CYSEC Cybersecurity TU Darmstadt | System Security Lab | TECHNISCHE UNIVERSITÄT DARMSTADT

Masterthesis – Security Verification of Hardware Designs

Beschreibung

Systemsicherheit und Sicherheit eingebetteter Systeme wird im Zuge aktueller Cyberattacken immer wichtiger. Viele der Angriffe finden auf Softwareebene statt, nutzen jedoch zunehmend Fehlerinder zugrundelieg enden Hardware aus. Zwar warden in der Industrie bereits automatisierte Hardware-Tests eingesetzt, diese sind aber unzureichend. Deshalb ist es um so wichtiger, Hardware hinsichtlich ihrer Sicherheit auch während der Design- und Synthese-Phase zu untersuchen. Im System Security Lab erforschen wir ebenfalls neuartige sicherheitsrelevante Prozessor-Erweiterungen, unter anderem mittels Hardwaremodifikationen (RTL) für open-source Prozessorarchitekturen. In diesem Zusammenhang sollen auch die zahlreichen existierenden Prozessor-Security-Extensions analysiert werden. Dazu erforschen wir bereits Mechanismenzur Analyse von Sicherheitseigenschaften solcher Hardwaredesigns.

Projekt

Ein Weg, Programme auf Sicherheitslücken zu untersuchen ist Fuzzing. Fuzzing mutiert anfängliche Programmeingabenum so immer mehr Bereiche eines Programmsmit potentiell ungültigen Eingaben zu testen. Ziel des Projektes ist es, konventionelle Software-Fuzzing Konzepte auf Hardwaredesigns zu übertragen.

Erforderliche Voraussetzungen

- Erfahrung oder Interesse an Einarbeitung in Fuzzing-Tools (z.B. AFL)
- Erfahrung mit Python (oder Rust) und/oder C/C++
- Vertraut mit Verilog und/oder VHDL und grundlegender Digitaltechnik
- Gewillt, schnell neue Dinge, Tools und Programmiersprachen zu lernen

Kontakt

Bei Interesse an diesem hochaktuellen Forschungsthemas genügt eine Bewerbung (Lebenslauf, Zeugnisse/Leistungsübersichten und weitere relevante Dokumente) via Mail an:

Ghada Dessouky
ghada.dessouky@trust.tu-darmstadt.de

AK Professor Dr.-Ing. Ahmad-Reza Sadeghi
Gebäude S4|14 (CASED Gebäude)
Mornewegstraße 30
64293 Darmstadt
https://www.trust.informatik.tu-darmstadt.de

März 2019