A Security Architecture for Microprocessors (*SAM*)

Jörg Platte

15. November 2008

SAM ist eine Sicherheitsarchitektur, die aus einer Prozessorerweiterung und einem entsprechend angepassten Betriebssystem besteht. Die Prozessorerweiterung besteht primär aus einer für den Programmierer transparenten Sicherheitsschicht, die automatisch die Integrität aller geladenen Daten prüft und sämtliche Daten, die den Prozessor verlassen, verschlüsseln kann. Damit ist es selbst bei einem direkten Zugriff auf den Hauptspeicher nicht möglich, ungeschützte Daten zu lesen oder zu manipulieren. Entschlüsselte Daten sind dabei nur innerhalb des Prozessors verfügbar und werden dort durch die Architektur vor unerlaubtem Zugriff geschützt. Dieser Schutz schließt auch Schutz vor privilegierten Benutzern wie Administratoren mit erweiterten Rechten ein. Weiterhin stellt *SAM* sicher, dass ein Programm nur auf bestimmten Prozessoren entschlüsselt werden kann und somit nur auf diesen ausführbar ist.

Die Integritätssicherung wird über kryptographische Hashes erreicht. Diese ermöglichen eine Überprüfung der Daten und dienen damit der Erkennung von Manipulationen. Jede vom Prozessor erkannte Manipulation führt zu einem sofortigen Programmabbruch. Somit ist sichergestellt, dass nur unmodifizierte Programme ausgeführt werden können und Manipulationen die Datensicherheit beeinträchtigen können.

Der Prozessor muss verschlüsselte, gesicherte und ungesicherte (und damit auch unverschlüsselte) Speicherbereiche unterscheiden können. Bei *SAM* wird der Speicher dazu in einen gesicherten, einen verschlüsselten und einen ungesicherten Bereich aufgeteilt. Instruktionen, die in einem gesicherten Bereich liegen, können auf auf den gesamten Speicher zugreifen und verschlüsselte Daten werden transparent entschlüsselt. Ungesicherte Instruktionen können ebenfalls auf den gesamten Speicher zugreifen, allerdings bleiben verschlüsselte Bereiche verschlüsselt und können somit nicht analysiert werden.

Das Betriebssystem basiert auf einem für *SAM* geringfügig angepassten Linux-Kernel. Die Änderungen sind bestehen hauptsächlich aus der Anpassung hardwarenaher Funktionen des Prozessmanagements und des Multitaskings an die Sicherheitsfunktionen des Prozessors.

Die Prozessorerweiterung ist als optionale Erweiterung entwickelt worden, damit normale und ungesicherte Programme parallel zu verschlüsselten Programmen ausgeführt werden können. Damit können die mit *SAM* gesicherten Prozessoren ebenfalls für nicht sicherheitskritische Aufgaben verwendet werden um deren Auslastung zu erhöhen. Die Umwandlung bestehender Programme in für *SAM* gesicherte Programme ist einfach, und erfordert nur minimale Änderungen am Programmcode.