Architecture-related Risks

for 5G/6G Security

The 5G (and prospective 6G) architecture components and related risks

are the following:

» Service-Based Architecture (SBA), decomposed, virtualized, and

distributed network functions. The independence of network functions

from infrastructure poses challenges for network security.

» Application Programming Interfaces (API). Poorly encrypted,

inadequately secured APIs put network resources at risk of attack.

» Private and corporate 5G networks. Such networks, if not adequately

protected, can be a source of attacks for the network segments to which

they are connected.

» Multi-Access Edge Computing (MEC) [19]. Security management

becomes difficult in decentralized information processing, such as edge

computing, as significant network parts can be attacked anywhere.

» Radio Access Network (RAN) and Open-RAN. The radio segment of the

mobile communication network is inherently exposed to attacks related

to the omnipresent transmission medium. The open specification of

the radio interface (O-RAN) introduced in the 5G network [1,2] poses a

challenge to their security. Inadequately defined and poorly secured

O-RAN applications, e.g., in the physical or MAC layer, may be vulnerable

to these attacks.

The first three 5G security issues are similar to general software architec-

ture and applications security problems. The last two strictly address RAN

and its novel features, including its openness and intelligence.