CYSEC Cybersecurity TU Darmstadt | System Security Lab | TECHNISCHE UNIVERSITÄT DARMSTADT

HiWi Position – Machine Learning for Detection of Runtime Attacks

Background

Embedded systems security is becoming increasingly crucial now in the wake of rising cyber security attacks. Detecting different classes of runtime attacks with minimum latency is critical towards building and maintaining a secure and trustworthy system in today's world. The purpose of this work is to infer from the execution of a processor of a given application code *at runtime* whether execution is benign or compromised. This requires collecting a representative dataset of normal execution traces and training an LSTM architecture on them. We aim to craft multiple exploits and test our architecture against them. At our System Security Lab, we aim to investigate and evaluate the effectiveness of such an approach for low-end embedded devices.

Requirements

- Background and interest in machine and deep learning, particularly LSTMs
- Familiar with programming in Python
- Familiar with TensorFlow and Keras
- Familiar/willing to learn on RISC-based and x86 processor architectures and cross-compilation and emulation tools
- A problem-solver!

Contact

If you want to become part of this interesting project and participate in state-of-the-art research, please send your application (CV, certificate(s) and any supporting documents) via email to:

Ghada Dessouky
ghada.dessouky@trust.tu-darmstadt.de

Position

- Available immediately
- Duration: For as long as you do a good job!

AK Professor Dr.-Ing. Ahmad-Reza Sadeghi
Gebäude S4|14 (CASED Gebäude)
Mornewegstraße 30
64293 Darmstadt
https://www.trust.informatik.tu-darmstadt.de

August 2018