5G NR Security Course Plan – Day-wise Outline

Objective: Provide a structured two- day training outline for 5G NR security covering RAN and Core, segmented into four 4- hour sessions.

Outline

1. **Day 1 (First Half – 4 hours)** – Introduction to 5G NR security and RAN access- stratum security.
2. **Day 1 (Second Half – 4 hours)** – RAN security mode command and handover security, followed by core authentication & key management.
3. **Day 2 (First Half – 4 hours)** – Core service- based architecture (SBA) security and inter- PLMN security (SEPP & N32).
4. **Day 2 (Second Half – 4 hours)** – Monitoring & KPIs, threats & mitigation, and case studies/practical sessions.

Detailed Day- wise Schedule

Day 1 – First Half (4 hours)

Module 1: Introduction to 5G NR Security (2 hours)

- **Evolution of cellular security:** Review how security evolved from 2G to 5G, highlighting improved authentication, encryption and privacy introduced by 5G. Outline the 3GPP SA3 working group's specification of 5G security mechanisms in TS 33.501.
- **3GPP TS 33.501 architecture overview:** Explain the reference architecture, including key network functions (gNB, AMF, SMF, NRF, UDM, AUSF, SEAF).
- **Vendor implementation:** Discuss how Ericsson manages security domains through its Ericsson Network Manager (ENM) and the use of SECURITYLEVEL settings; compare with Nokia's management via NetAct and security profiles.

Module 2: RAN – Access Stratum Security (2 hours)

- **Security parameters:** Review the ciphering and integrity algorithms used in RAN: Ericsson's *SECCIPHERINGALG* and *SECINTEGRITYALG*; Nokia's integrity and cipher algorithm sets. Discuss algorithm selection and fallback.
- **Monitoring & KPIs:** Identify key indicators such as integrity failure counts, ciphering activation rate for Ericsson, and RRC security activation/failure counters for Nokia.
- **Tracing & tools:** Demonstrate how to capture and analyze Access Stratum security events using UETR logs on Ericsson and NetAct/AMIA traces on Nokia platforms.

Day 1 – Second Half (4 hours)

Module 3: RAN – Security Mode Command & Handover Security (2 hours)

- **Security Mode Command procedure:** Explain how the gNB triggers the Security Mode Command to activate ciphering and integrity protection for radio links. Show log examples from UETR and NetAct for both vendors.
- **Failure analysis:** Review counters and alarms that signal SMC failures and discuss troubleshooting steps.
- **Handover security:** Describe key derivation for intra- and inter- gNB handovers (e.g., *KeNB* derivation) and illustrate KPI monitoring (e.g., handover security failures on Nokia NetAct).

Module 4: Core Network – Authentication & Key Management (2 hours)

- **Authentication protocols:** Compare 5G- AKA and EAP- AKA' authentication methods specified by 3GPP. Discuss parameters configured in UDM/HSS and how SUCI protects the permanent identifier (SUPI).
- **Vendor configurations:** Outline how Ericsson configures authentication methods in ENM or vEPC; detail Nokia's UDM/UDR security profiles in NetAct.
- **KPIs & troubleshooting:** Explain relevant KPIs such as authentication success/failure rate, resynchronization rate, and how to interpret logs.

Day 2 – First Half (4 hours)

Module 5: Core Network – SBA Security (2 hours)

- **Service- based architecture overview:** Describe the SBA and the role of network functions (AMF, SMF, NRF, UDM, etc.). Explain how TLS 1.2/1.3 secures service- based interfaces and the need for certificate management.
- **Vendor- specific management:** Present Ericsson's TLS key management in ENM and Nokia's configuration of TLS cipher suites via its Security Manager. Discuss best practices for certificate rotation.

Module 6: Inter- PLMN Security (SEPP & N32) (2 hours)

- **Role of SEPP:** Introduce the Security Edge Protection Proxy (SEPP) and its placement at the PLMN perimeter. The SEPP provides authentication, confidentiality and integrity protection for inter- PLMN signalling and implements the N32 interface.
- **N32 sub- interfaces:** Discuss N32- c (control plane) used to negotiate security capabilities and N32- f (forwarding plane) used for encryption/decryption of messages.
- **Vendor implementations:** Compare Ericsson's SEPP deployment (including N32- c and N32- f support and PKI handling in ENM) with Nokia's SEPP in Cloud Packet Core and policy management via NetAct.

Day 2 – Second Half (4 hours)

Module 7: Monitoring & KPIs (1.5 hours)

- **RAN monitoring:** Review ENM and NetAct dashboards that track integrity protection success rates, security mode activation, SEPP failure events, and other RAN KPIs.
- **Core monitoring:** Explain how to monitor authentication metrics, SBA TLS handshakes, N32 security, and SEPP statistics in both vendor environments.

Module 8: Threats & Mitigation (1.5 hours)

- **Common threats:** Discuss denial- of- service (DoS/DDoS), rogue gNB/UE detection, and SUPI/IMSI catching; explain how 5G improves subscriber privacy through encrypted identifiers (*SUCI*).
- **Vendor mitigation tools:** Highlight Ericsson's intrusion alarms and rogue gNB detection in ENM; present Nokia's anomaly detection counters and firewall/IPS integration for mitigating rogue UE or DoS attacks.

Module 9: Case Studies & Practical Sessions (1 hour)

- **Ericsson labs:** Analyze failed Security Mode Command scenarios using UETR logs; practice SEPP certificate checks and TLS troubleshooting in ENM.
- **Nokia labs:** Perform NetAct traces for authentication failures; configure and troubleshoot SEPP in Cloud Packet Core and NetAct.