5G security testbed 1-pager (version 2.0)

Introduction

5G is hailed to be the much anticipated enabler of new technologies from IoT and smart cities to autonomous vehicles and virtual & augmented reality. However, these applications will rely on 5G's security to bolster the general public's trust in the technology to deliver a safe, secure and resilient mobile communication ecosystem. For this to happen, an even greater coordination across industry and academia will be needed to explore network attack simulations in order to identify vulnerabilities and potential backdoors.

Objectives

- Open industry-academia collaboration on 5G Security, based in Switzerland
- Independent (solely dedicated to this project) and realistic infrastructure for interdisciplinary research & application (testing), education & training purposes

Use case examples

- Security[1]: network attack simulations in order to identify vulnerabilities and potential backdoors, for example roaming testing, RAN sharing monitoring, simulating fake base stations, etc.
- Resilience: Study resilience strategies and metrics of 5G networks
- Training: capture the flag challenges (CTF)
- Other research: SDR platform to implement novel 5G communication concepts, in particular for IoT
- Development of testing protocols and ranking, for example for benchmarking vendors.

Project participants

Industry
armasuisse (workgroup initiator); **Swisscom** (5G security testbed operator); **Kudelski** (providing 5G security expertise); **ICRC, Roche, SwissPost, SICPA** (potential 5G users), **Microsoft?**

Academia
to be defined - We will approach C4DT/EPFL labs, which could be potentially interested in participating in the testbed, as well as lab's from other academic institutions which have 5G security/resilience/reliability competencies.
Remark: **C4DT** would take on the role of coordination of testbed activities, promotion and communication.

Infrastructure

- Ericsson T6 configuration (RAN with gNB & eNB, 4G/5G NSA core, Faraday cage).
- Migration strategy: NSA (non-standalone) LTE assisted NR connected to EPC (4G/5G NSA core) towards 5G SA (stand alone) dual core (i.e. EPC and 5G SA core).
- Location: core network & RAN @ **Cyber-Defence Campus**, Thun; additional RANs @ Swisscom, Ittigen and @ EPFL, Ecublens. Further RAN locations are possible according to partner needs.

Cost

- CAPEX: CHF1Mio,
- OPEX: CHF500K to 1Mio annually. This includes 3 FTEs (engineering and management), licensing, equipment upgrades, etc

Timeline

2021: **Q1** contracts, **Q2** design, **Q3** installation, **Q4** lab in operation (tbc)

Contact for more information

david.viollier@epfl.ch (C4DT), vincent.lenders@armasuisse.ch (armasuisse)

[1] For example, security architecture, authentication, security context and key management, radio access network (RAN), security, Security within NG-UE , authorization, subscription privacy, network slicing security, relay security, network domain security, security visibility and configurability, credential provisioning, interworking and migration, small data, broadcast/multicast security, management security, and cryptographic algorithms.