SENSIBLE-KI

SENSIBLE-KI

Sichere und vertrauenswürdige mobile KI

Motivation Methoden der Künstlichen Intelligenz (KI) kommen bereits in einer Vielzahl stetig wachsender heterogener mobiler und eingebetteter Plattformen zum Einsatz. Aufgrund ihrer Heterogenität ist es schwierig, solche Plattformen gegen Cyberangriffe zu schützen und die Manipulation der Machine Learing / Deep Learning-Modelle zu verhindern. Insbesondere gibt es keine einheitlichen Herangehensweisen zur Absicherung der KI-Systeme im mobilen und eingebetteten Kontext, was zu Sicherheitslücken führt.

Ziel Ziel des Projektes ist es, KI-gestützte Systeme sicher und einfach nutzbar in mobile und eingebettete Endgeräte (z. B. Smartphone, IoT Überwachungskamera, Edge Server) implemen-tierbar zu integrieren. In dem Projekt sollen Konzepte, Methoden und Demonstratoren entwickelt werden, die Angriffe auf KI-Systeme durch den Einsatz von bewährten Mechanismen des Trusted Computings deutlich erschwert bzw. verhindert werden.

Angestrebte Ergebnisse Bestehende und am Markt präsente mobile und eingebettete KI-Systeme, sowie State-of-the-Art Trusted Computing und softwarebasierte Sicherheitsmechanismen werden geprüft und klassifiziert. Auf Grundlage des Schutzbedarfs werden den funktionalen Anwendungsklassen passende Mechanismen des Trusted Computings und der softwarebasierten Sicherheitsmethoden zugeordnet und Referenzarchitekturen konzeptioniert. Die Referenzarchitekturen werden zur Implementierung von konkreten Prototypen genutzt und die gesammelten Erfahrungen und Erkenntnisse werden zusätzlich in Best-Practice Dokumenten und öffentlich verfügbaren Code-Bibliotheken gesammelt und geteilt.

Erwarteter Impact Neben dem Expertenwissen aus der Cybersicherheitsforschung und der Industrie setzt das Projekt auch auf eine breite Entwicklergemeinschaft aus verschiedenen Branchen und Domänen. So wird sichergestellt, dass die entwickelten Ansätze und Methoden auch den Schutz bieten, der in der Praxis benötigt werden. Generell wird das Projekt zur Erhöhung der Sicherheit und des Datenschutzes für die Nutzerinnen und Nutzer beitragen sowie Unterstützung für Entwicklerinnen und Entwickler bieten.

Tags KI, Sicherheit, Trusted Computing, Smart Living, Digitaler Identitäten und biometrischer Zugangssysteme

Ansprechpartner
Fraunhofer AISEC
Kinga Wróblewska-Augustin
kinga.wroblewska-augustin@aisec.fraunhofer.de

3 JAHRE LAUFZEIT

März 2021 – Februar 2024

4 PARTNER

Fraunhofer-Institut für Angewandte und Integrierte Sicherheit AISEC; Hochschule Darmstadt h_da; Bundesdruckerei GmbH; neXenio GmbH

1,5 MILLIONEN € FÖRDERUNG

Die Gesamtkosten des Projekts betragen 2,2 Millionen Euro, wovon 1,5 Millionen Euro gefördert werden.

Gefördert durch:
Bundesministerium für Wirtschaft und Energie
aufgrund eines Beschlusses des Deutschen Bundestages