5G SECURITY DRIVEN BY DEUTSCHE TELEKOM

T-Systems

Stefan Schröder
Dr. Sven Lachmund
INNOVATION IS TOP PRIORITY FOR DT
DT DRIVE AND CONTRIBUTE TO INTERNATIONAL STANDARDS

Mobile networks require global interworking and compatibility
Standards are key

DT drive important global standards - including security
Everybody can benefit from standardised security controls

DT experts have key roles in relevant standardisation organisations
Most relevant for the mobile network are 3GPP and GSMA
FLEXIBILITY FOR NEW BUSINESS AUTHENTICATION FRAMEWORK
5G – AUTHENTICATION FRAMEWORK
FLEXIBILITY FOR NEW USE CASES

Access credential
= Name + proof (secret)

Security requirements
• Strong authentication
• Create keys for radio security
• Customer side store with evaluated security
• Secure distribution logistics

Need for alternatives
• Physical aspects
• Environment: factory, campus
• Cost?
• Different risk (sharing) models

5G supports EAP:
Extensible Authentication Protocol

Hard-coded within 2G-4G protocols!
5G – NEW USE CASE: FACTORY/CAMPUS NETWORKS
SECURITY AND RISK SHARING

Factory Network

Public Network 1

Public Network 2

IPX

T·Systems·
5G – INTRANET ACCESS WITH CUSTOMER CONTROL
SECONDARY AUTHENTICATION

Primary Authentication

Secondary Authentication (EAP)

Public 5G Network

Corporate Intranet

AAA-Server

T-Systems
5G USES WEB TECHNOLOGIES – WE SECURE THEM
5G ARCHITECTURE EVOLUTION

WIDELY USED WEB PROTOCOLS – SECURITY ISSUES INHERITED

Service-Based Architecture

- Flexible design, inspired by micro-services
- Open standards facilitate future innovation
- Built on established web technologies and best practices
- Software-driven network to enable dynamic slicing

SECURITY PROBLEMS BUILT-IN?
IMPROVED ROAMING SECURITY

LESSON: STANDARDISE SECURITY FROM THE START

- Legacy inter-operator signalling in 2G/3G source of varieties of malicious traffic
- Complex SS7 protocol stack proven vulnerable by several research papers

- 4G/LTE improves on that, but carries over some legacy protocol vulnerabilities
- Requires special mitigation by use of additional filter elements

- 5G architecture incorporates DTAG-defined Security Edge Protection Proxy
- Mandatory network function and cornerstone of enhanced roaming security
SECURITY EDGE PROTECTION PROXY (SEPP)
PROTECTS MOBILE NETWORK & TRANSMITTED DATA

- Protects mobile network from incoming malicious traffic
- Enforces operator-defined security policies, plausibility checks, rate limit
- Protects outgoing traffic from eavesdroppers and unintended modifications
- Use of asymmetric cryptography ensures authentication and traceability
- Dynamically configurable level of protection for various use cases
- Built on established security frameworks and formatting standards
ENHANCED USER PRIVACY IN 5G
**5G ENHANCEMENTS TO USER PRIVACY**  
**NO IDENTIFIER SENT IN THE CLEAR**

- Objective: Defeating the infamous „IMSI-Catcher“
- Earlier generations allowed cleartext transmission of permanent subscriber ID in certain scenarios
- With 5G only the Subscription Concealed Identifier (SUCI) is ever revealed on the air interface
- Solely the home network provider can decipher a subscriber’s identity by use of its private key
- Future-proof by algorithm agility
SECURITY ASSURANCE FOR (5G) NETWORK PRODUCTS
What it is
A security baseline to evidence that:
- Network equipment satisfies a list of security requirements;
- Network equipment has been developed according to standard guidelines

Security evaluation of network equipment + Accreditation of equipment vendors

Security gain
- DT will run a robust and secure (5G) network
  Increasingly important due to ever growing complexity and interconnectedness
- Roaming will become more secure for DT customers
  If other operators follow DT
NETWORK EQUIPMENT SECURITY ASSURANCE
MEASURABLE BASELINE OF SECURITY FOR THE INDUSTRY

How it works

Equipment Vendor
- defines
- builds

Secure development lifecycle process
- accredits

Test lab
- evaluates

Test cases

Auditor

Network equipment