Bundesministerium
Landwirtschaft, Regionen
und Tourismus

2. FORTISSIMO Fachtagung

SD4MSD – Single Device for Multiple Security Domains

Kontakt
Dr. Dr. Florian Skopik
E-Mail: florian.skopik@ait.ac.at
Web: https://www.ait.ac.at/cyber-security/

Projektziel

An die IKT-Ausrüstung zur militärischen Nutzung im Feld werden Hard- und Software-seitig extrem hohe Anforderungen in Bezug auf Robustheit, Zuverlässigkeit und Sicherheit gestellt. Die Endgeräte sollen in kurzen Zeitabständen, Missions-spezifisch in multiplen Sicherheitsdomänen eingesetzt werden können und die SoldatIn muss sich auf ein zuvor in anderen Einsätzen verwendetes IKT-Gerät, seine Funktionsfähigkeit und Integrität zu jeder Zeit verlassen können. 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 mit dem Österreichischen Bundesheer bereits umgesetzte Hardware-Prototyp ist eine Kombination aus eigenständigem, funktionellem Design und Karbonfaser-verstärktem Kunststoff CFK, wurde gegen elektromagnetische Angriffe geschirmt und durch zusätzliche Features sicherheitstechnisch gehärtet. Das Projekt *SD4MSD* setzt auf diesen Ergebnissen auf und entwickelt ein innovatives, umfassendes Sicherheitskonzept zur weiteren hardwaremäßigen, aber v.a. softwaremäßigen Härtung des mobilen Endgeräts, 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. *SD4MSD* erstellt eine modulare Systemarchitektur für multiple Einsatzzwecke und entwickelt Methoden zu einer nachvollziehbaren Validierung des Gesamtkonzepts in Form eines Demonstrators.

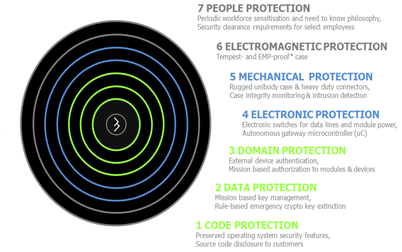
Projektlaufzeit: 01.01.2021 – 31.12.2022

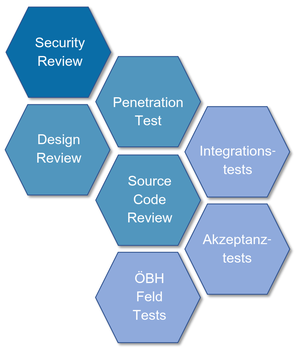
AIT AUSTRIAN INSTITUTE OF TECHNOLOGY

Anforderungen an Single Device Lösungen

Zielsetzungen
- Identifikation von Praxis-Anwendungsfällen
- Formulierung von funktionalen und nicht-funktionalen Anforderungen
- Komplettierung mit Anforderungen aus theoretischen Quellen

Fragestellungen
- Welche konkreten Anforderungen aus der militärischen Praxis bestehen für ein IKT-Endgerät (Hardware) und den darauf befindlichen IKT-Services (Software)?

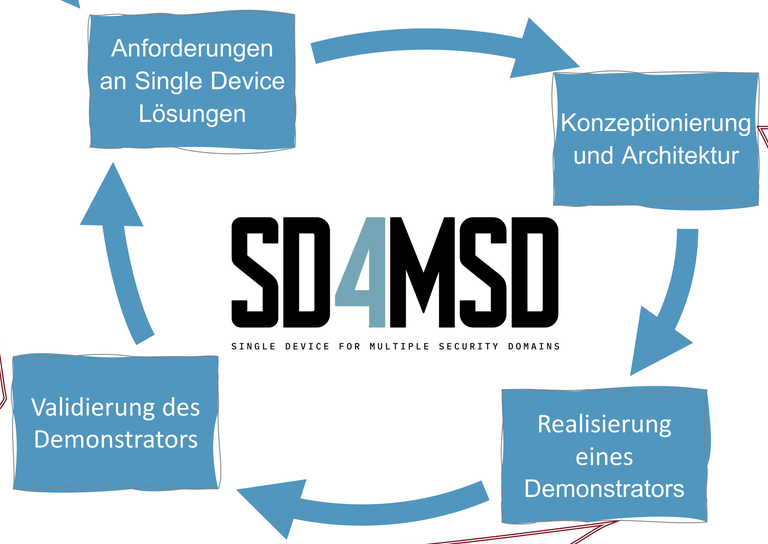




Validierung des Demonstrators

Zielsetzungen
- Exzerpt von Demo-Szenarien für die Demonstrator-Validierung
- Validierung des erstellten Demonstrators gegen die formulierten Anforderungen
- Theoretisches Review des Designs
- Durchführung und Evaluierung von standardisierten und gerichteten Penetrationstest

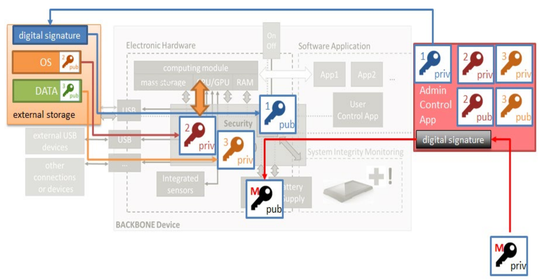
Fragestellungen
- Wie kann umfassend aus verschiedenen Blickwinkeln die Funktionsweise des Demonstrators validiert werden?
- Wie können die integralen Sicherheitsmechanismen explizit getestet und auf ihre Widerstandsfähigkeit hin validiert werden?
- Wie kann die Resilienz des Demonstrators im Zuge eines Penetrationstests validiert werden?
- Wie fließen die hier gewonnenen Erkenntnisse in die Weiterentwicklung wieder ein?

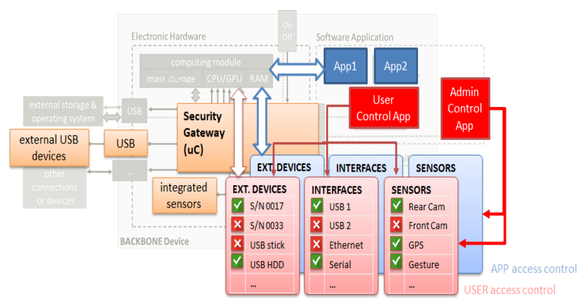


Konzeptionierung und Architektur

Zielsetzungen
- Erarbeitung eines umfassenden High-Level-Gesamtkonzepts nach Security-by-Design-Prinzipien
- Konzeption von relevanten Sicherheitsmechanismen und integraler Einbau in das Gesamtkonzept
- Design der operativen Administrations- und Konfigurationsprozesse

Fragestellungen
- Wie kann ein umfassendes Architektur-Gesamtkonzept gestaltet sein, das sich über mehrere verzahnten Ebenen (Physik, Hardware, Software) erstreckt und Security-by-Design-Prinzipien implementiert?
- Wie sieht ein angemessenes, resilientes kryptographisches Konzept für ein robustes Endgerät aus?
- Welche konkreten Verschlüsselungs- und Authentifizierungsprotokolle kommen in welcher Art und Weise zum Einsatz?
- Wie sind die den gesamten Lebenszyklus unterstützenden operativen Administrations- und Konfigurationsprozesse dazu gestaltet?



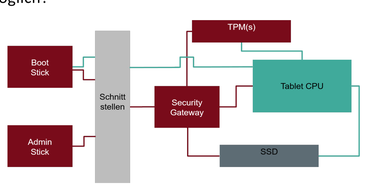


Realisierung eines Demonstrators

Zielsetzungen
- Konzeption und Realisierung eines Demonstrators, der die wesentlichen Kernelemente des Gesamt-Architektur-Konzepts praktisch implementiert

Fragestellungen
- Wie können die wesentlichen Architekturelemente über einen Demonstrator praktisch validiert werden?
- Wie praxisnahe kann der Demonstrator erstellt und wie kann die Gesamtintegration wiederholbar gestaltet werden?
- Wie spielen Physik, Software, Hardware zusammen und welche Flexibilität für Multi-Sicherheits-Umgebungen ist möglich?

Angemessene Ressourcen des Security Gateways	Interaktion Externer Geräte mit dem Security Gateway	Authentizität des Betriebssystems
•Ausführung komplexer parallele Prozesse •Delegation von Verschlüsselungsoperationen	•Lesen/Schreiben •Authentifizierte Medien	•Authentizität des gebooteten Betriebssystems •TPM Modul mit Bindung an mehrere OS



FFG Forschung wirkt.

FORTE

Bundesministerium
Landesverteidigung