Schutz von Embedded-Software und Firmware

Beim IoT und Industrie 4.0 sind Geräte, Maschinen und Anlagen miteinander vernetzt, sodass sie sich austauschen können und dabei Daten und Signale verarbeiten, diese steuern, regeln und überwachen. Diese Tätigkeiten übernimmt die Embedded-Software, die heutzutage so viel Know-how enthält, dass sich Wirtschaftsspione, Produktpiraten oder Cyber-Angreifer dafür interessieren. Um erfolgreich zu sein, gehen Hersteller dazu über, diese Embedded-Software und das dazugehörige Know-how zu schützen.
Wibu-Systems unterstützt Hersteller mit Codemeter, einer technisch-präventiven Lösung, beim Schutz klassischer PC-Software, Embedded-Software und Know-how sowie bei der Lizenzierung von Software, damit Hacker, Produktpiraten und Saboteure abgewehrt werden können. Zusätzlich erfüllt Codemeter die unterschiedlichen Sicherheitsbedürfnisse der Industrie, einschließlich moderner Security für Industrie 4.0 und das Internet der Dinge.
Grundlage von Codemeter ist die Ver- und Entschlüsselung der Embedded-Software, das sichere Speichern der notwendigen Schlüssel und der Schutz von Programmcode vor Manipulation durch elektronisch signierten Code und Prüfung gegen eine Zertifikatskette. Die Schlüssel liegen als notwendige Einträge im sicheren SmartCard-Chip der Schutzhardware ‚CmDongle' oder in der Aktivierungsdatei ‚CmActLicense'. Codemeter benutzt moderne und sichere Algorithmen wie Advanced Encryption Standard (AES) für symmetrische Verschlüsselung und Elliptic Curve Cryptography (ECC) für asymmetrische Operationen wie Verschlüsselung und Signatur. Die zur Verschlüsselung benötigten Werkzeuge sind in der ‚Protection Suite' als grafische Oberfläche verfügbar oder können per Kommandozeilentool als Post-Build-Prozess in ein automatisches Build-System integriert werden. Zusätzlich zum automatischen Schutz mit Protection Suite ist eine Integration mit der Programmierschnittstelle CodeMeter API in die geschützte Software möglich. Abhängig von der Zielplattform können Hersteller zwischen den verschiedenen Laufzeitkomponenten wählen: für klassische Software auf PCs ‚Codemeter Runtime', für Embedded-Software ‚Codemeter Embedded' oder für Mikrocontroller ‚Codemeter µEmbedded'.

Codemeter Runtime

Entwickelt ein Hersteller Server- oder Desktop-Software, dann benutzt er Codemeter Runtime. Dieses Paket läuft auf gängigen Betriebssystemen wie Windows, Linux oder OS X und unterstützt Laufzeitumgebungen wie .NET und Java.

Codemeter Embedded

Speziell für Embedded-Systeme wie Windows Embedded, Linux Embedded, VxWorks, Android und QNX, sowie für Speicherprogrammierbare Steuerungen (SPS) stellt Wibu-Systems Codemeter Embedded als schlanke und modulare Variante von Codemeter Runtime zur Verfügung.

Datum: 20. April 2016

Firma: WIBU-Systems AG

Autoren:

Themen: Embedded Design IV 2016, embedded Security, Fachartikel

Webseite: www.wibu.de

Downloads:

Elektrobit ernennt Andreas Heim zum Executive Vice President Operations

Andreas Heim ist seit dem 1. Juni 2016 als Executive Vice President Operations bei Elektrobit tätig. In dieser Funktion leitet er das operative Geschäft für alle Entwicklungsbereiche (Navigation, Connected Car, Driver Assistance, HMI, Software Integration and Services sowie Car Infrastructure) bei EB.

Kontron berichtet über erste Fortschritte bei der Umsetzung der neuen Strategie

Die Kontron AG hat bei der Hauptversammlung Anfang Juni in Augsburg das Geschäftsjahr 2015 kommentiert und über die ersten Schritte zur Umsetzung der strategischen Neuausrichtung berichtet. Das Unternehmen hat nach einer im Oktober letzten Jahres durchgeführten Prognosekorrektur alle gesetzten Ziele für das Geschäftsjahr 2015 erreicht. Der Vorstandsvorsitzende Rolf Schwirz betonte, dass Kontron seit seiner Amtsübernahme Anfang 2013 in strategisch wichtigen Kernbereichen solide gewachsen und die Profitabilität deutlich gestiegen ist. Außerdem konnte der CEO von ersten Umsetzungserfolgen der im Mai 2015 angekündigten strategischen Neuausrichtung berichten. Ein Schwerpunkt dabei ist die Positionierung des Unternehmens als Middleware- und Hardware-Anbieter, um die langfristigen Trends 'Internet of Things' und 'Industrie 4.0' zu nutzen. Dabei ist Kontron mit der Entwicklung einer ersten IoT-Plattform einen entscheidenden Schritt vorangekommen.

VDE|DKE stellt den Geschäftsführer des

Schutz von Embedded-Software und Firmware

Codemeter µEmbedded

Codemeter µEmbedded ist die Codemeter-Variante, welche speziell als extrem schlanke Version für Mikrocontroller entwickelt wurde. Die Lösung ist auf den minimal notwendigen Funktionsumfang reduziert und hat mit einer Größe ab 60kB für die Schutzfunktionen oder etwa 80kB für die Lizenzierung von Embedded-Software nur einen geringen Speicherplatzbedarf.

Entwicklungsumgebung Dave 4 von Infineon

Hersteller, die mit der Eclipse-basierten Entwicklungsumgebung Dave 4 von Infineon ihre Software entwickeln, können ab sofort das kostenfreie Codemeter Plug-in, das in Dave 4 integriert wurde, für eigene Anwendungen nutzen. Dave 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-Technologie von Wibu-Systems, darunter den ‚Exprotector', sodass der Entwickler Programmcode verschlüsselt und signiert. Eine einfache, grafische Oberfläche im neuen Plug-in konfiguriert XMC4000-Mikrocontroller und erzeugt verschlüsselte Firmware-Updates oder Lizenzen.

Schutz von Firmware und sichere Firmware-Updates

Beispielsweise entwickelt ein Gerätehersteller ein neues Gerät und bringt es auf den Markt. Am Anfang wird aus Dave heraus eine Firmware v1.0 erzeugt, die dann mithilfe 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. Mithilfe eines automatisierten Programmierprozesses können die Geräte schnell programmiert werden; der Vorgang läuft technisch ähnlich ab wie ein herkömmlicher Firmware-Downloadprozess in der Serienfertigung.

Datum: 20. April 2016

Firma: WIBU-Systems AG

Autoren:

Themen: Embedded Design IV 2016, embedded Security, Fachartikel

Webseite: www.wibu.de

Downloads:

Elektrobit ernennt Andreas Heim zum Executive Vice President Operations

Andreas Heim ist seit dem 1. Juni 2016 als Executive Vice President Operations bei Elektrobit tätig. In dieser Funktion leitet er das operative Geschäft für alle Entwicklungsbereiche (Navigation, Connected Car, Driver Assistance, HMI, Software Integration and Services sowie Car Infrastructure) bei EB.

Kontron berichtet über erste Fortschritte bei der Umsetzung der neuen Strategie

Die Kontron AG hat bei der Hauptversammlung Anfang Juni in Augsburg das Geschäftsjahr 2015 kommentiert und über die ersten Schritte zur Umsetzung der strategischen Neuausrichtung berichtet. Das Unternehmen hat nach einer im Oktober letzten Jahres durchgeführten Prognosekorrektur alle gesetzten Ziele für das Geschäftsjahr 2015 erreicht. Der Vorstandsvorsitzende Rolf Schwirz betonte, dass Kontron seit seiner Amtsübernahme Anfang 2013 in strategisch wichtigen Kernbereichen solide gewachsen und die Profitabilität deutlich gestiegen ist. Außerdem konnte der CEO von ersten Umsetzungserfolgen der im Mai 2015 angekündigten strategischen Neuausrichtung berichten. Ein Schwerpunkt dabei ist die Positionierung des Unternehmens als Middleware- und Hardware-Anbieter, um die langfristigen Trends 'Internet of Things' und 'Industrie 4.0' zu nutzen. Dabei ist Kontron mit der Entwicklung einer ersten IoT-Plattform einen entscheidenden Schritt vorangekommen.

VDE|DKE stellt den Geschäftsführer des

Schutz von Embedded-Software und Firmware

Beispiel – 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.

Beispiel – 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.

Fazit

Embedded-Systeme, die vor allem für die intelligente Produktion und für das Internet der Dinge eingesetzt werden, benötigen einen besonderen Schutz. Wichtig ist, dass das gesamte Schutzkonzept den Schutz vor Nachbau und vor Manipulation berücksichtigt und beim Design der Hardware beginnt und bis zur Anwendung greift. Das bedeutet, der Schutz greift nicht nur einmalig bei der Auslieferung, sondern auch im Betrieb, bei der Aktualisierung der Firmware oder der Freischaltung neu erworbener Funktionen. CodeMeter als flexibles und vielseitiges Schutzkonzept erfüllt die unterschiedlichen Anforderungen, auch hinsichtlich Robustheit, Schlankheit und Echtzeitfähigkeit der Automatisierungsindustrie oder beliebigen industriellen Bereichen. Darüber hinaus können Hersteller mit CodeMeter flexible Lizenzmodelle für Embedded-Systeme aufsetzen und Zusatzfunktionen verkaufen, was weitere Umsätze generiert.

Datum: 20. April 2016

Firma: WIBU-Systems AG

Autoren:

Themen: Embedded Design IV 2016, embedded Security, Fachartikel

Webseite: www.wibu.de

Downloads:

Elektrobit ernennt Andreas Heim zum Executive Vice President Operations

Andreas Heim ist seit dem 1. Juni 2016 als Executive Vice President Operations bei Elektrobit tätig. In dieser Funktion leitet er das operative Geschäft für alle Entwicklungsbereiche (Navigation, Connected Car, Driver Assistance, HMI, Software Integration and Services sowie Car Infrastructure) bei EB.

Kontron berichtet über erste Fortschritte bei der Umsetzung der neuen Strategie

Die Kontron AG hat bei der Hauptversammlung Anfang Juni in Augsburg das Geschäftsjahr 2015 kommentiert und über die ersten Schritte zur Umsetzung der strategischen Neuausrichtung berichtet. Das Unternehmen hat nach einer im Oktober letzten Jahres durchgeführten Prognosekorrektur alle gesetzten Ziele für das Geschäftsjahr 2015 erreicht. Der Vorstandsvorsitzende Rolf Schwirz betonte, dass Kontron seit seiner Amtsübernahme Anfang 2013 in strategisch wichtigen Kernbereichen solide gewachsen und die Profitabilität deutlich gestiegen ist. Außerdem konnte der CEO von ersten Umsetzungserfolgen der im Mai 2015 angekündigten strategischen Neuausrichtung berichten. Ein Schwerpunkt dabei ist die Positionierung des Unternehmens als Middleware- und Hardware-Anbieter, um die langfristigen Trends 'Internet of Things' und 'Industrie 4.0' zu nutzen. Dabei ist Kontron mit der Entwicklung einer ersten IoT-Plattform einen entscheidenden Schritt vorangekommen.

VDE|DKE stellt den Geschäftsführer des