

Wenn technische Geräte intelligent werden, brauchen wir Sicherheit

Kriminelle Hacker können Befehle, die sich vernetzte Geräte im Smart Home gegenseitig erteilen, abhören und manipulieren. Ein Doktorand der Hochschule Stralsund hat eine Software entwickelt, die es Laien und Sicherheitsforschern ermöglicht, Funkprotokolle ohne tiefe Kenntnisse der Nachrichtentechnik zu untersuchen und vernetzte Geräte sicherer zu machen. Die öffentlich zugängliche und kostenfreie Software erhielt innerhalb kürzester Zeit weltweit beste Bewertungen. Im Interview spricht er zusammen mit seinem Doktorvater Andreas Noack von der Hochschule Stralsund über die Entwicklung der Software und warum sie international auf so großes Interesse stößt.

Ein Angstszenario, das bereits aus der Automobilbranche bekannt ist: Hacker greifen die Funkkommunikation zwischen einem elektronischen Schlüssel und einem Auto an, um den Wagen zu öffnen und zu stehlen. Was bisher noch in Einzelfällen und meist aus der Fahrzeugtechnik bekannt wurde, wird zukünftig eine entscheidende Frage der Sicherheit unserer Haushalte werden. Im Smart Home unserer Zukunft haben wir von überall die Kontrolle über unseren Haushalt und können per App, Funkschalter oder Sprachassistent unkompliziert vernetzte elektronische Geräte steuern. Johannes Pohl, Doktorand an der Hochschule Stralsund, hat eine Software entwickelt, um vernetzte Geräte sicherer zu machen.

Elektronische Geräte sind im so genannten Internet der Dinge (Internet of Things – IoT) verbunden, in dem sie eine eindeutige Identität, also eine Adresse, im Internet erhalten und mit elektronischer Intelligenz ausgestattet werden. Damit sind sie unter anderem in der Lage, sich gegenseitig Befehle oder Informationen per Funk zu senden. Dies findet in Unternehmen statt, aber auch im privaten Bereich. Hersteller von technischen Geräten forschen dafür seit vielen Jahren an vernetzbaren Geräten und Systemen, die als Smart Homes bereits auf dem Markt sind. Hacker können bei allen Arten von Funkverbindungen allerdings die so genannten Protokolle der Geräte abfangen und in krimineller Absicht weiterverwenden.

Herr Noack, für wen ist die Software „Universal Radio Hacker“ sinnvoll?

Andreas Noack:

Interessant ist die Software vorzugsweise für Menschen, die Funkprotokolle analysieren. Also Hersteller von Smart Systems und vernetzbaren Geräten, aber auch Sicherheitsforscher oder Technikbegeisterte, die sich mit dem Thema Internet of Things beschäftigen.

Was ist denn an der Software entscheidend?

Johannes Pohl:

Diese Software ermöglicht Laien und Sicherheitsforschern gleichermaßen die Untersuchung von Funkprotokollen, ohne dass sie tiefere Kenntnisse der Nachrichtentechnik haben müssen. Der Vorteil des Programms liegt darin, dass es Daten aus dem Funksignal filtert und zur Verfügung zu stellt. Das Physical Layer, also die Signalübertragung an sich, wird so aufbereitet, dass der Nutzer sich auf die logische Protokollebene konzentrieren kann. Dies geschieht automatisch im Hintergrund, man benötigt also keine tieferen Kenntnisse über Modulationen etc., um zu den Bits und Bytes zu gelangen.



Wer hat die Software genau entwickelt?

Johannes Pohl:

98 % der Software habe ich programmiert, ungefähr ein Prozent Andreas Noack. Der Rest der Beiträge wurde von Forschern aus aller Welt beigetragen. 2016 habe ich das Programm in GitHub veröffentlicht, einem Online-Dienst zur Versionsverwaltung für Software-Projekte. Das ist ein Open-Source-Projekt, wo interessierte Entwickler an einem Programm mitarbeiten können, ihre neu entwickelten Codes eingeben, und die Arbeitsergebnisse werden unmittelbar zusammengeführt.

Andreas Noack:

Die Software wurde hauptsächlich von Herrn Pohl entwickelt, kleine Teile habe ich beigetragen. Hinzu kommen noch geringfügige Anpassungen von ein paar internationalen Forschern. Ich bin als Betreuer und Gutachter sehr stolz auf die Leistung von Johannes Pohl und bedanke mich für die tolle Zusammenarbeit und Unterstützung, die wir auch von der Hochschule Stralsund und dem IACS erhalten haben. Die kooperative Promotion wurde in Zusammenarbeit mit der Friedrich-Alexander-Universität Erlangen-Nürnberg wurde von den Gutachtern Prof. Dr. Felix Freiling (FAU Erlangen-Nürnberg), Prof. Dr. David Oswald (University of Birmingham) und mir bewertet. Die Disputation war dabei eine der ersten Online-Verteidigungen einer Doktorarbeit – via Zoom.

Herr Pohl, wie lange hat der Entwicklungsprozess gedauert?

Johannes Pohl:

Nachdem ich 2013 meinen Master an der Hochschule abgeschlossen hatte, dachte ich zunächst über ein anderes Promotionsthema nach. Dann war für uns das Thema Sicherheit von Smart Homes interessanter. Das Projekt Universal Radio Hacker habe ich 2015 als Promotionsthema aufgenommen. Der Erstrelease, also die Veröffentlichung der Software, war im April 2016. Seitdem wird kontinuierlich daran gearbeitet, wobei die Software bereits vollständig einsatzbereit ist. Wir sind jetzt bei Version 2.8.8. Eine Software ist in dem Sinne nie ganz fertig, aber diese Version ist jetzt gebrauchsfertig und nutzbar.

Wie haben Sie die Software erfolgreich bekannt machen können?

Johannes Pohl:

Seitdem wir die Software 2016 etabliert, also veröffentlicht haben, habe ich an zahlreichen Konferenzen zur IT-Sicherheit teilgenommen und sie dort präsentiert. Das waren die wichtigsten und in Fachkreisen angesehensten Veranstaltungen zur IT-Sicherheit mit internationalen Teilnehmern. Einige fanden in Wien und London in Europa statt, die größten Konferenzen in Santa Clara/Kalifornien, Baltimore, Las Vegas und Dallas in den USA.

Zu den Konferenzen habe ich jeweils Publikationen veröffentlicht, in denen ich die Software vorstelle und unter verschiedenen Gesichtspunkten beleuchte. In Fachkreisen sprach sich das schnell herum.

Herr Noack, forschen Sie in Zukunft weiter an der Sicherheit der Smart Homes oder Internet der Dinge?

Andreas Noack:

Ja, ich möchte die Forschung auf diesem Gebiet sehr gerne fortsetzen und habe auch schon einige konkrete Ideen für die Zukunft. Vielleicht lassen sich künftig auch noch zusätzliche Disziplinen, wie die künstliche Intelligenz, in die Forschung der drahtlosen Protokollsicherheit integrieren. Wer sich für diese Themen interessiert, ist bei uns im Studiengang „IT-Sicherheit und Mobile Systeme“ willkommen. Vom Bachelorstudiengang kann man sich an der Hochschule Stralsund über den Master bis hin zum Doktor im Bereich IT-Sicherheit spezialisieren und forschen.



Zur Person:

Dr. Johannes Pohl, 2013 Absolvent der Informatik an der Hochschule Stralsund, hat sich in seiner Promotion mit der Sicherheit von IoT-Geräten beschäftigt und die Software „Universal Radio Hacker“ entwickelt, die er international höchst erfolgreich positionieren konnte. Am 15. Mai 2020 hat Johannes Pohl seine Doktorarbeit mit dem Titel "Automatic Security Testing of the Wireless IoT" erfolgreich verteidigt und mit der Gesamtnote "sehr gut" abgeschlossen.

Bilddatei: Johannes Pohl. Fotograf: Claas Abraham

Zur Person:

[Prof. Dr.-Ing. Andreas Noack](#), seit 2011 Professor für Kommunikationsnetze und IT-Sicherheit an der Hochschule Stralsund, forscht in den Bereichen Internet der Dinge, Smarthome-Protokolle, Netzwerksicherheit und Kryptographie. 2012 gründete er die [IT-Sicherheitskonferenz](#), zu der jährlich zahlreiche namhafte IT-Experten Vorträge halten und Forschungsergebnisse austauschen. Andreas Noack war betreuender Dozent der Doktorarbeit von Johannes Pohl an der Hochschule Stralsund.

Bilddatei: Andreas Noack. Fotograf: Timo Roth.

Kontakt:

HOST - Hochschule Stralsund – University of Applied Sciences

Hochschulkommunikation

Fon +49 3831 456528

hochschulkommunikation@hochschule-stralsund.de

<http://www.hochschule-stralsund.de/>