Medieninformation

TECHNISCHE UNIVERSITÄT DARMSTADT

Spionage-Abwehr gegen mithörende Alexa & Co.

Team der TU Darmstadt entwickelt Gerät, das nicht autorisierte Aktivitäten erkennt

Kommunikation und Medien
Corporate Communications

Karolinenplatz 5
64289 Darmstadt

Ihre Ansprechpartnerin:
Silke Paradowski
Tel. 06151 16 - 20019
Fax 06151 16 - 23750
silke.paradowski@tu-darmstadt.de

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

Darmstadt, 03. Juli 2020. Ein Forschungsteam an der TU Darmstadt hat mit Partnern aus den USA und Frankreich ein Gerät entwickelt, das die Smart Home-Geräte mit Sprachassistenz erkennen kann, die ohne Zustimmung der Nutzenden aufgezeichnete Audioaufnahmen ins Internet streamen.

Hersteller von sogenannten „Smart Home“ Geräten fügen zunehmend Sprachassistenzfunktionen zu einer breiten Palette von Geräten hinzu, zum Beispiel zu intelligenten Lautsprechern, Fernsehern, Thermostaten, Sicherheitssystemen und Türklingeln. Infolgedessen sind viele dieser Geräte mit Mikrofonen ausgestattet, was erhebliche Bedenken hinsichtlich des Datenschutzes aufwirft: Die Benutzerinnen und Benutzer sind nicht immer darüber informiert, wann Audioaufnahmen in die Cloud gesendet werden oder wer Zugang zu den Aufnahmen erhält.

Das Forschungsteam der TU Darmstadt konnte gemeinsam mit seinen Partnern nachweisen, dass viele Geräte mit integrierter Sprachassistenz unabsichtlich Gespräche mithören können. Typischerweise werden Sprachassistenten mit einem Weckwort, englisch „wake-word“, aktiviert wie Amazons Echo, das üblicherweise mit dem Satzanfang „Alexa, …“ geweckt wird. Das Team hat extensiv Experimente mit Sprachassistenten wie Alexa durchgeführt und zahlreiche englische Wörter identifiziert, die Alexa fälschlicherweise als Weckwort interpretiert. Dadurch wird der Sprachassistent aktiviert, was zu einer unerwarteten Audioübertragung führt. Darunter sind auch alltägliche Wörter wie zum Beispiel „letter“ oder „mixer“. Diese Wörter können sowohl von einer künstlich erzeugten Roboter-Stimme oder einem Menschen gesprochen werden. Die ungewollt von Alexa aufgezeichneten Audio-Daten werden dann in die Cloud hochgeladen und von Amazon analysiert. Um dem entgegenzuwirken, haben die Forscherinnen und Forscher ein Gerät als Gegenmaßname entwickelt und einen funktionstüchtigen Prototypen gebaut.

Das Gerät mit dem Namen „LeakyPick“ kann im Smart Home eines Benutzers platziert werden und in regelmäßigen Abständen die anderen Sprachassistenten in seiner Umgebung mit Audio-Befehlen testen. Der nachfolgende Netzwerkverkehr wird auf statistische Muster hin überwacht, die auf eine Audioübertragung hinweisen. LeakyPick weist dann auf die Geräte hin, die die ungewollte Audioaufzeichnung durchführen.

Das LeakyPick-Gerät könnte auch gegen einen raffinierten Angriff auf den Sprachassistenten Alexa helfen: Dabei werden Weckwörter und Befehle von Angreifern in dem für die Menschen unhörbaren Ultraschall-Bereich gesendet und so zum Beispiel Bestellungen beim Online-Versandhändler Amazon getätigt. Die Ultraschall-Befehle sind nicht hörbar für das menschliche Ohr, werden aber von Alexa verstanden. Wenn das LeakyPick-Gerät also eine Aktivität feststellt, obwohl kein hörbarer Befehl erfolgt ist, könnte das auf einen solchen Angriff hindeuten.
Das Gerät existiert derzeit als Prototyp und ist noch nicht im Handel erhältlich.

Seine Ergebnisse hat das Forschungsteam auf einer Fachkonferenz eingereicht. Der vollständige Bericht ist verfügbar unter
https://arxiv.org/abs/2007.00500

Ansprechpartner für Medienanfragen:
Prof. Dr.-Ing. Ahmad-Reza Sadeghi
Fachbereich Informatik, System Security Lab
Tel.: 06151/16-25328
E-Mail: ahmad.sadeghi@trust.tu-darmstadt.de

Ann-Kathrin Braun
Profilbereich Cybersecurity (CYSEC) der TU Darmstadt
Tel.: 06151/16-22662
E-Mail: akbrauch@cysec.tu-darmstadt.de

Über die TU Darmstadt

Die TU Darmstadt zählt zu den führenden Technischen Universitäten in Deutschland. Sie verbindet vielfältige Wissenschaftskulturen zu einem charakteristischen Profil. Ingenieur- und Naturwissenschaften bilden den Schwerpunkt und kooperieren eng mit prägnanten Geistes- und Sozialwissenschaften. Weltweit stehen wir für herausragende Forschung in unseren hoch relevanten und fokussierten Profilbereichen: Cybersecurity, Internet und Digitalisierung, Kernphysik, Energiesysteme, Strömungsdynamik und Wärme- und Stofftransport, Neue Materialien für Produktinnovationen. Wir entwickeln unser Portfolio in Forschung und Lehre, Innovation und Transfer dynamisch, um der Gesellschaft kontinuierlich wichtige Zukunftschancen zu eröffnen. Daran arbeiten unsere 308 Professorinnen und Professoren, 4.500 wissenschaftlichen und administrativ-technischen Mitarbeiterinnen und Mitarbeiter sowie rund 25.200 Studierenden. Mit der Goethe-Universität Frankfurt und der

TECHNISCHE UNIVERSITÄT DARMSTADT

Johannes Gutenberg-Universität Mainz bildet die TU Darmstadt die strategische Allianz der Rhein-Main-Universitäten.

www.tu-darmstadt.de

MI-Nr. 38/2020, Richard Mitev/Ann-Kathrin Braun/sip