Mikrocontroller im IoT vor Einbrechern schützen

Mikrocontroller ermöglichen nicht nur die Vernetzung von intelligenten Geräten, sondern stellen zugleich hohe Anforderungen an die IT-Security und den Datenschutz. Um möglichst viele Angriffsszenarien abzudecken, sind relevante Sicherheitsaspekte schon im Produktdesign zu berücksichtigen.

Fachartikel von Marco Blume,

Mikrocontroller jeglicher Art und Größe sind allgegenwärtig und verrichten ihre Funktionen in einer Vielzahl von Geräten – von der Digitaluhr am Handgelenk über das Smartphone in der Jackentasche bis hin zum Festnetztelefon oder zum Lichtschalter im Netzwerk für das Gebäudemanagement sowie in Steuergeräten im Auto. Der Trend hin zur Vernetzung von möglichst vielen Geräten erhöht den Funktionsumfang und bewirkt einen Mehrwert für die einzelnen Devices. So kann zum Beispiel die Armbanduhr Daten vom Handy in der Tasche anzeigen und die intelligente Raumsteuerung die Klimaanlage nur bei Anwesenheit von Personen starten.

Softwareentwickler können mit Code-Meter µEmbedded Anwendungscode und geistiges Eigentum auf FPGAs und in Mikrocontrollern gegen Reverse Engineering schützen und eine Lizenzkontrolle implementieren. (Bild: Infineon)

Damit eine Welt mit vielen praktischen Geräten und Helfern Realität werden kann, sind neue Herausforderungen beim Datenschutz zu bewältigen und Strategien zu implementieren, die mögliche Angriffe auf Netzwerke und Geräte abwehren und den Nachbau von Geräten sowie den Diebstahl von Know-how verhindern.

Frühzeitig an den Einbruchschutz denken

ECKDATEN

Softwareanbieter, Gerätehersteller sowie Maschinen- und Anlagenbauer können ihre Produkte mit Code-Meter von Wibu-Systems vor Raubkopierern, Reverse Engineering und unerlaubten Änderungen schützen und zugleich flexible Lizenzmodelle implementieren. Außerdem lassen sich mit Code-Meter Manipulationsversuche verhindern und externe Angreifer abwehren.

Ähnlich wie der Bauherr bei einem Neubau frühzeitig an den Einbruchschutz denkt, muss dies auch zu Beginn der Entwicklung neuer Geräte erfolgen. Hier gilt es, Entwickler, Produktmanager und Systemarchitekten bereits beim Produktdesign für die Einhaltung der Sicherheitsaspekte zu sensibilisieren. Schließlich soll eine integrierte Sicherheitslösung entstehen, die möglichst viele Angriffsszenarien abdeckt.

Dabei ist die erzielte Sicherheit von der Qualität der Implementierung und der späteren prozesskonformen Nutzung abhängig. Spätestens an dieser Stelle begibt sich das Entwicklungsprojekt oft auf neues Terrain. Denn die Entwickler sind Spezialisten für ihr Kerngeschäft, aber nicht unbedingt für Kryptographie und sicheres Softwaredesign. Und Anwender möchten sich mit Sicherheits- und Lizenzfunktionen am liebsten nicht befassen.

Firmware-Schutz für IoT oder Industrie 4.0

Das IoT verspricht nicht nur enormes Wachstum, sondern verlangt gleichzeitig die Einhaltung von zahlreichen Sicherheitsaspekten. Diese betreffen alle beteiligten Systeme, von PCs und IPCs über Embedded-Systeme, Mobilgeräte und SPSs bis zu den eingesetzten Mikrocontrollern. Wibu-Systems hat zusammen mit Infineon den Firmware-Schutz Code-Meter µEmbedded für Systeme auf Basis der Mikrocontroller XMC4000 entwickelt, der insbesondere für Anwendungen wie IoT oder Industrie 4.0 verfügbar ist.

Das Internet der Dinge in den unterschiedlichen Ausprägungen erfordert ein hohes Maß an Sicherheit. Typische Anwendungsfälle sind die Authentifizierung oder Lizenzierung von Komponenten hinsichtlich ihrer eindeutigen Identität, die Überwachung und Sicherung der Systemintegrität, der Schutz von Daten und der Kommunikation sowie sichere Updates oder Upgrades. Um Vertrauen in neue Dienstleistungen und Technologien aufzubauen, ist darüber hinaus der IP-Schutz von Bedeutung.

Für geeignete Lösungskonzepte sind integrierte Systemlösungen erforderlich, die auf sicherer Hardware basieren und die Infrastruktur sowie Komponenten vor Angreifern, Betrug und Sabotage schützen. Da alle Embedded-Systeme in IoT-Konzepten auf Mikrocontrollern basieren, befindet sich hier die erste Ebene, auf der Schutzfunktionen aufsetzen müssen.

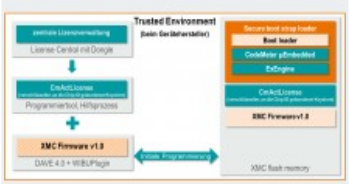

Bild 1: Übersicht aller beteiligten Komponenten – links beim Entwickler und rechts auf dem XMC-Controller. (Bild: Wibu-Systems)

Systeme in rauen Industrieumgebungen schützen

Die Herausforderung bei der Implementierung von Sicherheit besteht bei Mikrocontroller-Anwendungen darin, dass die Lösung auch unter rauen Industrieumgebungen einsetzbar und einfach zu integrieren sein muss. Auf Basis des Code-Meter-Konzepts von Wibu-Systems für den Schutz, die Lizenzierung und die Sicherheit von Systemen wurde Code-Meter µEmbedded entwickelt. Die Lösung adressiert insbesondere die Sicherheitsaspekte bei Firmware-Updates sowie bei funktionellen Erweiterungen von Systemen mit Mikrocontrollern. Darunter fallen beispielsweise die Codeintegrität, die Lizenzüberwachung, der Schutz vor Reverse Engineering und das Kopieren von Programmcode.

Während in Bezug auf die funktionale Sicherheit (Safety) gesetzliche Regelungen greifen, gibt es in Sachen Security (Sicherheit für das Gerät) kaum Gesetze oder allgemein verbindliche Vorschriften, dafür aber viel Raum für Spekulation und Theorie. Deshalb steht am Anfang grundsätzlich eine Sicherheitsanalyse, die im einfachsten Fall Fragen wie diese adressiert: Was kann passieren? Wie hoch ist die Eintrittswahrscheinlichkeit – jetzt und während der Lebensdauer? Wie hoch ist der mögliche Schaden – wirtschaftlich und für das Image?

Mit dem Ergebnis dieser Betrachtung lässt sich definieren, vor welchen Szenarien das Produkt zu schützen ist und was der Schutz kosten darf. Sind die Kosten für den Schutz höher als der mögliche Schaden, stellt sich die Frage, ob ein Schutz aus wirtschaftlicher Sicht sinnvoll ist. Sind die Kosten niedriger, sollten die Verantwortlichen über eine Umsetzung unter Berücksichtigung der Eintrittswahrscheinlichkeit nachdenken.

Mögliche Anwendungsfälle

An dem hier beschriebenen Beispiel des Mikrocontrollers XMC4000 wurden als zentrale Aspekte folgende Anwendungsfälle definiert:

- Integritätsschutz: Der Mikrocontroller darf nur mit Firmware aus einer definierten Quelle funktionieren und diese darf nicht unbefugt verändert worden sein.
- IP-Schutz: Die Firmware soll auch im Feld durch Dritte ladbar sein und muss daher verschlüsselt sein, um Reverse Engineering zu verhindern.
- Lizenzierung: Es soll möglich sein, ohne Austausch der Firmware im Feld weitere Funktionalitäten in Form von Upgrade-Lizenzen freizuschalten.

Um Entwicklern eine einfache und sicher handhabbare Lösung anzubieten, haben Wibu-Systems und Infineon ein Komplettpaket entwickelt, das mehrere Produkte vereint. Die Version 4 der Entwicklungsumgebung Dave (Digital Application Virtual Engineer) von Infineon lässt sich als kostenfreies Entwicklungstool herunterladen, während die Eclipse-basierende Entwicklungsplattform Anwender bei der Softwareentwicklung unterstützt. Dazu stellt Infineon ein peripherie- und anwendungsorientiertes Code Repository bereit.

Außerdem generiert Dave passenden Code für die Peripherie der XMC-Mikrocontroller. Durch den komplementären Ansatz können Anwender den in Dave konfigurierten und generierten C-Quellcode mit den verfügbaren Third-Party-Tools für ARM übersetzen, linken und auf den Mikrocontroller laden. Damit ist der Entwicklungszyklus von der Evaluierung über den ersten Prototyp bis zum Produkt vollständig abgedeckt. Anwender haben dabei zahlreiche Möglichkeiten für eine schnelle und effiziente plattformorientierte Software- und Produktentwicklung.

SPSs und PCs schützen

Code-Meter µEmbedded wurde speziell für Mikrocontroller und FPGAs entwickelt. Softwareentwickler können mit dieser Technologie Anwendungscode und geistiges Eigentum auf FPGAs und in Mikrocontrollern gegen Reverse Engineering schützen und eine Lizenzkontrolle implementieren. Für größere Systeme wie speicherprogrammierbare Steuerungen (SPS) oder PCs gibt es mit Code-Meter Embedded und Code-Meter Runtime zwei lizenzkompatible Varianten.

Code-Meter µEmbedded benötigt mit weniger als 80 kByte nur wenig Speicherplatzbedarf (Footprint), was durch eine Reduzierung der Lösung auf den minimal notwendigen Funktionsumfang für die beschriebenen Anwendungsfälle erreicht wurde. Die erzeugten Lizenzen für alle Code-Meter-Varianten sind kompatibel und werden an eine eindeutige ID des Mikrocontrollers gebunden und bei der Produktion aktiviert. Nachträglich lassen sich per Dateiaustausch weitere Leistungs- und Funktionsmerkmale freischalten.

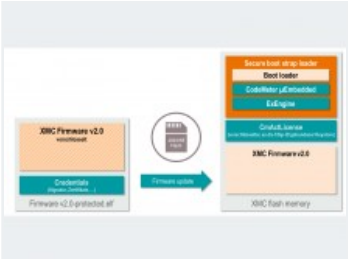

Bild 2: Die verschlüsselte Firmware wird erst durch den SBSL (Secure Boot Strap Loader) entschlüsselt und verbleibt dann lesegeschützt im XMC-Controller. (Bild: Wibu-Systems)

Schlüssel sicher speichern

Code-Meter µEmbedded lässt sich zusätzlich zum sicheren Speichern von symmetrischen und asymmetrischen Schlüsseln nutzen. Dabei befindet sich der Schlüssel in einem geschützten Speicher und ist nur auf dem Gerät mit der passenden ID verwendbar. Typische Anwendungsfälle sind die Lizenzkontrolle von Geräten (Mikrocontroller und FPGAs), die Überwachung der Produktionsmenge durch Lizenzierung der einzelnen hergestellten Geräte sowie die sichere, verschlüsselte Übertragung des Anwendungscodes in das Gerät.

Anwender können gewohnte Werkzeuge wie Dave und die Code-Meter Protection-Suite, ein Paket mit allen erforderlichen Tools zur Ausführung der kryptographischen Operationen, sofort verwenden. Mit einem Plugin für die Entwicklungsumgebung Dave erhalten Entwickler eine einfache grafische Oberfläche zur Konfiguration der XMC4000-Mikrocontroller sowie zum Erzeugen der verschlüsselten Firmware-Updates oder Lizenzdateien.

Mikrocontroller für digitale Leistungswandlung

Die Mikrocontroller der Familie XMC4000 für Industrieanwendungen eignen sich auch für die digitale Leistungswandlung sowie für elektrische Antriebe und Sensoranwendungen. Sie enthalten den ARM Cortex-M4-Prozessor mit eingebauter DSP-Funktionalität, Floating Point Unit (FPU), Direct Memory Access (DMA) und Memory Protection Unit (MPU). Zur Peripherie gehören Analog-/Mixed-Signal-Wandler, Timer/PWM-Kanäle und Schnittstellen für alle gängigen industriellen Kommunikationsstandards. Die mit Onchip-Ethercat (Ethernet for Control Automation Technology) ausgestattete Mikrocontroller-Serie XMC4800 ermöglicht die Implementierung von Echtzeit-Ethernet-Kommunikation.

Das funktionale Kernstück der Lösung ist ein Secure Boot Strap Loader (SBSL), der bei der Produktion eines Gerätes initial in den XMC-Controller geladen wird. Der SBSL greift auf eine individuell an den XMC-Controller gebundene Cm-Act-Lizenz zu. Diese Datei enthält das benötigte Schlüsselmaterial zum Entschlüsseln der Firmware. Nach dem Laden von SBSL und Lizenz schaltet der Controller automatisch in die Betriebsart Read-Protect. Von außen ist jetzt kein Zugriff mehr auf den Flash-Speicher möglich. Die Kommunikation zum Laden von Firmware läuft nur noch über den SBSL, der beim Einschalten automatisch startet.

Der vorbereitende Schritt erfolgt in der Produktentwicklung beim Gerätehersteller, wo Entwickler mit gewohnten Methoden und Tools ein Gerät zur Produktreife bringen. Aus Dave heraus wird dabei eine Firmware v1.0 erzeugt und anschließend mithilfe des Dave-Plugins, das das Verschlüsselungstool Ex-Protector von Wibu-Systems ansteuert, verschlüsselt.

Schlüsselmaterial via Dongle

Zusätzlich wird aus Dave heraus ein Projekt für den SBSL erzeugt. Hier ist nur über das Plugin der Speicherplatz des Schlüssels im Dongle anzugeben. Danach baut der SBSL ohne weitere Modifikationen und kann direkt in den XMC-Controller geladen werden.

Für Firmware-Entwickler ist dies der einzige Schritt, bei dem sie mit der Sicherheitslösung in Berührung kommen. Da das benötigte Schlüsselmaterial in einem Dongle gespeichert ist, müssen sich Entwickler nicht um das sichere Schlüsselhandling kümmern (Bild 1).

In der sicheren Umgebung der Produktion wird ein Mikrocontroller der Serie XMC4000 zunächst mit dem sicheren Bootloader betankt. Dieser verbleibt geschützt im Controller. Der nächste Schritt erzeugt eine Lizenzdatei, die an die ID des Controllers gebunden ist.

Bild 3: Der Hersteller erzeugt eine Lizenz und erweitert die Funktionalität ohne Austausch der Firmware.
(Bild: Wibu-Systems)

Lizenz erzeugen, Firmware laden, fertig

Im Anschluss erfolgt die eigentliche Erzeugung der Lizenz. Erst jetzt wird die Firmware v1.0 auf das Gerät geladen. Alle Schritte können innerhalb eines automatisierten Programmierprozesses erfolgen, der sich technisch nicht von einem herkömmlichen Prozess zum Herunterladen von Firmware in der Serienfertigung unterscheidet. Damit ist das Gerät fertig zur Auslieferung. Alternativ unterstützt auch das Dave-Plugin alle erforderlichen Schritte. Dies vereinfacht die Evaluierung der Lösung oder die Produktion geringer Stückzahlen. Für die Großserienfertigung lassen sich alle Schritte auch scripten.

Anwendungsfall 1: Firmware-Update im Feld

In diesem Fall besteht der Schutzanspruch darin, dass kein Reverse Engineering der Firmware erfolgen kann und das Gerät nur unveränderte Originalfirmware lädt.

Dazu wird, wie schon bei der Erstauslieferung, die Firmware in Dave erzeugt und getestet sowie mit dem Ex-Protector automatisch signiert und verschlüsselt (Bild 2). Die Datei lässt sich anschließend ohne weitere Sicherheitsvorkehrungen zum Kunden transferieren und dort aufspielen. Das verwendete Medium ist dabei nicht von Belang, da es nicht möglich ist, die Firmware außerhalb des XMC4000 zu entschlüsseln oder zu verändern. Jeglicher Manipulationsversuch lässt die Signatur brechen und der Secure Boot Loader unterlässt das Laden der Firmware.

Erst während des Ladeprozesses wird die Firmware entschlüsselt und im Speicher des XMC4000 abgelegt. Dies erfolgt flussgesteuert im Ladeprozess, sodass kein doppelter Speicher erforderlich ist. Am Ende des Prozesses steht die Prüfung der Signatur. Ist sie korrekt, wird der Vorgang abgeschlossen. Sollte die Signatur gebrochen sein, wird die Firmware verworfen.

Anwendungsfall 2: Funktionsupgrade im Feld

In diesem Anwendungsfall geht es darum, eine universelle Firmware auszuliefern, die sich bei Bedarf später um zusätzliche Funktionen erweitern lässt. Ein Austausch der Firmware soll dazu nicht nötig sein, um eventuell notwendige Test- und Zertifizierungsprozesse des Betreibers zu vermeiden. Es erfolgt lediglich ein Upgrade der Lizenzdatei.

Beim ersten Programmieren wurde die ID des Controllers idealerweise bereits in dem Tool „License Central“ gespeichert. Kunden können nun über ein Lizenzportal beim Hersteller eine Funktionserweiterung erwerben, indem sie die Seriennummer ihres Controllers angeben. Daraufhin erzeugt das System eine verschlüsselte Lizenzdatei, die nur auf dem einen Zielsystem lauffähig ist

(Bild 3). Wird diese eingespielt, schaltet sie zum Beispiel weitere Achsen einer Steuerung frei, ohne dass dazu die Firmware auszutauschen ist.

Wibu-Systems bietet ein Gesamtpaket an, das es Entwicklern leicht machen soll, einen wirkungsvollen und flexiblen Schutz für ihre Software auf einem Mikrocontroller zu erreichen. Alle Funktionen für die Verschlüsselung der Software bis hin zur Verwaltung der Lizenzen sind bereits integriert.
(hb)

ÜBER DIE AUTOREN

Marco Blume

arbeitet bei Wibu-Systems

WEITERE INFOS

Wibu Systems

Rüppurrer-Straße 54

76137 Karlsruhe

Deutschland

Zum Firmenprofil >