Der Spionage einen Dongle vorschieben

Ein Kit erleichtert Herstellern den Einstieg in den Schutz ihrer Embedded-Systems

Eingebettete Systeme erhöhen die Gefahr von Sabotage, Spionage oder Manipulation. Und mit der Industrie 4.0 wird die Bedeutung des Integritätsschutzes noch weiter wachsen, weil jede der vernetzten Maschinen vor Manipulation geschützt sein muss. Doch es gibt Abhilfe.

Ob Herzschrittmacher, Stickmaschinen oder Fertigungsstraßen – die meisten Geräte, Maschinen oder Anlagen werden heutzutage von eingebetteten Systemen und der zugehörigen Embedded-Software überwacht, geregelt oder gesteuert. Deren Flexibilität eröffnet den Herstellern neue Möglichkeiten: Mittels Software-Update können Fehler korrigiert oder der Betrieb einer Maschine optimiert werden. Sogar neue Funktionen können nachträglich hinzugefügt werden. Geschäftsmodelle wie Pay-per-Use oder Feature-on-Demand, die früher nur in der klassischen Software-Industrie möglich waren, können heute dank Embedded-Software auch in Geräten und im Maschinen- und Anlagenbau genutzt werden. Durch Freischaltung unterschiedlicher Funktionen einer Maschine kann der Kunde genau das nutzen, was er gekauft hat.

Cyber-Angriff in die Maschine

Mit den neuen Möglichkeiten kommen auch neue Gefahren: Die Embedded-Software enthält Firmen-Know-how – wertvolles Wissen, für das sich Produktpiraten und Wirtschaftsspione interessieren und das vor diesen geschützt werden muss. Darüber hinaus

Bild: Fotolia; Grafvision

kann eine Maschine oder Anlage durch Manipulation ihrer Embedded-Software leicht sabotiert werden, falls der Hersteller keine Vorsichtsmaßnahmen ergreift. Bei vernetzten Systemen muss der Angreifer dazu nicht einmal in die unmittelbare Nähe der anvisierten Maschine oder Anlage gelangen; ein Cyber-Angriff aus sicherer Entfernung kann genügen.

Schutz vor Manipulation

Um Maschinenherstellern mehr Schutz zu bietet, arbeitet Wibu-Systems, ein Anbieter von Softwareschutz- und Lizenzierungslösungen durch technisch präventiven Schutz, mit dem Unternehmen Wind River als Anbieter des Echtzeitbetriebssystems VxWork, zusammen. Als Ergebnis haben sie CodeMeter – dabei handelt es sich um einen CmStick, der sicherheitsrelevante Daten verschlüsselt auf dem geschützten Speicher eines integrierten Mikro-Chips speichert – in VxWorks integriert. Und zwar beginnend ab der Version 6.8 von VxWorks. Entwickler können sich damit nich nur vor Produktpiraterie schützen, die CodeMeter-Technologie ermöglicht zusätzlich den Schutz des Programmcodes vor Manipulation, das sichere Booten des VxWorks-Betriebssystems oder das sichere Betreiben einer Anwendung. Darüber hinaus kann der Hersteller mit CodeMeter verschiedene Lizenzmodelle wie Pay-per-Use oder Feature-on-Demand abbilden.

Um Herstellern und Entwicklern einen leichten Einstieg in diese Schutzfunktionen zu bieten, haben Wibu-Systems, Wind River und Emerson Network Powers gemeinsam das „Wind River Embedded Development Kit“ auf den Markt gebracht. Dieses enthält unter anderem vorbereitete CmDongles, also die Schutzhardware der CodeMeter-Technologie, von Wibu-Systems, die Entwicklungsumgebung von Wind River und ein NITX-315-Target-Board mit Intel Atom-CPU der E6xx-Serie von Emerson Network Powers sowie eine Schritt-für-Schritt-Anleitung zur Evaluation der Schutzfunktionen.

Wibu-Systems hat CodeMeter in die Wind-River-Workbench integriert und stellt verschiedene Werkzeuge zur Verschlüsselung bereit. Eines davon ist der AxProtector. Ohne Quellcodeänderung schützt er als Eclipse-Plug-in verschiedene Projekt-Typen wie VxWorks Image (VIP), Downloadable Kernel Modul (DKM) oder Real-Time-Process (RTP) und führt mit passendem CmDongle sowohl die Ver- und Entschlüsselung des VxWorks-Projekts als auch die Lizenzierung durch. Und das sind die Schutzstrategien und Parameter im AxProtector: Zum Schutz gegen Reverse-Engineering und zum Lizenzmanagement legt der Entwickler im Abschnitt License die entsprechenden Parameter für CodeMeter fest. Der Firm-Code wird von Wibu-Systems vorgegeben, während der Hersteller selbst Product-Code und Feature-Code festlegen kann. Der Kunde bekommt eine passende Lizenz im CmDongle, damit der Code im Zielsystem entschlüsselt und die Anwendung ausgeführt werden kann. Zum Schutz vor Manipulation mittels Codesignaturen wird im Abschnitt Signature festgelegt, wo die Schlüsselquelle für den privaten Schlüssel zur Codesignatur gespeichert ist. Dies ist üblicherweise ein Eintrag im CmDongle beim Entwickler. Weiterhin wird das Zertifikat angegeben, das benötigt wird, um im Zielsystem die Signatur zu prüfen.

Leichter Einstieg in den Know-how-Schutz: Das „Wind River Embedded Development Kit“ enthält drei CodeMeter-Komponenten von Wibu-Systems.

Durch ständige Weiterentwicklung den Spionen voraus

Damit das Schutzkonzept von CodeMeter greift, ist es notwendig, dass der Entwickler den Standard-VxWorks-Loader durch den CodeMeter-VxWorks-Loader ersetzt. Nur dann stehen die Sicherheits- und Lizenzmanagementfunktionen zur Verfügung und korrekt signierte Projekte werden auf dem Zielsystem entschlüsselt und ausgeführt, während nicht passend signierte Projekte gar nicht erst starten. Wird das Zielsystem gestartet, überprüft der CodeMeter-VxWorks-Loader das Laden des Betriebssystem-Images, danach das Laden der Anwendung, sofern die Codesignatur korrekt ist, und entschlüsselt anschließend den Programmcode, vorausgesetzt, die passende Lizenz ist vorhanden. *aru* ■

Autor Oliver Winzenried, Wibu-Systems

***ke NEXT* Crossmedia**

Ein interessantes Video mit einer Kurzpräsentation finden Sie unter www.konstruktion.de/22969

Oder Sie nutzen den nebenstehenden QR-Code mit Ihrem internetfähigen Handy. Einfach abfotografieren und lossurfen. Infos zur Nutzung des QR-Codes finden Sie unter www.konstruktion.de/qrcode

ke NEXT hakt nach

Eine Frage an Oliver Winzenried, Vorstand von Wibu-Systems und Vorsitzender des Vorstands der VDMA-Arbeitsgemeinschaft Produkt- und Know-how-Schutz

Herr Winzenried, angenommen, jemand, der überhaupt keine Personal- und Zeit-Ressourcen zur Verfügung hat, kommt zu Ihnen und fragt Sie danach, was die wichtigste Schutzmaßnahme wäre, die er treffen sollte. Was würden Sie ihm antworten?

Er soll die Embedded-Software in seinem Produkt schützen. Mit technisch präventiven Lösungen wie CodeMeter sowie professioneller Beratung ist CodeMeter mit minimalem Aufwand implementiert. Dann ist das Know-how geschützt und die unveränderte Ausführung der Software sichergestellt. Sicherheit kostet etwas Geld – Nicht-Sicherheit kostet jedoch viel mehr! *aru*

Weiß, wie man Wissen schützt: Oliver Winzenried