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

Bachelor Thesis/HiWi Task

"Do you *really* trust your computer…and who else does?" – Evaluation of Remote Attestation Protocols in Trusted Computing

Background

Remote attestation is an important security mechanism designed to detect software attacks, typically realized as a challenge-response protocol. It allows a trusted *verifier* to capture the state of a piece of software, before execution, of a (potentially untrusted or malware-infected) remote device - a *prover*. Static attestation only provides assurance of the integrity of the piece of software (the binaries) but does not verify its execution. More recently, several attestation schemes are proposed to also capture the dynamic state of a remote device to enable detection of a wide range of runtime attacks. However, all schemes in literature mainly focus on the different mechanisms at the prover's side. In their attempts to reduce the workload on the prover (often a low-end embedded device), many assumptions are made with regards to the capabilities of the verifier. In this thesis/HiWi, we aim to investigate and evaluate the verifier's end of these schemes to evaluate remote attestation protocols comprehensively.

Tasks

Analyzing the state-of-art remote attestation schemes in order to validate their assumptions.

Implementation of the different verifier models for different schemes.

Evaluation and comparison of the different verifier models.

Position

- Available immediately
- Duration: 6-months, extendable

Requirements

- C, C++ Programming required
- Experience with code static and dynamic analysis
- Familiar with cryptographic libraries

Contact

Please send your application (incl. CV and certificate(s)) via email to:
Shaza Zeitouni
Shaza.zeitouni@trust.tu-darmstadt.de
Ghada Dessouky
Ghada.dessouky@trust.tu-darmstadt.de

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

February 2017