TLS-Sicherheit

IT-Sicherheit Schulung

Schulungsinhalte

(2 TAGE)

Erst durch TLS wird „http“ zu „https“. Werden im Internet Daten verschlüsselt übertragen, kommt dabei in den meisten Fällen TLS (der Nachfolger von SSL) zum Einsatz. Ob Web, Mail, Telefonie, Chat oder VPN – es gibt kaum eine Kommunikationsart, die nicht auch mit TLS verschlüsselt wird. Es ist jedoch nicht immer trivial, TLS zu verwenden. Es existieren unterschiedliche TLS-Versionen, die diverse kryptographische Algorithmen, Transportmechanismen oder Erweiterungen unterstützen. Durch die Komplexität des TLS-Protokolls gibt es viele verschiedene Angriffe, die in unterschiedlichen Szenarien anwendbar sind. Diese Angriffe müssen, damit TLS seinen Zweck erfüllen und die Kommunikation effektiv schützen kann, mit aktuellen Bibliotheken und passenden Konfigurationen verhindert werden.

Besonders da TLS fast überall zu finden ist, lohnt es sich, es genauer zu betrachten und seine Sicherheit zu analysieren. In der Schulung werden die nachfolgenden Fragen beantwortet:

- Welche kryptographischen Grundlagen muss ich verstehen? Wie werden diese bei TLS eingesetzt?
- Welche TLS-Implementierungen gibt es? Und wie kann ich mich dagegen schützen?
- Wie generiere ich meine eigenen TLS-Zertifikate?
- Welche Angriffe auf TLS gibt es?
- Wie konfiguriere ich meine Server sicher?
- Was bringt die Zukunft von TLS?

Voraussetzungen

Diese Schulung richtet sich vor allem an Systemadministratoren und Entwickler mit grundlegenden Kenntnissen über SSL/TLS. Sie lernen dabei, welche Angriffe auf TLS anwendbar sind und was für eine Auswirkung sie auf Ihren Server haben. Anschließend lernen Sie wie man einen eigenen Server sicher konfiguriert und wie man die sichere Konfiguration mit gängigen Tools überprüfen kann.

TAG 1

- Kurze Einführung in die Kryptographie
- TLS-Protokollablauf
- TLS-Erweiterungen
- Zertifikate und Zertifikatsvalidierung
- Angriffe – Kurzer Überblick
  - BEAST, CRIME und u.a. Heartbleed

TAG 2

- TLS-Implementierungen
- Sichere Serverkonfiguration
  - Apache HTTP Server (mod_ssl)
  - Apache Tomcat
- Überprüfung eigener Serverkonfiguration mit gängigen Tools

Dozent

Dr. Juraj Somorovsky

Juraj Somorovsky ist ein Sicherheitsforscher an der Ruhr-Universität Bochum und Mitgründer von Hackmanit. Mit mehr als 10 Jahren Erfahrung im Bereich der IT-Sicherheit hat er fundiertes Wissen über die Themen Kryptographie und Websicherheit erlangt. Er ist der Hauptentwickler des Analysewerkzeugs „TLS-Attacker“ und Autor zahlreicher Angriffe auf TLS. Dazu gehören beispielsweise die Angriffe DROWN oder ROBOT, die mit den Pwnie Awards für beste kryptographische Angriffe in den Jahren 2016 und 2018 ausgezeichnet wurden. Juraj Somorovsky präsentierte seine Arbeit auf renommierten wissenschaftlichen und industriellen Konferenzen, darunter USENIX Security, Black Hat, DeepSec oder OWASP Europe.

Kontakt

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

HACKMANIT

Universitätsstraße 150 (ID 2/469)
44801 Bochum