Applied Cryptography Security Workshop

Course Objectives

At the end of the course, participants will:

- Understand the basic building blocks of cryptography
- Understand how basic blocks are used to build secure protocols
- Understand weaknesses and attacks against protocols
- Understand how cryptographic attacks are mounted through several real-life examples
- Learn about real-world cryptographic attacks
- Review current known issues in cryptography
- Analyse case studies of a product with failed cryptographic implementations or design decisions
- Understand the current stage of cryptographic building blocks and how they are affected by quantum computing

Course Overview

The growth and central role that the Internet of Things play in the technology world is a proven fact. IoT is bringing the network to the physical aspects of our lives; our cars, utilities, homes, cities, industries and more. With such influence, IoT security is the main concern for the whole industry of IoT stakeholders, from developers to service providers, customers, and end-users. This course outlines the state-of-the-art prevailing practices for IoT security and how this topic is evolving. It is intended for IoT developers and managers to make a strategic decision for their IoT products both as a vendor and as a customer.

The use of cryptography permeates our daily digital lives, from securing the internet to banking transactions - we usually never hear of cryptography, until it fails. The failure of cryptographic building blocks is rare - and often the case is either wrongly implemented cryptographic software or bad design decisions of such products. The goal of this course is to supply the participants with tools and knowledge of how to better analyze such systems, pitfalls to watch for and focus areas to strengthen their approach.

The course does not assume a background in mathematics

Course Duration

2-day instructor-led training

Course Outlines

- Symmetric cryptography primitives
- Asymmetric cryptography primitives
- Hashing algorithms
- Reviewing and discussing the difference in the best-in-class primitives
- Randomness
- Secure protocols

- Solving real-world issues with cryptography
- Failures: case study review of cryptographic failures

Subjects

- Cryptographic building blocks
- Building a secure protocol with cryptographic building blocks
- Solving real-world problems with secure protocols
- Key exchange and forward secrecy
- Signal protocol
- Zero-knowledge proofs
- Side-channel attacks
- Quantum cryptography - challenges