TLS-Security

IT-Security Training

Training Contents

(2 DAYS)

TLS is what turns "http" to "https". If data is transmitted encrypted on the Internet, in most cases TLS (the successor of SSL) is used. Whether web, email, phone calls, chat or VPN - there is hardly a type of communication which cannot be encrypted with TLS. However, using TLS is not always trivial. There are different TLS versions which support various cryptographic algorithms, transport mechanisms or extensions. Due to this variety and the resulting complexity of the TLS protocol, there are many diverse attacks which can be used in different scenarios. In order for TLS to effectively protect the communication, up-to-date libraries and apporpriate configurations must be used to prevent these attacks.

Especially since TLS can be found almost everywhere, it is worthwhile to understand it precisely and to analyze its security.

The training will address the following questions:

- Which cryptographic basics do I need to understand? How are they used in TLS?
- Which TLS implementations are available?
- How do I generate my own TLS certificates?
- What are the known TLS attacks? How can I protect my systems?
- How do I configure my servers in a secure way?
- What does the future hold for TLS?

Requirements

This course is designed for system administrators and developers with basic knowledge of SSL/TLS. You will learn which attacks are applicable to TLS and how they affect your own server. Afterwards, you will learn how to securely configure your own server and how to check a secure configuration with common tools.

Lecturer

Dr. Juraj Somorovsky

Juraj Somorovsky is a co-founder of Hackmanit and a security researcher at the Ruhr University Bochum. With more than ten years of experience in the field of IT security, he has acquired profound knowledge regarding cryptography and web security. He is the main developer of the analysis tool "TLS-Attacker" and author of numerous attacks on TLS. These include, for example, DROWN and ROBOT, which each won the Pwnie award for the Best Cryptographic Attack. Juraj Somorovsky presented his work at renowned scientific and industrial conferences, including USENIX Security, Black Hat, DeepSec and OWASP Europe.

Contact

juraj.somorovsky@hackmanit.de
www.hackmanit.de

HACKMANIT

Universitätsstraße 150 (ID 2/469)
44801 Bochum
Germany

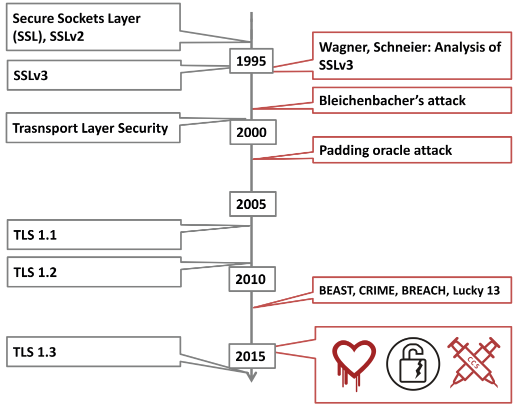
DAY 1

- Short Introduction to Cryptography
- TLS Protocol Flow
- TLS Extensions
- Certificates and Validation of Certificates
- Attacks - Short Overview
  - including BEAST, CRIME, Heartbleed and more

DAY 2

- TLS Implementations
- Secure Server Configuration
  - Apache HTTP Server (mod_ssl)
  - Apache Tomcat
- Review of Your Own Server Configuration with Common Tools

TLS History


Secure Sockets Layer (SSL), SSLv2
1995
Wagner, Schneier: Analysis of SSLv3
SSLv3
Bleichenbacher's attack
Trasnsport Layer Security
2000
Padding oracle attack
2005
TLS 1.1
TLS 1.2
2010
BEAST, CRIME, BREACH, Lucky 13
TLS 1.3
2015
CCS