5G Security – 2 days

CONTENTS

This course presents old and new threats, security aspects, requirements, recommendations from various organizations and then the new, improved functions and procedures designed to improve the security of the future 5G networks for communication with regular users and the growing number of IoT devices.

The training course starts with a brief introduction to the 5G system architecture, various dangers, threats and attack scenarios and short introduction to basic cryptographic techniques used in digital communication. This is followed by a presentation of security requirements on the 5G system and recommendations from various organizations. The next parts of the course present various standardized security mechanisms and their details for securing communication with users/devices, inside the network, towards external entities, and other networks.

PREREQUISITES

Medium level of technical knowledge of the structure and procedures in the 5G networks is required. We recommend our “5G System Overview” or “5G Core Network Architecture” courses for the background knowledge.

5G Security: Basics, Aspects, Threats

- What is security: confidentiality, integrity, identity protection, intrusion prevention, etc.
- Security aspects of end-user and IoT devices, radio access network, core network, application servers and communication with other networks.
- 5G system introduction: architecture, relation to 4G networks, selected deployment scenarios, use cases, Service-Based Architecture principles, Centralized RAN option.
- Possible attack vectors: malware in devices/app servers, misbehaving UEs, compromised base stations, fake base stations, passive air interface monitoring, active interception, physical tampering with IoT devices, etc.
- Overview of UE security functions, mobility and session-related procedures, identifiers.
- Basic cryptographic techniques: symmetric/asymmetric encryption, key exchange, hash functions, signatures, certificates, etc.
- Overview of assets and threats in Generic Network Products as identified by 3GPP.
- Overview of assets, threats, threat agents as identified by ENISA.

Requirements and Recommendations

- 3GPP 5G security requirements on UE, gNB, Centralized RAN, AMF, UDM, AUSF, NRF, SEPP, NEF, and Network Functions using Service-Based Interfaces.
- NGMN Alliance recommendations on 5G security for: network and access, DoS/DDoS attacks prevention, network slicing, Multi-access Edge Computing, low latency communication, etc.
- GSM Association recommendation on security for: network operators, IoT service ecosystem and IoT end-device ecosystem.
- GSM Association: lists of critical and high-priority security recommendations, details of selected recommendation examples.
- Network Equipment Security Assurance Scheme and 3GPP Security Assurance Specifications (SCAS), selected SCAS examples for gNB, AMF, etc.
- Overview of ETSI recommendations for NFV security.
- Evolution of the trust model and principles of Zero-Trust Security approach to networks security.

UE-related Security Procedures in 5G

- Evolution from 2G to 5G: authentication, ciphering, integrity protection.
- 5G air interface security algorithms.
- Pre-R99 SIM and R99+ USIM security features comparison.
- 5G system authentication methods: 5G AKA and EAP-AKA'.
- Visited PLMN verification: handling of XRES* and HXRES*.
- SUPI protection: concealment and de-concealment to/from SUCI, selected details of the protection schemes.
- Protection of initial NAS messages.
- EPS security key hierarchy.
- 5GS security key hierarchy, for NR and non-3GPP access, for 5G-AKA and EAP-AKA' authentication methods.
- Selected details of Key Derivation Functions in 5GS key hierarchy.
- Air interface user-plane security.
- RAN-based periodic local re-authentication.

5G Network Security Functions and Procedures

- Security for non-3GPP access: untrusted Wi-Fi, trusted Wi-Fi, wireline.
- Selected details of secure UE parameters update from HPLMN procedure.
- "Vertical" security for 4G/5G network exposure via SCEF and NEF.
- Security of Service Based Architecture of 5G System and non-SBA 5G interfaces.
- Security principles for inter-operator communication via SEPP and pre-5G interfaces.
- PRINS protocol overview and security capability negotiation between SEPPs.
- Security comparison of protocols for roaming communication: MAP, Diameter, HTTP.
- Network slice security principles, Network Slice-Specific Authentication and Authorization.
- NWDAF-based anomaly detection
- Securing UE-AF communication with Authentication and Key Management for Applications using 3GPP UE credentials
- Overview of security handling at intra-/inter-RAT mobility, horizontal and vertical key derivation for forward security.