Course ID
CDMASEC
Course Duration
5 days

Course Title
WCDMA & CDMA2000 Architecture, Operation, and Security

Related Courses

- GSM Architecture, Operation, and Security (GSMSEC, 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 CDMA technology who wish to study WCDMA/CDMA/CDMA2000 in depth with particular focus on the security issues.

Group Size

5-25

Prerequisites

While there are no formal prerequisites for this course, some prior background in wireless technologies along with an understanding of CDMA concepts is required to benefit from this course.

Course in a Nutshell

This is an intermediate-level in-depth course on CDMA/CDMA2000 (CDMAOne, 1xRTT, EVDO) and WCDMA (UMTS/HSPA as well as LTE) with a particular emphasis on the issues of security and vulnerability

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: Introduction to Cellular Communications

- Cellular phone concept
  - Base station
  - Mobile station
  - Mobile switching center
- Uplink and downlink
  - Time division duplexing
  - Frequency division duplexing
  - Comparisons
- Multiple access methods
  - Frequency division multiple access
  - Time division multiple access
  - Code division multiple access
- Networking
  - Circuit and packet switching
- History of cellular communications
  - 1G to 4G
  - Phone comparisons

Part 2: Radio Wave Spectrum, Propagation, and Antennas

- The electromagnetic spectrum
  - Types of radio services
  - Spectrum characteristics
- Radio frequency (RF) system measurements
  - Power measurement using the decibel
  - Signal to noise and interference ratios
- Antennas
  - Terminology
  - Gain and loss
  - Law of reciprocity
  - Base station antennas
  - Smart antennas
- RF propagation in fixed and mobile environments
  - Propagation mechanisms
  - Path loss models
  - Maximum range calculations
  - Multipath and fading
- Cell planning and frequency reuse

- Frequency reuse calculations
- Cell sectoring
- Cell splitting
- Antenna downtilt

Part 3: Modulation and Coding

- Basic modulation methods
  - Modulated signal structure
  - Amplitude, frequency, and phase shift keying
  - Bit error rate performance in Gaussian noise

- Advanced modulation methods
  - Gaussian filtered frequency shift keying (GFSK)
  - Quadrature phase shift keying (QPSK)
  - Quadrature amplitude modulation (QAM)
  - Orthogonal frequency division multiplexing (OFDM)

- Spread spectrum systems
  - Frequency hop
  - Direct sequence
  - Multiple access methods

- Error control
  - Error detection
  - Error correction
  - Automatic repeat request

- Speech coding
  - Speech quality rating
  - Speech coding techniques
  - Speech coders in practice

Part 4: 3GPP, 3GPP2, and IEEE LAN/MAN Standardization

- Motives behind 3G evolution
  - Driving forces
  - Radio access evolution
  - Core network evolution

- Summary of 3GPP standards
  - GSM, GPRS, and EDGE
  - UMTS/WCDMA and HSPA
  - LTE

- Summary of 3GPP2 cellular standards
  - cdmaOne
  - cdma2000

  - EVDO

- Summary of IEEE LAN/MAN standards
  - Wi-Fi
  - Bluetooth
  - WiMAX

- Market penetration and deployment status

Part 5: 3GPP2 CDMA: cdmaOne, cdma2000, and EVDO Operations

- CDMA codes and sequences
  - Maximal length sequences
  - Walsh codes

- Forward link channel
  - Modulation
  - Pilot channel
  - Synchronization channel
  - Control channels
  - Paging channels
  - Traffic channels

- Reverse link channels
  - Pilot channel
  - Access channel
  - Control channels
  - Traffic channels

- Call processing
  - Initialization
  - System access
  - Authentication

- Resource management
  - Power control
  - Handoff

- Evolution-Data Optimized (EVDO) operation
  - Requirements
  - Reference model
  - Forward and reverse channels
  - Modulation and coding
  - Power control
  - Scheduling

Part 6: 3GPP CDMA: UMTS and HSPA Operations

- UMTS architecture and protocols
  - UTRAN radio network controller and NodeB
  - Core network architecture and protocols

- UMTS physical layer
  - WCDMA modulation and coding
  - Transport channels
  - User data transmission
  - Signaling
  - Cell search and access

- Radio interface protocols
  - Medium access control
  - Radio link control
  - Packet data convergence protocol
  - Radio resource control

- Radio resource management
  - Power control
  - Handovers
  - Admission control

- High-speed packet access (HSPA) operation
  - HSDPA physical layer structure
  - HSDPA performance
  - Enhanced uplink

Part 7: CDMA System Security

- Wireless security challenges
  - Threat categories and attack methods
  - General security setup process

- Attacks in mobile environments
  - Spoofing and illicit use
  - Man-in-the-middle
  - Interception of data
  - Denial of service

- Cryptography basics
  - Symmetric and asymmetric cryptography
  - Public key infrastructure
  - 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
- Legacy GSM security operation and weaknesses
  - GSM security model and encryption algorithms
  - Attacks on GSM
- UMTS security
  - Improvements to GSM security
  - Confidentiality algorithm and extensions
  - Integrity algorithm
  - KASUMI kernel
  - Authentication and key agreement (AKA)
- cdma2000 security
  - Air interface parameters for authentication
  - Secure parameters
  - Challenge-response authentication procedure
  - Authentication during MS registration
  - Authentication during MS call origination and termination
  - The CAVE algorithm for authentication and encryption

Part 8: Long-Term Evolution (LTE) Operations

- General LTE operation
  - System architecture
  - Frequency bands
  - Downlink and uplink modulation and resource structure
  - Error control
  - Spatial multiplexing
  - Performance requirements
- LTE downlink
  - User protocol architecture
  - Channel mapping
  - Logical, transport, and physical channel functions
  - Cell acquisition
  - IP packet processing and physical data mapping
  - Control and radio resource management
- LTE uplink
  - UL/DL similarities and differences
  - Channel mapping
  - Random access
  - Data transfer
  - Power save methods

- Link activity and capacity

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

How You Will Learn

- A highly qualified instructor, well-versed in a range of 3G and 4G 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 *2TDmz*