Daten- und Know-how-Sicherheit

Sicherheit für Mikrocontroller

18.02.2016 von Marco Blume und Dirk Heinen

Wir sind umgeben von Mikrocontrollern: von der Digitaluhr über das Smartphone zum Festnetztelefon und Tablet, dem Lichtschalter im Gebäudemanagement, der Zentralheizung bis ins Auto mit seinen Steuergeräten. Auch das Garagentor ist vom Mikroprozessor gesteuert wie die Kaffeemaschine und andere Geräte. Sicherheit vor Hackern spielt eine immer größere Rolle.

© INFINEON Technologies

Die unvollständige Liste zeigt, dass wir von programmierbaren Geräten umgeben sind, die heute mehr können als nur »An« und »Aus«. Und der Trend geht eindeutig dahin, diese Geräte untereinander zu vernetzen. Das erhöht in erster Linie die Funktionalität und stellt einen deutlichen Mehrwert für die Geräte dar. Auf einmal kann die Armbanduhr Daten vom Handy in der Tasche anzeigen und die intelligente Raumsteuerung startet die Klimaanlage nur, wenn auch jemand im Büro ist. Das Navigationsgerät im Auto bekommt die Verkehrslage in Echtzeit von unzähligen anderen Nutzern, die schon unterwegs sind und allen Verkehrsteilnehmer im Hintergrund ihre Durchschnittsgeschwindigkeit an einen zentralen Server melden.

Das ist die eine Seite der Medaille – die schöne, neue und zweifelsohne auch praktische Welt. Leider sieht es auf der anderen Seite manchmal noch düster aus. Von neuen Herausforderungen beim Datenschutz, über verschiedenste mögliche Angriffe auf die Netzwerke und Geräte bis zum Nachbau und Know-how-Diebstahl erstrecken sich die Punkte, die beachtet werden müssen.

Doch dafür gibt es Lösungen. So wie man bei einem Neubau schon in der frühen Phase bei der Auswahl der Fenster, Türen und Beschläge an den Einbruchschutz denkt, muss das auch beim Design neuer Geräte von Anfang an geschehen. Baut man in eine schöne, aber mechanisch simple Haustür am Ende ein hochwertiges Schloss ein, so ist der Schutz nur so hoch wie die Stabilität der Tür. Dieser Vergleich soll den Entwickler, Produktmanager und Systemarchitekten dafür sensibilisieren, dass die Sicherheitsaspekte schon im Produktdesign berücksichtigt werden müssen, damit am Ende eine vollintegrierte
Sicherheitslösung herauskommt, 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. Die Entwickler sind Spezialisten für ihr Kerngeschäft, aber nicht unbedingt für Kryptographie und sicheres Softwaredesign. Der Anwender möchte von Sicherheits- und Lizenzfunktionen am liebsten gar nicht behelligt

werden, und ein Kostentreiber darf die Sicherheit keinesfalls sein.

Über Safety (die Sicherheit für den Benutzer) wird nicht mehr diskutiert – dort greifen gesetzliche Regelungen; für Security (Sicherheit für das Gerät) gibt es kaum Gesetze oder verbindliche Vorschriften, dafür aber viele Spekulationen, Theorien, Studien und immer jemanden, der das Konzept mit einem Killerargument wieder zu Fall bringt. Deshalb ist der steht am Anfang grundsätzlich eine Sicherheitsanalyse. Im einfachsten Fall stellt man sich folgende Fragen:

- 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, wogegen das Produkt geschützt werden soll, wogegen nicht und was der Schutz kosten darf. Sind die Kosten für den Schutz höher als der mögliche Schaden, so ergibt das in der Regel wirtschaftlich keinen Sinn. Sind die Kosten niedriger, sollte über eine Umsetzung unter Berücksichtigung der Eintrittswahrscheinlichkeit nachgedacht werden. Mit dieser Definition lässt sich auch nach einem Schadenseintritt oder gegenüber dem Kollegen mit den Killerargumenten noch schlüssig argumentieren, warum gerade dieses Szenario nicht abgedeckt ist.

Als wichtigste Schutzaspekte für den Anwender des Mikrocontrollers XMC4000 wurden folgende Use Cases 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 ein Reverse Engineering zu verhindern.
- Lizenzierung: Es soll möglich sein, ohne Austausch der Firmware im Feld weitere Funktionalitäten in Form von Upgrade-Lizenzen freizuschalten.

Um dem Entwickler ein sicher zu handhabendes Komplettpaket anzubieten, hat Infineon zusammen mit Wibu-Systems ein Paket geschnürt, das folgende Produkte zusammen bringt: Die DAVE-Entwicklungsumgebung von Infineon in der Version 4 steht als kostenfreies Entwicklungstool zum Download bereit. Die professionelle Eclipse-basierte Entwicklungsplattform begleitet und unterstützt den Anwender bei der Software-Entwicklung. Dafür stellt Infineon unter anderem ein umfangreiches peripherie- und anwendungsorientiertes Code-Repository bereit. Außerdem generiert DAVE passenden Code für die Peripherie der XMC-Microcontroller. Durch den komplementären Ansatz kann der Anwender den in DAVE konfigurierten und generierten C-Quellcode mit den kommerziellen 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 abgedeckt und der Anwender hat die maximalen Freiheitsgrade für eine effiziente plattformorientierte Software- und Produktentwicklung.

Die CodeMeter-Technologie von Wibu-Systems

»CodeMeter µEmbedded« ist ein Produkt, welches speziell für Field Programmable Gate Arrays (FPGAs) und Mikrocontroller entwickelt wurde. Damit können Software-Entwickler ihren Anwendungs-Code und ihr geistiges Eigentum auf FPGAs und in Mikrocontrollern gegen Reverse Engineering schützen und eine Lizenzkontrolle implementieren. Für größere Systeme wie beispielsweise speicherprogrammierbare Steuerungen (SPS) oder einen PC stehen mit »CodeMeter Embedded« und »CodeMeter Runtime« zwei lizenzkompatible Varianten zur Verfügung.

CodeMeter µEmbedded zeichnet sich durch einen extrem kleinen Speicherplatzbedarf von weniger als 80 KB aus.

Dies wurde erreicht, indem die Lösung auf den minimal notwendigen Funktionsumfang für die beschriebenen Use Cases reduziert wurde. Dabei sind die erzeugten Lizenzen kompatibel zwischen allen CodeMeter-Varianten. Die Lizenz wird dabei an eine eindeutige ID des Mikrocontrollers gebunden und bei der Produktion aktiviert. Nachträglich können per Dateiaustausch auch weitere Features freigeschaltet werden.

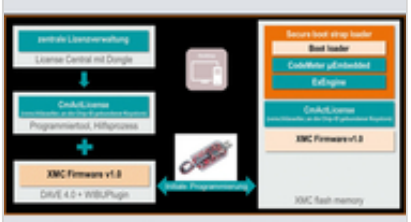
CodeMeter µEmbedded kann zusätzlich zum sicheren Speichern von symmetrischen und asymmetrischen Schlüsseln genutzt werden. Das Schlüsselmaterial liegt in einem geschützten Speicher und kann nur auf dem Gerät mit der passenden ID verwendet werden. Typische Anwendungen sind: Lizenzkontrolle von Geräten (Mikrocontroller und FPGAs), Überwachung der Produktionsmenge durch Lizenzierung der hergestellten Geräte sowie die sichere, verschlüsselte Übertragung des Anwendungscodes in das Gerät.

Kunden profitieren, indem sie Werkzeuge wie DAVE und die »CodeMeter Protection Suite«, ein Paket mit allen Tools, das die kryptographischen Operationen ausführt, sofort verwenden können. Ein neues Plug-In für die Entwicklungsumgebung DAVE bietet Entwicklern eine einfache grafische Oberfläche zur Konfiguration der XMC4000-Mikrocontroller und das Erzeugen der verschlüsselten Firmware-Updates oder Lizenzdateien.

Die Microcontroller-Familie XMC4000

Die XMC4000-Familie für Industrieanwendungen eignet sich besonders für die digitale Leistungswandlung, elektrische Antriebe und Sensoranwendungen. Alle XMC4000-Mikrocontroller sind für Temperaturen bis +125° C qualifiziert. Sie verwenden ARMs Cortex-M4-Prozessor mit DSP-Funktionalität, Gleitkomma-Einheit (FPU), Direct Memory Access (DMA) und Speicherschutzeinheit (MPU). Zur umfangreichen Peripherie gehören Analog/Mixed-Signal-Wandler, hochauflösende Timer/PWM-Kanäle und Schnittstellen für alle gängigen Industrie-Kommunikationsstandards. Die XMC4800-Serie mit On-Chip-Ethercat (Ethernet for Control Automation Technology) ermöglicht die einfache und kosteneffektive Umsetzung von Echtzeit-Ethernet-Kommunikation. Weitere Details zum XMC4000 finden sich unter [1 [1]].

Zurück zu den Use Cases und der praktischen Anwendung: Der vorbereitende Schritt erfolgt in der Produktentwicklung des Geräteherstellers (OEM). Hier wird mit den gewohnten Methoden ein Gerät zur Produktreife entwickelt. Aus DAVE heraus wird dabei eine Firmware v1.0 erzeugt und am Ende verschlüsselt mit Hilfe des DAVE-Plug-Ins, das das Verschlüsselungstool »ExProtector« von Wibu-Systems ansteuert.



© Wibu Systems

Bild 1: Initiale Programmierung des XMC4000

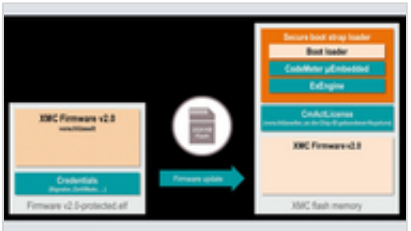
In der sicheren Umgebung der Produktion wird der XMC4000-Mikrocontroller zunächst mit einem mitgelieferten sicheren Bootloader betankt (**Bild 1**). Dieser verbleibt schreibgeschützt im Controller. Der nächste Schritt erzeugt eine Lizenzdatei, die an die ID des Controllers gebunden ist.

Die eigentliche Erzeugung der Lizenz erfolgt dann auf einem System des OEM, der damit die Kontrolle über die gebaute Stückzahl sowie deren Hardware-ID erhält. Erst jetzt wird die Firmware v1.0 auf das Gerät geladen. All das kann innerhalb eines automatisierten Programmierprozesses erfolgen, der sich technisch nicht von einem herkömmlichen Firmware-Downloadprozess in der Serienfertigung unterscheidet. Damit ist das Gerät fertig zur Auslieferung.

Use Case 1 – Firmware Update im Feld

Der Schutzanspruch ist hier, dass die Firmware nicht reverse engineered werden kann und das Gerät nur unveränderte Original-Firmware lädt. Dazu wird wie auch schon bei der Erstauslieferung die Firmware in DAVE

erzeugt, getestet und am Ende mit dem ExProtector automatisch signiert und verschlüsselt. Die Datei kann dann ohne weitere Sicherheitsvorkehrungen zum Kunden transferiert und dort aufgespielt werden. Das verwendete Medium ist dabei nicht von Belang, da es nicht möglich ist, die Firmware außerhalb des XMC4000 zu entschlüsseln oder zu verändern.



© Wibu Systems

Bild 2: Update der Firmware beim Kunden

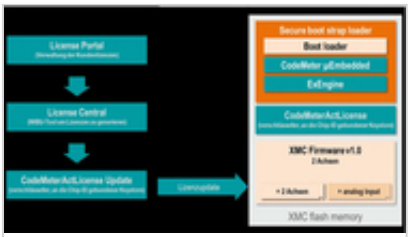
Jegliche Manipulation lässt die Signatur brechen und der Secure Boot Loader wird die Firmware nicht laden. Erst während des Ladeprozesses wird die Firmware entschlüsselt und im Speicher des XMC4000 abgelegt. Dies erfolgt flussgesteuert im Ladeprozess, sodass kein doppelter Speicher vorgehalten werden muss. Am Ende des Prozesses wird die Signatur geprüft. Ist sie korrekt, ist der Vorgang abgeschlossen; sollte sie gebrochen sein, wird die Firmware verworfen. Der Prozess ist in **Bild 2** dargestellt.

Use Case 2 – Funktions-Upgrade im Feld

Es soll eine universelle Firmware ausgeliefert werden, die bei Bedarf später durch zusätzliche Funktionen erweitert werden kann. Ein Austausch der Firmware soll dazu nicht nötig sein, um auch eventuell notwendige Test- und Zertifizierungsprozesse des Betreibers zu vermeiden. Es erfolgt nur ein Upgrade der Lizenzdatei.

Beim initialen Programmieren wurde die ID des Controllers idealerweise bereits in dem Tool »License Central« gespeichert. Ein Kunde kann jetzt über ein Lizenzportal beim Hersteller eine Funktionserweiterung erwerben, indem er die Seriennummer seines Controllers angibt.

Daraufhin wird eine verschlüsselte Lizenzdatei erzeugt, die nur auf dem einen Zielsystem lauffähig ist. Wird diese eingespielt, schaltet sie zum Beispiel weitere Achsen einer Steuerung frei, ohne dass dazu die Firmware ausgetauscht werden muss. **Bild 3** zeigt den Ablauf.



© Wibu Systems

Bild 3: Upgrade der Funktionalität beim Kunden

Mit CodeMeter µEmbedded erweitert Wibu-Systems sein Produktspektrum auf die Mikrocontroller-Ebene und bietet durchgängige Aufwärtskompatibilität bis hin zu den Serverlösungen. Infineon hat mit dem XMC4000 einen Controller am Markt, der »out of the Box« die wichtigsten Sicherheitsanforderungen aus Sicht des Geräteherstellers mitbringt. Das alles nicht als Funktion, die der Kunde erst selbst implementieren muss, sondern als Gesamtpaket, das auch das Lizenzmanagement und die Verteilung beinhaltet. Der Anwender konzentriert sich auf sein Kerngeschäft und nutzt die Sicherheit von CodeMeter wie einen Funktionsbaustein.

Über die Autoren:

Dirk Heinen arbeitet als Manager Product Marketing Mikrocontroller, Industrial and Multimarket bei der Infineon AG und Marco Blume arbeitet als Product/R&D Manager Embedded bei der Wibu-Systems AG.

ri

Links im Artikel

1. http://www.elektroniknet.de/halbleiter/sonstiges/artikel/85180/%20