Wir sind ein ehrgeiziges Team kreativer Köpfe aus dem Bereich IT-Sicherheit, die ihr Interesse am Thema zum Beruf gemacht haben. Wir unterstützen unsere Kunden, vom innovativen Startup bis zum DAX Konzern, die vielfältigen Herausforderungen der IT-Sicherheit zu meistern.

Werde Teil unseres Teams! Wir suchen dich (m/w/d) ab sofort für eine

Master- oder Bachelor-Thesis im Bereich Embedded IT-Security

„Extraktion von neuronalen Netzen über GPU Seitenkanäle“

als Kooperation mit der Universität Ulm Institut für Verteilte Systeme
Institute of Distributed Systems

Deine Aufgabe:

- Du wolltest schon immer mal herausfinden wie du ein neuronales Netz extrahierst?
- Du hast bereits dein eigenes Modell mit Maschine Learning trainiert und dich gefragt wie man es angreifen kann?
- Du entwickelst Strategien zur Extraktion von neuronalen Netzen mit Seitenkanälen.
- Dabei untersuchst du, welche Seitenkanalangriffe möglich sind und verifizierst diese an einem echten Modell.
- Durch deine Arbeit sollen Gefahren für die Extraktion von neuronalen Netzen aufgezeigt werden, die als Grundlage für weitere Angriffe verwendet werden können.

Wir bieten dir:

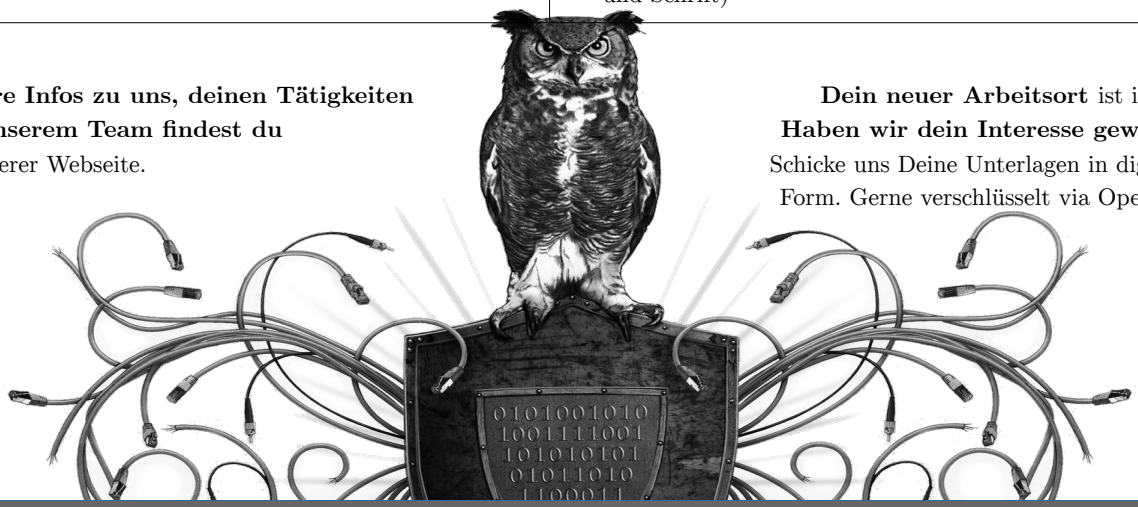
- Eine Testplattform für neuronale Netze
- Eine Einführung in die wissenschaftliche Arbeit mit neuronalen Netzen
- Hands on Mentoring ‚neuronale Netze‘ durch das Institut für Verteilte Systeme der Universität Ulm
- Einen modernen Arbeitsplatz und Ausstattung (Laptop unter Linux)
- Weiteres fachliches und methodisches Mentoring
- Ein gemütliches Studi-Büro für den Austausch mit Gleichgesinnten
- Beginn der Arbeit: Am besten ab sofort, ggf. auch zunächst als Werkstudent (m/w/d)
- Dauer: Mind. 6 Monate
- Wochenarbeitszeit: 40 Stunden (Thesis)

Dein Profil:

Du interessierst dich für neuronale Netze und IT-Sicherheit, verfolgst die neuesten Entwicklungen, kennst dich schon etwas mit deep learning von CNN und DNN aus und hackst gern LLMs in Deiner Freizeit. Gepaart mit elementaren Grundwerten wie Zuverlässigkeit und Ehrlichkeit passen wir schon gut zusammen. Weiterhin bringst du mit:

- Erste Erfahrung mit neuronalen Netzen
- Grundlagen IT Sicherheit und statistischer Analysemethoden
- Begeisterung für neuronale Netze bzw. KI und IT Sicherheit
- Laufendes Studium an der Universität Ulm, idealerweise in einem der Bereiche IT Security, Informatik, Mathematik oder verwandte Fächer
- Analytisches Denken, Leistungsbereitschaft und die Fähigkeit sich schnell und eigenständig in neue Themen einzuarbeiten
- Gute Sprachkenntnisse in Deutsch und Englisch (Wort und Schrift)

Weitere Infos zu uns, deinen Tätigkeiten und unserem Team findest du auf unserer Webseite.



Dein neuer Arbeitsort ist in Ulm.
Haben wir dein Interesse geweckt?
Schicke uns Deine Unterlagen in digitaler Form. Gerne verschlüsselt via OpenPGP.

SCHUTZWERK

Deine Ansprechpartner:
Lea Miller: lmiller@schutzwerk.com, https://www.schutzwerk.com
Dennis Eisermann: dennis.eisermann@uni-ulm.de, https://www.uni-ulm.de/in/vs