AdaptiveMobile Security
an Enea company

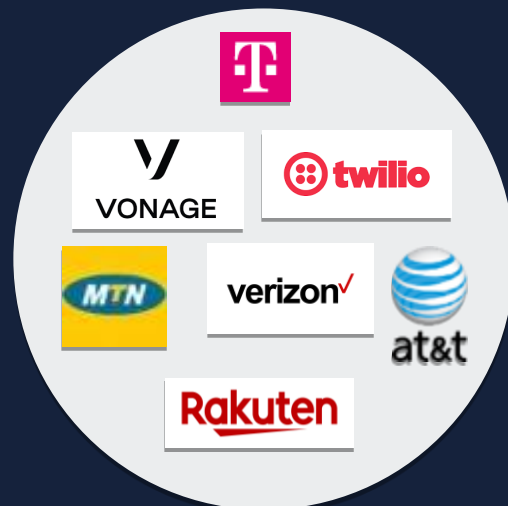# Secure Integration of 5G Private Networks

Dr. Silke Holtmanns

EU ENISA Telecommunication Security Forum – 13. October 2021

World Leader in Cyber Telecom Security

Protecting 2.2 billion of mobile subscribers and devices worldwide

Unique security perspective of mobile traffic

Processing 50 billion events/day

Trusted in over 80 operator networks

Our software sits in the heart of mobile networks, identifying threats and securing their services in real time

Global specialisation in signalling and messaging security enabling the most comprehensive intelligence lead protection solutions

Industry Recognition of Leadership

Key differences Telecommunication vs IT Security

Nation States or Surveillance as a Service	Focused on THE target	Criminals or hacking services	Opportunistic - Go for the weakest
Well-funded and experienced in IT & telecommunication protocols	Attacks are launched from trusted partners	Know IT protocols, but not telco	Attacks are coming from the outside
Fast and flexible attacks & slow standards countermeasure	Private Networks just a new "attack vector"	Fast and flexible attacks & fast patching	Private network based on IT – new business

3

5G Private Networks

- 5G is made for businesses

- Many different "flavors" of private network

- Many requirements lead to "opening up"
  - Virtualization
  - Mobility
  - Network as a service
  - Coverage
  - External content server
  - Slicing
  - Customer management

data·respons

ABOUT   CO

Home > 5G is a game changer for the military

5G is a game changer for the military

Secure wireless data communication is hugely important for the military, both at home and abroad. Besides the apparent administrative use, this goes not least the military tactical communication management system.
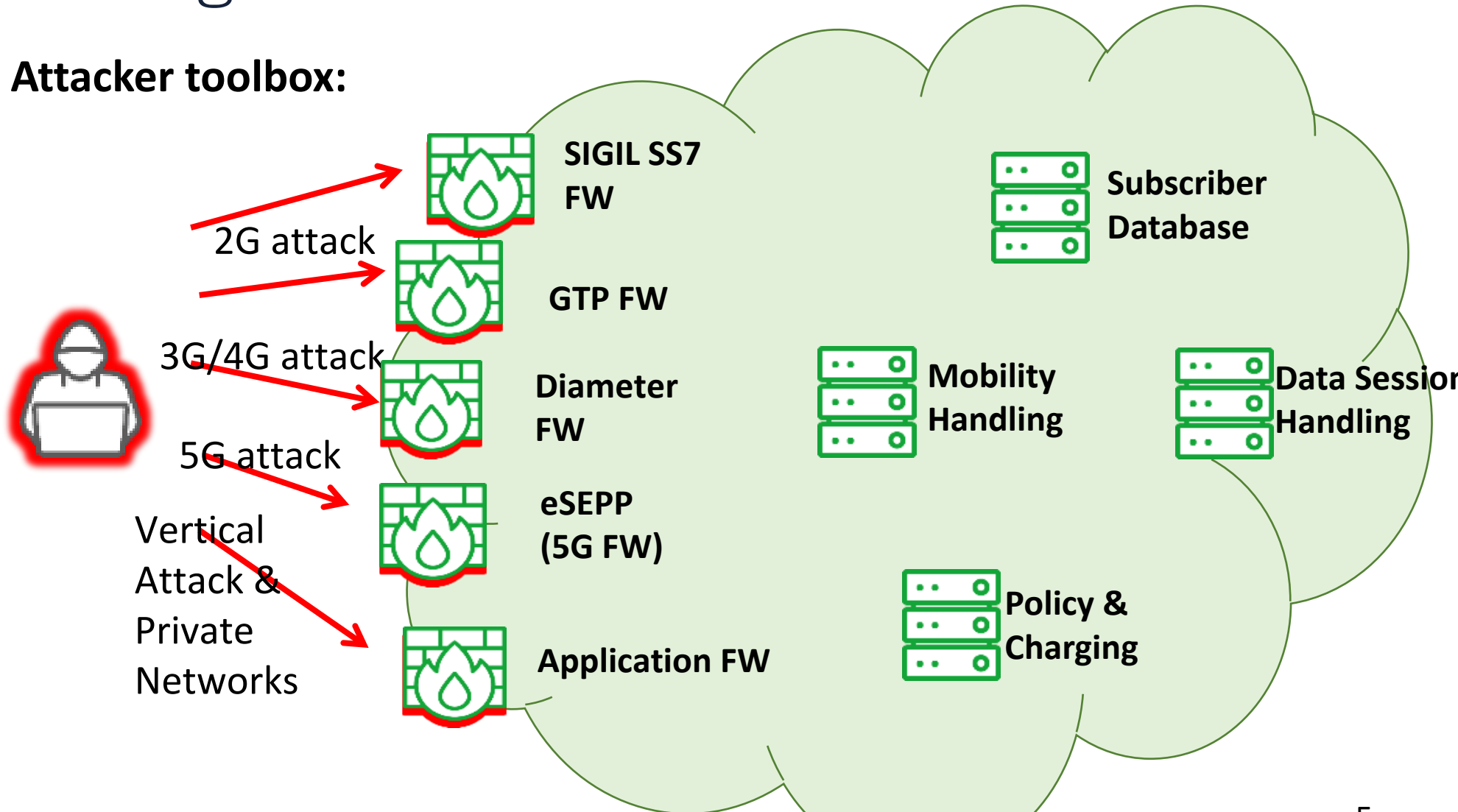
An Interrupt Inside article

4

Attackers use different technologies to achieve their goals

Attacker toolbox:

Attacker goals:
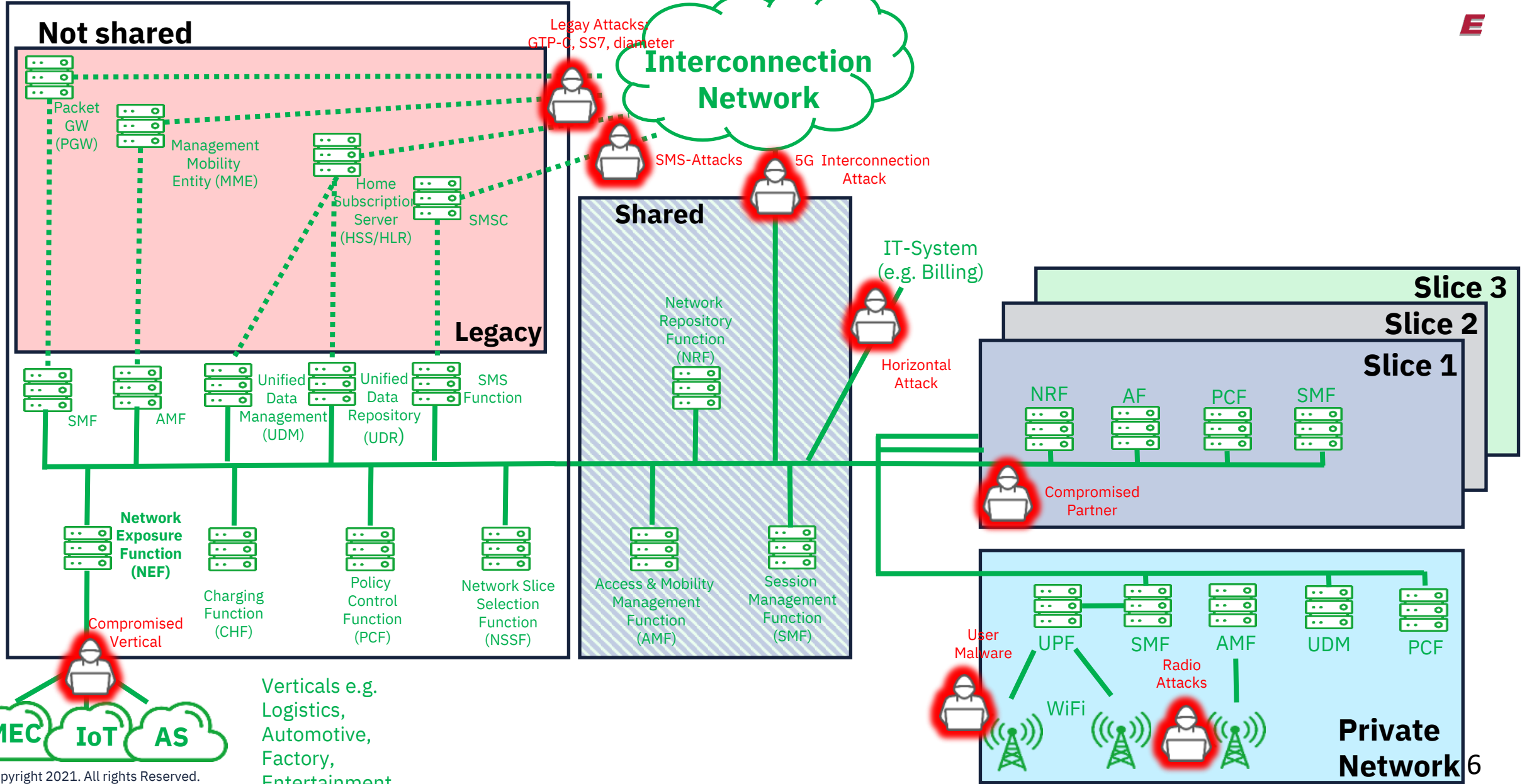- User location
- Information
- Fraud
- Call interception
- PIN interception
- User DoS
- Data interception
- Spam
- Ransomware

2G attack → **SIGIL SS7 FW**

3G/4G attack → **GTP FW**

5G attack → **Diameter FW**

Vertical Attack & Private Networks → **eSEPP (5G FW)**

→ **Application FW**

Subscriber Database

Mobility Handling

Data Session Handling

Policy & Charging

5

Example Risks

Not shared

Packet GW (PGW)

Management Mobility Entity (MME)

Home Subscription Server (HSS/HLR)

SMSC

Legacy

Legay Attacks
GTP-C, SS7, diameter

Interconnection Network

SMS-Attacks

5G Interconnection Attack

Shared

Network Repository Function (NRF)

IT-System (e.g. Billing)

Horizontal Attack

SMF

AMF

Unified Data Management (UDM)

Unified Data Repository (UDR)

SMS Function

Network Exposure Function (NEF)

Charging Function (CHF)

Policy Control Function (PCF)

Network Slice Selection Function (NSSF)

Access & Mobility Management Function (AMF)

Session Management Function (SMF)

Compromised Vertical

Verticals e.g. Logistics, Automotive, Factory, Entertainment

MEC IoT AS

Slice 3

Slice 2

Slice 1

NRF AF PCF SMF

Compromised Partner

UPF SMF AMF UDM PCF

User Malware

Radio Attacks

WiFi

Private Network 6

Holistic 5G Security for Private Networks

Security depends on Private Network Topology

- **Protecting the edge**
  - 5G enables new business opportunities by opening up the core
  - Prevent information theft and fraud at the edge
  - **Vertical API Protector**

- **Protecting Roaming:**
  - 5G Threat Intelligence Enhanced Security Edge Protection Proxy (eSEPP)
  - Protect legacy roaming interfaces (2G,3G,4G,SMS)
  - Defending against unwanted traffic coming via the roaming interface

- **Protecting sensitive network zones**
  - Detection of potential security breaches
  - Prevention of cross-slice information leakage
  - Enhanced Service Communication Proxy (eSCP)

- **Threat Intelligence**
  - Correlate attack patterns across protocols
  - Benefit from global signalling intelligence
  - Zero Trust without threat intelligence is not good enough

- **Protect Content**
  - Data traffic filtering for malware, spam and ransomware
  - GTP-U FW with latest content filter

Secure Integration of Private Networks

- Understand the topology
  - Interfaces & protocols
  - Who operates and hosts what?

- Understand the risks
  - Exposure and Accessibility
  - Threats via legacy, roaming, partners, MEC
  - Attackers behaviour

- Manage the risks:
  - Service Level Agreements
  - Standard security baseline as a requirement
  - Understanding the creation of security zones with "gateways" and filters
  - Security is also a business enabler for high value customers

- Be agile and efficient:
  - Threat intelligence to be able to focus on the real attacks and filter out "noise"

Questions?

Silke.Holtmanns@adaptivemobile.com

AdaptiveMobile
Security

an Enea company