Pokerface für den Computer

Spektakuläre Fälle wie die in Prozessoren entdeckten Sicherheitslücken fordern die Wissenschaft heraus: Informatik-Professor Heiko Mantel und sein Team forschen zur Problematik von schwer nachweisbaren Angriffen über sogenannte Seitenkanäle.

Abbildung: Katrin Binner

Alexandra Weber, Dr. Damien Marion und Professor Heiko Mantel (v.l.n.r.) forschen zu Seitenkanälen.

Von Ann-Kathrin Braun

„Ein schlechtes Pokerface ist auch eine Art Seitenkanal“, sagt Professor Heiko Mantel, um sein Forschungsgebiet der „Seitenkanäle“ zu erläutern. Beim Kartenspiel können die Mimik oder andere Verhaltensweisen den Mitspielenden einiges über die Qualität der Karten verraten. In der Informatik nutzen sogenannte Seitenkanalangriffe bestimmte Kanäle aus, auf denen geheime Informationen übertragen werden, die aber nicht für diesen Zweck gedacht waren.

Die Sicherheit von vertraulichen Daten hängt nicht nur von Sicherheitsmechanismen wie Kryptographie oder Zugriffskontrolle ab, sondern auch von der Kontrolle über den Informationsfluss, das heißt wo und wie Informationen während einer Programmausführung fließen. Informationsflusskontrolle verbietet den Zugriff auf geheime Informationen nicht als Ganzes, sondern schränkt nur ein, wozu sie verwendet werden können. Informationsflusssicherheit begleitet Heiko Mantel schon seit seiner Dissertation und auf seinem Weg als Informatikprofessor, zum Beispiel war es der Themenschwerpunkt im von ihm geleiteten Schwerpunktprogramm „Reliably Secure Software Systems“ der Deutschen Forschungsgemeinschaft (DFG). Seine Arbeiten im Sonderforschungsbereich CROSSING der TU Darmstadt bauen hierauf auf.

„Die Frage ist nicht, ob das System sicher ist, sondern wie sicher ist es?“

Die Komplexität von IT-Systemen hat durch die rasante Weiterentwicklung seit deren Erfindung stark zugenommen. „Eine große Errungenschaft der Informatik ist es, Systeme in Abstraktionsschichten zu teilen und damit komplexe Systeme beherrschbar zu machen“, sagt Mantel. Dieses Vorgehen ist für die meisten Anwendungen essentiell – schließlich können beispielsweise Softwareentwicklerinnen und -entwickler beim Programmieren nicht alle Details der Hardware- und Betriebssysteme berücksichtigen. In der Sicherheitsforschung sei es aber „ein Einfallstor für Seitenkanäle“, nur eine Ebene zu betrachten, denn der Geheimnisverrat muss nicht innerhalb der Ebene des Softwareprogramms stattfinden. „Seitenkanäle halten sich nicht an Abstraktionen“, betont der Informatiker.

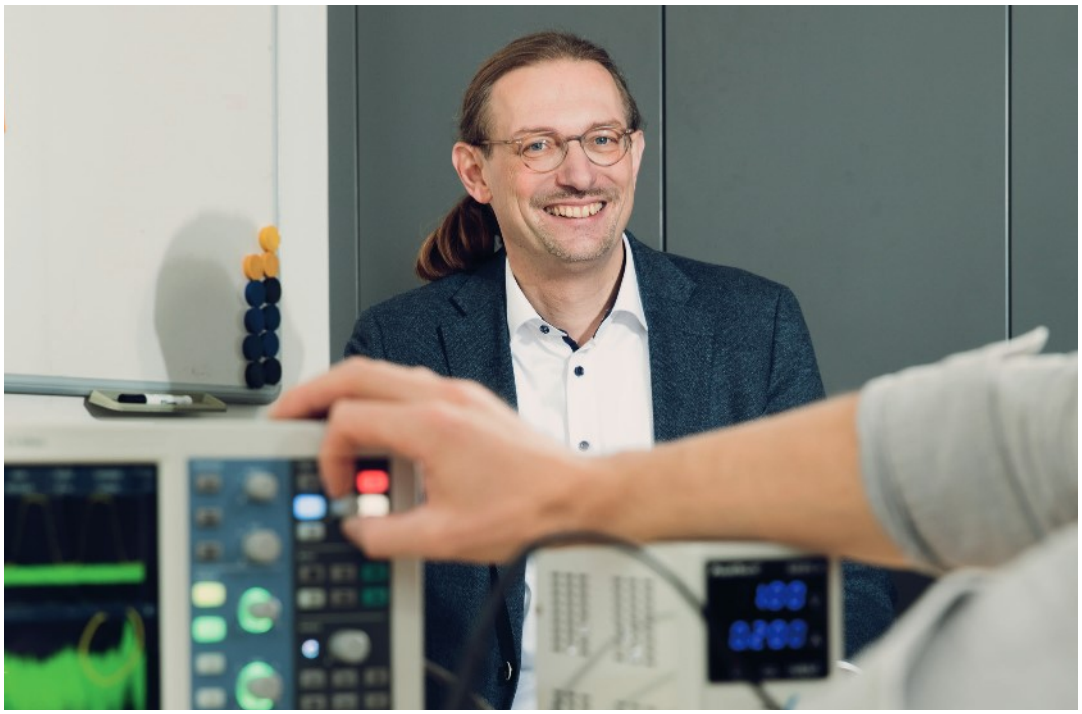
Beim Poker wird der Seitenkanal „Mimik“, also das schlechte Pokerface, ausgenutzt. Seitenkanäle in der Informatik können über verschiedene physikalische Eigenschaften wie zum Beispiel Wärmeentwicklung, Berechnungszeit, elektromagnetische Wellen, Töne oder den Stromverbrauch geheime Informationen quasi unfreiwillig preisgeben. Die Forschung von Mantels Gruppe konzentriert sich auf Seitenkanalangriffe, die keinen physikalischen Zugriff benötigen, das heißt software-basierte Seitenkanäle. Um diese identifizieren zu können, gibt es mehrere Ansätze, die die Wissenschaftlerinnen und Wissenschaftler im Sonderforschungsbereich CROSSING anwenden.

Zum einen nutzen sie formale Methoden: Das sind mathematisch fundierte Ansätze, um die Funktionsweise eines Programms durch ein Modell verständlich und analysierbar zu machen. „Normale“ Sprache wäre für die Entwicklung von Modellen nicht geeignet, sie ist mehrdeutig und kann von verschiedenen Personen auf verschiedene Weisen interpretiert werden.

In diesem Bereich der Forschung zu Seitenkanälen geht es darum, eine obere Schranke für das Ausmaß des Geheimnisverrats zu finden. Daran arbeitet Doktorandin Alexandra Weber in Mantels Gruppe. „Im

Informationen

Computer Science
Prof. Dr.-Ing. Heiko Mantel
Telefon: 06151/16-25252
E-Mail: mantel@cs.tu-darmstadt.de
http://www.mais.informatik.tu-darmstadt.de



Mit dem Oszilloskop kann man den Stromverbrauch von Hardwarekomponenten messen und diese Information für Seitenkanalangriffe ausnutzen.

Abbildung: Katrin Binner

worst case fließt die Menge X an Informationen“, so die Nachwuchswissenschaftlerin. „Solche Garantien durch meine Forschung bestimmen zu können, finde ich sehr motivierend.“ Ist der kryptographische Schlüssel beispielsweise 256 Bit lang, kann mit formalen Methoden berechnet werden, wie viele Bit davon ein Angreifer höchstens über den Seitenkanal erbeuten kann. „Das mathematische Modell bildet dabei ab, wo Informationen fließen dürfen, was das Geheimnis ist und was der Angreifer „sehen“ kann“, so Weber. Ziel der Forschung in CROSSING sei es, Werkzeuge zum Automatisieren der Untersuchung auf Seitenkanäle zu finden.

Zumindest bereits teilautomatisiert wurden die Schwachstellen in einer sehr erfolgreichen interdisziplinären Kooperation zwischen der Forschungsgruppe von Professor Mantel und dem Team von „q-TESLA“ gefunden. q-TESLA ist ein im Sonderforschungsbereich CROSSING entwickeltes Post-Quantum-Signaturverfahren, das zum weltweit ersten Standardisierungsprozess in diesem Bereich eingereicht wurde. In der Implementierung der Vorgängerversion konnten die Teams einen Cache-Seitenkanal in der Funktion, die die Signatur berechnet, ausfindig machen. Durch das Beheben dieser Schwachstelle wurde die Sicherheit des Signaturverfahrens verbessert, was auch die Chancen im Standardisierungsprozess erhöhen könnte.

Im Sonderforschungsbereich CROSSING gibt es noch einen zweiten Ansatz, um die Gefahren durch Seitenkanäle zu bewerten. Die Forscherinnen und Forscher identifizieren mit einem angriffsorientierten Vorgehen – quasi aus Sicht eines Angreifers – experimentell potenzielle Seitenkanäle. Dabei wollen sie herausfinden, welche Informationen über das Geheimnis ein Angreifer mindestens erhält. Es kann also bestimmt werden, wie riskant die Möglichkeit des Geheimnisverrats auf jeden Fall ist. „Der angriffsorientierte Ansatz macht es möglich, eine sogenannte untere Schranke zu finden“, so Mantel. Liegen obere und unter Schranke nahe beisammen, bestätige das die Genauigkeit der Berechnungen. Die Sicherheit eines Systems wird so nicht absolut – also null oder eins – bewertet, sondern erfolgt in Abstufungen. Das macht es möglich, auch für ein potenziell unsicheres System Sicherheitsgarantien geben zu können. „Die Frage ist also nicht, ob das System sicher ist, sondern wie sicher ist es?“, fasst Mantel zusammen.

Heiko Mantel sieht Seitenkanäle als wissenschaftlich interessantes Forschungsgebiet, das in der Praxis immer mehr an Bedeutung gewinnt: „Mit Spectre und Meltdown gab es in letzter Zeit gleich zwei medial prominente Angriffe, die Seitenkanäle ausnutzen.“ Seitenkanalangriffe sind forensisch sehr schwer nachzuweisen, auch deswegen brauche es weitere Forschung auf dem Gebiet, meint der Informatikprofessor. Denn während man beim Pokerspielen nach ausreichendem Geldverlust merkt, dass etwas nicht gut läuft und man etwas ändern oder aufhören sollte, so Mantel, „erhält man bei Seitenkanalattacken diese hilfreiche Rückmeldung leider nicht. Die Geheimnisse werden preisgegeben, man bemerkt das aber nicht. Erst wenn auffällt, dass jemand die Geheimnisse kennt, hat man kaum Chancen für Rückschlüsse, wann, wo und wie die Weitergabe erfolgt sein könnte.“ Deswegen wird in Darmstadt weiter daran gearbeitet, dass der Computer ein gutes Pokerface hat.

Die Autorin ist Online-Journalistin und Mitarbeiterin im Profilbereich CYSEC.

CROSSING

Im Sonderforschungsbereich CROSSING an der TU Darmstadt arbeiten mehr als 65 Wissenschaftler und Wissenschaftlerinnen aus Kryptographie, Quantenphysik, Systemsicherheit und Softwaretechnik zusammen und betreiben sowohl Grundlagen- als auch anwendungsorientierte Forschung. Ziel ist es, Sicherheitslösungen zu entwickeln, die auch in der Zukunft sichere und vertrauenswürdige IT-Systeme ermöglichen. CROSSING wird seit 2014 von der Deutschen Forschungsgemeinschaft gefördert.
www.crossing.tu-darmstadt.de