Bachelor-/Masterarbeit

Embedded-Testing, Fuzzing, Emulation

Ziel

Embedded-Systeme werden zunehmend untereinander und mit dem globalen Internet vernetzt, was sie zu attraktiven Angriffszielen für böswillige Akteure macht. Automatisiertes Embedded-Testing hilft, Schwachstellen frühzeitig zu erkennen. Z.B. kann Fuzzing, also das Übergeben zufällig generierter Inputs an die Anwendung, Speicherfehler aufdecken.

In Embedded-Systemen herrscht eine enge Verknüpfung von Soft- und Hardware. Das Einbinden der Hardware erschwert es i.d.R, einen hohen Automatisierungsgrad, gute Performance und hilfreiche Einblicke in das Testsystem zu gewährleisten. Um dies trotzdem zu ermöglichen kann z.B. kreative Instrumentierung der Hardware, neuartige Test- und Analysemethoden oder die Emulation des Testsystems helfen.

In den Abschlussarbeiten sollen Techniken und Tools, die diese Probleme angehen, entwickelt und/oder eingesetzt werden und bzgl. ihrer Praxistauglichkeit und der oben genannten Kriterien bewertet werden. Das genaue Thema hängt von den Interessen der Studierenden und aktuellen wissenschaftlichen und technischen Entwicklungen auf dem Gebiet ab.

Anforderungen und Voraussetzungen

- Inbetriebnahme von und Arbeiten mit Embedded-Systemen
- Recherche und Auswahl geeigneter Techniken und Tools
- Umsetzung in einer Testumgebung mit Anwendung auf echte Embedded-Systeme

Ansprechpartner

Prof. Dr. Lothar Braun | ✉ lothar.braun@tha.de | ✆ +49 821 5586-3378
Lukas Senger | ✉ lukas.senger@tha.de

THA_innos

Das Institut für innovative Sicherheit (THA_innos) bietet eine Vielzahl von Abschluss- und Projektarbeiten im Themenfeld Cyber Security an. Unser Team unterstützt Studierende dabei mit Know-How und Praxiserfahrung und ist zudem offen für eigene Themenvorschläge. Studierende lernen sowohl das Institutsleben, als auch die aktuelle Forschung von THA_innos kennen.

Weitere Informationen auch unter `https://innos.tha.de`