



Tor-Browser vor Angriffen geschützt

Forscher der TU Darmstadt präsentieren neue Verteidigungslösung auf IT-Sicherheitswoche

Darmstadt, 20. Juli 2016. Nutzer des Tor-Browsers können ihre Anonymität künftig wirksam gegen Hackerangriffe verteidigen. IT-Sicherheitsforscher der TU Darmstadt haben dafür auf der Security & Privacy Week der TU Darmstadt eine neue Lösung vorgestellt. Zu der Wissenschaftswoche sind bis Freitag 400 Cybersecurity-Wissenschaftler aus 25 Ländern in Darmstadt versammelt.

Bei jedem Start ordnet „selfrando“ den Code des Browsers. „Der Angreifer müsste jetzt jeden Nutzer einzeln attackieren, was sehr aufwändig ist. Vorher war es möglich, auf einen Schlag alle Tor-Browser anzugreifen“, sagte Prof. Ahmad-Reza Sadeghi auf der Security & Privacy Week der TU Darmstadt.

Weltweit nutzen Millionen Menschen den Tor-Browser, darunter viele Journalisten, Whistleblower und Menschenrechts-Aktivisten. Wie eine „digitale Tarnkappe“ verschleiert der Browser die Adresse des Internetanschlusses, die Polizei und Geheimdienste zur Identifikation nutzen können. Laut Sadeghi versuchen staatliche Stellen, wie die US-Bundespolizei FBI, immer wieder, die Anonymität von Tor-Nutzern aufzudecken und deren Verhalten im Internet zu verfolgen. Dagegen schützt das „selfrando“ genannte Verteidigungswerkzeug, das Sadeghis Team zusammen mit kalifornischen Forschern entwickelte. In der Beta-Version ist es bereits im Einsatz.

Cybersecurity-Forscher um TU-Professor Matthias Hollick zeigten den Kollegen aus aller Welt, dass verschlüsselte Datenübertragung nicht nur im WLAN nötig ist: Große Teile der Internet-Infrastruktur sind drahtgebunden. Wie sie demonstrierten, können Angreifer ohne ein Netzkabel zu zerschneiden dessen elektromagnetische Abstrahlung nutzen, um von außen fast alle übermittelten Daten abzuhören.

Sicherheit für Biometrie, Medizin und Cloud-Speicher

Neue biometrische Authentifizierungsverfahren, wie Augenbewegungen oder Fingerabdruck, bergen Gefahren, warnte Angela Sasse, Professorin aus London. Diese Methoden seien zwar einfach zu benutzen, dennoch könnten sie deutlich mehr über den Nutzer verraten, als dessen Identität. Es drohe dauerhafte Überwachung, ohne dass die Nutzer dies bemerkten.

Jean-Pierre Hubaux, Sicherheitsforscher aus Lausanne, zeigte auf, dass zunehmender Gebrauch von Fitness-Armbändern oder die massenhafte Speicherung persönlicher Erbgut-Informationen zwar medizinische

Kommunikation und Medien
Corporate Communications

Karolinenplatz 5
64289 Darmstadt

Ihr Ansprechpartner:

Jörg Feuck

Tel. 06151 16 - 20018

Fax 06151 16 - 23750

feuck@pvw.tu-darmstadt.de

www.tu-darmstadt.de/presse
presse@tu-darmstadt.de



Diagnosen und Therapien verbessern können. Andererseits könnten solche sensible Daten auch für Erpressung, Überwachung oder Diskriminierung missbraucht werden.

Der australische Professor Vijay Varadharajan stellte in Darmstadt eine neue Technologie vor, die Cloud-Computing sicherer machen soll, indem sie Verschlüsselung mit rollenbasierter Zugangskontrolle verknüpft.

Weitere Themenschwerpunkte der Security & Privacy Week, die drei Konferenzen und acht Workshops zusammenfasst, sind neben Cyberkriminalität und grenzenloser Überwachung zum Beispiel auch benutzerfreundliche IT-Sicherheit, Verschlüsselung der nächsten Generation und langfristig sichere Archivierung von Daten.

Bildmaterial

Eine Infografik zu „selfrando“ können Sie im Internet unter www.tu-darmstadt.de/pressebilder herunterladen.

Kontakt und weitere Informationen

www.spw2016.de/presse

Ann-Kathrin Braun

CYSEC, Profilbereich IT-Sicherheit

Tel.: 06151 / 16-22662

E-Mail: akbraun@cysec.tu-darmstadt.de

MI-Nr. 55/2016, Braun/KM