SD4MSD

Single Device for Multiple Security Domains – Technische Machbarkeitsstudie und Validierung

Programm / Ausschreibung	FORTE, FORTE, FORTE - Kooperative F&E-Projekte 2019	**Status**	abgeschlossen
Projektstart	01.01.2021	**Projektende**	30.06.2023
Zeitraum	2021 - 2023	**Projektlaufzeit**	30 Monate
Keywords	Single Device Lösung, gehärtete Tablets, Sicherheitskonzept, Machbarkeitsstudie, Validierung im Feldeinsatz		

Projektbeschreibung

Militärische Einsätze im Feld stellen hohe Anforderungen an Geräte für Informations- und Kommunikationstechnologie (IKT) hinsichtlich Zuverlässigkeit und Sicherheit. Hierzu gehören zum einen die Robustheit gegenüber Umgebungseinflüssen wie Erschütterungen, Wasser und Feuchtigkeit, sowie zum anderen der Absicherung gegenüber physischen Attacken und Cyber-Angriffen. Kompromittierungsversuche müssen jederzeit feststellbar sein und gegebenenfalls automatisierte Gegenmaßnahmen, wie Alarmierung, (Teil-) Deaktivierungen oder Notlöschung auslösen.
Derzeit erhältliche robuste Endgeräte von namhaften außereuropäischen Herstellern im Tablet-Formfaktor sind zwar am internationalen Markt verfügbar, jedoch unterstützt keines dieser Geräte ein zuverlässiges Monitoring der Geräteintegrität, noch vereint es tatsächlich alle wesentlichen Schutzklassen (International Protection, IP), die für einen militärischen Einsatz erforderlich sind. Im Sinne der Wiederverwertbarkeit muss zudem durch weitere Maßnahmen sichergestellt werden, dass bereits in anderen Einsätzen verwendete und von jeglichen Anwendungsdaten gesäuberte IKT-Geräte genauso zuverlässig und sicher in einer multiplen Sicherheitsumgebung arbeiten wie Neugeräte.
Das Unternehmen MUSE baut mit Partnern im Gegensatz zu anderen Herstellern nicht auf bestehende Produktpaletten auf, sondern entwickelt eine eigenständige cyber-physische Gesamtarchitektur für ein robustes Tablet. Der Prototyp wurde auf Basis von Industriell orientiertem Design und verstärkten Kunststoffen erstellt, der auch gegenüber elektromagnetischen Angriffen resistent ist. Zusätzlich wurden weitere Hard- sowie Software-technische Maßnahmen zur Härtung des Gerätes vorgesehen, etwa Hardware-Sicherheits-Gateways, welche den Datenfluss zwischen den Komponenten regeln, sowie Authentifizierungsmechanismen über Kryptographie und Signaturverfahren mit der auf der Plattform laufenden Software zur Sicherstellung der Integrität.
Das Projekt SD4MSD setzt auf diese bisherigen Teilergebnisse auf und möchte ein integrales Gesamtkonzept auf physischer, Hardware- und Software-technischer Ebene für hochrobuste Endgeräte mit der individuellen Konfigurierbarkeit für spezifische Einsatzzwecke kombinieren. Es soll ein umfassendes Konzept zur Härtung eines mobilen IKT-Geräts entwickelt werden, um einer hinreichenden Breite an physischer, elektromagnetischer und cybersicherheitsorientierter Angriffsvektoren zu widerstehen. Hierbei ist die Sicherstellung von Authentizität, Integrität, Vertraulichkeit über den gesamten Lebenszyklus des IKT-Geräts entscheidend. Eine modulare Systemarchitektur soll multiple Einsatzzwecke bei gleichzeitiger Plattformflexibilität bieten. Dabei müssen Wartungs- und Serviceprozesse, sowie Best-Practices und Normen berücksichtigt

werden. Letztlich soll eine nachvollziehbare Validierung des Gesamtkonzepts anhand eines Demonstrators die praxistaugliche Umsetzung und Reproduzierbarkeit garantieren. Die gewonnenen Erkenntnisse sollen in einer zweiten Iteration in ein verfeinertes Systemkonzept einfließen. Neben der funktionalen Validierung durch den Bedarfsträger, sollen auch Penetrationstests durchgeführt werden, um die Erfüllung der nicht-funktionalen Sicherheitsanforderungen sicherzustellen. Dies beinhaltet insbesondere auch die Betrachtung geschlechtsspezifischer Anforderungen an die Verwendung dieser Geräte (Größe, Haptik etc.) im militärischen Einsatz.

Abstract

Military field operations place high demands on information and communication technology (ICT) devices, both in terms of reliability and security. These requirements include robustness against environmental influences such as vibrations, water and humidity as well as protection against physical attacks and cyber-attacks. Attempts to compromise a device must be detectable at any time and, if necessary, trigger automated countermeasures such as alarms, (partial) deactivation or emergency wiping of all data.
Currently, there are robust end devices from well-known non-European manufacturers in tablet form factor available on the international market. However, none of these devices support reliable monitoring of device integrity, nor do they combine all relevant protection classes (International Protection) required for military use. In the interest of reusability, further measures must also be taken to ensure that devices which have already used in one mission can as be reliably and securely deployed in other security environment as new devices.
In contrast to other manufacturers, the MUSE and its partners do not repurpose existing products but develop an independent cyber-physical architecture for a robust computer tablet. A prototype has been created based on industrial design and reinforced plastics, which is also resistant to electromagnetic attacks. In addition, further hardware and software measures are planned to harden the device, such as hardware security gateways that control the data flow between the components, authentication mechanisms via cryptography and signature procedures with the software running on the platform to ensure integrity.
The SD4MSD project builds on these previous partial results and aims to combine an integral overall concept at physical, hardware and software level for highly robust end user devices with individual configurability for specific (military) purposes. A comprehensive concept for hardening a mobile ICT device is to be developed in order to resist a sufficient range of physical, electromagnetic and cyber security-oriented attack vectors. Ensuring authenticity, integrity, confidentiality throughout the life cycle of the ICT device is crucial. A modular system architecture should offer multiple purposes of use with simultaneous platform flexibility. Maintenance and service processes as well as best practices and standards must be considered. Ultimately, a comprehensible validation of the overall concept using a demonstrator should guarantee practical implementation and reproducibility. In a second iteration, the knowledge gained will be incorporated into a refined system concept. In addition to the functional validation by the user, penetration tests will also be performed to ensure that non-functional security requirements are met. This includes, in particular, the consideration of gender-specific requirements for the use of these devices (size, feel, etc.) in military use.

Projektkoordinator

- AIT Austrian Institute of Technology GmbH

Projektpartner

- Bundesministerium für Landesverteidigung

- MUSE Electronics GmbH