LTE Security Overview

LTE is rolling out now, and security will be a key issue. LTE introduces many new security mechanisms, this course outlines them.

Who would benefit from this course?

Those in technical roles associated with the LTE rollouts. Course participants may include network operators, vendors, service providers, application developers, management staff and engineers.

Outline

Long Term Evolution (LTE) mobile infrastructure is now being deployed. LTE introduces a new radio interface and core network architecture, which will co-exist with current 3G UMTS and GSM networks. LTE also introduces a new security architecture. This one day course outlines the technical details of LTE security, and shows how it will interwork with existing mobile security infrastructure.

The course begins with an overview of GSM and 3G UMTS security mechanisms. LTE security requirements are then outlined, followed by an overview of LTE key management authentication and encryption procedures. LTE security operations are then reviewed, including signalling plane, user plane, base station security, handover procedures and UMTS/GSM interworking. The course concludes with an overview of IMS and LTE voice security mechanisms.

Course Objectives

Participants completing this course should be able to:

- Describe GSM and 3G UMTS security parameters, key management and authentication procedures
- Outline LTE security requirements
- Describe the LTE key hierarchy, key establishment and authentication procedures
- List the LTE encryption algorithms and describe their main features
- Describe the LTE architecture and interfaces
- Outline LTE Access Stratum and Non Access Stratum security procedures
- Outline security and key management procedures during handovers and the role of HTTP digests
- Describe the security mechanisms for LTE voice calls and emergency calls