Kryptografie

Kleine Rechenleistung, großes Geheimnis

von Alois Pumhösel | 15. März 2011, 19:22

- 

  Wiener Forscher entwickeln Verschlüsselungstechnik, die im Autoverkehr anwendbar ist.

Forscher an der FH Campus Wien gehen der Frage nach, wie moderne Verschlüsselungstechniken ein "Internet der Dinge" sicherer machen können

Ein aus 335 Messstationen bestehendes Frühwarnsystem überwacht das Aufkommen radioaktiver Strahlung in Österreich. Für Manuel Koschuch vom Kompetenzzentrum für IT Security der FH Campus Wien wäre diese - momentan sehr gefragte - Technologie ein "klassisches Anwendungsgebiet" seiner Forschung. Sein Team unter der Leitung von Matthias Hudler arbeitet unter anderem daran, vernetzte Sensorsysteme sicherer zu machen. Das Thema der Verschlüsselung der drahtlosen Kommunikation zwischen Minicomputern mit beschränkten Kapazitäten wird in Zeiten des oft beschworenen "Internets der Dinge", der elektronischen Vernetzung von Alltagsgegenständen, zu einem wichtigen Aspekt.

Einen Lösungsansatz, der die Sicherheit von Sensornetzen künftig maßgeblich verbessern soll, werden die Wissenschafter beim kommenden Forschungsforum der österreichischen Fachhochschulen am 27. und 28. April vorstellen, das heuer ebenfalls an der FH Campus Wien stattfindet. Eine Hauptfrage ihrer Arbeit ist: Wie kann man kryptografische Algorithmen, die eigentlich der Rechenleistung moderner PCs bedürfen, effizient auf kleinen Systemen mit geringem Energievorrat und sehr beschränkter Rechenleistung zum Laufen bringen?

Um zu verhindern, dass in Sensornetzen Daten ausspioniert oder manipuliert werden, müssen sie ausreichend gesichert werden. "Beim momentanen Standard der symmetrischen Kryptografie verfügen im einfachsten Fall alle Knoten über denselben Schlüssel", erklärt Koschuch. "Wenn es gelingt, einen Sensor zu knacken, hat man das ganze Netzwerk in seiner Gewalt."

Dem könne man mit der sogenannten Schwellwertkryptografie vorbeugen: "Die Idee ist, dass ich nicht den ganzen Schlüssel in jedem Knoten speichere, sondern das Geheimnis über eine gewisse Menge von Knoten verteile." Eine gewisse Anzahl nichtkompromittierter Knoten müssen also zusammenarbeiten, um zu einem korrekten Ergebnis, einer richtigen Signatur zu kommen. Einen einzelnen Knoten zu knacken bringt dann nichts. Das Netz zu unterwandern wird viel schwieriger.

Der Haken dabei ist die Rechenleistung: Für eine Verschlüsselung, die ähnlich aufwändig wie in gängigen Drahtlosnetzwerken für PCs ist (WLAN), steht an den einzelnen Sensorknotenpunkten nicht die Leistung eines technisch aktuellen Notebooks, sondern eher jene eines 30 Jahre alten Homecomputers zur Verfügung: 8-Bit- statt 64-Bit-Systeme, 100- statt 3000-Megahertz-Prozessoren, Arbeitsspeicher von 256 Kilobyte anstelle von 4 Gigabyte, und betrieben von einer Knopfbatterie, die mehrere Jahre halten soll.

Gemeinsam mit der Uni Regensburg haben es die Wiener Forscher bereits geschafft, die Geschwindigkeit der erforderlichen Rechenoperationen um 200 bis 300 Prozent zu erhöhen. "Was noch aussteht, ist die Integration in ein Gesamtsystem, etwa in ein Sensornetzwerk von 10.000 Knoten", so Hudler. Auch die Sicherung der Wasserversorgung in Österreich, etwa die Kontrolle von PH-Wert und Sauberkeit, wäre ein Anwendungsgebiet genauso wie der Informationsaustausch zwischen Autos im Verkehr oder die Überwachung von Vitalfunktionen in der Patientenbetreuung. Und in Kraftwerksanlagen könnten Werte wie Druck und Temperatur sicher überwacht und so vor Sabotage geschützt werden.

Alois Ferscha, Leiter des Instituts für Pervasive Computing der Kepler-Uni Linz, setzt sich mit einem anderen Ansatz eines "Internets der Dinge" auseinander. Mit Kommunikations-, Rechen- oder Speichertechnik ausgerüstete Gegenstände, die sich untereinander vernetzen, nennt er "Artefakte" (in Kontrast zu den "Objekten" der Programmiersprachen). Kleinstcomputer, die wie Aufkleber an Alltagsdingen angebracht sind, sollen in Interaktion Services aufbauen. "Entscheidend ist, dass es sich immer um zwei Dinge handelt, die sich gegenüberstehen. Sie tauschen Daten aus, wenn sie in Bedeutungszusammenhang stehen." Computertechnologie kann so den Gebrauch von Autoreifen, Geldscheinen oder Werbeplakaten optimieren.

Die Sicherheit von dieser Art der Kommunikation soll durch zwei Protokolle gewährleistet sein: Artefakte, die ihre Selbstbeschreibungen mit der Umgebung austauschen, bestimmen einerseits, wie viel Information für welches Gegenüber sichtbar ist, andererseits, wie viel Information sie an sich heranlassen. Diese Softwarearchitekturen funktionieren ohne zentrale Server ähnlich Peer-to-Peer-Systemen, mit denen über das Internet Daten (Torrents) ausgetauscht werden. Die Ressourcen, die Highend-Kryptografie benötigt, seien für Ferschas Systemeinheiten, die oft nicht einmal über aktive Rechenleistung verfügen, noch nicht aufzubringen. In seinem Bereich sei das ohne bessere Hardware nicht zu lösen. (Alois Pumhösel/DER STANDARD, Printausgabe, 16.03.2011)

Am 27. und 28. April findet an der FH Campus Wien das Forschungsforum der Fachhochschulkonferenz statt.