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.

One day Cryptography and Network Security: TLS Course

Course Overview

Transport Layer Security (TLS) and VPN's form an important part of network security.

TLS (and its predecessor SSL) is a protocol for securing information passed between two systems such as a server and client, and for authenticating one or both parties. VPNs provide secure connection between networks, or between an endpoint and a network, and methods include the use of TLS.

Cryptography is a set of fundamental security techniques that provide confidentiality, integrity and authentication, with wide application from protecting personal and commercial information using encryption to enabling trust in e-commerce.

TLS is built on combinations of many different cryptographic techniques, and is supported by key management - particularly certificates. As such, it is a good illustration of applied cryptography. This course first looks at the set of techniques that make up cryptography, including their different functions and properties, and how they are used together to achieve different security objectives. All of the fundamental techniques are covered, but with an emphasis on those more relevant to TLS and VPNs. The course then moves on to cryptographic key management. This includes the use of digital certificates and PKI, which is vital to the effective use of TLS.

Finally, building on the topics already covered, the course looks at TLS itself. This includes how it works, how it combines different cryptographic techniques to achieve its security objectives, the options for ciphersuites, and the different types of SSL certificate.

Course Objectives

- Cryptography: Develop a broad knowledge that can be applied across many different security applications; establish a solid foundation on which to make judgements or assessments of secure systems; appreciate the different cryptographic components and techniques on which TLS and VPNs rely
- Network security: develop knowledge of the TLS process; recognise what is required in terms of key management to support the use of TLS and make it effective; appreciate the different ciphersuites so as to make appropriate choices

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; Message Authentication Codes (MACs)
    - Public key systems, including Diffie-Hellman and RSA

- Hash functions, homomorphic encryption, Elliptic Curve systems, user authentication
- Digital signatures
- Key management, including generation and distribution, storage, PKI and certificates
- Transport Layer Security
    - Purpose and scope
    - How it works
    - Requirements, including certificate options
    - Configuration options such as ciphersuites

Configuration options such as ciphersuites Who Should Attend

Anyone with an interest in network security and cryptography, such as:

- Those with responsibility for managing, assessing or defining policy for cyber security and new applications, and who can benefit from a broader knowledge of cryptography
- Network security engineers
- Those with some familiarity with TLS who wish to broaden their knowledge, or use their TLS familiarity as a springboard to learn more about cryptography

Course Style

Location friendly and Face-to-face.