AWARE

Hardware-ensured Software Security

Programm / Ausschreibung	Bridge, Brückenschlagprogramm, Ausschreibungen Bridge 1 (GB 2021)	**Status**	abgeschlossen
Projektstart	01.05.2022	**Projektende**	30.04.2025
Zeitraum	2022 - 2025	**Projektlaufzeit**	36 Monate
Keywords	hardware security, verification, fault attacks, timing attacks, memory safety		

Projektbeschreibung

Die Digitalisierung hat einen großen Einfluss auf unsere Gesellschaft. Ein bedeutender Treiber dieser digitalen Transformation sind eingebettete Prozessoren und die dazugehörige Software, welche in diesen eingebetteten Systemen eingebaut sind. Diese Komponenten ermöglichen eine Vielzahl von Anwendungen, zum Beispiel im Bereich der Internet der Dinge und dem vollautonomen Fahren. Da diese eingebetteten Systeme einen großen Einfluss auf die Sicherheit und Privatsphäre haben, sind sie ein lukratives Ziel für Cyberangreifer.

Diese Geräte können aus der Ferne über das Internet oder lokal durch die Ausnutzung von physikalischen Effekten angegriffen werden. Bisherige Gegenmaßnahmen haben die Angriffsvektoren unabhängig voneinander betrachtet und haben dadurch oft Schwachstellen. Zudem werden die meisten Gegenmaßnahmen nicht auf ihre Korrektheit verifiziert und können deshalb unentdeckte Einfallstore haben.

Das Projekt AWARE zielt darauf ab, die Sicherheit von eingebetteten Systemen durch Forschung an neuen hardwarebasierten Gegenmaßnahmen und Verifikationstechniken zu verbessern. Um die sichere Softwareausführung von softwarebasierten und physikalischen Angreifern zu ermöglichen, verfolgt AWARE zwei Ziele:

Erstens werden Schutzmaßnahmen gegen Angriffe über das Netzwerk erforscht. Da Speicher-Schwachstellen besonders kritisch sind, fokussieren wir uns die Erforschung von entsprechenden Gegenmaßnahmen. Hier berücksichtigen wir besonders die Anforderungen von Ressourcen von limitierten Geräten und erforschen hardwarebasierte Ansätze. Um die Korrektheit der eingeführten Gegenmaßnahmen zu gewährleisten, formalisieren und verifizieren wir die Schutzmaßnahmen.

Zweitens werden wir, durch die Erforschung von maßgeschneiderten Gegenmaßnahmen, eingebettete Systeme gegen physikalische Angreifer schützen. Wir fokussieren uns auf verschiedene architekturelle Bausteine um sie gegen Fehlerangriffe abzusichern. Das Ziel ist es, dass diese Bausteine von der Software genutzt werden können, um starke Sicherheitsgarantien liefern zu können trotz eines physikalischen Angriffs. Zudem werden wir formale Verifikationstechniken erforschen, welche die Sicherheit dieser Gegenmaßnahmen garantieren. Um gegen einen physikalischen Angreifer zu

schützen, der zeitbasierte oder mikroarchitekturelle Seitenkanalangriffe ausnützt, erforschen wir hardwarebasierte Analyse und Verifikationstechniken, die diese Lecks schließen.

Zwischen den einzelnen Zielen beabsichtigen wir eine enge Interaktion um neue Schutzmechanismen und Verifizierungstechniken für eingebettete Systeme zu erforschen. Das Resultat des Projektes sind neuartige Konzepte, Methoden und erste Entwürfe von Prototypen für Schutzmaßnahmen und für Verifizierungstechniken. Um die Anforderungen der eingeschränkten Ressourcen von eingebetteten Systemen zu berücksichtigen, ist es unser Ziel die Laufzeit der ausgeführten Software durch die Schutzmaßnahmen um nicht mehr als 10% zu erhöhen.

Abstract

The ongoing digital transformation is reshaping our society. A central driver of this transformation is the integration of embedded processors and corresponding software into essentially every product and device. This enables a wide range of applications from the Internet of Things to autonomous driving. However, as embedded systems are processing safety- and privacy-critical data, they are also a prominent target for cyberattacks, and dedicated security protection mechanisms are required.

Devices can for example be attacked remotely via an Internet connection or locally by exploiting physical properties of the device. So far, countermeasures against these different attacks have typically been researched independently, which does not allow to explore synergies between countermeasures and which often only leads to incomplete protection. Moreover, typically no rigorous verification of countermeasures is done, which leaves specification or implementation errors of the security mechanisms undetected.

AWARE aims to improve the security of embedded devices by researching novel hardware-rooted countermeasures and corresponding verification techniques that ensure secure software execution in the presence of software attacks and physical attacks. The concrete objectives are as follows:

First, we research protection mechanisms for embedded devices against remote software adversaries. Due to the severity of memory vulnerabilities, we focus on researching novel memory safety and isolation defenses. We research protection mechanisms that respect the constrained resources of embedded systems through lightweight designs using hardware assistance. To ensure the correctness of the introduced security mechanisms, we formalize the developed countermeasures in order to verify their correctness and effectiveness.

Second, we protect embedded devices against physical adversaries by researching corresponding countermeasures. Here, we focus on providing secure architectural building blocks hardened against fault attacks, which can be utilized by the software to establish strong protection guarantees in the presence of a fault and software attacker. By researching formal verification techniques, we ensure the correctness of the introduced countermeasures. To thwart a physical adversary exploiting timing and micro-architectural side-channels, we research hardware analysis and verification methods to find, prevent, and eliminate such leakage.

There is a tight interaction between the objectives and in AWARE we jointly design, analyze, and verify systems and their countermeasures to mitigate software and physical attacks. The outcome of the project will be novel concepts and methods,

as well as proof-of-concept implementations of countermeasures and of tools for verification. To consider the resource constraints of embedded devices, we aim for an overhead for the protection mechanisms of less than 10%.

Projektkoordinator

- Technische Universität Graz

Projektpartner

- NXP Semiconductors Austria GmbH & Co KG