

# INTRODUCTION TO TLS

Training | 4 hrs.  

In this interactive training, you will gain the knowledge necessary to understand basic TLS concepts and configure your servers.

## YOUR BENEFITS

- > Learn how to analyze your TLS applications.
- > Select the right, efficient, and secure configuration for your applications.
- > Protect your applications from known TLS attacks.
- > Convince your customers by using state-of-the-art security configuration.

## TRAINING CONTENTS

Certificates

TLS Protocol flow

Why should I use TLS 1.3?

Secure Server Configuration

> Apache mod\_ssl

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](mailto: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!”

# INTRODUCTION TO TLS

Training | 4 hrs.  

## 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](mailto:juraj.somorovsky@hackmanit.de)

## ONLINE TRAINING | OVERVIEW

---

|                     |                            |
|---------------------|----------------------------|
| <b>Time:</b>        | from 9:00 to 13:30         |
| <b>Duration:</b>    | 4,5 hrs. (incl. breaks)    |
| <b>Total price:</b> | 490€ plus VAT (per person) |

# INTRODUCTION TO TLS

Online Training | 4 hrs.

Requested date for the Online Training

Contact for booking

Number of people

Company

Name and email

Address

Postal code, city

Billing address (if different)

Email

Phone

Notes

Please send your registration by email to:  
[juraj.somorovsky@hackmanit.de](mailto:juraj.somorovsky@hackmanit.de)