Bachelor Thesis/HiWi – Security Evaluation of Attestation Architectures

Background
Different security mechanisms are being continuously developed to provide different security guarantees for software against different adversarial capabilities. These are often deployed in tandem with trusted execution environments which provide isolated execution for security-critical software, such as Intel SGX. One such security mechanism is remote attestation where the integrity of the code being executed is verified by a trusted party. A more advanced mechanism, developed at the Systems Security Lab, is run-time attestation where the integrity of the execution of the code is verified at runtime. We have also developed several follow-up hardware-based runtime attestation extensions for monitoring and enforcing correct execution of software at run-time. This is because relying on hardware as a root of trust can provide increased security guarantees and reduced performance overheads as opposed to software-only defenses.

Task
The task required is to implement and evaluate these different schemes in software using a trusted execution environment such as Intel SGX or ARM TrustZone. Afterwards, the security guarantees of these schemes in mitigating different attacks will be assessed and their performance overheads evaluated.

Requirements
- Background and experience in low-level programming in C and C++
- Some background or familiarity with security/cryptography
- Familiar with processor architecture and digital design
- Willingness to learn new tools quickly and ability to do independent problem solving

Contact
If you are interested, please send your application (CV, certificate(s), etc.) via email (with subject: Application for HiWi – Security Evaluation of Attestation Architectures) to:
ghada.dessouky@trust.tu-darmstadt.de