Hochschule Offenburg
offenburg.university

ivESK Institut für verlässliche Embedded Systems und Kommunikationselektronik

Hochschule Offenburg

Institut für verlässliche Embedded Systems und Kommunikationselektronik (ivESK)

Differenzielles Fuzz-Testing von TLS 1.3 Implementierungen für Embedded Systeme

Am Institut für verlässliche Embedded Systems und Kommunikationselektronik (ivESK) werden Algorithmen, Protokolle und Plattformen für effiziente, sichere und zuverlässige, drahtlose und drahtgebundene Kommunikationslösungen unter Nutzung von Embedded Systemen entworfen, implementiert und getestet. Zur Unterstützung unserer Arbeit suchen wir

eine(n) Studierende(n) für eine Bachelor- oder Masterarbeit

in Kombination mit einer

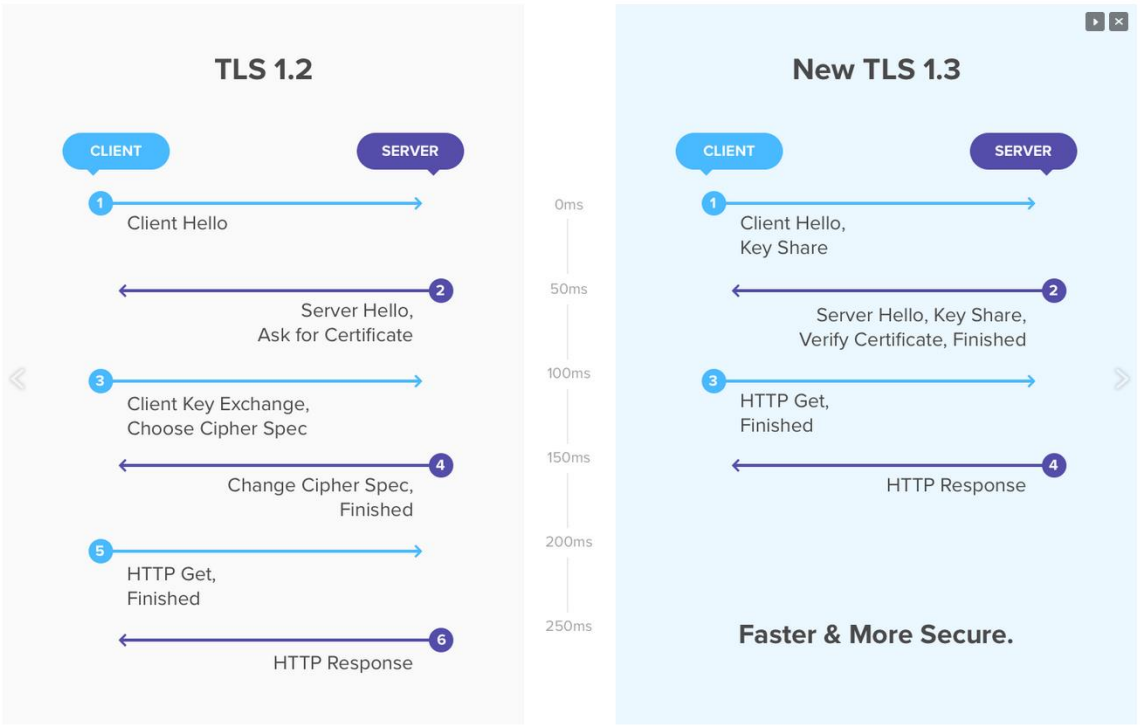
Tätigkeit als wissenschaftliche Hilfskraft

für die Bearbeitung des folgenden Themas aus dem Bereich der Datensicherheit / Security:

Fuzzing, das (teil-)randomisierte Erzeugen von Testeingaben, ist eine leistungsfähige Methode, um Software auf Fehler und Schwachstellen zu testen. *Differenzielles Testen* nutzt einen Vergleich mehrerer Implementierungen der gleichen Spezifikation, um fehlerhaftes Verhalten zu erkennen.

Wir untersuchen die Anwendung von Differenziellem Fuzz-Testing, einer Kombination von Fuzzing und Differenziellem Testen, zur Erkennung von Fehlern in Implementierungen des *Transport Layer Security* (TLS) Protokolls. Die Effektivität unseres Ansatzes konnten wir durch das Aufdecken zuvor unbekannter Sicherheitslücken in verbreiteten TLS-Implementierungen bereits demonstrieren.

Mit TLS 1.3 ist nun zuletzt Ende 2018 eine neue Version dieses wichtigen Protokolls standardisiert worden. Entsprechende Implementierungen sind daher noch recht jung und die Wahrscheinlichkeit von Implementierungsfehlern und Schwachstellen vermutlich höher als bei schon seit Jahren bestehenden Protokollversionen. Zudem unterscheidet sich TLS 1.3 von der Vorgängerversion 1.2 in einigen Punkten signifikant, so dass unsere Methodik und unsere Werkzeuge angepasst werden müssen.



Im Rahmen Ihrer Tätigkeit an unserem Institut sollen Sie …

- … sich in das TLS-Protokoll sowie unsere Methodik und Werkzeuge einarbeiten,
- notwendige Anpassungen identifizieren, beschreiben und umsetzen,
- eine sinnvolle Auswahl von zu testenden Implementierungen treffen und auf diese anwenden,
- und die Resultate auswerten.

Was Sie erwarten können:

- Eine interessante wissenschaftliche Fragestellung mit hoher Praxisrelevanz
- Eine gute Mischung aus theoretischer und praktischer Arbeit
- Aufbau von detaillierten Kenntnissen zur Funktionsweise von modernen Security-Protokollen

Was Sie mitbringen sollten:

- Programmiererfahrung, vorzugsweise in C/C++ und Python
- Solide Kenntnis von Netzwerkprotokollen (Sicherheitsprotokolle von Vorteil)
- Grundlegende Erfahrung mit Linux-basierter Softwareentwicklung

Bei Rückfragen:
Dipl.-Phys. Andreas Walz
andreas.walz@hs-offenburg.de
Telefon: 0781-205-4803
Raum: STB1.02

Für Bewerbungen:
Prof. Dr.-Ing. Axel Sikora
axel.sikora@hs-offenburg.de
Telefon: 0781-205-416
Raum: B130