Course ID
BLUEOP
Course Duration
4 days

Course Title
Bluetooth Course: Operation, Security, Applications, Coexistence

Aimed At

This Bluetooth course is for wireless system designers, developers, implementers, and others who require an in-depth understanding of the Bluetooth technology.

Prerequisites

Prior familiarity with wireless networks.

Course in a Nutshell

Bluetooth is a short range wireless technology used for applications such as Wireless Personal Area Networks (WPAN), Smart Homes, and Internet of Things (IoT). In this comprehensive four-day Bluetooth training session, you will acquire in-depth knowledge of all aspects of Bluetooth, including the technology, security, and coexistence issues.

Customize It!

We can customize your Bluetooth training session to your team's background and learning objectives by making it more or less technical, shortening or lengthening the course, adding or omitting topics, and tailoring it to your industry/application.

Course Outline

Part 1: Bluetooth Overview

- Bluetooth usage model and protocol stack
  - Categories of information transmission
  - Short range wireless features
  - Bluetooth protocol stack: Host and controller

Part 2: The Bluetooth Radio

- Propagation and ranging
  - RF modeling in indoor environments
  - Calculating maximum range
  - Eavesdropping vulnerability
- Modulation and radio performance
  - Frequency hopping spread spectrum and Bluetooth channel set
  - Basic rate (BR) and enhanced data rate (EDR) modulation
  - Low Energy (LE) modulation
  - Radio performance

Part 3: Baseband Signaling I

- BR/EDR functional operation
  - Master/slave timing
  - Automatic repeat request (ARQ)
  - Addressing methods
  - Packet structure
  - Error control
  - Frequency hop parameters
  - Logical transport
  - Throughput in perfect and imperfect channels

Part 4: Baseband Signaling II

- Bluetooth audio
  - Methods of voice encoding
  - SCO and eSCO packet structure and performance
  - SCO vs ACL for wireless audio
- BR/EDR device discovery, connection, and low-power modes
  - Operational state diagram
  - Paging and inquiry processes
  - Sniff, hold, and park modes
  - Scatternet operation
- LE baseband operation
  - State diagram
  - Addressing
  - Packet structure
  - Advertising, initiating, and connecting operation
  - Data channel and packet exchange

Part 5: Link Management

- Overview of Link Management Protocol (LMP)
- Link management operations
  - Link connection and detachment
  - Maintaining the link
- LMP packets and examples
  - Link setup
  - Link control

Part 6: Higher Protocols

- Logical Link Control and Adaptation Protocol (L2CAP)
  - L2CAP overview and purpose
  - Protocol multiplexing and channel definitions
  - L2CAP signaling and channel setup
- Service Discovery Protocol (SDP)

  - Client-server interaction
  - Service record and attributes
- LE Attribute Protocol (ATT)
  - ATT operation on attributes
  - ATT retrieval
- Host Controller Interface (HCI)
  - HCI overview and purpose
  - Summary of commands and events
  - HCI over USB transport example

Part 7: Profiles

- Profile purpose and interaction
- Generic Access Profile (GAP)
  - Purpose
  - BR/EDR operational modes
  - LE functions and roles
- Headset Profile (HSP) and Handsfree Profile (HFP) [BR/EDR]
  - Fundamentals
  - Connections and usage
  - HSP and HFP comparison
- Advanced Audio Distribution Profile (A2DP) [BR/EDR]
  - Protocol stack
  - Streaming process
  - A2DP and HSP comparison
- LE profile examples
  - Generic Attribute (GATT) Profile
  - Find-Me Profile (FMP)

Part 8: Security

- Overview
- Shared and Public Key cryptography
- Attack methods
- Summary of legacy security
  - Link key generation and initialization
  - Combination key derivation
  - Authentication
  - Encryption
- Secure Simple Pairing

Part 9: Qualification and Test

- Qualification
  - Requirements
  - Program overview
  - Types of Bluetooth products
  - Steps to qualification

- Testing
  - Development tools
  - Component test mode
  - Examples of devices and performance

Part 10: Coexistence

- Coexistence overview
  - Bluetooth and Wi-Fi signal spectra
  - Interference modeling
- Bluetooth-on-Bluetooth coexistence
  - Range of vulnerability
  - Simulation analysis
- Bluetooth and Wi-Fi coexistence
  - Separated nodes
  - Collocated nodes
  - Examples and throughput analysis
- Improving coexistence and interference mitigation

- **Wrap-up: Course Recap, Discussion, and Evaluation**

Website: www.eogogics.com or www.gogics.com
E-mail: info@eogogics.com
Tel. +1 (703) 345-4375
USA 1 (888) 364-6442