Swissbit AG: SD-Flash-Karte mit Secure Element trotzt Angriffen durch Quantencomputer

»Sichert die Kommunikation ab!«

Die Vernetzung von Geräten und Maschinen ist in vollem Gang, doch angesichts der Industrie-4.0-Begeisterung mahnt Hubertus Grobbel, Leiter des Geschäftsbereichs Security Products der Swissbit AG: »Sichert die Kommunikation ab!« Voraussetzung dafür ist die Identifikation der Teilnehmer, wofür SD-Karten mit Secure Element eine einfache und flexible Lösung bieten – auch um den Herausforderungen durch Quantencomputer gewachsen zu sein.

Für Fachleute im Bereich IT-Security wie Grobbel ist klar: »Identifikation, Authentisierung, Authentifizierung und Autorisierung sind die vier Schritte, mit denen sich ein ‚sicherer Kanal öffnet'.« Durch die Zwei-Faktor-Authentifizierung lasse sich die Sicherheit »deutlich« erhöhen. Das Token, das zur Authentisierung gehört, kann zugleich für die Verschlüsselung der Kommunikationsinhalte genutzt werden.

Hubertus Grobbel, Swissbit

„Eine besondere Bedrohung der Kryptografieverfahren geht vom Quantencomputer aus, mit dessen Verfügbarkeit in den nächsten Jahren gerechnet werden muss."

Während derartige Prozesse heutzutage für einen menschlichen Anwender im IT-Netzwerk »eigentlich selbstverständlich sind, ist das anders für die ‚Dinge' im Internet of Things«, betont der Swissbit-Manager: »Sensoren, Aktoren, Devices, Maschinen, IT-Systeme und nicht zuletzt kritische Infrastrukturen: Sie alle müssen sich bislang nur sehr selten ‚ausweisen', wenn sie mit Netzwerken verbunden werden.« Und wer Daten bei ihnen abfragen oder ablegen wolle, bleibe gegebenenfalls anonym.

In gut bewachten Industrieanlagen, die nicht mit dem Internet verbunden waren, »mögen die Risiken noch tolerabel sein; in den smarten, vernetzten Fabriken der Zukunft sind solche Sicherheitslücken nicht mehr zu akzeptieren«, sagt Grobbel. Zu groß sei die Gefahr, dass Unbefugte von außen über den Internetzugang Kontrolle über die Smart Factory bekommen. So gibt es etwa Berichte und Videos über Autos, deren Funktionen sich von Außenstehenden bedienen ließen. Dies verdeutlicht, dass sich Szenarien von fernkontrollierten Chemiefabriken und Kraftwerken oder fremdgesteuerten Fertigungsrobotern nicht einfach von der Hand weisen lassen. Deshalb müssen auch Dinge eine Art Ausweis bekommen, denn wenn nur Geräte miteinander kommunizieren können, die sich zuvor ausweisen und gegenseitig erkennen können, haben es Hacker bedeutend schwerer.

Ausweis im Speicher

Wenn man derzeit ein Gerät mit einem Secure Element versehen will, muss entweder eine identifizierbare Hardwarekomponente (TPM, Trusted Platform Module) in den Baugruppen aufgelötet werden oder es sind Prozessoren einzusetzen, die über integrierte Elemente eindeutig identifizierbar sind (TEE, Trusted Execution Environment). Deutlich flexibler ist der Ansatz des europäischen Flashkarten-Speicherherstellers Swissbit, Infrastrukturen mit dem Äquivalent von Ausweiskarten nachzurüsten. Das geschieht ganz einfach über eine SD-, µSD- oder USB-Schnittstelle und sichere Speicherkarten.

Die sicheren Memory Cards von Swissbit bestehen aus einem Flash-Speicherchip, einer Smart Card und einem Flash Controller. Dessen spezielle Firmware mit integriertem AES-Enkryptor ermöglicht weitere Anwendungsszenarien. Weil als Secure Element ein Krypto-Element genutzt wird, kann nicht nur die Kommunikation abgesichert, sondern es können Daten auch sicher verschlüsselt werden. So lassen sich Trusted-Boot-Konzepte realisieren und Lizenzen sichern. Zudem kann das Flash Memory mit Enkryptor dazu genutzt werden, weitere Datenspeicher (etwa klassische Festplatten) im System zu verschlüsseln. Die für Authentifizierung und Verschlüsselung im IIoT vorgeschlagenen Flash-Speicherkarten werden bereits in großem Umfang in abhörsicheren Mobiltelefonen, Polizei-Bodycams und zum Schutz von Patientendaten in der Medizintechnik eingesetzt.

Trusted-Platform-Modul zum Nachrüsten

Auf die Idee, das Identifizierungsmerkmal mit einem Standarddatenspeicher zu kombinieren, kam der Schweizer Speicherspezialist, weil die meisten Komponenten und Embedded-Systeme im IIoT sowieso Speicher benötigen – für Betriebssysteme oder Daten. »Die Implementierung ist vergleichsweise einfach, weil die Memory-Schnittstellen standardisiert sind und sogar Middleware für die Integration der TPM-Abfragen bei Bedarf mitgeliefert werden kann«, versichert Grobbel. Eine der größten Herausforderungen beim Aufbau von sicheren IIoTs sei, ältere Systeme und bestehende Kom-

ponenten nachzurüsten. Sofern diese aber über USB- oder SD-Schnittstellen verfügen, können diese Legacy-Systeme mit einer SD-Karte als TPM einfach mit fälschungssicheren Identitäten ausgerüstet und nachträglich in das Sicherheitskonzept integriert werden.

Ein ganz wichtiger Punkt bei der Sicherheitsbetrachtung ist im übrigen, dass sich Security über den Produktlebenszykylus sozusagen abnutzt, weil die Angriffsmethoden ausgefeilter werden. »Eine besondere Bedrohung der Kryptografieverfahren geht vom Quantencomputer aus, mit dessen Verfügbarkeit in den nächsten Jahren gerechnet werden muss«, prognostiziert der Swissbit-Manager. Asymmetrische Kryptografie werde damit leicht zu knacken sein. Die Entwicklung einer Post-Quanten-Kryptografie (PQC) werde nötig, sprich Algorithmen, die resistent gegen Angriffe mit Quantencomputern sind. Produktmanager müssen daher bei Sicherheitslösungen nicht zuletzt wegen des IT-Sicherheitsgesetzes, das stets den letzten Stand der Technik fordert, auf Aktualisierbarkeit achten. »Sichere Speicherkarten als leicht austauschbare Module bieten sich deshalb auch im Hinblick auf die PQC-Herausforderung an«, sagt Grobbel. (es)

Die Funktion eines TPM übernehmen Swissbits industrietaugliche SD- und µSD-Karten mit Secure Element und spezieller Firmware.