ARES - RESILIENZ VON IOT-BASIERTEN SENSOREN IN DER HEIMAUTOMATION GEGEN CYBERATTACKEN

Projektträger:
Universität für Weiterbildung Krems (Donau-Universität Krems)

Wissenschaftliche Leitung:
Thilo Sauter

Weitere beteiligte Einrichtungen:
Hochschule für Angewandte Wissenschaften St. Pölten GmbH

Forschungsfeld:
Sammlungen Niederösterreich
Fertigungs- und Automatisierungstechnik

Förderinstrument: Projekte Grundlagenforschung

Projekt-ID: FTI18-003

Projektbeginn: 01. November 2019

Projektende: folgt

Laufzeit: 24 Monate / beendet

Fördersumme: € 199.900,00

Kurzzusammenfassung:
Es steht außer Zweifel, dass das Internet der Dinge (IoT) und seine Anwendung in Heimautomationssystemen (HAS) eine Vielzahl an neuen Diensten ermöglichen wird. Diese Anwendungen können sich dynamisch an den aktuellen Kontext anpassen, automatisiert Entscheidungen treffen und ein besseres Situationsbewusstsein aufweisen. In privaten Haushalten werden sie vor allem zur Einsparung von Energie und zur Erhöhung von Komfort und Sicherheit eingesetzt. IoT-basierte HAS sind eines der bedeutendsten (zukünftigen) Felder der Digitalisierung, die unmittelbar direkt die Privatsphäre von vielen Menschen berühren.
Durch die zunehmende Integration der HAS in unser tägliches Leben, stellen sie ein attraktives Ziel für kriminelle Angreifer dar. HAS können genutzt werden, um die Bewohner auszukundschaften und kriminelle Handlungen wie Einbrüche, Identitätsdiebstahl, Stalking oder Erpressung durchzuführen.
Das ARES-Projekt untersucht, wie erfolgreiche Angriffe verhindert und angriffsresiliente HAS geschaffen werden können, in dem Meta-Informationen – das sind charakteristische Systemparameter, wie zum Beispiel Versorgungsspannung oder Prozessortemperaturen – zur Absicherung von Sensoren und zur Identifikation von Angriffen verwendet werden. Folgende Projektergebnisse werden in diesem Grundlagenforschungsprojekt dabei angestrebt:
• Eine Methodik Meta-Informationen als Sicherheitsmaßnahmen zum Schutz von Sensordaten direkt im analogen Teil des Sensors einzusetzen. Dadurch kann die aktuelle Sicherheitslücke zwischen Sensor und digitalen Sicherheitsalgorithmen verkleinert bzw. geschlossen werden.
• Eine umfassende Sicherheitsanalyse und Angriffsdetektion auf Basis von fusionierten Meta-Informationen. Die Analyse inkludiert auch eine evidenzbasierte Studie zur Identifikation der wichtigsten Sicherheitsrisiken und -bedürfnisse von privaten österreichischen Haushalten auf dem Gebiet IoT.
• Eine experimentelle Evaluierung und eine Technikfolgenabschätzung,
• die in Sicherheitsrichtlinien mit wesentlichen Ergebnissen für ein sicheres Design von Sensoren aber auch der Anwendung von Meta-Informationen zur Absicherung von Systemen beinhalten.
Im Gegensatz zu klassischer IT-Security und industriellen Anwendungen von IoT müssen Sicherheitsmaßnahmen in HAS folgende nachteilige Rahmenbedingungen berücksichtigen: ungeplante “Drop&Forget“-Installation, auf Grund des sehr hohen Kostendrucks extrem ressourcenlimitierte Geräte sowie insbesondere Nutzer, die keinerlei oder wenige Erfahrung mit der (sicheren) Installation und Betrieb der Systeme haben.
Um die genannten Ziele und Ergebnisse zu erreichen, verfolgt das Projekt daher einen mulitdisziplinären Ansatz, der die

Fachgebiete, Sensorik und Sensornetzwerke, IT Security und Sozialwissenschaften verbindet. Erst durch diese Verbindung der Wissenschaftsgebiete werden nicht nur technisch bessere und neue Sicherheitsmaßnahmen geschaffen, sondern diese von Nutzern akzeptiert und angewendet.