5G Security in an Hour

CONTENTS

This course presents selected security aspects, threats and security challenges for the 3GPP 5G networks. Brief look at available requirements, recommendations and guidelines is followed by introduction to functions and procedures designed to improve the security of the networks for communication with regular users and the growing number of IoT devices.

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 background knowledge.

NOTE: This course is not delivered with the FoldOut methodology.

Security aspects, threats, requirements, and recommendations

- Selected security aspects for the end users, the radio and the core network as well as Application Servers.
- Selected security threats for endpoint devices and mobile network elements.
- Selected threats to Generic Network Products as identified in 3GPP report.
- 5G versus legacy networks: sources of new security concerns and possible new attack vectors.
- Lists of requirements, recommendations, guidelines, tests from various organizations.

Security features and procedures

- Overview of UE security functions, new possibilities introduced in 5G networks.
- Options for UE authentication and authorization, 5G enhancements and additions.
- Comparison of details of authentication procedures in pre-5G and 5G 3GPP networks.
- 5GS security key hierarchy.
- Details of UE authentication response calculation for VPLMN and HPLMN verification.
- Overview of 5G Authentication and Key Management for Applications (AKMA).
- Details of handling of Subscription Concealed Identifier (SUCI)
- List of standard security mechanisms for the radio and the core network security; applicability on different network interfaces.
- Inter-PLMN security: introduction to SEPP, PRINS and IPUPS.