PhD Student/ Research Assistant (f/m/d) in the field of Security and Robustness of Machine Learning

Job description: The "Intelligent System Security" research group works on the application of machine learning in the area of computer security. We develop learning-based methods for attack detection on different levels or the discovery of vulnerabilities in software and embedded devices. Another central and very important subject of our research is the robustness and security of machine learning methods themselves. Here, we are particularly looking for reinforcement.

Possible research topics include, but are not limited to:
- Secure and robust learning methods
- Attacks against learning-based systems
- Robust learning on limited hardware (e.g., embedded systems, IoT)
- Explainability of machine learning in computer security

Qualification: You have a Diploma or Master's degree in computer science or any related field. You also require very good knowledge in machine learning and ideally computer security. Above all, however, you need to show enthusiasm for conducting research on cutting-edge topics in machine learning and computer security.

We offer: We offer an attractive and modern workplace with access to excellent facilities of KIT, diverse and responsible tasks, a wide scope of advanced training options, supplementary pension with the VBL (Pension Authority for Employees in the Public Service Sector), flexible working time models, and a cafeteria/canteen. Moreover, the research group has strong connections to and maintains active collaborations with national and international research facilities.

Salary: The remuneration occurs on the basis of the wage agreement of the civil service in TV-L group 13.

Institute: Institute of Theoretic Computer Sciences (ITI)
Research group "Intelligent System Security"

Contract duration: 18 months
While the position is limited at first, extending the contract to the entire duration of the PhD is possible and intended.

Starting date: As soon as possible

Application up to: January 17th 2021

Contact person in line-management: Feel free to contact Jun.-Prof. Christian Wressnegger (c.wressnegger@kit.edu) for technical details.
Application:

Please send your application including a cover letter, your CV, and all certificates/references in electronic form to: applications+phd@intellisec.de. Make sure to point out why you are a good fit for us and research in the field of security of machine learning.

We prefer to balance the number of female and male employees. Therefore, we kindly encourage female applicants to apply for this job.

Recognized severely disabled persons will be preferred if they are equally qualified.

KIT is certified as a family-friendly university (familienfreundliche Hochschule) and offers part-time employment, leaves for family-related reasons, dual career options, and individual coaching for family-work balance.