

Introduction to Secure Sockets Layer

Course Summary

Description

This course is designed as an introduction to cryptography with a focus on the understanding of how SSL/TLS enable secure connections in modern protocols. The course starts out with a general overview of cryptographic functions and builds on this toward examples of specific algorithms and specific applications. Time will be allotted for exercises where students can see the effects of these algorithms first hand and in such a way that each of their benefits and limitations are understood.

Objectives

At the end of this course, students will be able to:

- Understand the purpose of cryptographic functions
- Understand the benefits and limitations of each cryptographic function
- Describe where each cryptographic function would be best deployed
- Understand network security issues and which protocols would benefit from cryptography
- Describe how Public Key Infrastructure can be properly employed to provide trust and security
- Describe how SSL/TLS use PKI to secure private transactions

Topics

- Concepts of Cryptography
- Encryption Functions
- Encryption Algorithms
- Encryption in Applications and Protocols
- Public Key Infrastructure
- SSL/TLS

Audience

This course is intended for those who want to learn about Cryptography and its use in securing network protocols, specifically with SSL. Since improperly deploying encryption over an un-trusted network like the internet could have wide ranging and important side effects, anyone who is administrating or frequently working with services which use clear text data transmission that can be secured with SSL/TLS could benefit from this course. Those working with HTTP, POP3, IMAP4, or LDAP would benefit from this course as well as those interested in deploying a Certificate Authority or with interest in auditing a network.

Prerequisites

The student should have a basic operational knowledge of computers and some familiarity with networking.

Duration

Five ½ days

Due to the nature of this material, this document refers to numerous hardware and software products by their trade names. References to other companies and their products are for informational purposes only, and all trademarks are the properties of their respective companies. It is not the intent of ProTech Professional Technical Services, Inc. to use any of these names generically

Introduction to Secure Sockets Layer

Course Outline

- I. Introduction to Cryptography**
 - A. Hashing
 - B. Symmetric Key Algorithms
 - C. Asymmetric Key Algorithms

- II. Encryption Algorithms**
 - A. Hashing
 - 1. SHA
 - 2. MD5
 - 3. Others
 - B. Symmetric Key
 - 1. DES
 - 2. AES
 - 3. Others
 - C. Asymmetric Key Encryption
 - 1. Diffie-Hellman Key Exchange
 - 2. RSA
 - 3. PGP/GPG

- III. Protocols and Applications**
 - A. Hashing
 - 1. Applications
 - 2. Network Protocols
 - B. Symmetric Encryption
 - 1. Applications
 - 2. Network Protocols
 - C. Asymmetric Encryption
 - 1. Applications
 - 2. Network Protocols

- IV. Public Key Infrastructure**
 - A. Digital Signatures
 - B. x.509 Certificates
 - C. Certificate Authorities

- V. SSL and TLS**
 - A. Traditional TCP Services
 - B. SSL/TLS Modified Services
 - C. How it Works
 - D. Implementation Issues