TLS SECURITY

Training | 2 days, 8 hrs. per day

In this interactive training, you will gain the knowledge you need to understand, analyze, and securely configure TLS on your servers.

YOUR BENEFITS

- Understand how cryptography is used in TLS and how to analyze your TLS applications.
- Select the right, efficient, and secure configuration for your applications.
- Protect your applications from known TLS attacks like ROBOT, DROWN, or CRIME.
- Convince your customers by using state-of-the-art security with HSTS and TLS 1.3.

TRAINING CONTENTS

Certificates

> Formats
> Creation and validation with OpenSSL
> PKI and Let's Encrypt

TLS 1.2

> Protocol flow
> Extensions
> Analysis with Wireshark

Attacks

> Short overview (e.g. DROWN, ROBOT, Heartbleed)

TLS 1.3

> Protocol flow
> Security and performance improvements

Secure Server Configuration

> Apache mod_ssl
> Apache Tomcat

Verification of Own Configuration With Common Tools

> testssl.sh
> TLS-Scanner

Trainer and your contact for this training

Prof. Dr. Juraj Somorovsky | CTO

juraj.somorovsky@hackmanit.de

+49 (0)234 / 54459996 | Dept. Cryptography

Juraj Somorovsky assists customers with his expertise in cryptography. He is a professor of system security at the University of Paderborn. He is the main developer of the analysis tool „TLS-Attacker“ and author of numerous attacks on TLS. These include, for example, the DROWN or ROBOT attacks, which were awarded the Pwnie Awards for best cryptographic attacks in 2016 and 2018.

REFERENCES

“Pleasant number of participants and atmosphere, so questions could be answered quickly. The instructor was very helpful and provided active support.”

“Very good insight into historical and current TLS versions.”

“Juraj's professional qualities are undisputedly outstanding.”

“Very well structured, many interesting examples.”

“The expertise was clear from the start. Great!”

TLS SECURITY

Training | 2 days, 8 hrs. per day

TARGET AUDIENCE

This training is intended for people who configure and manage TLS applications.

This course is helpful for, among others:

> Server administrators
> Developers
> Security researchers

It is helpful if you have basic knowledge of cryptography, server administration or TLS. To participate, you will need a computer with a Linux system. As an alternative, we provide you with a virtual machine for the virtualization software VirtualBox.

BOOKING OPTIONS

Whether a fixed date, team online training or on-site training, we adapt to your wishes. Contact the person responsible for the desired training to receive an individual and non-binding offer.

Send the registration form or the individual booking request by email to Prof. Dr. Juraj Somorovsky:

juraj.somorovsky@hackmanit.de

ONLINE TRAINING | TLS SECURITY | OVERVIEW

Time:	from 9:00 to 17:00
Duration:	2 days, 8 hrs. per day (incl. breaks)
Total price:	1.290€ plus VAT (per person)

TLS SECURITY

Online Training | 2 days, 8 hrs. per day

Requested date for the Online Training

Number of people

Name and email

Contact for booking

Company

Address

Postal code, city

Billing address (if different)

Email

Phone

Notes

Please send your registration by email to:
juraj.somorovsky@hackmanit.de