Publication date : 08/14/2024

Course : TLS/SSL, installation, configuration and implementation

Practical course - 2d - 14h00 - Ref. LSL
Price : 1730 CHF E.T.

3,9 / 5

The TLS (Transport Layer Secure) standard is the most widely deployed protocol for securing application exchanges. This course will introduce you to the architecture, protocol and security services of TLS. You'll learn how to implement it on the client and server sides of secure exchanges.

Teaching objectives

At the end of the training, the participant will be able to:

- Implementing the TLS protocol
- Strong and secure configuration of TLS clients and servers
- Analyze TLS traffic
- Understanding attacks on TLS

Intended audience

System and network technicians and administrators, security architects and managers.

Prerequisites

Basic knowledge of computers and networks.

Course schedule

PARTICIPANTS

System and network technicians and administrators, security architects and managers.

PREREQUISITES

Basic knowledge of computers and networks.

TRAINER QUALIFICATIONS

The experts leading the training are specialists in the covered subjects. They have been approved by our instructional teams for both their professional knowledge and their teaching ability, for each course they teach. They have at least five to ten years of experience in their field and hold (or have held) decision-making positions in companies.

ASSESSMENT TERMS

The trainer evaluates each participant's academic progress throughout the training using multiple choice, scenarios, hands-on work and more.
Participants also complete a placement test before and after the course to measure the skills they've developed.

1 Cryptography and security services

- Terminology and cryptographic principles.
- Main cryptographic algorithms and their use in TLS: AES, DHE, ECC, RSA, DSA.
- Hash functions (MD5, SHA1, SHA2, SHA3) with and without key (Hmac).
- Cryptographic operating procedures.
- Cryptanalysis and attacks on cryptographic functions.
- Security services: confidentiality, authentication, integrity.

Hands-on work

OpenSSL-based encryption and decryption and cryptanalysis.

2 Certificates and digital signatures

- Digital signature.
- Attacks on public keys.
- Certificates and PKCS12 key implementation.
- Certificate profiles for TLS.

Hands-on work

Certificate design (client and server side) and PKCS12 on the client side.

3 TLS architecture and services

- Positioning of different versions: SSLv3, TLS1.0, TLS1.1, TLS1.2.
- Architecture, security protocol and services, TLS exchanges.
- Configuring cipher suites.

Hands-on work

Configure a TLS client and analyze TLS traffic.

4 Configuring and implementing the TLS protocol

- Client- and server-side configuration.
- Configuration for simple server authentication.
- Implement certificates and set up encryption algorithms on the server side.
- Server authentication, certificate store configuration.

Hands-on work

Configuring and implementing TLS on the Apache Web server side.

5 Advanced TLS protocol services

- TLS extensions and features.
- Various authentication modes: OpenPGP certificate, PSK.
- Ticket and reopen session.
- Session benchmarking.
- TLS client configuration (PKCS12).

Hands-on work

Configure TLS clients and servers for strong mutual authentication.
Implementation of extensions, performance analysis.

TEACHING AIDS AND TECHNICAL RESOURCES

• The main teaching aids and instructional methods used in the training are audiovisual aids, documentation and course material, hands-on application exercises and corrected exercises for practical training courses, case studies and coverage of real cases for training seminars.
• At the end of each course or seminar, ORSYS provides participants with a course evaluation questionnaire that is analysed by our instructional teams.
• A check-in sheet for each half-day of attendance is provided at the end of the training, along with a course completion certificate if the trainee attended the entire session.

TERMS AND DEADLINES

Registration must be completed 24 hours before the start of the training.

ACCESSIBILITY FOR PEOPLE WITH DISABILITIES

Do you need special accessibility accommodations? Contact Mrs. Fosse, Disability Manager, at psh-accueil@orsys.fr to review your request and its feasibility.

6 Security analysis and outlook for the TLS protocol

- Attacks on the TLS protocol.
- Best practices, configuration control.
- DTLS protocol overview.
- Presentation of the future version of TLS 1.3.

Hands-on work
Audit the TLS protocol. Implement attacks on TLS. Configure and implement DTLS.

Dates and locations

REMOTE CLASS
2026 : 26 Mar., 18 June, 28 Sep., 3 Dec.