Verlässliche Ausführung von WebAssembly durch Encoded Execution

Clemens Tiedt
clemens.tiedt@hpi.uni-potsdam.de
Operating Systems and Middleware Group, Hasso Plattner Institute, University of Potsdam
Germany

Robert Schmid
robert.schmid@hpi.uni-potsdam.de
Operating Systems and Middleware Group, Hasso Plattner Institute, University of Potsdam
Germany

Andreas Polze
andreas.polze@hpi.uni-potsdam.de
Operating Systems and Middleware Group, Hasso Plattner Institute, University of Potsdam
Germany

ABSTRACT

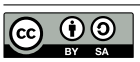
Für sicherheitskritische Systeme herrschen oft besonders strenge Verlässlichkeitsanforderungen. Für *Commercial-of-the-Shelf*-Hardware (COTS) garantieren Hersteller häufig nicht, dass sie diesen Anforderungen gerecht wird. Deshalb kommt in sicherheitskritischen Systemen spezialisierte Hardware zum Einsatz, die teurer und weniger leistungsfähig als COTS-Hardware ist.

Encoded Execution ist ein etablierter Ansatz, um eine höhere Verlässlichkeit gegen Hardwarefehler auf COTS-Hardware zu erreichen. Dabei wird ein Kodierungsverfahren festgelegt und alle Operationen arbeiten auf kodierten Operanden. Um ein Ergebnis zu prüfen, wird es dekodiert. Ist die Dekodierung fehlerfrei möglich, ist wahrscheinlich kein Hardwarefehler während der vorhergehenden Berechnungen aufgetreten. Die Wahrscheinlichkeit, einen Fehler zu erkennen, hängt von der verwendeten Kodierung ab.

Weiterhin werden sicherheitskritische Systeme häufig als Kombination von Software und Hardware zugelassen. Wenn die Hardwareplattform für ein bestehendes System geändert werden soll, erfordert dies also eine kostspielige Neuzulassung. Ein Lösungsansatz, um die Software von einer konkreten Hardwareplattform zu lösen, sind *Compile-Once-Run-Everywhere*-Formate. Damit wird ein Softwaresystem einmal für dieses Format kompiliert und kann dann mit gleichem Verhalten auf verschiedenen Hardwareplattformen ausgeführt werden, die das Format unterstützen.

Ein solches Format ist WebAssembly. Es wurde ursprünglich für die Verwendung im Browser konzipiert, wird aber inzwischen auch darüber hinaus eingesetzt. Da unter anderem C, C++ und Rust WebAssembly als Kompilierziel unterstützen, ist es auch für die Systemprogrammierung nutzbar.

Um WebAssembly verlässlich auf COTS-Hardware ausführen zu können, haben wir Encoded Execution in einem WebAssembly-Interpreter implementiert. Andere Implementierungen von Encoded Execution arbeiten mit einem modifizierten Compiler. Da unsere Lösung in der Laufzeitumgebung funktioniert, werden darin auch Programme, die mit einem Standard-Compiler kompiliert wurden, durch Encoded Execution geschützt.



 DOI: https://dx.doi.org/10.1145.nnnnn. GI/ITG FG Operating Systems, September 2023, Bamberg, DE.