

## Training:

# TLS in the Enterprise

Date of the training: **March 18–19, 2019** in Heidelberg, Germany

Book Now using the voucher code: **TR19\_HMTS** and save an additional 5% of the current valid rate of any package!

### Overview

In our training we will cover attacks against TLS/SSL in theory and in practice, discuss their relevance for the enterprise and talk about reasonable mitigating controls.

The training will demystify TLS/SSL Security because today it seems to be hard to run a secure TLS configuration without breaking functionality. So, after some basic introduction about history and cryptology we will dig into certificate problems, crypto attacks, work with most important tools and walk through the common SSL vulnerabilities. We will explain each vulnerability, do a demo or hands-on if possible, discuss relevance and pitfalls within the enterprise context and give recommendations for mitigating controls (e.g. example configs for Apache, Nginx, IIS, Tomcat, Jboss).

Finally, we will also take a look into the future, because a lot of important things will change shortly, so everyone should be well prepared to avoid any major disruption of important services. And don't forget to bring a laptop with administrative privileges, this is a hands-on training and you have to install tools, if you would like to participate in the exercises.

## Requirements

- Basic knowledge about networking and protocols (tcp, udp, http, smtp)
- Working with Linux/\*nix on the command line
- Basics about configuration of web, mail and application servers«
- Laptop with administrative privileges (Linux OS preferred)
- VirtualBox or VMWare Player installed, if the laptop is running windows or if the attendee doesn't want to make changes to the host OS
- SSH client

## About the Speaker: Michael Thumann

Michael Thumann is Lead Architect of the ERNW Sectools team. He has published security advisories regarding topics like 'Cracking IKE Preshared Keys' and Buffer Overflows in Web Servers/VPN Software/VoIP Software. Michael enjoys sharing his self-written security tools (e.g. 'tomas - a Cisco Password Cracker', 'ikeprobe - IKE PSK Vulnerability Scanner' or 'dnsdigger - a dns information gathering tool') and his experience with the community. Besides numerous articles and papers he wrote the first (and only) German Pen-Test Book that has become a recommended reading at German universities. In addition to his daily tasks he was a regular conference-speaker (e.g. Troopers, Blackhat, HITB and RSA Conference) and has also contributed exploit code to the Metasploit Framework. With more than 20 years of experience in computer security Michaels' main interest is to uncover vulnerabilities and security design flaws from the network to the application level and reverse almost everything to understand the inner working.

## Booking

Recommended Online Booking of Trainings Through:

Sign-Up Form <https://troopers.de/tickets/>

Voucher code: **TR19\_HMTS**

Using this voucher code automatically gives you an additional 5% off the current valid price! You can register with this code up until March 11th, 2019 or until seats have run out.

## Contact

**Need assistance?** Don't hesitate to call us. We are fluent in English and German.

Zögern Sie nicht uns zu kontaktieren. Wir sprechen fließend Englisch und Deutsch.

### Troopers Organization Team

+49 151 16228365 or [info@troopers.de](mailto:info@troopers.de)

**Booking is also possible offline through your trusted partner from:**



**HM Training Solutions**, Falkenstrasse 6, 63820 Elsenfeld, Germany

+49 6022 508200 / [info@hmtrainingsolutions.com](mailto:info@hmtrainingsolutions.com)

+49 6022 5089999 / [www.hmtrainingsolutions.com](http://www.hmtrainingsolutions.com)