JOHANNES KEPLER
UNIVERSITÄT LINZ

Mag. Christian Savoy
Universitätskommunikation

T +43 732 2468 3012
F +43 732 2468 9038
christian.savoy@jku.at

Linz, 25. Februar 2016

Sicherheitslücken: JKU-ForscherInnen schützen Herzschrittmacher vor Hackern

Herzschrittmacher sind heute nichts anderes als kleine, in den Körper implantierte Computer. Was aber, wenn sie gehackt werden? Am Institut für Wirtschaftsinformatik/Software Engineering (Vorstand: Univ.-Prof. Gustav Pomberger) der Johannes Kepler Universität wird daran gearbeitet, dass genau das nicht passiert.

In der US-TV-Serie Homeland wird ein Vizepräsident durch einen gehackten Herzschrittmacher ermordet. Damit dieses Szenario reine Fiktion bleibt, müssen „medical devices" hohe Sicherheitsanforderungen erfüllen. *„Dass medizinische Geräte heutzutage unzureichend vor Angriffen von außen geschützt sind, wurde von Security-ExpertInnen vielfach gezeigt"*, weiß a.Univ.-Prof. DI Dr. Johannes Sametinger. Dass PatientInnen zu Schaden gekommen wären, ist zum Glück nicht bekannt. Aber die HerstellerInnen von medizinischen Geräten haben offensichtlich einen Aufholbedarf im Bereich Security.
„Security hat viele Facetten. Im Software Engineering geht es uns vor allem um die Erstellung von Software, die auch dann korrekt arbeitet, wenn jemand versucht, sie zu manipulieren oder zu hacken", so der JKU-Experte für Software-Security.

Bei einem Aufenthalt an der University of Arizona (USA) hat Sametinger daher gemeinsam mit US-KollegInnen die speziellen Herausforderungen für sichere medizinische Geräte erarbeitet. Ein wichtiger Schritt, denn der Software-Anteil in medizinischen Geräten nimmt kontinuierlich zu. Zusätzlich werden diese Geräte in Netzwerke eingebunden und kommunizieren untereinander, was sie aber auch angreifbarer macht.
„Darauf aufbauend haben wir vorgeschlagen, für medizinische Geräte sogenannte ‚Security Scores' einzuführen. Dabei bewerten wir, wie schützenswert Daten sind, die auf einem Gerät verarbeitet werden, welche Wirkung ein Gerät auf PatientInnen haben kann und wie exponiert ein Gerät ist. Daraus leiten wir dann ab, wie groß der Aufwand im Security-Bereich sein soll."
Zusätzlich schlägt Sametinger die Ermittlung des jeweiligen Bedrohungszustandes vor. Dieser wird u.a. aus den vorhandenen Schwachstellen ermittelt. Auch an möglichen Gegenmaßnahmen bei akuter Bedrohung wird gearbeitet.

Die ersten Ergebnisse wurden bereits im renommierten *„Communications of the ACM"* vorgestellt und von Sametinger diese Woche bei einer internationalen Tagung in Rom der Fachwelt genauer präsentiert. Das Interesse war enorm: Das Paper war sogar für den Best Paper Award nominiert; auch eine Einladung zu einer Fachkonferenz in Pasadena (USA) ist bereits erfolgt.

Kontakt:

Univ.-Prof. DI Dr. Johannes Sametinger
Institut für Wirtschaftsinformatik
Tel.: 0732 2468 4251
E-Mail: johannes.sametinger@jku.at