Fraunhofer AISEC

Studentische Hilfskraft (m/w/), IDP, Forschungspraxis*

Resiliente x86 Plattform auf Basis der Intel PSE

Motivation und Aufgabenstellung

Viele kritische Systeme, wie beispielsweise in der Energieerzeugung, setzen auf softwarebasierte Steuerungssysteme. Diese werden auch zunehmend Ziele von Angriffen [1]. Um die Systeme weiterhin aufrechterhalten zu können, müssen neue Wege gefunden werden, um existierende Systeme resilient gegenüber Angriffen zu machen. Ein resilientes System kann auch im Angegriffenen Zustand einen minimalen Betrieb aufrechterhalten oder wieder in einen sicheren Zustand zurückkehren.
Für ARM Platformen hat das Fraunhofer AISEC bereits eine Technologie entwickelt, die es ermöglicht kompromittierte Systeme durch einen extern steuerbaren Reset-Mechanismus wieder in einen vertrauenswürdigen Zustand zu bringen [2, 3]. Dieser Ansatz basiert auf der ARM-Trustzone und ist somit nur auf ARM Prozessoren möglich.
Durch neue Entwicklungen im x86 Umfeld steht nun auf Elkhart-Lake Prozessoren eine ähnliche Architektur zur Verfügung [4]. Dabei kann eine logisch getrennte, aber physisch zusammenhänge Entität die Plattform neu starten und Änderungen erzwingen. Ermöglicht wird das mit der Intel Programmable Service Engine (PSE), welche einen ARM basierten Coprozessor zur verfügung stellt. Ein Ansatz wie er bereits für die ARM Plattform entwickelt wurde, lässt sich damit nun auch für Intel x86 implementieren.

Tätigkeitbeschreibung

Im Rahmen der Arbeit soll prototypisch eine resiliente Plattform auf Intel x86 Elkhart-Lake implementiert werden. Dabei soll die Plattform, mithilfe der Intel PSE einen Watchdog implementieren der von einem externen Server kontrolliert werden kann. So kann der Server durch nicht erneuern des Watchdogs den Reboot, oder Reset der Plattform erzwingen. Die PSE ist Quelloffen [5, 6] kann durch den Nutzer selbst programmiert werden, und basiert auf ZehpyrOS [7]. Durch die minimale Gestaltung der PSE, sollen allerdings die Netzwerkfunktionen weiterhin im Host-OS ausgeführt werden und lediglich an die PSE weitergereicht werden. Eine entsprechende Client-Server-/ und Host-OS-Architektur ist bereits für die ARM Plattform entwickelt und kann wiederverwendet werden [8].

Mögliche Aufgaben umfassen:

- Funktionsanalyse der Intel PSE
- Implementierung der resilienten Plattform
  - Implementierung des *Authenticated Watchdogs*
  - Evaluationen zu *authentifiziertem Boot (Gated Boot)*
  - Evaluationen zu *Hardwarebasierter Authentifizierung*
- Evaluation der Plattform

Ziel des Prototyps ist der Nachweis, dass eine resiliente Plattform auf der Basis der PSE entwickelt werden kann. Der Source Code der ARM basierten Implementierung steht ebenfalls zu Verfügung, und kann mit geringem Aufwand portiert werden.

Anforderungen

- Motivation und Interesse an Embedded Systemen
- Grundkentnisse im Umgang mit Linux Umgebungen und dessen Werkzeugen
- Grundkentnisse von IT-Security und Schutzzielen
- Programmierkentnisse in C für die PSE Applikation

Kontakt

Bitte senden Sie Ihre Bewerbung mit aktuellem Lebenslauf und Leistungsnachweis an:

Albert Stark
Fraunhofer Institut für Angewandte und Integrierte Sicherheit (AISEC)
Secure Operating Systems
Lichtenbergstr. 11, 85748 Garching b. München
Mail: albert.stark@aisec.fraunhofer.de
Tel.: +49 89 322 9986-1038

Lukas Auer
Fraunhofer Institut für Angewandte und Integrierte Sicherheit (AISEC)
Secure Operating Systems
Lichtenbergstr. 11, 85748 Garching b. München
Mail: lukas.auer@aisec.fraunhofer.de
Tel.: +49 89 322 9986-198

Referenzen

[1] ZDF. *Tausende Windkraftanlagen weiter gestört — Politiker vermutet Cyber-Attacke*. 2022. URL: https://web.archive.org/web/20220302180917/https://www.zdf.de/nachrichten/politik/windkraftanlagen-gestoert-russland-ukraine-krieg-100.html (besucht am 16. 01. 2024).

[2] M. Xu u. a. *Dominance as a New Trusted Computing Primitive for the Internet of Things*. 2019. DOI: 10.1109/SP.2019.00084. URL: https://publica.fraunhofer.de/handle/publica/405868.

[3] Manuel Huber u. a. "The Lazarus Effect: Healing Compromised Devices in the Internet of Small Things". In: *Proceedings of the 15th ACM Asia Conference on Computer and Communications Security*. ASIA CCS '20. Taipei, Taiwan: Association for Computing Machinery, 2020, S. 6–19. ISBN: 9781450367509. DOI: 10.1145/3320269.3384723. URL: https://doi.org/10.1145/3320269.3384723.

[4] Intel. *Driving Performance, Integration, and Versatility with Intels First Enhanced for IoT Platform*. 2022. URL: https://www.intel.com/content/www/us/en/products/docs/processors/embedded/enhanced-for-iot-platform-brief.html (besucht am 16. 01. 2024).

[5] Intel. *Intel Elkhart Lake PSE*. 2022. URL: https://github.com/intel/pse-fw (besucht am 16. 01. 2024).

[6] Intel. *Intel SEDI Library*. 2022. URL: https://github.com/intel/sedi-drivers/tree/pse (besucht am 16. 01. 2024).

[7] Zephyr Project. *Zephyr Homepage*. 2022. URL: https://www.zephyrproject.org/ (besucht am 16. 01. 2024).

[8] Fraunhofer AISEC. *Lazarus Source Repository*. 2022. URL: https://github.com/Fraunhofer-AISEC/lazarus (besucht am 16. 01. 2024).

Ausschreibungsdatum: 12.03.2024