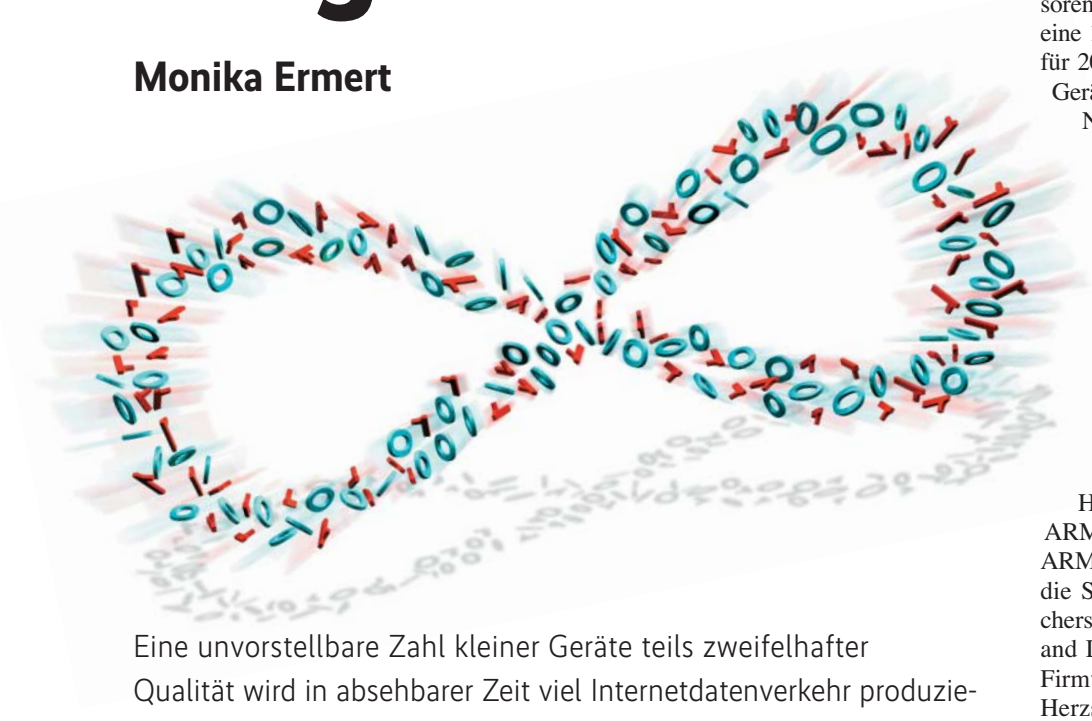
RIPE-Arbeitsgruppe für das Internet der Dinge

Dinglichkeit

Monika Ermert



Eine unvorstellbare Zahl kleiner Geräte teils zweifelhafter Qualität wird in absehbarer Zeit viel Internetdatenverkehr produzieren. Die bei den RIPE versammelte Community der Netzadministratoren hat deswegen eine eigene Arbeitsgruppe gegründet.

Auf dem 76. Treffen der Reseaux IP Europeens im Frühjahr 2018 in Marseille konstituierte sich die offizielle RIPE-Arbeitsgruppe fürs Internet der Dinge. Neue Arbeitsgruppen gibt es bei der IP-Adressvergabestelle für Europa und den Nahen Osten selten: Eine der zuletzt eingerichteten betraf IPv6. Die Entscheidung der Operator-Community, die sich zweimal jährlich trifft und über Regeln der IP-Adressvergabe und Best Practices für den Betrieb der Netze diskutiert, illustriert die Bedeutung, die die Netzadministratoren der Entwicklung beimessen.

Dabei beinhaltet „IoT“ noch gar nicht so viel Internet, wie der Name vermuten lässt. RIPE-Techniker Marco Hogewonig erklärte in Marseille: „Das Internet der Dinge bedeutet derzeit viele Dinge und wenig Internet.“ Viele der angeblich smarten Dinge würden das Netz als billigen Transportkanal für Daten nutzen, ähnlich einem Virtual Private Network. Die Hersteller bewegten sich entweder weit oben auf der Anwendungsebene oder nutzten sogar proprietäre Protokolle abseits von IP.

Wo IP zum Einsatz kommt, ist aber üblicherweise der Netzbetreiber verantwortlich für die Konnektivität. Der ISP, also ein RIPE-Mitglied, wird daher immer mehr zur direkten Gegenstelle der sich ins WLAN einbuchenden Fernseher oder anderer Smart-Home-Gerätschaften.

Massenhaft Geräte und Datenverkehr

Die erwartete Datenflut von Geräten, die von nicht IP-versierten Herstellern und Betreibern auf die Provider zurollt, war ein wesentliches Motiv der RIPE für die Einrichtung der IoT-Arbeitsgruppe. 1000 Milliarden IoT-Devices in den kommenden 20 Jahren prognostiziert Chiparchitekt und IoT-Plattform-Betreiber ARM in einer Studie für seine neue Mutter Softbank (siehe ix.de/ix1809094). Solche Zahlen bereiten Netzadministratoren verständlicherweise Sorgen.

Der Datenverkehr derart vieler Klein- und Kleinstgeräte, die das Netz als billigen Transportkanal nutzen, könne die derzeitige Infrastruktur leicht überlasten, mahnte Matthias Wählisch, Professor an der Freien Universität Berlin und Initiator des Projekts RIOT, das sich selbst als Linux des IoT bezeichnet. Wählisch rechnete auf dem RIPE-Treffen vor, dass 600 000 per Bluetooth verbundene Kleinstprozessoren oder 476 000 WLAN-Geräte leicht eine 100-Gigabit-Leitung auslasten – und für 2020 seien bereits 50 Milliarden IoT-Geräte prognostiziert.

Neben dem großen Verkehrsaufkommen und der Staugefahr bereitet den Managern der Netze die fehlende Absicherung der kleinen Knoten schlaflose Nächte. Einen Vorgeschmack bot aus Sicht der Experten der Angriff auf Kunden des DNS-Providers Dyn mit vernetzten Billigkameras – die vielzitierte „Mirai-Attacke“. Schwachstellen in Software lassen sich kaum ausschließen, selbst in hochsensiblen Bereichen.

Hugo Vincent, Security-Experte bei ARM und einer der Verantwortlichen der ARM-eigenen IoT-Plattform, erinnerte an die Schwachstelle eines Herzschrittmachers der US-Firma Abbott. Die US Food and Drug Administration forderte daher Firmware-Updates für die Software des Herzschrittmachers. Betroffen war eine halbe Million Patienten. Doch der Patchvorgang über Funk birgt selbst Risiken: Die FDA schätzt, dass der Schrittmacher im Fall eines Updates dieser Größenordnung bei 14 Patienten ausfällt.

Patchen stößt bei den Klein- und Kleinstprozessoren in der IoT-Welt auf eine Reihe von Hürden: Das Fehlen eines User Interface ist eine; fehlende Standardisierung, die technischen Einschränkungen der Minisysteme und proprietäre, nicht öffentlich dokumentierte Eigenheiten sind weitere.

„Vielleicht reichen Speicherkapazität und Prozessorleistung eines Gerätes anfangs wunderbar aus, werden aber mit der Zeit zum Engpass“, so Vincent. Am Ende stehe man womöglich vor der unerfreulichen Wahl, entweder Sicherheitslücken in Kauf nehmen oder Funktionen löschen zu müssen. Außerdem sei ein Firmware-Update natürlich teuer, wenn es viel Batteriekapazität benötigt. Laut Vincent fehlt ein automatisierter, fehlertoleranter und vollständiger Prozess, der den Betrieb des IoT-Gerätes nicht stört.

Unterstützung könnte – neben den Absicherungen, die ARM als Anbieter für outgesourcte IoT-Anwendungen in seine Plattform einbaut – von den IP-Standardisierern kommen. Bei der Internet Engineering Task Force (IETF) arbeitet ein Kollege von Vincent, Hannes Tschofenig,

an einer Bedrohungsanalyse und der für sichere Firmware-Updates im IoT notwendigen Architektur. Ein Dutzend möglicher Angriffspunkte listet einer der beiden IETF-Entwürfe auf: Sie reichen von Versuchen, alte Firmware aufzuspielen, bis zum Unterschieben nicht identifizierter oder nicht authentifizierter Updates. Parallel dazu entsteht ein Standard-Manifest für ein besser abgesichertes IoT-Patching.

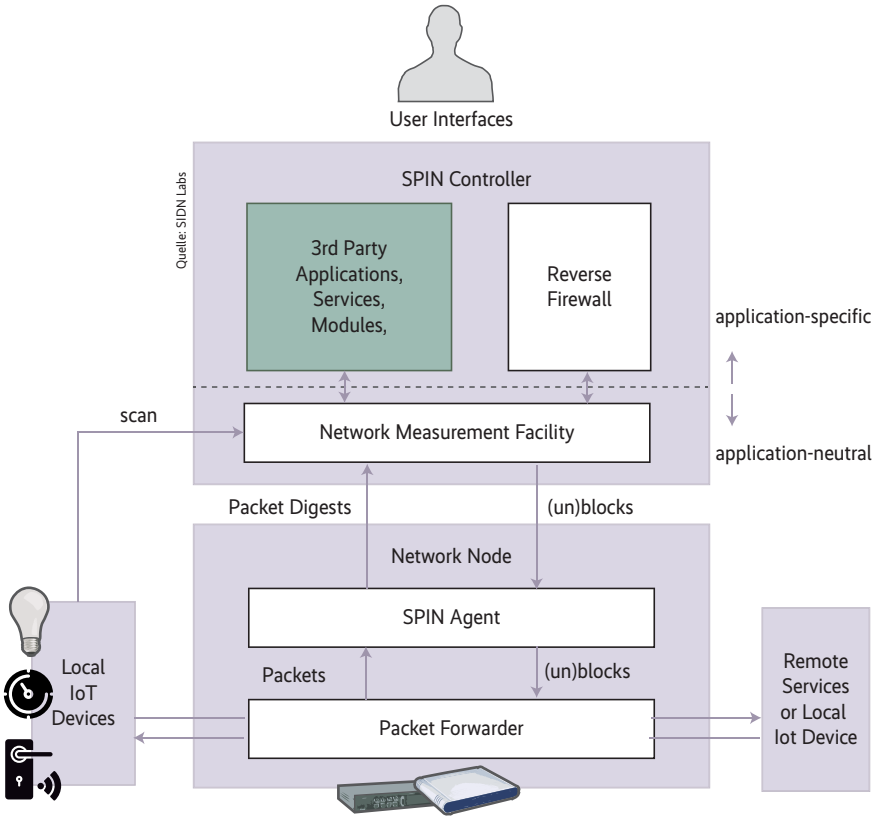
Die IETF arbeitet darüber hinaus an einer allgemeinen Risikoanalyse fürs IoT. Neben Softwareschwachstellen, Schwierigkeiten mit Firmware-Updates und DDoS-Angriffen vermerkt sie darin auch Manipulationen wie das Klonen oder Ersetzen von IoT-Knoten.

Eine erste Reihe von Standards für IoT-Systeme hat man dazu längst abgeschlossen. 6LoWPAN (RFC4944) regelt den Transport von IPv6-Paketen über IEEE 802.15.4 (Low-Rate Wireless Personal Area Networks). Mit dem Constrained Applications Protocol (RFC 7252) schuf man eine auf UDP basierende Entsprechung von HTTP für die schwachbrüstigen smarten Dinge. Die Absicherung per DTLS ist mit im Angebot (Datagram Transport Layer Security, RFC 7925), die Authentifizierung und Autorisierung soll zum Beispiel O-Auth übernehmen. Optimierte Routing-Protokolle gehören ebenfalls dazu, etwa das IPv6 Routing Protocol for Low-Power and Lossy Networks (RPL, RFC 6550). Natürlich wird konsequent auf die Nutzung von IPv6 geachtet – IPv4-Adressen gibt es für Milliarden von Dingen einfach nicht genug.

Standard als Hilfestellung

Man werde am Ende alle nötigen Bausteine beisammen haben, sagte der ehemalige Vorsitzende der Internet Engineering Task Force und Ericsson-Entwickler Jari Arkko kürzlich auf dem IoT-Tag der Association for Computing Machinery in München. Trotzdem blieben, so Arkko, wichtige Fragen offen: „Erstens, wer hat meine Daten und was macht er damit? Und, zweitens, wie verhindern wir, dass wir attraktive, weil viele Daten konzentrierende Ziele bekommen?“ Datenportabilität und Dezentralität seien daher wichtige Ziele, um die es im Zusammenspiel nicht nur zwischen den verschiedenen Standardisierern, sondern zwischen allen IoT-Initiativen gehen müsse, einschließlich denen in der Politik.

Gute Standardsoftwarebibliotheken sind ein Schritt in die richtige Richtung. Darüber waren sich die Teilnehmer der IoT-Arbeitsgruppe einig, auch wenn sich Standards unter Herstellern, die vor allem die eigene Cloud zum Gerät verkaufen wollen, erst einmal durchsetzen müssen. Best Practices für Hersteller und Betreiber könnten die Verbreitung genauso unterstützen wie internationale regulatorische Maßnahmen. Auch Zertifikate werden von den Experten immer mal wieder angesprochen, ebenso wie eine mögliche Negativregulierung: Wer nicht zertifizierte Geräte im Smart Home einsetzt, bekommt keinen Versicherungsschutz. Durch solche Kniffe ließen sich Anreize für sicherere Produkte schaffen, hoffen die Experten.



Die Open-Source-Plattform SPIN der niederländischen SIDN Labs soll die Endanwender und die Systeme ihres Internetproviders vor unsicheren Smart-Home-Geräten schützen.

Die Internetprovider diskutieren als eigene Maßnahme unter anderem, ob sie künftig verstärkt IoT-Verkehre in ihren Netzen überwachen und im Zweifel drosseln sollten. Einen gewissen Beitrag können das RIPE und seine Mitglieder auch dadurch leisten, dass sie Politik, Hersteller und Nutzer besser informieren.

Eine ganz praktische Maßnahme, mit der Provider etwas tun können für die bessere „Netzhygiene“, stellte Jelte Jansen von SIDN vor. Die niederländische Domain-Registry für die Top-Level-Domain .nl investiert seit einiger Zeit kräftig in die Umsetzung von DNS-Privacy und will mit „SPIN“ dem Smart-Home-Anwender selbst die Kontrolle über den Datenverkehr seiner smarten Geräte vom Kühlschrank bis zur Heizung zurückgeben: „Security and Privacy in In-Home Networks“ visualisiert den ausgehenden Datenverkehr, kann unerwünschten Verkehr blockieren und erwünschten zulassen.

Anwender können mitreden

Die SPIN-Software, die die Organisation derzeit gebündelt mit einer „Valibox“ zur DNSSEC-Validierung anbietet, liest und aggregiert Paketdaten und leitet sie zur Auswertung und Router-Steuerung weiter. Die Nutzer bedienen das Ganze per Web-Frontend.

Gearbeitet wird laut Jelte Jansen von SIDN noch an weiteren Features, etwa Profilen, mit denen der Nutzer gerätebezogen bestimmte Datenverkehre zulassen oder blockieren kann. Der Vorteil einer solchen Software, so Jansen, bestehe nicht nur darin, dass der Nutzer die Kontrolle über seine smarte Welt zurückerhält und etwas für die Datensparsamkeit tun kann. Auch die Registry – also SIDN selbst – und andere Provider profitierten von solcher Netzhygiene. (un@ix.de)

Monika Ermert

ist freie Journalistin mit dem Schwerpunkt Internetpolitik.

Alle Links: ix.de/ix1809094