Security in Embedded-Systemen durch Integritätsschutz

Ausgabe: Embedded Design IV 2015, 03.06.2015

Die Online-Ausgabe von 'Die Welt' berichtete am 26.02.2015 über Cyberangriffe auf Infrastrukturen und Industrieanlagen: Täglich verzeichnen Großkonzerne 50-100 Millionen Eindringversuche. Welche Schäden entstehen, zeigt der Angriff auf die Steuerung eines Hochofens in Deutschland. Die Anlage konnte danach nicht geregelt herunter gefahren werden, ein Schaden in Millionenhöhe entstand. Wie können sich Hersteller vor Cyberangriffen schützen? Der klassische Schutz wie Werkschutz oder Firewall sind ungeeignet zum Schutz eines Embedded-Systems in Maschinen, Anlagen oder Geräten. Hersteller müssen ihr Know-how, das in Embedded-Systemen in Form von Programmcode, benötigte Produktionsdaten und digitalen Maschinentagebüchern steckt, schützen und Manipulationen und Sabotagen abwehren.

Mit CodeMeter bietet Wibu-Systems eine technisch-präventive Lösung zum Softwareschutz, zur Lizenzierung und zum Integritätsschutz. Der SmartCard-Chip in der Schutzhardware CmDongle der CodeMeter-Technologie verschlüsselt die Embedded-Software, speichert Berechtigungen, auch die Signaturen und Zertifikate, und authentifiziert einzelne, berechtigte Akteure. Dies sorgt bei der intelligenten Produktion nach Industrie 4.0 für Security: Nur zugelassene Sensoren, Geräte oder Maschinen kommunizieren miteinander und nur zugelassene Personen können durch Aufstecken ihres CmDongles einen Produktionsauftrag starten. CodeMeter funktioniert auf gängigen Embedded-Systemen wie Windows Embedded oder Embedded Linux, auf Echtzeitbetriebssystemen wie VxWorks oder auf SPS-Steuerungen wie Codesys, Bernecker & Rainer oder Rockwell Automation.

Integritätsschutz mit VxWorks

Um Manipulationen und Veränderungen zu verhindern, wird ein System über signierte Programmcodes als vertrauenswürdig eingestuft. Die Signatur wird gegen eine Zertifikatskette geprüft, sodass das System erkennt: der Programmcode kommt von einem berechtigten Herausgeber und es wurde kein Schadcode untergeschoben. Gemeinsam haben Wind River und Wibu-Systems ihre Produkte VxWorks 7 und CodeMeter so verknüpft, dass Integrität und Know-how eines VxWorks-Projekts geschützt sind - von der Entwicklung bis zum Betrieb. Einzelne Softwarekomponenten wie Real-Time Processes (RTPs), Downloadable Kernel Modules (DKMs) oder VxWorks-Images (VIPs) werden beim Integritätsschutz durch kryptographische Signaturen und Zertifikate geschützt. Entwickler bekommen vom Hersteller Zertifikate, um ihren Programmcode zu signieren. Dafür nutzt der Hersteller eine eigene Zertifizierungsstelle, die von CodeMeter zur Verfügung gestellt wird. Mit der Secure-Boot-Funktion, die Plattformen mit UEFI (Nachfolger des alten BIOS) unterstützt, ist die Integrität des Gesamtsystems lückenlos gewährleistet. Die folgenden Schritte werden dabei durchlaufen: zuerst wird der Bootloader überprüft, dann wird das signierte Firmware-Image gestartet und von dort aus werden nur signierte Programmteile ausgeführt. Manipuliert ein Hacker ein Programmteil oder versucht er, Fremdsoftware aufzuspielen, dann erkennt der Schutz eine ungültige Signatur und das Programm wird nicht gestartet oder abgebrochen. Das UEFI ist der sichere Anker, an dem die ganze Sicherheitskette für Secure Boot hängt.

Starter-Kit für Raspberry Pi

Mit dem Starter-Kit für Raspberry Pi können Hersteller einfach und mit wenigen Klicks den Schutz, die Lizenzierung und das sichere Booten (Secure Boot) von Embedded-Systemen trainieren und ausprobieren. Die Ergebnisse mit dem Starter-Kit helfen dem Entwickler, das Schutzkonzept vom Raspberry Pi auf das Zielsystem zu übertragen. Der CodeMeter Embedded Driver als auch die Werkzeuge AxProtector und IxProtector schützen Embedded-Systeme.

Fazit

Zu beobachten ist: die Angreifer sind Profis und sehen in schlecht oder gar ungeschützten Maschinen oder Anlagen ein leichtes Ziel. Sind sie erst einmal ins Produktionsnetzwerk eingedrungen, können sie absichtlich oder unabsichtlich Schäden in unkalkulierbarem Ausmaß anrichten - das zeigt auch der Vorfall mit dem Hochofen. Damit die Hersteller einfach und wirkungsvoll ihren Programmcode schützen können, bietet CodeMeter bereits ausgefeilte Schutzkonzepte für das Echtzeitbetriebssystem VxWorks und für SPSen an, ohne dass diese Kryptographie-Fachleute beschäftigen müssen. Durch weitere Kooperationen will Wibu-Systems sein Portfolio so erweitern, damit Hersteller die Schutzmöglichkeiten von CodeMeter in bisher nicht unterstützen Betriebssystemen und SPSen einsetzen können.

www.wibu.de

Fotostrecke

SPS MAGAZIN IT Production VISION GD i-need.de SCHALTSCHRANKBAU

Datenschutz Rechtliche Hinweise Impressum Kontakt

© 2012 TeDo-Verlag GmbH. Alle Rechte vorbehalten.