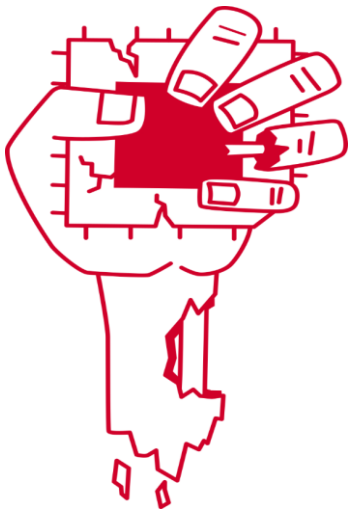
SUCCESS STORY

DeSSnet
Dependable, secure and time-ware sensor networks

Programm: COMET – Competence Centers for Excellent Technologies

Förderlinie: COMET-Projekt

DeSSnet, Key Enabling Technologies for Security, 06/2017-05/2021, strateg./ multi-/single-firm



Copyright: Natascha Eibl

ZOMBILOAD: DIE NEUE CPU SCHWACHSTELLE

Im Beginn des Jahres 2018 stellte die Veröffentlichung der Sicherheitslücken “Meltdown” und “Spectre” die gesamte IT Industrie auf den Kopf. Angreifer können beliebigen Speicher und somit sensitive Information wie Passwörter und vertrauliche Dokumente von Geräten ausspionieren. Allein die Art und Weise wie modernen Prozessoren in Hardware gebaut werden, erlaubte es Angreifern diese Angriffe durchzuführen. Da diese Prozessoren überall verbaut werden, wurde diese Art von Angriffen eine wichtige Fragestellung für das Projekt DeSSnet um festzustellen, in welchen Szenarien und mit welchen Auswirkungen diese ein Problem darstellen.

Im Jänner 2018 veröffentlichten ein vierköpfiges Team an Wissenschaftlern der Technischen Universität Graz in internationaler Kooperation die Sicherheitslücken “Meltdown” und “Spectre”. Die zwei Entdecker Moritz Lipp und Stefan Mangard, die im Projekt DeSSnet involviert sind, zeigten, dass diese Sicherheitslücken es unprivilegierten Angreifern ermöglicht sensitive Informationen von einem Computer, einem Mobiltelefon oder einem Server auszuspionieren ohne dass ein Fehler in der ausgeführten Software vorliegt. Einzig allein die Art und Weise wie moderne Prozessoren gebaut werden, ermöglichen es den Angreifern die Prozessoren so zu manipulieren, dass diese sensiblen Daten wie Passwörter oder vertrauliche Dokumente Preisgeben. Die Sicherheitslücken sorgten für internationales Aufsehen, da sie verschiedenste Prozessoren von verschiedenen Herstellern betrafen und diese in allen Geräten, die wir heutzutage benutzen, verbaut werden. Somit stellte sich selbstverständlich auch die Frage für das Projekt DeSSnet, ob diese Sicherheitslücken auch Probleme in den projektbezogenen Szenarien darstellen und welche Auswirkungen diese haben. In weiterer Forschungsarbeit wurden die Angriffe und Gegenmaßnahmen systematisch aufgearbeitet und dabei neue Schwachstellen in den Prozessoren entdeckt, die weltweit medial für Aufsehen sorgten.

Bundesministerium Verkehr, Innovation und Technologie

Bundesministerium Digitalisierung und Wirtschaftsstandort

Version 01/2019

SUCCESS STORY

Kurz und gut - Meltdown and Spectre: In den letzten Jahrzehnten wurden Prozessoren vorwiegend in ihrer Performance optimiert, da immer schneller werdende Prozessoren von der Industrie und Privatkunden gefordert wurden. Diese Optimierungen bringen meist unerwünschte Nebeneffekte mit sich, die ein Angreifer beobachten kann. So genannte Seitenkanalangriffe nutzen diese ungewollte Nebeninformation, wie den Stromverbrauch oder die Dauer eines Programms aus, um daraus sensible Daten rückschließen zu können. Als klassisches Beispiel dient ein Bandit im Wilden Westen, der einen Safe knackt. Mit Hilfe eines Stethoskops lauscht er auf Klickgeräusche des Safes, die ihm erlauben auf die geheime Kombination zurück zu schließen. Die genannten Angriffe benötigen hingegen keinen physischen Zugriff auf das Gerät, aber nutzen solche Nebeneffekte in modernen Prozessoren aus um Informationen zu übertragen. In der konkreten Umsetzung der Prozessoren (der Mikroarchitektur) ignorieren Hersteller gewisse Sicherheitsgarantien der definierten Prozessorarchitektur während sie versuchen Programme so schnell wie möglich auszuführen. Hierbei versucht der Prozessor teilweise Programmabläufe vorherzusagen. Im Fall einer korrekten Vorhersage hat der Prozessor die Ausführung schneller abgeschlossen; im Fall einer falschen Annahme verwirft der Prozessor die irrtümlich berechneten Resultate und gibt sie dem Benutzer nicht Preis. Mit Hilfe von Seitenkanälen kann ein Angreifer aber diese Resultate rekonstruieren und somit sensible Daten entwenden. Da diese Angriffe keine Sicherheitslücken in Software ausnutzen, ist die Umsetzung von Gegenmaßnahmen schwierig. Um Meltdown und Spectre zu verhindern, mussten Microcode-Updates von CPUs, Änderungen am Betriebssystem und an der laufenden Software vorgenommen werden. Wenn eine Komponente nicht oder unzureichend aktualisiert wurde, waren die Angriffe weiterhin möglich.

ZombieLoad - Der neueste Angriff: Mit der Veröffentlichung von Meltdown und Spectre zeichnete sich ein neues Feld in der Wissenschaft ab und somit folgten weitere Angriffe, die andere Optimierung in der Hardware ausnutzen. Während Updates von Betriebssystemen und CPU Microcodes bestehende Systeme sicher machen, besitzt die neueste Generation an Prozessoren schon Gegenmaßnahmen in Hardware. Der neueste Angriff ZombieLoad ermöglicht es Daten von laufenden Programmen auszuspionieren und funktioniert auch auf aktueller Hardware trotz implementierter Gegenmaßnahmen. Der Angriff wurde vom selben Team der Technischen Universität Graz entdeckt und sorgte medial weltweit für Aufsehen.

Wirkungen und Effekte: Die aus der Forschung resultierenden Ergebnisse sorgten nicht nur medial auf der ganzen Welt für Aufsehen, sondern wurden auch auf Top Konferenzen veröffentlicht. Die Ergebnisse haben auch eine bedeutende Auswirkung für die Wirtschaft, da die Gegenmaßnahmen Performance-Einbußen mit sich bringen. In der Forschung ist dieser Themenbereich aktuell einer der brisantesten.

Project coordination (Story)
Univ.-Prof. DI Dr. Stefan Mangard
Graz University of Technology
Institute of Applied Information Processing and Communication
Stefan.Mangard@iaik.tugraz.at

DeSSnet / COMET-Project
JOANNEUM RESEARCH Forschungsgesellschaft mbH/ Consortium leader
Steyrergasse 17, 8010 Graz
Herwig.Zeiner@joanneum.at
www.dessnet.at

Projektpartner

- Infineon Technologies Austria AG, Austria

Diese Success Story wurde von der Zentrumsleitung/ der Konsortialführung und den genannten Projektpartnern zur Veröffentlichung auf der FFG Website freigegeben. Weitere Informationen zu COMET: www.ffg.at/comet

Bundesministerium Verkehr, Innovation und Technologie

Bundesministerium Digitalisierung und Wirtschaftsstandort

Österreichische Forschungsförderungsgesellschaft mbH
Sensengasse 1, A-1090 Wien
T +43 (0) 5 77 55 - 0
office@ffg.at
www.ffg.at