publish industry verlag

E&E FASZINATION ELEKTRONIK

DAS INDUSTRIE-PORTAL INDUSTR.COM

GABE 2 | MÄRZ 2016 | 16. JAHRGANG | WWW.INDUSTR.COM/EUE | FACEBOOK.DE/EUE24.NET

KEINE GROSSE KUNST?

Hinter Security steckt mehr, als man denkt!

Angreifer erfolgreich abwehren

Embedded-Systeme benötigen einen wirkungsvollen Schutz, um Produktpiraten und Saboteure abzuwehren. Und da sie so vielfältig sind, muss auch ihr Schutz vielseitig sein und die Anforderungen hinsichtlich Robustheit, Schlankheit und Echtzeitfähigkeit im Automatisierungs- und Embedded-Bereich berücksichtigen. Die Codemeter-Technik ist ein Beispiel für eine solche Schutzlösung.

TEXT: Oliver Winzenried, Wibu-Systems **BILDER:** gunnarAssmy, iStock; Wibu-Systems

Geräte, Maschinen, Anlagen: Sie alle kommen ohne Embedded-Systeme nicht mehr aus. Diese verarbeiten Daten und Signale, steuern, regeln, überwachen oder kommunizieren in der vernetzten Produktion mit anderen Geräten. Die nötige Embedded-Hardware können Hersteller „von der Stange" kaufen; in Größe, Leistungsfähigkeit oder Robustheit passend zum jeweiligen Einsatzzweck.

Das Herz des Embedded-Systems ist aber die Embedded-Software, die der Hersteller dafür entwickelt – sie bestimmt letztlich, was das Gerät, die Maschine oder die Anlage kann. Damit wird die Embedded-Software zum verlockenden Ziel verschiedener Angreifer. Zum Beispiel wie den Produktpiraten, die am Know-how des Herstellers interessiert sind, das in der Embedded-Software enthalten ist. Oder den Saboteuren, die durch Manipulation der Embedded-Software versuchen, Geräte, Maschinen oder ganze Anlagen lahmzulegen oder zu schädigen. Laut dem „Cyber Security Report 2015" der Deutschen Telekom sind etwa neun von zehn Unternehmen mehr oder weniger häufig von Cyberangriffen betroffen, wobei die Häufigkeit im Vergleich zu den Vorjahren leicht angestiegen ist – und dies sind nur die Fälle, in denen die Angriffe auch erkannt wurden.

Zur Abwehr von Hackern, Produktpiraten und Saboteuren bietet das Karlsruher Unternehmen Wibu-Systems seine Schutzlösung Codemeter sowohl für die Entwickler klassischer PC-Software als auch für die Entwickler

von Embedded-Software an. Damit lassen sich Software und Daten hard- oder softwarebasiert mittels Verschlüsselung, Signaturen und Zertifikaten schützen, egal ob es sich dabei um Anwender- oder Embedded-Software, Betriebssystem-Images oder Maschinendaten handelt. Die besonderen Bedürfnisse und Anforderungen im Automatisierungs- und Embedded-Bereich erfüllt Codemeter mit seiner robusten Schutzhardware in unterschiedlichen Bauformen sowie einer Vielzahl unterstützter Plattformen wie Industrie-PCs, speicherprogrammierbare Steuerungen, programmierbare Logikbausteinen oder Mikrocontroller. Je nach Größe und Leistungsfähigkeit der Plattform kommen dabei die Varianten Runtime, Embedded oder µEmbedded zum Einsatz.

Codemeter ist aber nicht nur eine Schutz-, sondern auch eine Lizenzierungslösung. Flexible Lizenzmodelle wie Pay-per-Use oder Feature-on-Demand, die bislang eher in der Welt der Anwender- und Bürosoftware verbreitet waren, stehen damit auch den Herstellern im Maschinen- und Anlagenbau zur Verfügung.

Schutz für Embedded-Systeme

Codemeter Embedded ist eine schlanke Variante der Codemeter Runtime, die für den Betrieb auf Embedded-Systemen wie Windows Embedded, Linux Embedded, VxWorks, QNX oder der SoftSPS Codesys optimiert ist. Die Embedded-Software wird beim Hersteller verschlüsselt, signiert und als geschützte Version auf einem Gerät, einer Maschine oder einer Anlage an den Anwender ausgeliefert. Damit der Anwender das Gerät nutzen kann, bekommt er vom Hersteller eine passende Schutzhardware CmDongle oder eine Aktivierungsdatei CmActLicense, die den jeweils zur Laufzeit benötigten Teil der Software prüft und entschlüsselt.

Hersteller können die Verschlüsselungsfunktionen der Codemeter-API selbständig in ihre Embedded-Software einbauen oder ein Tool namens AxProtector for CmE nutzen. Dieses schützt die Software automatisch und sicher ohne Änderungen am Quellcode. Es ist als graphische Oberfläche verfügbar oder lässt sich als Kommandozeilenwerkzeug als Post-Build-Prozess in ein automatisches Build-System integrieren.

Noch schlanker als Codemeter Embedded ist die Variante µEmbedded. Die Lösung enthält den minimal nötigen Funktionsumfang und hat nur einen geringen Speicherplatzbedarf: 60 Kilobyte für die Schutzfunktionen oder etwa 80 Kilobyte, wenn Module der Embedded-Software lizenziert werden sollen. Lizenzen

Unterschiedliche Bauformen der Codemeter-Schutzhardware und der softwarebasierten Lösung

werden an die eindeutige ID des Logikbausteins oder des Mikrocontrollers gebunden und bei der Produktion aktiviert. Sie sind mit allen Codemeter-Varianten kompatibel. Beim Kauf weiterer Funktionen kann der Hersteller per Dateiaustausch diese für den Kunden auch nachträglich freischalten.

Codemeter µEmbedded legt darüber hinaus symmetrische und asymmetrische Schlüssel in einem geschützten Speicherbereich ab, der nur von Geräten mit passender ID nutzbar ist. Typische Anwendungsfälle sind: Lizenzkontrolle von Geräten, Überwachung von Produktionsmengen durch Lizenzierung der einzelnen hergestellten Geräte sowie die sichere, verschlüsselte Übertragung von Programmcode und Updates in ein Gerät.

Plattform Dave 4 mit Codemeter µEmbedded

Hersteller, die mit der Entwicklungsumgebung Dave 4 von Infineon arbeiten, können nun das kostenfreie Codemeter-Plug-In für Dave 4 für eigene Anwendungen nutzen: Die Eclipse-basierte Entwicklungsumgebung Dave begleitet und unterstützt den Anwender bei der Softwareentwicklung. Sie generiert den passenden Code für die XMC-Mikrocontroller; der Anwender kann vorhandene kommerzielle Third-Party-Tools für ARM nutzen, linken und auf den Mikrocontroller laden. Das Plug-In enthält die Codemeter-µEmbedded-Technik, darunter den ExProtector, um den Programmcode zu verschlüsseln und zu signieren. Eine einfache, grafische Oberfläche im Plug-In für Dave konfiguriert XMC4000-Mikrocontroller und erzeugt verschlüsselte Firmware-Updates oder Lizenzen.

Ein konkretes Anwendungsbeispiel: Ein Gerätehersteller entwickelt ein neues Gerät und bringt es auf den Markt. Zu Beginn wird aus Dave heraus eine Firmware v1.0 erzeugt, die am Ende mit Hilfe des neuen Plug-Ins und des ExProtectors automatisch verschlüsselt wird. Vor der Auslieferung wird der XMC4000-Mikrocontroller in der sicheren Umgebung des Geräteherstellers mit einem mitgelieferten, sicheren Bootloader ausgestattet, der schreibgeschützt im Controller gespeichert wird. Dann wird ein an die ID dieses Controllers gebundener Lizenzcontainer erstellt und schließlich die verschlüsselte Firmware v1.0 auf das Gerät geladen. Mit Hilfe eines automatisierten Programmierprozesses lassen sich die Geräte schnell programmieren; der Vorgang läuft technisch ähnlich ab wie ein herkömmlicher Firmwaredownloadprozess in der Serienfertigung.

Firmware-Update im Feld: Die neue Firmware v2.0 wird über Dave erzeugt, getestet und dann mit dem ExProtector automatisch signiert und verschlüsselt. Danach ist die Firmware gesichert und kann zum Kunden geschickt und dort aufgespielt werden, ohne dass Angreifer sie beim Transport oder beim Kunden mitlesen oder ändern können. Der Ladeprozess beim Kunden entschlüsselt die Firmware im Mikrocontroller, legt sie in dessen Speicher ab und prüft die Signatur. Ist diese korrekt, kann das Gerät starten, anderenfalls wird der Start abgebrochen. Funktions-Upgrade im Feld: Wurde das Gerät mit einer universellen Firmware ausgestattet, kann der Hersteller zusätzliche Funktionen nachträglich freischalten. Das separate Codemeter-Tool License Central speichert beim ersten Programmieren die ID des Controllers. Mit der Seriennummer seines Controllers kann ein Kunde über ein Lizenzportal des Herstellers weitere Funktionen in Form einer neuen Lizenzdatei erwerben. Die neue Lizenzdatei passt nur zu diesem Controller; ein Austausch der Firmware ist nicht nötig.

Für einen wirkungsvollen Schutz von Hardware ist es also wichtig, dass er nicht nur einmalig bei der Auslieferung gewährleistet ist, sondern auch im Betrieb, bei der Aktualisierung der Firmware oder der Freischaltung neu erworbener Funktionen. ❐