Zertifikate für Dinge

Projekt CEBOT liefert ein neues „PKI-Protokoll" für das IoT

Das schwedische Forschungsinstitut RISE SICS und der IAM-Anbieter Nexus haben ein Protokoll für die Zertifikatsverteilung im „Internet of Things" (IoT) entwickelt, das auch ressourcenarme Geräte mit einer vertrauenswürdigen Grundlage für eindeutige Identifikation und sichere Kommunikation versorgen soll.

Von Ralph Horner, Ettlingen

Das Internet der Dinge (IoT) verheißt Potenzial für neue Geschäftsmodelle, aber auch Einfallstore für Cyberangriffe. Der Zugang zu solchen Geräten muss deshalb kontrolliert, ihre Kommunikation gesichert werden – dabei sind eindeutige und vertrauenswürdige digitale Identitäten gefragt. In der Regel übernehmen Zertifikate bei solchen Aufgaben eine wichtige Rolle.

Doch eine Zertifikatsverteilung an Geräte mit beschränkten Ressourcen, etwa mit wenig Arbeitsspeicher und geringer Verarbeitungskapazität, sowie an Systeme ohne kontinuierliche Energieversorgung ist problematisch. Manche „Dinge" müssen bis zu zehn Jahre mit nur einer Batterie auskommen, was in einem Sensornetz zu einer echten Herausforderung wird – denn klassische Internet-Protokolle kommunizieren häufig und versenden oft mehr Daten als notwendig. Notwendig wäre außerdem eine bessere Hardware – die aber meist zu teuer ist.

Vielen Geräten fehlt zudem eine grafische Bedienoberfläche: Wo es keine Möglichkeit gibt, einen Aktivierungscode oder ein Passwort einzugeben, sind automatisierte Methoden zur Zertifikatsverteilung erforderlich. Dafür existieren zwar bereits Protokolle, die aber für Geräte mit begrenzten Ressourcen wiederum zu komplex sind.

Verschiedene Anbieter haben deshalb bereits eigene Protokolle entwickelt – nicht selten jedoch ohne hinreichende Sicherheit und Interoperabilität. Ein Protokoll für die Zertifikatsverteilung, das sich in der Praxis bewährt hat, ist das „Constrained Application Protocol" (CoAP, RFC 7252, [1]) – auch dieses eignet sich aber nicht ohne Weiteres für Geräte, die nur temporär aktiv sind. Und nicht zuletzt ist oft auch die IoT-Umgebung noch nicht auf die „smarten" Zeiten vorbereitet: Typischerweise fehlt es verfügbaren Netzwerken an Stabilität und Bandbreite.

CEBOT

Um für all diese Probleme eine Lösung zu finden, wurde im September 2015 das Projekt „Certificate Enrollment for Billions of Things" – kurz CEBOT – ins Leben gerufen [5]. Das Ergebnis ist ein neues Protokoll, das eine automatische und sichere Verteilung digitaler Zertifikate vor allem an IoT-Geräte mit begrenzten Ressourcen ermöglicht. Als Basis dienen bestehende Protokolle wie CoAP [1] und DTLS (Datagram Transport Layer Security, RFC 6347, [2]) sowie EST (Enrollment over Secure Transport, RFC 7030, [3]).

Bei der Entwicklung des neuen Protokolls hatten die IoT-Experten eine ganze Reihe von Rahmenbedingungen im Blick zu behalten: Zum einen sollte die erforderliche Kommunikation der Geräte im Netz auf ein Minimum reduziert werden, um die Batteriebelastung niedrig zu halten – auch der Prozessor sollte so kurz wie möglich aktiviert werden müssen. Darüber hinaus mussten die Entwickler gewährleisten, dass die vom Gerät gesendeten Informationen immer vollständig übertragen werden, was bei den bereits existierenden Protokollen nicht immer der Fall war.

Mittlerweile liegt ein entsprechender Protokollentwurf [6] vor, der über die „ace"-Arbeitsgruppe (Authentication and Authorization for Constrained Environments, [4]) der Internet Engineering Task Force (IETF) zur Standardisierung vorgesehen ist. SICS hat hierzu auch bereits eine Referenzimplementierung für das freie IoT-Betriebssystem Contiki (www.contiki-os.org) entwickelt, die voraussichtlich im Herbst als Open Source veröffentlicht werden soll (Release-Hinweis erscheint auf der Projekthomepage [5]).

„Stellen Sie sich vor, Sie kaufen eine ‚smarte' Glühbirne, auf der bereits ein Zertifikat installiert ist", erläutert Dr. Shahid Raza (www.shahidraza.info), zuständiger Projektleiter bei RISE SICS. „Sobald Sie die Glühbirne anschließen, verbindet sie sich automatisch mit der Certificate-Authority (CA), um sich ihr Zertifikat mit einem Einmal-Passwort bestätigen zu lassen. Für diese Kommunikation wird unser neues Protokoll eingesetzt." Nach der Bestätigung des Zertifikats durch die CA verfügt die bewusste Glühbirne über eine vertrauenswürdige Identität und kann von da an mit anderen Geräten – beispielsweise mit einem System für die Heimautomatisierung – sicher kommunizieren.

Adaption bestehender Standards

Für die Entwicklung des neuen Protokolls wurde letztlich das EST-Protokoll [3] zur Verteilung digitaler Zertifikate auf die Nutzung des IoT-Protokolls CoAP [1] hin adaptiert. CoAP wurde ja bereits speziell für den Einsatz in Netzwerken mit begrenzten Kapazitäten entwickelt: Es zielt darauf, Geräte, die nicht in der Lage sind, einen eigenen kryptografischen Schlüssel selbst zu generieren, vollautomatisch mit Schlüsseln sowie digitalen Zertifikaten auszustatten. Damit lassen sich derartige Geräte auch ohne Eingabe eines Aktivierungscodes sicher in ein Netzwerk integrieren – denn hierfür böten diese Systeme ja keine Bedienoberfläche. Das neue CEBOT-Protokoll gewährleistet außerdem, dass immer das richtige Gerät mit der richtigen unzweifelhaften Identität versehen wird – so lassen sich Störungen und Manipulationen ausschließen.

Die Aufgaben im Rahmen des Projekts waren klar verteilt: RISE SICS kümmerte sich um die Client-Seite und die Implementierung des Protokolls auf IoT-Geräten mit begrenzten Ressourcen. Das Forschungsinstitut konnte dabei seine umfassenden Erfahrungen bei der Entwicklung von Protokollen einbringen. Nexus hingegen kümmerte sich um die Server-Seite, also um die Certificate-Authority (CA). Das Unternehmen hat dafür das CEBOT-Protokoll bereits in seinen „Nexus Certificate Manager" integriert, der digitale Identitäten bereitstellt und verwaltet.

Das neue Protokoll, dessen endgültiger Name erst im Laufe der Standardisierung feststeht, wird zwar noch weiterentwickelt, ist aber bereits einsatzfähig und herstellerunabhängig nutzbar. Nach der Anerkennung durch die IETF dürfte es nach Einschätzung von Projektleiter Raza schnell Verbreitung finden: „CEBOT ist für viele Unternehmen interessant, weil es *das* fehlende Puzzlestück in Sachen IoT-Sicherheit ist", betont er. Unter den Unternehmen, die das Projekt befürworten, finden sich bereits jetzt bekannte Namen wie Husqvarna, Ericsson, Saab, SUST, Yanzi Networks, Intel und Scypho.

Falls „CEBOT" wider Erwarten kein IETF-Standard werden sollte, kann man es natürlich dennoch einsetzen – wie andere Protokolle, die sich noch im „Entwurf" befinden. Die weiteren Pläne der Projektpartner sind ambitioniert: Nach dem Ende des eigentlichen CEBOT-Projekts am 30. Juni 2017 wollen RISE SICS und Nexus das Protokoll in einem auf drei Jahre angelegten Folge-Projekt namens SecureIoT einsetzen [7]. Ziel ist es, weitere Sicherheitslösungen für IoT-Anwendungen zu entwickeln – gefördert von Eurostars, einem gemeinsamen Programm der europäischen Forschungsinitiative EUREKA und der Europäischen Kommission.

Fazit

Das Internet of Things (IoT) braucht ein standardisiertes Protokoll für die Zertifikatsverteilung – Eigenentwicklungen, die nur auf den Geräten der jeweiligen Anbieter funktionieren, sind keine tragfähige Lösung. Eine anbieterunabhängige Methode, um digitale Zertifikate an ressourcenarme Geräte ohne Benutzeroberfläche zu verteilen, gab es bis vor Kurzem jedoch nicht.

33. Jahrgang / Nr. 3, Juli 2017

<kes>

Die Zeitschrift für Informations-Sicherheit

ISSN 1611-440X

BSI Forum
offizielles Organ des BSI
Bundesamt für Sicherheit in der Informationstechnik

Phishing-Awareness:
Schon fünf Minuten helfen

S. 62

15. Dt. IT-Sicherheitskongress:
Stimmen aus Bad Godesberg

S. 27

Malware: Trends und Abwehr
Malware as a Service – Desinfektion – Whitelisting – Threat-Hunting

S. 46

DATAKONTEXT

Dauerbaustelle: **Sicherheit der Operational Technology** S. 6