

Basic IoT, Networking and Security

Connected-system concepts, network inspection and cryptographic foundations

FA-0779 · 3 days

Embedded Systems and Hardware · Cybersecurity

Introduction

Explore IoT architecture and applications alongside the networking and security concepts that support connected systems. Use prepared Linux, Wireshark and OpenSSL demonstrations to examine traffic, encryption, signatures and certificates. Cryptographic mathematics and platform research are introductory explanations, not a claim of advanced research or production security expertise.

Learning outcomes

- Describe IoT concepts, architectures, enablers, applications and data-management challenges.
- Discuss trust, reliability, privacy and security across an IoT system lifecycle.
- Use basic Linux commands and inspect prepared HTTP/TLS network examples with Wireshark.
- Distinguish encryption, hashing, message authentication, signatures and key agreement.
- Explain certificate chains and the roles of symmetric cryptography and ECDHE in TLS.

Prerequisites

Basic computer, internet and file-handling skills and English-language technical reading. Access to a prepared Linux environment, Wireshark and OpenSSL, with permissions for the course exercises.

Training outline

1. Day 1 — IoT architecture and lifecycle

- IoT Ecosystem, concepts and architecture
- IoT Enablers and Solutions
- IoT Data and Knowledge Management
- IoT Reliability, Security and Privacy
- IoT Applications

Consider SDLC, scalable architecture, open versus closed systems, interaction protocols, management, sensing/storage/processing and ethical/privacy questions. Future platform directions are discussed as possibilities rather than promised outcomes.

2. Day 1 — Linux and network inspection

- Linux basics
- Linux CLI
- Overview of historical SSL and current TLS/HTTPS
- Overview of the certificates of some popular websites
- Difference between HTTP and HTTPS
- Analyzing traffic using Wireshark
- TCP/IP stack by example
- Analyzing HTTP protocol using Wireshark
- Analyzing HTTPS and TLS using Wireshark

SSL is historical; demonstrations use current supported TLS. Encrypted payloads cannot simply be read from a capture without suitable keys and an authorised lab setup.

3. Day 2 — Cryptographic primitives

- Symmetric Key Encryption
- Symmetric Key Encryption Algorithms
- Hashing Overview
- MD5 as a legacy hashing example
- SHA hashing algorithm and HMAC overview
- Encryption using asymmetric keys
- Signing data using asymmetric keys
- RSA Overview

- Certificate overview
- Installing OpenSSL
- Using OpenSSL for RSA keys generation

MD5 is discussed as a legacy hash, not a recommended security mechanism. Distinguish hashes, HMAC, asymmetric encryption and digital signatures.

4. Day 2 — Certificates and trust

- Inspect certificates from prepared public-site examples rather than relying on a named vendor/domain snapshot.
- Root CAs and operating-system trust stores.
- Certificate chains, verification, domain scope and PKI.

5. Day 3 — TLS and key agreement

- Introduction to historical SSL and current TLS
- History and versions of the SSL and TLS
- Roles of asymmetric cryptography and symmetric bulk encryption in HTTPS
- How TLS session is established
- Analyzing TLS session setup using Wireshark
- Overview of cipher suites
- Deriving session keys during the TLS handshake
- Establish shared key material using Diffie-Hellman key agreement
- Diffie Hellman overview
- Modulus operation
- Diffie Hellman algorithm

TLS1.3 removes static RSA key transport. Session traffic uses symmetric authenticated encryption; signatures authenticate, while suitable key-agreement mechanisms establish shared key material.

6. Day 3 — Elliptic-curve concepts and review

- Point Addition on Elliptic Curve
- Multiple Point Addition
- Point Doubling and Optimization
- Elliptic Curve Discrete Log Problem
- Comparing formulas
- ECDHE - Elliptic Curve Diffie Hellman Exchange

- Exploring ECDHE with ECDSA

Elliptic-curve arithmetic is a guided conceptual demonstration; compare ECDHE key agreement and ECDSA signatures. Review the course and complete the assessment.