



# Internet der Dinge bringt verblüffende Anwendungen

Ob smarterer Rucksack, cleveres Abstimmungsgerät oder hochsichere Verschlüsselungstechnologie: Bei der Vernetzung von alltäglichen Geräten mittels Internet wollen die Forscher der **Hochschule für Technik Rapperswil** ganz vorne mit dabei sein.

von **Jérôme Stern**

**C**hristian Bermes forscht am Institut für Laborautomation und Mechatronik (ILT) der **Hochschule für Technik Rapperswil (HSR)**.

In seiner Freizeit unternimmt er gerne Skitouren – an eine davon erinnert er sich eher ungerne: «Ich musste schon bei der Zugreise umkehren, weil ich meine Skischuhe vergessen hatte. So was sollte mir nicht noch mal passieren.»

Bermes hatte auch schon eine Idee: Sein Rucksack sollte haargenau über seinen Inhalt Bescheid wissen. «Ich wollte einen smarten Rucksack konstruieren, der jedes Teil erkennt und die Bestandsliste via Bluetooth an mein Smartphone sendet.»

## Massgeschneiderte Antenne

Für Bermes war der smarte Rucksack ein perfektes Beispiel für das «Internet of Things» (IoT). Dabei sollen Gegenstände mittels Sensoren und Funktechnik mit dem Smartphone eines Benutzers vernetzt werden.

Für seinen Rucksack brauchte Bermes nun einen Scanner, welcher Funketiketten lesen kann. Das bewährte Industrieverfahren namens RFID (Radio-Frequency Identification) bedingt allerdings, dass man jedem einzelnen

Gegenstand eine Funketikette verpasst. Einen Hersteller für seinen Rucksack hat Bermes noch nicht gefunden. Doch die Idee hat Interesse geweckt: Turbinenhersteller General Electric plant, seine Servicetechniker mit einem smarten Werkzeugkasten nach Bermes Idee auszurüsten. Der Werkzeugkasten meldet so dem Techniker, ob er alle benötigten Ersatzteile und Werkzeuge eingepackt hat.

Der HSR-Professor kann sich noch etliche andere Anwendungen vorstellen. «Rucksack oder Werkzeugkiste sind bloss zwei Beispiele.» Dass das IoT mittlerweile zum Schlagwort für alle möglichen Anwendungen geworden ist, weiss Bermes. «Aber was für den Verbraucher letztlich Sinn macht, muss sich erst noch zeigen.» Für seinen «Smart-Bag» verwendete er noch eine handelsübliche Antenne. «Für eine massgeschneiderte Lösung arbeiten wir jetzt mit dem Institut für Kommunikationssysteme (ICOM) zusammen.»

## Strom durch Knopfdruck

Am ICOM tüfteln die Forscher schon seit Jahren an konkreten Anwendungen für das IoT. «Vor fast zehn Jahren hatten Studierende die Idee zu diesem Abstimmungsgerät», sagt Institutslei-

ter Heinz Mathis. Er deutet auf ein handtellergrosses Ding mit vier Druckknöpfen. «Ein Nutzer kann damit Fragen beantworten – entsprechend der Anzahl von Knöpfen hat er dazu vier verschiedene Antwortmöglichkeiten.»

In dem Party-Gag, zusammengeschaubt aus Gross-Serien-Teilen, erkannte Mathis weiteres Potenzial. Er wollte das Gerät im Unterricht einsetzen – und liess seine Studenten und Assistenten eine zweite Version herstellen, die bis aufs Gehäuse ganz aus selbst konstruierten Spezialteilen bestand. Die neueste Generation des «HSRvote» genannten Abstimmungsgeräts entwickelten die Forscher vor eineinhalb Jahren. Damit kam eine entscheidende Neuerung: Diese Version benötigte erstmals keine Batterien mehr. Alleine durch den Druck auf die Tasten wird Strom zur Übermittlung eines Bluetooth-Signals erzeugt. Das Prinzip, Energie dort zu erzeugen, wo sie verbraucht wird, heisst Energy Harvesting und eignet sich laut Mathis besonders für IoT-Anwendungen.

Eine Kleinserie von 100 Köffern mit je 30 Abstimmungsgeräten haben er und seine Mitarbeiter für die **HSR** und andere Schulen gebaut. Diese Version hat ein Gehäuse, welches ebenfalls an der **HSR** entwickelt wurde. Und zwar vom Institut für Werkstofftechnik und



Kunststoffverarbeitung (IWK).

### Verschlüsselung auf höchster Stufe

Das dritte Institut im Bereich «Mechatronik und Kommunikationssysteme» ist das Institut für Mikroelektronik und Embedded Systems (IMES).

Und wer mit dessen Leiter Paul Zbinden über die neueste HSR-Entwicklung für kryptografische Verfahren spricht, wähnt sich in einem Agenten-thriller. «Nach den Enthüllungen des ehemaligen CIA-Mitarbeiters Edward Snowden weiss man, dass amerikanische Verschlüsselungssysteme nicht genügend Sicherheit bieten.» Zbinden erklärt, dass amerikanische Firmen den einschlägigen Geheimdiensten ein Hintertürchen zum Mitlauschen offen hielten.

Die Schweizer Firma Securosys möchte ihren Kunden Lösungen anbieten, die sicherer als die amerikanischen Systeme sind. Von Securosys kam der Auftrag, zu erforschen, wie trotz herkömmlicher Schutzmassnahmen geheime Daten aus einem Gerät gestohlen werden könnten, und Gegenmassnahmen vorzuschlagen.

Genauer ging es darum, beim sogenannten Interbank-Clearing sicherzustellen, dass der Empfänger einer Nachricht absolut sicher sein kann, dass die empfangenen Daten vom richtigen Absender stammen. Extrem wichtig, da hier pro Tag rund zwei Millionen Überweisungen über durchschnittlich 300 Milliarden Franken zwischen den Schweizer Banken fliessen. «Unsere Aufgabe war, die Umsetzung der digitalen Authentifizierung sicher zu gestalten, sodass keine Hintertürchen entstehen», erklärt Zbinden.

### Zahlen als Schlüssel

«Ein langer Schlüssel bietet bei solchen Anwendungen nicht unbedingt mehr Sicherheit», sagt der Verschlüsselungsexperte. Es komme auch auf das Verschlüsselungsverfahren an. Einige Verfahren könnten selbst bei sehr langen

Schlüsseln mit herkömmlicher Hardware schnell geknackt werden. Deshalb sei es wichtig, die Sicherheit und Effizienz theoretisch sicherer Verfahren in Produkten auf die Probe zu stellen, die für die reale Anwendung gedacht sind. Und angepasste Massnahmen zu entwickeln.

Absolute Sicherheit gebe es auch beim für Securosys entwickelten Verfahren nicht, erklärt Zbinden lächelnd. «Bloss würde die Entschlüsselung mit heute verfügbarer Hardware länger dauern, als die Erde noch existiert.»

# 100

## Koffer mit Geräten

baute das HSR-Institut für Kommunikationssysteme und **rüstete** damit verschiedene **Schulen** aus.



Ein Rucksack, der garantiert nichts übersieht: Christian Bermes entwickelte seinen Smart-Bag aufgrund eigener Erfahrungen.

Bild Jérôme Stern