Zusammenfassung: Sicherheitsanalyse der Intel® Software Guard Extensions sowie deren Integration in das Linux Unified Key Setup zum Schutz vor Cold-Boot-Angriffen

Die Intel® Software Guard Extensions - kurz SGX - sind Intels neuste Entwicklung im Bereich Trusted Computing. Sie erlauben es Programmcode in sogenannten Enklaven auszuführen, welche diesen vor anderen Programmen, sowie sogar dem Betriebssystem selbst, schützen. SGX versprechen sogar Widerstand gegen aufwändige Hardware-Angriffe, was sie zu einem zukunftsträchtigen Werkzeug für sicheres Cloud-Computing macht. Mittels SGX besteht des Weiteren die Möglichkeit einer sogenannten Remote-Attestation. Diese Funktionalität erlaubt es dem SGX nutzenden System, gegenüber einem externen Dritten, glaubhaft zu versichern, dass es das auszuführende Programm korrekt geladen und frei von unautorisiertem Code ausführt. Diese Eigenschaft ist insbesondere für Cloud-Computing bzw. Digital-Rights-Management sinnvoll, da sie dem Nutzer erlaubt, zuerst ein sicherheitstechnisch unbedenkliches Programm laden zu lassen, welches dann seinen eigenen Zustand mittels SGX einem externen Server versichert, so dass dieser danach kritisches Schlüsselmaterial nachladen kann, ohne das Risiko eines Auslesens durch modifizierten Programmcode. Im Rahmen dieses Projektes soll festgestellt werden, ob die Software Guard Extensions die von Intel versprochenen Sicherheitseigenschaften tatsächlich erfüllen, so dass diese in sicherheitskritischen Anwendungen angewendet werden können. Drüber hinaus soll das Anwendungsspektrum von SGX erweitert werden und insbesondere im Kontext des Linux Unified Key Setups zum Schutz der Verschlüsslungsoperation sowie der Berechnung von Schlüsseln nutzbar gemacht werden.

Abstract: Security Analysis of Intel® Software Guard Extensions and Protection of the Linux Unified key Setup against Cold-Boot-Attacks

The Intel® Software Guard Extensions (short SGX) are Intel's latest development in the area of trusted computing. SGX allows program code to be executed in so-called enclaves that ensure that the code is protected from other programs as well as the operating system itself. SGX promise resistance even against resource intensive hardware attacks, which makes them particularly attractive in the context of secure cloud computing. SGX also allows for remote attestation. This functionality allows the system using SGX to convincingly assure external third parties that it correctly loaded a program and executes it without any unauthorized code. This functionality is particularly useful in the context of cloud computing and digital rights management, as it enables a user to first load an uncritical program and then use SGX to assure an external server that it is save to load critical keying material, i.e. that there is no risk that modified program code will get access to it. In the context of this project we will explore if SGX indeed meets the promises made by Intel. Moreover, we plan to extend the scope of application of SGX to the Linux Unified Key Setup in order to protect encryption operations as well as the computation of keying material.