3. gemeinsamer Workshop

des

Vereins zur Förderung der Fakultät für Informatik und Automatisierung der Technischen Universität Ilmenau e.V.

und der

Regionalgruppe Ilmenau der Gesellschaft für Informatik e.V.

24.04.2023
17.00 Uhr – 18.30 Uhr
Meitnerbau
Raum 1.1.102/103
TU Ilmenau

Ab 16.40 Uhr
Gelegenheit zu einer Tasse Kaffee

17.00 Uhr
Begrüßung durch Prof. Dr.-Ing. Günter Schäfer

17.05 – 17.45 Uhr
Prof. Dr.-Ing. habil. Daniel Ziener
Technische Universität Ilmenau

Thema: Embedded Security: Sicherheit durch angepasste Hardware?

Durch die zunehmende Anzahl und Vernetzung von eingebetteten Systemen werden diesen verschiedensten Angriffen ausgesetzt mit dem Ziel Informationen zu entwenden oder ihre Funktionalität zu beeinflussen.
Besonders anfällig sind eingebettete Systeme für sogenannte physikalische Angriffe wie Seitenkanalangriffe, Fehlerinjektionsangriffe oder klassisches Reverse Engineering. Das Fachgebiet RAES (Rechnerarchitektur und Eingebettete Systeme) erforscht und entwickelt daher eine angepasste Hardware um diese Angriffsvektoren deutlich zu reduzieren oder gar komplett zu unterbinden.

Darüber hinaus erlauben solche angepassten, spezialisierten Systeme auch die Optimierung weiterer nicht funktionaler Eigenschaften. Ein Beispiel hierfür ist die verbesserte Effizienz und Geschwindigkeit in der Datenverarbeitung durch spezialisierte, dynamisch austauschbare Hardwarebeschleuniger. Dabei können Anwendungen der klassischen Bildverarbeitung sowie Klassifikationsaufgaben mittels Neuronaler-Netze bis hin zu Datenverarbeitung in Datenbanken optimiert werden.
Dynamische Adaptivität kann zudem zur bedarfsgerechten Verbesserung der Zuverlässigkeit genutzt werden wie sie etwa in Satelliten wünschenswert ist. Hierbei wird

auf die fluktuierende Strahlenbelastung durch die Sonne reagiert um flexibel zwischen erhöhter Zuverlässigkeit und Leistungsfähigkeit bzw. Verarbeitungsgeschwindigkeit umschalten zu können.

In diesem Vortrag wird gezeigt, wie speziell angepasste Hardware die Sicherheit gegenüber physikalischen Angriffen verbessern kann. Des Weiteren werden angepasste, adaptive Systeme eingeführt, welche sich zur Laufzeit restrukturieren können. Durch die Ausnutzung dieser Eigenschaften werden effiziente Beschleuniger für Datenbankabfragen und Neuronale Netze ermöglicht. Darüber hinaus wird dargestellt, wie Schaltungen und dazugehörige zu verarbeitende Daten gegenüber Strahlung geschützt werden können.

17.45 – 18.25 Uhr
Dr. Andreas Weichslgartner
CARIAD

Thema: Automotive Security: Software-Schwachstellen finden und verhindern

Software wird immer mehr zum Hauptbestandteil moderner Fahrzeuge. Von Batteriemanagement, virtuellen Cockpits bis zu Fahrerassistenzsystemen und autonomen Fahren, Software bestimmt das automobile Kundenerlebnis und treibt maßgebliche Innovationen. Zusammen mit erhöhter Konnektivität, steigt aber auch das Risiko von Hackerangriffen. Einfallstor für Angriffe sind häufig Schwachstellen in Design und Quellcode von Software. Je später solche Schwachstellen im Lebenszyklus der Software erkannt werden, desto komplexer und teurer ist es diese zu beheben. Deshalb ist es wichtig, bereits in der Konzeptionierung und Implementierung mögliche Defizite zu erkennen oder zu verhindern.

Dieser Vortrag bietet einen Überblick über häufige und historische Schwachstellen im Kontext der Entwicklung von Automotive Software. Aufbauend drauf stellt er Techniken und Werkzeuge vor, um bereits Schwachstellen während des Entwicklungsprozesses zu erkennen und zu verhindern. Abschließend gibt er einen Ausblick auf Entwicklungen und Trends um Automotive Software sicherer zu machen.

18.30 Uhr
Austausch bei einem Mini-Imbiss

Sollte dieses Programm auf Ihr Interesse stoßen, bitten wir Sie um eine verbindliche Anmeldung per E-Mail an nadja.kuehler@tu-ilmenau.de bis zum **04. April 2023** (die Teilnahme am Workshop ist kostenlos).