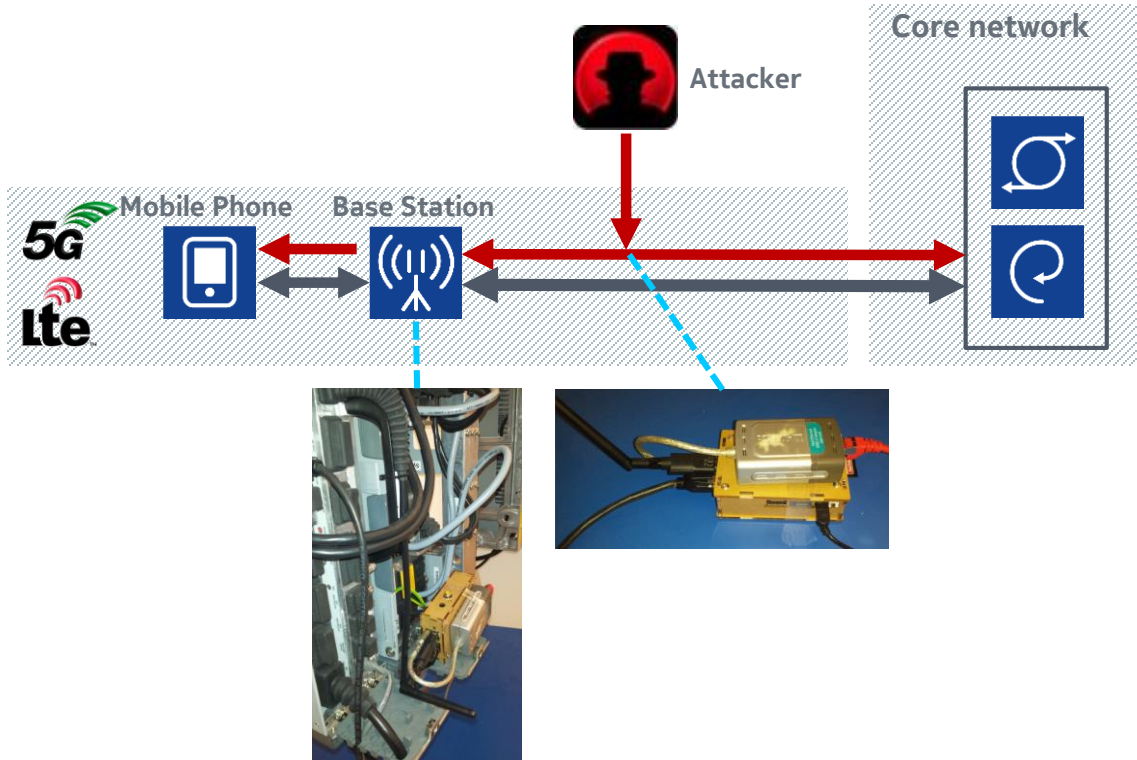
Zero Trust (assurance and verification)

- Trust in system configurations and security compliance (NIST, 2701 .. etc.)
- Trust in administrators accessing the network
- Trust in communication between network layers (use of digital certificates)
- Automated system security status
- Automated system hardening

Endpoint Security

- Network based malware, botnet and threat detection & traffic anomaly detection
- Connected devices monitoring
 - DDoS Protection and mitigation

Radio Access Security



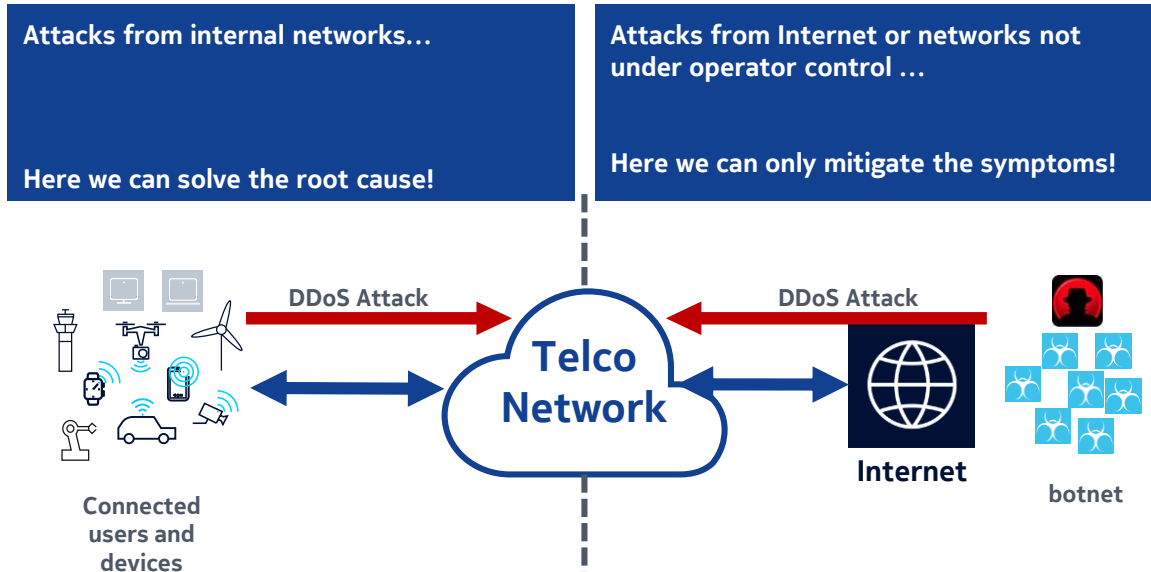
Vulnerabilities:

- Eavesdropping on subscriber data and voice
- Injection of malicious traffic (signaling and user plane)
- Unauthorized access to operator network, base station and mobile
- Denial of service attack against core network

Solution:

- 3GPP standardized solution using IPSec
- Not deployed in all mobile operators - Risk vs. investment decision

DDoS Attacks



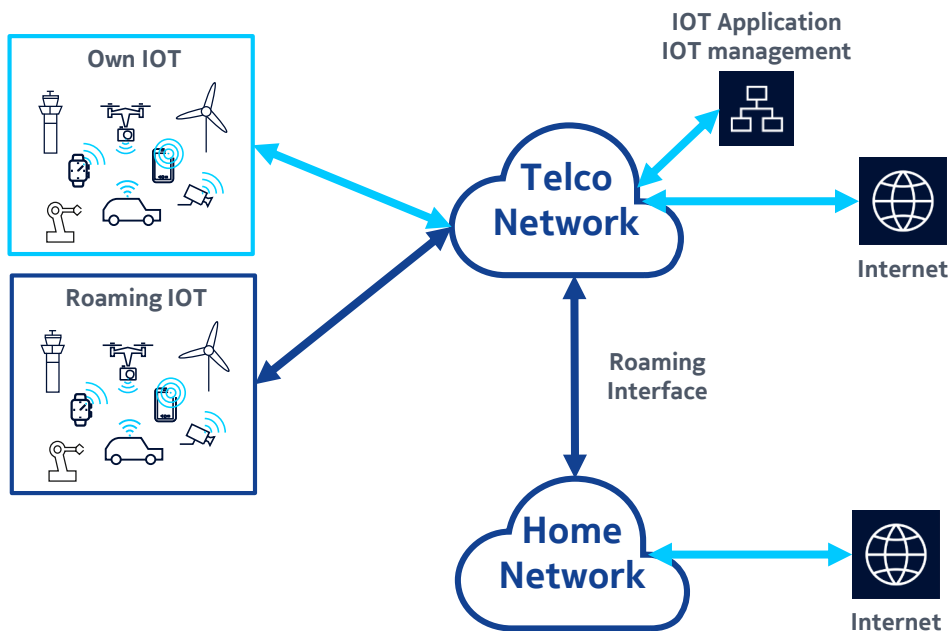
Internet DDoS Mitigation

- DDoS mitigation solutions
- Local scrubbing centers
- Global scrubbing centers

Internal DDoS Mitigation:

- Prevent the build up of a botnet inside the network
- Dedicated Telco based IDS systems
- Attacks detection
- Traffic anomalies detection based on traffic patterns
- Malware signature detection
- Recognition of end device MSISDN, IMSI, IMIE etc, from traffic flow

IoT Security



IoT in Telco networks

- Own IoT devices: covered by contracts and SLA's
- IoT devices breaking out locally to the internet
- Roaming IoT devices breaking out via the roaming interface towards their home telco network

Mitigation:

- Dedicated Telco based IDS systems
- Attacks detection
- Traffic anomalies detection based on traffic patterns
- Malware signature detection
- Recognition of end device MSISDN, IMSI, IMIE etc., from traffic flow

Chance:

- Offer security as a service to IoT vendors and operators

IoT Security

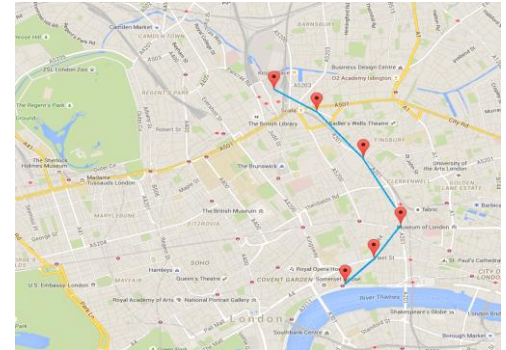
Dedicated Telco IDS System

Benefits of inspecting GTP session:

- Without any assistance, we can identify:
 - IMSI of the device
 - IMEI of the device
 - MSISDN of the subscriber
 - Cell location
- Not only signature detection, also attacks detection from internet to subscribers or from subscribers to other subscribers or to the network
- Roaming attacks covered

IMSI: 4405014220222
MSISDN: 00818093111111
IMEI: 01234567890

Cell ID - location



NOKIA

NOKIA

Copyright and confidentiality

The contents of this document are proprietary and confidential property of Nokia. This document is provided subject to confidentiality obligations of the applicable agreement(s).

This document is intended for use of Nokia's customers and collaborators only for the purpose for which this document is submitted by Nokia. No part of this document may be reproduced or made available to the public or to any third party in any form or means without the prior written permission of Nokia. This document is to be used by properly trained professional personnel. Any use of the contents in this document is limited strictly to the use(s) specifically created in the applicable agreement(s) under which the document is submitted. The user of this document may voluntarily provide suggestions, comments or other feedback to Nokia in respect of the contents of this document ("Feedback").

Such Feedback may be used in Nokia products and related specifications or other documentation. Accordingly, if the user of this document gives Nokia Feedback on the contents of this document, Nokia may freely use, disclose, reproduce, license, distribute and otherwise commercialize the feedback in any Nokia product, technology, service, specification or other documentation.

Nokia operates a policy of ongoing development. Nokia reserves the right to make changes and improvements to any of the products and/or services described in this document or withdraw this document at any time without prior notice.

The contents of this document are provided "as is". Except as required by applicable law, no warranties of any kind, either express or implied, including, but not limited to, the implied warranties of merchantability and fitness for a particular purpose,

are made in relation to the accuracy, reliability or contents of this document. NOKIA SHALL NOT BE RESPONSIBLE IN ANY EVENT FOR ERRORS IN THIS DOCUMENT or for any loss of data or income or any special, incidental, consequential, indirect or direct damages howsoever caused, that might arise from the use of this document or any contents of this document.

This document and the product(s) it describes are protected by copyright according to the applicable laws.

Nokia is a registered trademark of Nokia Corporation. Other product and company names mentioned herein may be trademarks or trade names of their respective owners.

Revision history and metadata

Please delete this slide if document is uncontrolled

Document ID: DXXXXXXXXX

Document Location:

Organization:

Version	Description of changes	Date	Author	Owner	Status	Reviewed by	Reviewed date	Approver	Approval date
		DD-MM-YYYY					DD-MM-YYYY		DD-MM-YYYY