Internet of Things meets Business

Studiengang: MAS Information Technology
Betreuer: Stephan Sutter
Experte: Prof. Max Felser
Industriepartner: ti&m AG, Zürich

Das Internet der Dinge (IoT) bezeichnet die Vernetzung von physischen Objekten mit dem Internet. Gemäss Prognosen sollen bis im Jahre 2020 rund 50 bis 100 Milliarden Geräte vernetzt sein. Diese Zahlen machen offensichtlich, dass auch das Thema Security in diesem Bereich immer wichtiger werden wird. Im Auftrag der Firma ti&m* wurde mit dieser Arbeit ein Konzept für die sichere Anbindung eines IoT-Gerätes an eine Cloud-Umgebung ausgearbeitet und als Prototyp implementiert.

Problemstellung

Anders als bei den heute gängigen Web- oder Mobile-Technologien existieren im IoT-Bereich noch praktisch keine standardisierten Sicherheitsmechanismen. Solche sind aber die Voraussetzung für ein weltweites Netzwerk, in welchem unterschiedlichste Geräte miteinander kommunizieren sollen. Zudem werden die Sicherheitsaspekte auf den Endgeräten selber oft vernachlässigt und deren Wichtigkeit unterschätzt. Gelingt es einem Angreifer jedoch, die Kontrolle über ein IoT-Gerät zu erlangen, oder ein solches in ein System einzuschleusen, hat er mit grosser Wahrscheinlichkeit Zugriff auf etliche Daten oder kann sogar industrielle Prozesse manipulieren.
Im IoT-Kontext besteht die Herausforderung nun darin, Sicherheitsmechanismen unter Berücksichtigung des Kostenfaktors, sowie den begrenzten Speicher- und Energieressourcen der Endgeräte zu implementieren.

Ziel

Ziel dieser Arbeit war die Ausarbeitung und Implementierung eines Konzepts für eine sichere Anbindung eines IoT-Gerätes an eine Cloud-Umgebung mit Hilfe einer Mobile-App. Dabei sollten wo immer möglich bereits etablierte Technologien und Verfahren verwendet oder adaptiert werden. Weiter war die Kompatibilität der Mechanismen mit dem Krypto-Chip zu berücksichtigen, welcher parallel als Teil einer anderen Arbeit evaluiert wurde und später zusätzlich implementiert werden soll.

Ergebnis

Das Endergebnis der Arbeit ist schliesslich der Prototyp einer IoT-Umgebung, bestehend aus den folgenden Komponenten:

- **IoT-Gerät** – Zu authentifizierender Client, welcher Daten erfassen und an einen Cloud-Service übertragen kann.
- **Mobile-App** – Als User-Interface für die Registrierung und Konfiguration der IoT-Geräte durch den Endbenutzer.
- **Cloud-Umgebung** – Für die Authentifizierung der IoT-Geräte und Benutzer, sowie zum Speichern der übertragenen Gerätedaten.

Der Zentrale Teil der Lösung ist der Authentifizierungsprozess des IoT-Gerätes mittels Elliptic Curve Digital Signature Algorithm (ECDSA). Es handelt sich dabei um ein standardisiertes Verfahren zur Erzeugung und Überprüfung von asymmetrischen Schlüsselpaaren und digitalen Signaturen, unter Verwendung von Elliptischer-Kurven-Kryptographie. Im IoT-Kontext ist der wesentliche Vorteil von Kryptosystemen welche auf elliptischen Kurven basieren, dass im Vergleich zu anderen Verfahren wie RSA für eine ähnliche Sicherheit wesentlich kürzere Schlüssel notwendig sind. Dies verringert den Rechenaufwand enorm, was auf Systemen mit begrenzten Ressourcen ein entscheidender Faktor ist.
Die Hardware für den Prototyp des IoT-Gerätes basiert auf einem Mikrocontroller der Plattform ESP8266. Es handelt sich dabei um ein Produkt der chinesischen Firma Espressif, welches sich dank integriertem WLAN-Chip sehr gut für IoT-Anwendungen einsetzen lässt. Durch die Unterstützung verschiedener Sleep-Modes ist zudem ein sehr stromsparender Betrieb möglich. Ein weiteres Argument für diesen Chip ist der tiefe Preis, welcher aktuell bei ca. 2,4 USD liegt.

Samuel Schärer

Fazit

Die erarbeitete Lösung zeigt, wie im IoT-Bereich trotz fehlender Standards und limitierten Ressourcen Security-Aspekte unter Verwendung bereits etablierter Konzepte und Technologien implementiert werden können. Das Ganze ist im Wesentlichen unabhängig von spezifischer Hardware oder einem bestimmten Technologie-Stack und kann somit für verschiedenste IoT-Szenarien adaptiert werden.
Für die Firma ti&m dient diese Arbeit als Grundlage für den Ausbau und die Weiterentwicklung eines Konzepts, welches schliesslich als IoT Security-Lösung zu einem neuen Produkt von ti&m werden soll.

*www.ti8m.ch