

PRESSEINFORMATION

IT-Sicherheit fürs Smarthome

Ein Forschungsprojekt untersucht Sicherheitslücken und erstellt Richtlinien für sichere Technik

Mit Sprache das Licht ein- und ausschalten, bei einem Unwetter vom Büro aus die Jalousien herunterfahren oder einfach im Urlaub nachsehen, ob alles in Ordnung ist: Sogenannte Smarthomes und ihre Technik bieten viele angenehme Dienste. Aber sie sind eine offene Tür für IT-Angriffe. Ein Forschungsprojekt der Universität für Weiterbildung Krems und der FH St. Pölten untersucht, wie diese Informationssysteme widerstandsfähiger gemacht werden können.

St. Pölten, 16.03.2022 – Das Internet der Dinge (Internet of Things – IoT) ermöglicht eine Vielzahl an neuen Diensten. Die Technik kann sich dynamisch an ein Umfeld anpassen, automatisiert Entscheidungen treffen und ein besseres Situationsbewusstsein liefern. In privaten Haushalten werden sogenannte Heimautomationssysteme vor allem zum Energiesparen und für mehr Komfort und Sicherheit eingesetzt.

„IoT-basierte Heimautomationssysteme sind eines der bedeutendsten Felder der Digitalisierung, die unmittelbar die Privatsphäre von vielen Menschen berühren. Durch die zunehmende Integration dieser Systeme in unser tägliches Leben, stellen sie ein attraktives Ziel für kriminelle Angriffe dar: Die Systeme können genutzt werden, um Bewohner*innen auszukundschaften und kriminelle Handlungen wie Einbrüche, Identitätsdiebstahl, Stalking oder Erpressung durchzuführen“, sagt Henri Ruotsalainen, Forscher am Institut für IT-Sicherheitsforschung der FH St. Pölten.

Angriffe abwehren

Im Projekt „ARES - Attack resilience for IoT-Based sensor devices in home automation“ untersucht Ruotsalainen, wie Angriffe verhindert und die Systeme widerstandsfähiger gemacht werden können. Dazu werden sogenannte Meta-Informationen genutzt: charakteristische Systemparameter, wie zum Beispiel Versorgungsspannung oder Prozessortemperaturen. Sie dienen dazu, Sensoren abzusichern und Angriffe zu identifizieren.

St. Pölten University
of Applied Sciences

Fachhochschule
St. Pölten GmbH

Campus-Platz 1
3100 St. Pölten
T: +43 (2742) 313 228
F: +43 (2742) 313 228-339
E: csc@fhstp.ac.at
I: www.fhstp.ac.at
FN 146616m
LG St. Pölten
DVR Nr. 1028669F

Kontakt

Mag. Mark Hammer
Fachverantwortlicher Presse
Marketing und
Unternehmenskommunikation

T: +43 (2742) 313 228 269
M: +43 (676) 847 228 269
E: mark.hammer@fhstp.ac.at
I: www.fhstp.ac.at/presse

„Wir entwickeln Methoden, um diese Meta-Informationen als Sicherheitsmaßnahmen zum Schutz von Sensordaten einzusetzen. Dadurch kann die Sicherheitslücke zwischen Sensor und digitalen Sicherheitsalgorithmen verkleinert bzw. geschlossen werden“, sagt Ruotsalainen.

Die Forscher*innen rund um Ruotsalainen identifizieren zudem die wichtigsten Sicherheitsrisiken und -bedürfnisse von privaten österreichischen Haushalten auf dem Gebiet des IoT. Die Forscher*innen erstellen auch eine Technikfolgenabschätzung sowie Richtlinien für ein sicheres Design von Sensoren und das Nutzen der Meta-Informationen zur Absicherung der Systeme.

Multidisziplinärer Ansatz

Im Gegensatz zu klassischer IT-Security und industriellen Anwendungen von IoT müssen Sicherheitsmaßnahmen in Smarthomes nachteilige Rahmenbedingungen berücksichtigen: ungeplante “Drop&Forget“-Installation (darunter versteht man, dass viele Smarthome-Geräte wie etwa Sensoren nur einmal konfiguriert werden und danach viele Jahre ohne Wartung laufen), extrem ressourcenlimitierte Geräte aufgrund des sehr hohen Kostendrucks sowie Nutzer*innen, die keine oder wenig Erfahrung mit der (sicheren) Installation und dem Betrieb der Systeme haben.

Das Projekt verfolgt daher einen multidisziplinären Ansatz, der die Fachgebiete Sensorik und Sensornetze, IT Security und Sozialwissenschaften verbindet. Dadurch werden nicht nur technisch bessere und neue Sicherheitsmaßnahmen geschaffen, sondern auch Akzeptanz und Anwendung verbessert.

Die Projektleitung liegt bei der Universität für Weiterbildung Krems. Die Gesellschaft für Forschungsförderung Niederösterreich finanziert das Projekt.

Projekt ARES - Attack resilience for IoT-Based sensor devices in home automation

<https://research.fhstp.ac.at/projekte/ares-attack-resilience-for-iot-based-sensor-devices-in-home-automation>

IT-Sicherheit studieren

Für die Studiengänge IT Security (BA), Information Security (MA) und Cyber Security and Resilience (MA) kann man sich noch bis Ende April bzw. Ende Mai bewerben.

<https://www.fhstp.ac.at/de/studium-weiterbildung/informatik>

Fotos:

Symbolbilder IT-Security, Credit: FH St. Pölten / Martin Lifka Photography

Über die Fachhochschule St. Pölten

Die Fachhochschule St. Pölten ist Anbieterin praxisbezogener und leistungsorientierter Hochschulausbildung zu den Themen Medien, Kommunikation, Innovation, Digitale Technologien, Informatik, Security, Bahntechnologie, Gesundheit und Soziales. 26 Studiengänge und zahlreiche Weiterbildungslehrgänge bieten ca. 3.700 Studierenden eine zukunftsweisende Ausbildung. Neben der Lehre widmet sich die FH St. Pölten intensiv der Forschung. Die wissenschaftliche Arbeit erfolgt zu den oben genannten Themen sowie institutsübergreifend und interdisziplinär. Die Studiengänge stehen in stetigem Austausch mit den Instituten, die laufend praxisnahe und anwendungsorientierte Forschungsprojekte entwickeln und umsetzen.

Informationen und Rückfragen:

Mag. Mark Hammer

Fachverantwortlicher Presse

Marketing und Unternehmenskommunikation

T: +43/2742/313 228 269

M: +43/676/847 228 269

E: mark.hammer@fhstp.ac.at

I: <https://www.fhstp.ac.at/de/presse>

Presstext und Fotos zum Download verfügbar unter <https://www.fhstp.ac.at/de/presse>

Allgemeine Pressefotos zum Download verfügbar unter

<https://www.fhstp.ac.at/de/presse/pressefotos-logos>

Die FH St. Pölten hält ausdrücklich fest, dass sie Inhaberin aller Nutzungsrechte der mitgesendeten Fotografien ist. Der Empfänger/die Empfängerin dieser Nachricht darf die mitgesendeten Fotografien nur im Zusammenhang mit der Presseaussendung unter Nennung der FH St. Pölten und des Urhebers/der Urheberin nutzen. Jede weitere Nutzung der mitgesendeten Fotografien ist nur nach ausdrücklicher schriftlicher Zustimmung (Mail reicht aus) durch die FH St. Pölten erlaubt.

Natürlich finden Sie uns auch auf Facebook und Twitter:

<https://www.facebook.com/fhstp> und https://twitter.com/FH_StPoelten

Sollten Sie in Zukunft keine weiteren Zusendungen der Fachhochschule St. Pölten wünschen, senden Sie bitte ein Mail mit dem Betreff „Keine Presseaussendungen“ an presse@fhstp.ac.at .