Course ID

GSMSEC

Course Duration

5 days

Course Title

GSM Architecture, Operation, and Security

Related Courses

- GSM: Network Architecture, Operation, and Design (GSM-I, 5 days)
- Architecture & Operation of Wireless Networks for Technical Investigators: From Their Analog Origins to the Emerging 3G Technologies (WIRELESS-TI, 4-5 days)
- Everything Wireless: RF/Cellular Basics, WiFi, Bluetooth, WiMAX, CDMA, GSM/GPRS/EDGE, UMTS/HSPA, and LTE (ALL-WIRELESS, 5 days)
- Emergency, Priority Access, and Public Safety Support in LTE (LTE-PUBSAFE, 3 days)
- 5G Wireless: Federal and Defense Applications and Implications (5GSEC, 1 day)
- IEEE 802.11 (WiFi) Wireless LAN Security (WIFI-SEC, 3 days)
- Principles of Network Security: CompTIA Security+ and US DoD Directive 8570.1 (NETSEC, 3 days)

Aimed At

This course is aimed at audiences with some prior knowledge of wireless basics as well as the GSM technology who wish to study GSM in depth with particular focus on the security issues.

Group Size

5-25

Prerequisites

- GSM: A Technology Overview (GSM-B, 1 day)

Course in a Nutshell

This is an intermediate-level in-depth course on GSM, GPRS, and EDGE with an overview of UMTS, HSPA, and LTE with a particular emphasis on the issues of security and vulnerability.

Covered in depth are: Key GSM concepts, modulation and coding, GSM air interface, GSM protocol and call processing, roaming and handover, GSM data services (GPRS/EDGE), QoS and KPI's, location based services, types of security threats, attacks in mobile environment, mobile malware, cryptography, access control and authentication, smart card security, GSM security, 3G network security, and comparison of GSM with other technologies.

Customize It!

If you already possess knowledge on some of the topics covered in the course we can remove those topics and shorten the course. We can also emphasize or deemphasize or include/exclude topics as necessary to align the course with your job requirements.

Course Outline

Part 1: Key GSM Concepts (Day 1)

- Cellular concept and radio propagation
  - Base and mobile stations
  - RF propagation and path loss
  - Antennas a frequency reuse
- Duplexing and multiple access
  - Time and frequency division duplexing
  - Time and frequency division multiple access
  - Code division multiple access
  - Frequency hopping concept
- Evolution of cellular communications
  - Circuit and packet switching
  - 3GPP, 3GPP2, and IEEE LAN/MAN standardization
  - 1G to 4G
  - Phone comparisons
- Overview of GSM architecture, protocols, and services
  - System architecture
  - Protocol layer overview
  - Protocol functions and standards
  - Operating frequencies
  - GSM data: GPRS and EDGE overview
- Addressing and numbering
  - Cell identities
  - Mobile station identities

Part 2: Modulation and Coding for GSM (Day 1)

- GSM modulation methods
  - Modulated signal structure
  - Amplitude, frequency, and phase shift keying
  - Gaussian minimum shift keying (GMSK)
- Error control
  - Error detection
  - Error correction
  - Automatic repeat request
- Speech coding
  - Speech quality rating
  - Speech coding methods and complexity

  - GSM speech coding techniques
  - GSM speech frame construction

Part 3: GSM Air Interface (Day 2)

- GSM TDMA and physical channels
  - Time slots and their use within a frame
  - Frame structures and hierarchy
  - Physical channels and their properties
  - Uplink and downlink timing
- GSM logical channels
  - Broadcast channels (BCH): Broadcast control, frequency correction, synchronization
  - Common control channels (CCCH): Paging, random access, access grant
  - Dedicated control channels (DCCH): Stand-alone dedicated control channels
  - Associated control channels (ACCH): Slow and fast
  - Traffic control channels (TCH): Full rate, half rate, cell broadcast
- GSM burst family: Mapping logical channels to physical channels
  - Normal
  - Frequency correction
  - Synchronization
  - Access
  - Dummy
- Radio subsystem link control
  - Radio performance requirements
  - Channel measurements
  - Transmission power control
  - Channel failure disconnect
  - Power conservation

Part 4: GSM Protocols and Call Processing (Day 2)

- User plane architecture
  - Speech transmission
  - Data transmission
- Signaling plane architecture
  - Layered processing
  - Radio resource management
  - Mobility management
  - Connection management
  - Mobile application part

- Radio resource management
  - Connection setup and release
  - Mobility management
  - Connection management

Part 5: Roaming and Handover (Day 3)

- Call routing and termination
  - Routing calls to the MS
  - Call termination
- Handover
  - Intra-MSC handover
  - Handover decision process and timing
  - MAP and inter-MSC handover
- Key Performance Indicators (KPI)
  - Speech quality
  - Bit and frame error rate
  - Dropped call rate
  - Call and handover success rates

Part 6: GSM Data Services (Day 3)

- Quality-of-Service (QoS) requirements
  - The QoS challenge
  - General QoS categories
  - QoS parameter negotiation
  - QoS management
- General Packet Radio Service (GPRS)
  - Network architecture
  - Protocol structures
  - GPRS on the GSM air interface
  - Medium access control
  - Radio link control
  - Mobility management
- Enhanced Data Rates for GSM Evolution (EDGE)
  - EDGE modulation and coding
  - EDGE air interface protocols
  - MAC and RLC procedures
- Key Performance Indicators (KPI)
  - Reliability
  - Throughput
  - Delay

Part 7: Location-Based Services (Day 4)

- Introduction to LBS
  - Definitions
  - Classifications and applications
- Location management
  - Location update and paging
  - Location management in circuit and packet switched networks
- Location services methods and performance
  - Accuracy requirements
  - Cell identity and timing advance (TA)
  - Enhanced observed time difference (E-OTD)
  - Uplink time difference of arrival (U-TDoA)
  - Assisted GPS
- LBS operation
  - Patterns and privacy
  - Architecture and protocols

Part 8: Communication Security (Day 4)

- Wireless security challenges
  - Threat categories and attack methods
  - General security setup process
- Attacks in mobile environments
  - Illicit use
  - Spoofing
  - Man-in-the-middle
  - Interception of data
  - Denial of service
- Mobile malware
  - Basics and characteristics of malware
  - Types of malware: Worm, virus, phishing, etc.
  - Examples of malware in mobile devices
- Cryptography basics
  - Symmetric cryptography
  - Asymmetric cryptography
  - Public key infrastructure
  - Digital signature
  - Cryptographic attacks
- Access control and authentication
  - Weak and strong authentication schemes

  - Attacks on authentication
  - Authorization and access control

- Smart card security
  - Smart card basics
  - Smart card communication
  - Invasive and non-invasive attacks on smart cards

- GSM security
  - GSM security model
  - Basic attacks on GSM
  - GSM encryption algorithms
  - Advanced attacks on GSM
  - Improving GSM security

- Overview of 3G network security
  - Access and domain security
  - Mitigating GSM security weaknesses
  - Attacks on 3G networks

Part 9: Beyond GSM (Day 5)

- Universal Mobile Telecommunications System (UMTS)
  - Network structure and protocols
  - Overview of code division multiple access
  - Summary of the UMTS air interface
  - CAMEL: Bringing intelligent networking to GSM and UMTS

- High-Speed Packet Access (HSPA)
  - HSDPA (down link) and HSUPA (up link)
  - Review of the HSPA air interface

- Long-Term Evolution (LTE)
  - Network structure and protocols
  - Overview of orthogonal frequency division multiplexing (OFDM)
  - Summary of the LTE air interface

- Technology comparisons
  - Summary of cdmaOne
  - Summary of cdma2000
  - Summary of WiMax
  - GSM vs cdmaOne
  - UMTS vs cdma2000
  - LTE vs WiMAX

- Wrap-up
  - Course Recap and Q/A
  - Evaluations

How You Will Learn

- A highly qualified instructor, well-versed in GSM/GPRS/EDGE and other wireless technologies, will present this course in interactive lecture format.
- Along with the lecture, we will use examples, analogies, case studies, exercises, and group discussion to enrich the instruction and drive home the essential points.
- If you already know something about the technology, we will build on that. We'll compare and contrast what's familiar with what's new, making the new ideas easier to learn as well as more relevant.
- If your background is less technical, we will use meaningful examples and analogies to simplify the complex subject matter.
- You will receive a printed Participant Handbook which will help you remember and retain what you learned in class and apply it on your job.

Revised *2Rnj*