IT-Sicherheit: Auszeichnung mit Signalwirkung für Wuppertaler Informatiker

20.8.2026 - | Bergische Universität Wuppertal

Christian Mainka, Informatik-Professor an der Bergischen Universität Wuppertal, und Kollegen der Ruhr-Universität Bochum und Hochschule Heilbronn wurden auf einer der weltweit renommiertesten Konferenzen für IT Sicherheit für ihre Arbeit zu Sicherheitslücken beim Einsatz von Passkeys ausgezeichnet. Die Technologie ermöglicht Nutzer*innen ein passwortloses Anmeldeverfahren auf Webseiten.

„Passkeys sind ein bedeutender Fortschritt für die IT-Sicherheit. Unsere Analyse zeigt, wo noch Nachbesserungen nötig sind“, erklärt Christian Mainka, Professor für Robust, Secure and Privacy Preserving Smart Systems an der Bergischen Universität Wuppertal. Sein Bochumer Kollege und Hauptautor der Studie, Louis Jannett, verdeutlicht: „Bislang fehlte es an einer umfassenden Sicherheitsanalyse, die Passkey-fähige Webseiten bewertet. Unsere Forschung schließt diese Lücke nicht nur, sondern gibt Entwickler*innen und Betreibenden von Webseiten Werkzeuge an die Hand, um zukünftige Authentifizierungstechnologien noch sicherer zu machen.“

Die USENIX Security-Konferenz ist ein weltweit führender, herstellerneutraler Treffpunkt für internationale Spitzenforschung in der IT-Sicherheit. Der dort an das Forscherteam aus Deutschland verliehene *Distinguished Paper Award* gilt als eine der bedeutendsten Auszeichnungen im Bereich IT-Sicherheit.

Warum Passkeys so wichtig sind

Die ausgezeichnete Arbeit befasst sich mit der Sicherheit einer modernen Authentifizierungstechnologie, die als extrem sicher gilt: Passkeys. Passkeys ersetzen das klassische Passwort durch ein digitales Schlüsselpaar – ein Teil bleibt sicher auf dem eigenen Gerät, zum Beispiel dem Smartphone oder dem Laptop, während der andere beim Betreiber der Webseite gespeichert wird.

In Anbetracht der Tatsache, dass Passwörter weltweit weiterhin in Milliardenhöhe gestohlen werden, ergeben sich für Nutzer*innen bedeutende Vorteile. „Passkeys schützen uns vor dem sogenannten Phishing: Im Gegensatz zu Passwörtern können sie nicht durch gefälschte Webseiten gestohlen werden. Der Webbrowser erkennt automatisch, ob die Webseite echt ist, bevor er den digitalen Schlüssel freigibt“, erklärt Mainka. Damit entfalle das Risiko, das von zu schwachen Passwörtern ausgehe, oder auch das mühsame Merken komplexer Passwörter, das Anmeldeerlebnis sei für Nutzer*innen deutlich angenehmer und sicherer.

Umsetzung noch fehlerhaft

Mit ihrer Studie wollten die Wissenschaftler mehr über den Status quo der noch jungen Technologie wissen, die Nutzer*innen erst seit etwas mehr als fünf Jahren zur Verfügung steht. Dabei fanden die Wissenschaftler heraus, dass die Umsetzung auf vielen Webseiten noch fehlerhaft ist. So wurden Sicherheitstests nicht korrekt umgesetzt, wodurch sich reale Gefahren wie eine Kontoübernahme oder das Aussperren aus dem Konto ergeben könnten. „Die Grundtechnologie bleibt sicher. Die Schwachstellen finden wir bei den Webseiten, die das Verfahren zur Anmeldung anbieten. Mithilfe unserer Ergebnisse können sie die Implementierung der Technologie in ihre Systeme nun verbessern“, berichtet Louis Jannett. So wurden die betroffenen Webseitenbetreiber auch von den

Forschern kontaktiert und auf die teils gravierenden Sicherheitslücken hingewiesen.

Für Nutzer*innen ändert sich durch die Ergebnisse nichts. Aktuell werden Passkeys meist nur als zusätzliche Login-Möglichkeit angeboten und noch nicht als vollständiger Ersatz von Passwörtern vorgeschlagen. „Das Aufdecken solcher Sicherheitslücken ist ein normales Forschungsvorgehen, das neue Technologien weiter verbessert und sozusagen von ihren Kinderkrankheiten heilt. Daran zeigt sich auch, wie wichtig die Forschung ist“, erklärt Prof. Mainka.

Award mit Signalwirkung

Für den Wuppertaler Wissenschaftler steckt hinter dem gewonnenen Award dementsprechend mehr als eine bedeutende, persönliche Auszeichnung aus der Wissenschaftscommunity. Dem Informatik-Professor ist die damit verbundene Signalwirkung wichtig. Trotz des KI-Booms bleibe die Informatik unverzichtbar, insbesondere im Bereich Cyber- und Informationssicherheit. Unternehmen zum Beispiel benötigten dringend Fachkräfte, die sichere Authentifizierungs- und Schutzsysteme entwickeln und implementieren.

„An der Bergischen Universität geht es uns genau darum: unsere digitale Zukunft sicher zu gestalten. In der Forschung leisten wir dafür einen wichtigen Beitrag zur weltweiten Weiterentwicklung der Cybersicherheit – auch dafür steht die Auszeichnung. In der Lehre setzen wir auf eine praxisnahe Ausbildung, um die nächste Generation Informatiker*innen auszubilden“, betont Mainka, der das Vorgehen und die Ergebnisse aus der Passkey-Studie in seinen Vorlesungen direkt zum Thema gemacht hat. Er appelliert damit auch an Studieninteressierte, sich die Motivation für ein Informatikstudium nicht nehmen zu lassen.

Vorgehen und Ergebnisse der Studie

In ihrer Arbeit entwickelten die Forscher zwei zentrale Werkzeuge: Der **Passkey-Radar** liefert als Datenbank die bislang größte Übersicht über Passkey-fähige Webseiten und ihre Verbreitung seit 2021. Der **Passkey-Attacker** ist ein Test-Tool, mit dem die Forschenden 15 verschiedene Angriffsszenarien simulieren und damit gezielt Schwachstellen in der Anwendung der Technologie überprüfen können.

Die Analyse von insgesamt 103 getesteten Webseiten zeigt: Keine der untersuchten Seiten erfüllt alle geforderten Sicherheitsprüfungen, mehr als die Hälfte der Seiten weist schwere Schwachstellen auf, in 18 Fällen wurden besonders kritische Lücken gefunden.

Link zur Veröffentlichung

Jannett, L., Mayer, A., Westers, M., Mladenov, V., Mainka, C., & Schwenk, J. The State of Passkeys: Studying the Adoption and Security of Passkeys on the Web.

https://www.uni-wuppertal.de/de/news/detail/it-sicherheit-auszeichnung-mit-signalwirkung-fuer-wuppertaler-informatiker