Nur wenige Zeilen Code lösen große Probleme aus: So funktioniert ZombieLoad.
Bildquelle: Lunghammer – TU Graz

Wenige Zeilen Code mit gravierenden Folgen

2018 deckten sie die schweren Sicherheitslücken Meltdown und Spectre mit auf. 2019 startete für Daniel Gruss, Michael Schwarz und Moritz Lipp ähnlich: mit ZombieLoad und Store-to-Leak Forwarding.

Birgit Baustädter

ZombieLoad und Store-to-Leak Forwarding heißen die neuen Angriffsmethoden, die die TU Graz-Sicherheitsforscher Daniel Gruss, Moritz Lipp und Michael Schwarz gemeinsam mit einem internationalen Team entdeckt haben. Die schweren Sicherheitslücken betreffen – wie ihre Vorgänger – vermutlich Millionen von Computern.

ZOMBIELOAD

ZombieLoad nutzt einen ähnlichen Ansatz wie Meltdown. Um schneller arbeiten zu können, bereiten Computersysteme mehrere Arbeitsschritte parallel vor und verwerfen dann jene wieder, die entweder nicht gebraucht werden oder für die es keine notwendigen Zugriffsrechte gibt. Aufgrund seiner Bauweise muss der Prozessor immer Daten weitergeben, auch wenn es nicht die richtigen sind. Der Check der Zugriffsrechte passiert aber erst, wenn bereits sensible Rechenschritte vorausgearbeitet wurden, die auf Annahmen des Computersystems beruhen. „In diesem kurzen Moment zwischen Befehl und Check können wir mit der neuen Attacke die bereits geladenen Daten von anderen Programmen sehen“, erklärt Gruss. So können die Forschenden im Klartext mitlesen, was gerade am Computer gemacht wird.

Für Meltdown gab es mit dem vom TU Graz-Team entwickelten KAISER-Patch eine einfache Lösung, die die Geschwindigkeit des Computers beeinträchtigte. Für ZombieLoad-Angriffe könnte sich eine Lösung schwieriger gestalten, wie Gruss erklärt: „Jede CPU hat mehrere Kerne und jeder Kern ist noch einmal geteilt. So können mehrere Programme gleichzeitig laufen. Wir glauben, dass einer dieser zwei Bereiche gelöscht werden muss.“ Das würde Leistungseinbußen von 50 Prozent bedeuten. Oder in einer Cloud, die von der Angriffsmethode ebenfalls bedroht ist, bis zu 50 Prozent weniger mögliche Nutzerinnen und Nutzer auf der gleichen Hardware.

STORE-TO-LEAK FORWARDING

Auch beim Store-to-Leak Forwarding wird die optimierte Arbeitsweise von Computerprozessoren ausgenutzt und vorab geladene Daten ausgelesen. „Der Computer geht davon aus, dass ich Daten, die ich gerade in den Prozessor geschrieben habe, auch gleich wieder weiterverwenden möchte. Also behält er sie im Buffer, um schneller darauf zugreifen zu können“, erklärt Gruss. Diese Arbeitsweise kann wiederrum ausgenutzt werden, um die Architektur des Computerprozessors auszuforschen und den genauen Ort zu finden, an dem das Betriebssystem ausgeführt wird. „Wenn ich weiß, wo genau das Betriebssystem vom Prozessor ausgeführt wird, dann kann ich gezielt Angriffe auf Lücken im Betriebssystem starten.“

Die Forschung wurde über das ERC-Projekt Sophia, das Projekt DESSNET und das Projekt ESPRESSO sowie aus einer Spende vom Hersteller Intel finanziert. ■

Cybersecurity studieren

Die TU Graz bietet die drei englischsprachigen Masterstudien Computer Science, Computer and Information Engineering sowie Software Engineering and Management an. In allen drei Masterstudien können sich Studierende im Bereich Informationssicherheit spezialisieren. Es werden vertiefende Lehrveranstaltungen von Hardwaresicherheit und Kryptografie bis hin zu E-Government-Anwendungen angeboten. Master-Studierende werden dabei eng in die aktuelle Cybersecurity-Forschung an der TU Graz eingebunden. Durch die Gründung des Cybersecurity Campus Graz wird das aktuelle Lehrveranstaltungsangebot laufend weiter ausgebaut. Für die Bachelorstudien Informatik, Information and Computer Engineering und Softwareentwicklung/Wirtschaft treten mit dem Wintersemester 2019/2020 neue Studienpläne in Kraft, in denen Informationssicherheit ein wichtiger Bestandteil ist. Damit wird die Basis für die Spezialisierung im Masterstudium gelegt. ■

Verlässlichkeit im Internet der Dinge

In seinen ersten drei Projektjahren lieferte das TU Graz-Leadprojekt „Dependable Internet of Things in Adverse Environments“ vielversprechende Ergebnisse: Das Team entwickelte ein effizientes und genaues Ortungssystem, sicherte die Kooperation von Geräten verschiedener Hersteller im IoT mittels lernfähigem Algorithmus ab, schützte die integrierte Software vor Sicherheitsattacken und entwickelte ein Vorhersagesystem für autonome Fahrzeugkolonnen. Das Forschungsprojekt wurde nach der Zwischenevaluierung für drei Jahre verlängert. ■

Erfolg für ASCON-Algorithmus

Nachrichten so zu übertragen, dass sie niemand lesen oder verändern kann, ist das Ziel der authentifizierten Verschlüsselung von Informationen. Ein Team am Institut für Angewandte Informationsverarbeitung und Kommunikationstechnologien der TU Graz reicht den hier entwickelten ASCON-Algorithmus 2014 beim renommierten CAESAR-Wettbewerb ein. Dort wurde der Algorithmus fünf Jahre lang getestet, geprüft sowie auf seine kryptanalytische und praktische Sicherheit untersucht. Die hochkarätig besetzte Jury hat das Grazer Verschlüsselungsverfahren nun als primäre Wahl für sogenannte leichte Anwendungen empfohlen. ■

Zuverlässig trotz Funkstörungen

Carlo Alberto Boano vom Institut für Technische Informatik organisiert gemeinsam mit Markus Schuß jährlich die „Dependability Competition“. Die Herausforderung in diesem Jahr: ein Set-up, das in einem industriellen, drahtlosen Multi-Hop-Netzwerk trotz starker Funkstörungen Daten zuverlässig erfasst und Betätigungsbefehle weitergibt. 13 Teams aus zehn Ländern stellten sich erfolgreich der Aufgabe. Eine Veröffentlichung ist geplant. ■

Der Wettkampf der Neuro-Assistenzsysteme

Wenn bewegungsbeeinträchtigte „Pilotinnen und Piloten“ im CYBATHLON-Wettbewerb Computerfiguren mit ihren Gedanken steuern, dann zeigt sich live, wie weit die Forschung an Brain-Computer-Interfaces (BCI) bereits gediehen ist. Das nächste CYBATHLON BCI-Rennen findet am 17. September 2019 in Graz im Vorfeld der BCI-Konferenz statt.

Werner Schandor

„Beim CYBATHLON 2016 in Zürich war die Halle voll“, erinnert sich Gernot Müller-Putz, Leiter des Instituts für Neurotechnologie an der TU Graz. „7.500 Leute haben bei den Wettkämpfen vor Ort zugeschaut, bei dem 66 Athletinnen und Athleten aus 25 Nationen angetreten sind. Das Schweizer Fernsehen hat live übertragen, und auch unsere Delegation wurde von einem ORF-Team zu den Spielen begleitet.“

Der von der ETH Zürich ins Leben gerufene CYBATHLON ist so etwas wie die WM der technischen Assistenzsysteme: In diesem sportlichen Wettkampf zeigen Athletinnen und Athleten mit Behinderung, was Prothe-