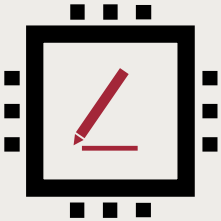
Institut für Verteilte Systeme
Institute of Distributed Systems

ulm university universität ulm

Entwicklung einer Softwarekomponente für einzigartige Signaturen mit Intel SGX



Bachelor-arbeit 12 LP

Projekt 8/16 LP

Replizierte Systeme basieren oft auf Einigungsalgorithmen. Im Falle von beliebigen (byzantinischen Fehlern) werden N = 3f+1 Replikate benötigt bei f zu tolerierenden Fehlern. Mit Hilfe von vertrauenswürdigen Komponenten kann dies auf N = 2f+1 reduziert werden. Ein so genannter USIG ist so eine Komponente. Sie signiert eine Nachricht und zählt dabei eine von außen unveränderliche Sequenznummer hoch.

Aufgabe der Arbeit ist es, ein Konzept und eine Implementierung mit Hilfe von Intel SGX zu entwickeln, die aus einer Java-Anwendung heraus genutzt werden kann. Herausforderungen ist neben der Implementierung die geeignete Initialisierung der Komponente.

Geeignet für Studierende mit Erfahrung in Java, C oder C++, mit Basiskenntnissen über digitale Signaturen und für alle, die lernen wollen, wie SGX funktioniert.
This project can also be completed in English. Please contact me for further details.

Prof. Franz J. Hauck | franz.hauck@uni-ulm.de | O27-349

Bei Interesse und für weitere Details kontaktieren Sie mich oder kommen einfach unverbindlich vorbei.