Introduction to Communications Security (COMSEC)

Course Syllabus Overview

Duration – 4 days

01. COMSEC Introduction

- Communications system
- Node
- Link
- Layered architecture
- Communications system security
- COMSEC Objectives
- Encryption
- Symmetric key cryptography
- Asymmetric key cryptography
- Trust
- Threats
- Trusted Platforms
- Protected communications

02. Introduction to Cryptographic Techniques

- Pseudorandom sequence generators
- Stream cyphers
- Block cyphers
- Hash functions
- Message authentication code
- Identity-based cryptography

03. Security Infrastructure

- Authentication
- Certificate authority
- Public Key Infrastructure (PKI)
- Certificate chain
- Revocation
- Authentication protocol 1
- Forgery and its prevention
- Definitions of forgery
- Authentication protocol 2
- Key generation and distribution
- Signing

TRAINING SYLLABUS

04. Protected Communications

- Authentication
- Key establishment
- Authenticated key establishment
- Mutual authentication with key transport protocol
- Key derivation
- Key confirmation
- Perfect forward secrecy
- Man-in-the-middle attack
- Cryptographic algorithm negotiation

05. Network Security Protocols

- Internet security protocols
- Transport Layer Security
- Secure Shell
- Cellular Systems

06. Network Access Authentication

- Basic concepts
- Authentication and Key Agreement
- Authentication, Authorisation, and Accounting

07. Wireless Network Security

- Special aspects
- UMTS and LTE air link protection
- IEEE 802.11 (Wi-Fi)
- Wired Equivalence Privacy (WEP)
- WEP authentication
- WEP security flaws
- Authentication and key establishment
- Wireless protection mechanism
- Temporal Key Integrity Protocol (TKIP)

08. Security for Mobility

- Introduction
- Challenges
- Secure Handover
- Mobile IP Security
- Media Independent Handover

09. Broadcast and Multicast Key Distribution

- Models for Multicast key distribution
- Pre-conditions
- Security requirement
- Key-sharing scenarios
- Logic tree-based multicast key distribution
- Hash chain-based authentication
- Merkle trees for authentication

10. Trusted Platform

- Threats
- Objectives
- Challenges
- Root of trust
- Transitive trust principle
- Secure boot
- Boot string
- Secure boot for a trusted platform
- Root public key
- Authenticate to remote parties
- Validation and authorisation
- Technologies and Methods
- In Practice

11. Physical Layer Security

- Wiretap
- Multiple Input Multiple Output

12. Spread Spectrum Techniques

- Basic Concepts
- Benefits
- Binary Phase Shift Keying
- Frequency Hopping
- Jamming Attacks
- Multiple access schemes