Hardwarebasierte IoT-Sicherheit inklusive Personalisierungsservice

**Mehr Sicherheit für IoT-Innovationen**

Esther Cairos, Product Marketing Manager Chip Card & Security, Infineon Technologies

Christian Krieber, Marketing Director Security & Identification, EBV Elektronik

*Mit Milliarden von Geräten, die in Wohnungen, intelligenten Fabriken, Büros und sogar in abgelegenen Gegenden mit dem Internet verbunden sind, ist das Internet der Dinge (IoT) eine der am schnellsten wachsenden technologischen Revolutionen, die die Welt gesehen hat. Doch mit der Verbreitung des IoT wachsen auch die potenziellen Angriffspunkte für Hacker und damit die Sicherheitsrisiken. Da beim IoT die Machine-to-Machine (M2M)-Kommunikation im Mittelpunkt steht, sind diese Angriffe in vielerlei Hinsicht weitaus gefährlicher für Mensch und Leben als ‚normale‘ Computerangriffe, da in diesem Fall die Kontrolle über real arbeitende Maschinen übernommen werden kann.*

*In diesem Artikel zeigen Infineon Technologies und EBV Elektronik einige der Auswirkungen von Sicherheitsverletzungen auf und erläutern, wie Entwickler bei der Planung und Implementierung einer gesicherten IoT-Infrastruktur vorgehen sollten. Schwerpunkte sind hier die hardwarebasierte Sicherheit sowie Gerätepersonalisierungsdienste, die den Einsatz von hardwarebasierten Sicherheitslösungen erheblich erleichtern.*

**Großer Bedarf an IoT-Sicherheit**

Es gibt eine große Anzahl von Unternehmen, die ihren zukünftigen Geschäftserfolg teilweise oder ganz auf Cloud-Services und künstliche Intelligenz stützen, um neue Einnahmequellen zu erschließen. Cisco schätzte beispielsweise vor kurzem, dass dieser Geschäftsbereich in den nächsten fünf Jahren rund 19 Billionen Dollar zur globalen Wertschöpfung beitragen wird.

Die Milliarden von über das Internet verbundenen Geräten, die bereits im Einsatz sind, sind die Schlüsselfaktoren für diesen bedeutenden neuen Wirtschaftszweig. Erst mit ihnen wird es möglich, diese neuen Werte zu schaffen. Gleichzeitig erhöhen sie aber auch das Potenzial böswilliger Angriffe, die zum Raub geistigen Eigentums, Diebstahl persönlicher Daten, Unterbrechung des Geschäftsbetriebs und sogar zur Gefährdung des Markenimages und letztlich der Existenz eines Unternehmens führen können.

Die Bedrohung ist dabei sehr real und global; und sie betrifft viele große Organisationen – sowohl kommerzielle als auch staatliche. Erfolgreiche Angriffe sind zudem schädlicher als einfache Computerviren, da viele IoT-Geräte unmittelbar mit Maschinen und kritischer Infrastruktur verbunden sind. Berichten zufolge haben Angriffe auf IoT-Infrastrukturen bereits zum Ausfall von Stahlwerken, Kraftwerken und sogar einer kerntechnischen Anlage geführt. Auf Verbraucherebene berichtete Incontrol zudem, dass 71% der Verbraucher befürchten, dass ihre persönlichen Daten gestohlen werden könnten, was die Akzeptanz dieser neuen Technologie deutlich verlangsamt.

Parallel zum schnellen Fortschritt bei der IoT-Technologie entwickeln Hacker immer raffiniertere Methoden, Sicherheitsmaßnahmen zu kompromittieren. Beliebt sind die physikalische Mikrosondierung der ICs und die Analyse der elektromagnetischen Emissionen zur Spionage sowie die Induktion von Fehlern im laufenden Betrieb durch Manipulation der Stromversorgung oder durch das Hinzufügen von Taktstörungen (Clock Glitches) zur Sabotage. Hiervor müssen sich Device-Hersteller aller Art schützen.

**IoT-Sicherheit für Entwickler**

Für einen angemessenen Schutz sind dabei alle Aspekte der Systemsicherheit zu berücksichtigen: Maßgeblich sind sowohl die Applikation selbst als auch die Kommunikation vom und zum Gerät sowie die Kommunikation innerhalb des physischen Geräts. Richtig ausgeführt, schützt dieser ganzheitliche Ansatz die Vertraulichkeit, Integrität und Verfügbarkeit einer Applikation umfassend.

Abbildung 1

Der erste Schritt für jeden Entwickler besteht darin, zu überlegen, welche Sicherheitsmechanismen und -level für die jeweilige Aufgabe geeignet sind. Zu berücksichtigen sind hierbei sowohl die Art des Objektes und sein Wert als auch mögliche Angriffsmethoden, die Wahrscheinlichkeit solcher Angriffe sowie die Auswirkungen eines erfolgreichen Angriffs. In Abhängigkeit dieser Faktoren kann dann überlegen werden, wie Angriffe vermieden werden können und welche Kosten damit verbunden sind, sowie welche Auswirkungen diese Maßnahmen auf die Gesamtleistung des Systems sowie seine Wartung haben. IoT-Geräte verfügen dabei – ihrer Aufgabe entsprechend – über einige ganz spezifische Anforderungen und Herausforderungen, die Entwickler meistern müssen.

Abbildung 2

Im Allgemeinen haben IoT-Geräte sehr begrenzte MCU- und Speicherressourcen. Auch kommen keine komplexen Betriebssysteme zum Einsatz. Die zu implementierenden Sicherheitskomponenten müssen deshalb die genutzten Embedded Betriebssysteme unterstützen und sollten zudem nur einen kleinen Teil des Hostspeichers beanspruchen. Physikalisch gesehen sind IoT-Geräte unter Umständen sehr klein und das muss sich auch in der gewählten Sicherheitslösung widerspiegeln. Viele IoT-Geräte werden mit Knopfzellen oder über Energy Harvesting Technologien betrieben. Daher müssen auch die eingesetzten Sicherheitskomponenten äußerst sparsam mit ihrem Energieverbrauch umgehen und niedrige Produktionskosten ermöglichen, um der Preissensitivität der meisten IoT-Geräte zu entsprechen.

IoT-Designer sind jedoch zumeist keine ausgewiesenen Experten in Sachen Sicherheit. Deshalb muss die gewählte Lösung zudem auch einfach zu implementieren sein. In den meisten Fällen bedeutet dies die Auswahl eines Lieferanten mit umfangreicher Support-Infrastruktur – sowohl direkt als auch über technisch kompetente Distributoren, wie die EBV Elektronik, die eine große Servicemannschaft im Feld hat.

**Hardware ist ein wesentlicher Bestandteil**

Software kann bei der Verschlüsselung zwar ein hohes Maß an Sicherheit gewährleisten. Ein rein softwarebasierter Ansatz hat jedoch einige bemerkenswerte Schwächen. Beispielsweise werden während der Authentifizierung eines IoT-Knotens Zertifikate und öffentliche/private Schlüssel ausgetauscht und verarbeitet, um sicherzustellen, dass das Empfängergerät ordnungsgemäß identifiziert und autorisiert wird. In einem reinen Softwaresystem kann dies jedoch bedeuten, dass der private Schlüssel in einen nicht sicheren Speicher verschoben wird, um die Verarbeitung zu ermöglichen. Dadurch kann der private Schlüssel jedoch wiederum böswilligen Angreifern ausgesetzt sein, wodurch die Gesamtsicherheit des Systems beeinträchtigt wird.

Abbildung 3

Hardware-basierte Sicherheitslösungen wie der OPTIGA™ Trust X von Infineon Technologies sind hier eine Alternative, denn man kann sie als Secure Element einsetzen, welches den privaten Schlüssel auch während der Verarbeitung schützt. Der private Schlüssel wird bei dieser Methode nur innerhalb dieses Secure Elements verarbeitet, wodurch er vor Offenlegung in einem ungesicherten, normalen Speicher geschützt wird und so die Systemsicherheit nicht gefährdet wird.

Der OPTIGA™ Trust X ist eine vollumfängliche Lösung mit reichhaltigem Funktionsumfang für die Gerätesicherheit, die auf einem CC EAL 6+ (High) zertifizierten Sicherheitscontroller basiert, der TLS/DTLS und X.509 Zertifikate unterstützt. Es ist TRNG AIS-31 zertifiziert und unterstützt USB Type-C Authentifizierung sowie eine Kryptografie-Toolbox für flexible kundenspezifische Anpassungen.

Diese vielfältigen Optionen ermöglichen unterschiedlichste Anwendungsszenarien für den OPTIGA™ Trust X, beispielsweise die gegenseitige Authentifizierung und gesicherte Kommunikation, der Schutz von Datenspeichern, das Lifecycle- und Energiemanagement sowie die extrem wichtigen gesicherten Updates, über die IoT-Geräte fehlerfrei und aktuell gehalten werden.

Trotz der hohen Leistungsfähigkeit des OPTIGA™ Trust X ist die schlüsselfertige Lösung einfach in IoT-Anwendungen zu integrieren. Infineon bietet hierzu alle notwendigen Hostcodes, ein kundenspezifisches Public-Key-System und ein Evaluation-Kit sowie nicht zuletzt auch umfassendes Know-how, das Designern bei Bedarf zur Verfügung gestellt werden kann.

**Gerätepersonalisierung**

Das Hinzufügen eines Secure Elements zu einem Design und die Nutzung seiner Authentifizierungs- und/oder Verschlüsselungsfunktionen ist nur ein Aspekt. Hinzu kommt auch die Erzeugung der Kryptoschlüssel. Sie sind nämlich das Herzstück jeder Sicherheitsmaßnahme. Deshalb müssen sie auch auf sichere Weise und in einem Bereich erzeugt werden, in dem nur berechtigte Personen Zugang haben. Außerdem müssen Zertifikate mit einem privaten Schlüssel erzeugt und signiert werden, der das HSM (Hardware-Sicherheitsmodul) niemals verlassen darf. All diese Anforderungen verlangen erhebliche Investitionen in Zeit, Wissen und Equipment.

Hierbei kann der Distributor EBV Elektronik seine Kunden mit seinem hauseigenen Personalisierungsservice Secure-it unterstützen und so die hochqualifizierten Entwickler des Kunden vom Programmieraufwand für diese Aufgaben entlasten. Secure-it bietet die Generierung von Zertifikaten sowie die Erstellung und Programmierung von Sicherheitsschlüsseln auf entsprechend gesichertem Equipment an, sodass Kunden hierfür weder Aufwand noch Investitionen betreiben müssen und auf einfache Weise kundenspezifische Secure Elements für IoT-Anwendungen erhalten.

**Abbildung 4**

Die Programmierung erfolgt mit Data-I/O-Hardware, die sich in einer physisch gesicherten Umgebung befindet und in einem umzäunten Bereich bei EBV in Deutschland untergebracht ist. Zum Schutz der von EBV programmierten Devices ist keines dieser Programmiergeräte mit dem Internet verbunden und daher nicht anfällig für Cyber-Angriffe oder böswillige Manipulationen.

Der Personalisierungsservice Secure-it integriert sich zudem nahtlos in bestehende Beschaffungsprozesse von Kunden, sodass der Bestellvorgang identisch mit dem für Standardbauelemente ist. Es können jederzeit sowohl große als auch kleine Volumen programmiert werden. Letzteres ist beispielsweise für Spezialanwendungen und Prototypen neuer Produkten nützlich. Da der Zugang zu dem flexiblen Programmierdienst für jede Losgröße sehr einfach, zuverlässig und kosteneffizient ist, können sich Kunden die Entwicklung eigener Sicherheitsverfahren zum Schutz von Schlüsseln sparen, was Investitionen in das Programmierenvironment von Hardware überflüssig und Secure Elements dadurch für nahezu jedes IoT-Device erschwinglich macht.

**Zusammenfassung**

Eine softwarebasierte Verschlüsselung bietet zwar einen gewissen Grad an Sicherheit, der hardwarebasierte Sicherheitsansatz, wie ihn Infineons OPTIGA™ Trust X bietet, ist jedoch die deutlich stärkere Lösung. Sie ist schlüsselfertig und bietet umfangreiche Sicherheitsfunktionen für IoT-Systeme. Hierzu zählt auch ein hohes Maß an Support wie der Gerätepersonalisierungsservice des Infineon Distributionspartners EBV Elektronik. Mehr Informationen über diesen finden Sie auf der ['Secure-it' Produktwebsite](https://www.avnet.com/wps/portal/ebv/products/product-highlights/secure-personalized-hardware/).

- Ende -

Abbildung 1: Ein ganzheitlicher Sicherheitsansatz gewährleistet Vertraulichkeit, Integrität und Verfügbarkeit innerhalb von IoT-Systemen

Abbildung 2: Das IoT stellt Entwickler von Sicherheitsinfrastrukturen vor besondere Herausforderungen und Einschränkungen

Abbildung 3: Hardware-Sicherheit schützt private Schlüssel durch Verarbeitung in einem Secure Element

Abbildung 4: Der Personalisierungsservice von EBV integriert sich nahtlos in bestehende Lieferketten