TeleTrusT
Pioneers in IT security.

TeleTrusT-interner Workshop

Berlin, 13.06.2019

Secure Platform

Dr. André Kudra, esatus AG

Plattformsicherheit – eine äußerst aktuelle Problemstellung

- Aktuelle IT-Systeme sind oft schwer durchdringbare und unnötig komplexe Gebilde aus Hard- und Software
- Sicherheit von IT-Systemen hängt vom sicheren Design jeder einzelnen Komponente ab und deren sicherer Interaktion
- Schwachstellen und versteckte Einfallstore auf jeder Ebene möglich, auch in der Hardware
- Tatsächliche Sicherheit kann kaum verlässlich eingeschätzt werden – oft auch nicht von Experten
- Risiko für Vertraulichkeit, Integrität und Verfügbarkeit, insbesondere im professionellen Umfeld (bspw. KRITIS)

Übersicht Designprinzipien Secure Platform

1. **Komplexitätsreduktion** → Enthält nur Code der auch benötigt wird
2. **Sicherheit im Design** → Sicherheit auf jedem Level der Architektur
3. **Offene Architektur** → Alle Komponenten einsehbar und prüfbar
4. **Sicherheit als Prozess** → Sicherheitsprüfungen durch Betriebsorganisation
5. **Kontrollierte Lieferkette** → Fertigung in Europa
6. **Investitionsschutz** → Langfristige Verfügbarkeit der Komponenten
7. **Nachhaltigkeit** → Hardware in Betriebslaufzeit umkonfigurierbar
8. **Disruptive Nutzung** → FPGA in praktischer Anwendung für jedermann

Praxisorientierte Konzeption einer offenen und sicheren IT-Plattform – 6 Ebenen der Konzeption

Ebene

Zielsetzung

Lösungen

1 Hardware	2 Chiparchitektur	3 Betriebssystem	4 Anwendungen	5 Mobilbetrieb	6 Betriebskonzept
▪ Akquise FPGA-Expertise ▪ Auswahl FPGA Plattform ▪ Sicherheitsbewertung der Hardware ▪ Support für Installation RISC-V auf FPGA ▪ Tests: Funktionalität, Sicherheit, Stabilität, Performance	▪ Akquise RISC-V-Expertise ▪ Auswahl RISC-V Core ▪ Sicherheitsbewertung der Chiparchitektur ▪ RISC-V auf FPGA lauffähig machen ▪ Tests: Funktionalität, Sicherheit, Stabilität, Performance	▪ Akquise Linux-Expertise ▪ Auswahl Linux-Distro ▪ Sicherheitsbewertung des Betriebssystems ▪ Linux-Distro auf RISC-V lauffähig machen ▪ Tests: Funktionalität, Usability, Sicherheit, Stabilität, Performance	▪ Erarbeitung abzudeckender Use Cases ▪ Auswahl Open Source Komponenten ▪ Sicherheitsbewertung der Komponenten ▪ Installation auf Linux-Distro ▪ Tests: Funktionalität, Usability, Sicherheit, Stabilität, Performance	▪ Auswahl notwendiger Erweiterungen für das Betriebssystem ▪ Auswahl Modifikationen bzw. Alternativen für Anwendungen ▪ Inbetriebnahme der Erweiterungen, Änderungen, Modifikationen ▪ Tests: Funktionalität, Usability, Sicherheit, Stabilität, Performance	▪ Ausarbeitung eines organisatorischen Konstrukts für Produktion, Vertrieb und Support ▪ Konzeption für regelmäßige dedizierte Sicherheitsprüfungen durch unabhängige Institutionen ▪ Nachhaltige Weiterentwicklung der Plattform

FPGA RISC-V SECURE LINUX OPEN SOURCE OPEN SOURCE

Zusammenfassung möglicher Lösungsansatz

- Durchführung eines Entwicklungsprojekts „Secure Platform“, gemeinsam mit geeigneten Partnern
- Konzeption einer offenen, nachhaltigen und sicheren IT-Plattform und Prüfung auf praktische Anwendbarkeit
- Aufbau einer konkreten Plattform-Alternative aus Deutschland zu etablierten internationalen Hard-/Softwareherstellern
- Verschiedene Gerätevarianten zur optimalen Unterstützung von stationärem und mobilem Einsatz
- Langfristige Verfügbarkeit und Betreibbarkeit der technischen Komponenten, idealerweise Produktion in Europa
- Sicherheitsprüfung gem. Common Criteria (CC, ISO/IEC 15408) ggf. erstrebenswert und markterfolgsfördernd
- Erste Zielgruppe sind sicherheitsbewusste Organisationen, bspw. KRITIS

Zeit zur Diskussion…

Vielen Dank für Ihr Interesse!

Wie geht es weiter?