h_da
HOCHSCHULE DARMSTADT
UNIVERSITY OF APPLIED SCIENCES
fbi
FACHBEREICH INFORMATIK

ATHENE
National Research Center
for Applied Cybersecurity

– Bachelorarbeit –

Trusted Computing für KI-Systeme auf der Android Plattform

da/sec

da/sec ist die Forschungsgruppe für Biometrie und Internetsicherheit und ist der Hochschule Darmstadt und dem Nationalen Forschungszentrum für angewandte Cybersicherheit (ATHENE) angegliedert. Die Gruppe wird von Prof. Dr. Christoph Busch geleitet. Der Fokus der Gruppe liegt auf hochinnovativer und angewandter IT-Sicherheitsforschung in den Spezialgebieten der Biometrie. Lesen Sie mehr auf www.dasec.h-da.de .

Motivation & Ziel

Methoden der Künstlichen Intelligenz (KI) kommen bereits in einer Vielzahl mobiler Anwendungen auf der Android Plattform zum Einsatz. Aufgrund ihrer Heterogenität ist es schwierig, diese Methoden gegen Cyberangriffe zu schützen und deren Manipulation zu verhindern.
Ziel ist es zu untersuchen, ob die von der Android-Plattform unterstützten Mechanismen für Trusted Computing dafür geeignet sind, um KI-Systeme sicher und einfach nutzbar zu schützen.

Aufgaben

- Erstellen einer Übersicht aktueller Trusted Computing Mechanismen unter Android
- Implementierung von Beispielanwendungen aus dem Bereich der KI unter Verwendung von Trusted Computing
- Messung der Inferenz und Evaluierung der Limitierungen des Ansatzes

Wir bieten

- Abschlussarbeit an einem aktuell relevantem Thema in Zusammenarbeit mit verschiedenen Forschungseinrichtungen

Vorraussetzungen

- Hohe Motivation
- Vorwissen im Bereich der Android Entwicklung, Trusted Computing und / oder KI wünschenswert

Start

Ab sofort / nach Vereinbarung

Kontakt

Jannis Priesnitz
jannis.priesnitz@h-da.de

h_da
Faculty of
Computer Science

ATHENE–National Research Center for Applied Cybersecurity
da/sec – biometrics and internet security research group
Schöfferstraße 8b
64295 Darmstadt