17 June 2019 Study · Transparency · Mobile Security

Remote Attestation State-of-the-Art

The full text is currently only available in the Deutsch version. A translation will follow.

Archived. This content is no longer updated. It remains available for reference.

Version 2019-06-17
Source https://technology2.a-sit.at/en/publications/remote-attestation-state-of-the-art/

Remote attestation and trusted computing are becoming increasingly important – especially in the mobile sector and in the DRM context. However, the implementations of the underlying concepts differ significantly between mobile and desktop computing. This project assessed the current state of remote attestation techniques in the desktop and mobile domain, focusing on practicality in the context of open systems without explicit enrolment procedures. This project provides an overview of basic trusted computing concepts, introduces Intel's Software Guard Extensions (SGX) as an example of trusted computing on the desktop, and describes relevant concepts in the mobile sector. In addition, a trusted computing model for current Android devices is introduced, which will presented in July this year as part of the 16th International Conference on Security and Cryptography.