About the Course Presenter

The ID-3 training partner Dr Blundell is crypto specialist with a PhD in cryptography and mathematics from Royal Holloway, University of London. A cryptographer in both the telecommunications and defence sectors, and an example of an academic paper authored and published while working in industry can be found here.

Two day Crypto and Key Management Course

Course Overview

Cryptography is a vital part of cyber security.

Cryptography is a set of techniques that enable security and trust by providing confidentiality, authentication, and data integrity. Many secure applications and protocols rely on combinations of properly applied and supported cryptographic techniques, from protecting personal and commercial information using encryption, to e-commerce, secure communication, IoT and network security.

This crypto course develops in a progressive way an overall understanding of cryptography and its application. It adopts a generic approach to establish a core competence that can be taken away and readily applied to many different products, systems and architectures.

The course covers all of the main cryptographic techniques, including their different functions and characteristics, how they are properly applied, and how they work together to accomplish different security objectives. The course then looks at a subject vital to the effective use of such techniques, namely cryptographic key management. This encompasses the whole key management life cycle, including digital certificates and PKI.

Finally, the course looks at two examples of applied cryptography. The first is network security, with a focus on the Transport Layer Security (TLS) protocol and its predecessor SSL. The second is Blockchain. This includes describing what they do, how they work from a cryptographic perspective, and what is required for them to be effective.

Course Objectives

- Develop a broad knowledge that can be applied across many different systems and applications
- Establish a solid foundation on which to make judgements or assessments of security solutions, and support system administration, development and implementation
- Appreciate the different key management options and requirements necessary for the use of cryptographic techniques to be truly effective and appropriate
- Applications: develop knowledge of applied cryptography using TLS and Blockchain as examples:
    - For TLS: its purpose and scope, how it works, its requirements - including certificate options - and ciphersuites
    - For Blockchain: recognise what it does, how it works and its implications

Course Description

The course assumes no prior knowledge and includes the following:

- Cryptographic services
- Design principles
- Cipher types and characteristics
    - Symmetric ciphers & encryption: provably secure encryption; stream ciphers; block ciphers (including DES and AES); modes of operation (such as CBC and GCM); Message Authentication Codes (MACs)
    - Public key systems, including Diffie-Hellman and RSA
- Hash functions, zero-knowledge protocols, homomorphic encryption, Elliptic Curve systems
- Digital Signatures
- Key management, including generation, distribution, storage, PKI and certificates
- Transport Layer Security
    - Purpose and scope
    - How it works
    - Requirements, including certificate options
    - Configuration options such as ciphersuites
- Blockchain
    - What is does and how it works
    - Its implications
    - Cryptographic strengths
    - ZKsnarks

Who Should Attend

Anyone with a need to know or interest in cryptography, key management, network security or Blockchain, such as:

- Those with some familiarity with cryptography and key management who wish to broaden their knowledge and gain a perspective over the entire subject
- Security engineers
- Those responsible for implementing security functions, or for developing secure applications and architecture
- Those with responsibility for managing, assessing or defining policy for cyber security and new applications
- Application developers
- Those already familiar with network security or Blockchain who wish to use this familiarity as a springboard to learn more about cryptography

Course Style

Location friendly and Face-to-face.