Unified Automation

Partner Solution

OPC-UA-Sicherheitserweiterung von Wibu-Systems

Höhere Sicherheit und eine vielseitige Softwarelizenzierung für die M2M-Kommunikation

Hintergrund

Der OPC-UA-Standard ist ein plattformunabhängiges Kommunikationsframework, das in verschiedensten Industriebereichen adaptiert wird. Sicherheit ist beim Informationsaustausch zwischen Systemen von entscheidender Bedeutung. Ein leistungsfähiges, gestaffeltes Sicherheitskonzept ist ein integraler Bestandteil und OPC UA definiert Sicherheit sowohl auf der Anwendungs- als auch auf der Transportebene. Zusätzlich zu SSL (Secure Sockets Layer) und TLS (Transport Layer Security), die in den HTTPS-Standards aktueller Webapplikationen genutzt werden, definiert OPC die UA-Secure-Conversation-Schicht. Es werden vorab ausgehandelte Sicherheitsprofile verwendet und es wird ein abgesicherter Ende-zu-Ende-Kommunikationskanal zwischen Client und Server aufgebaut. Applikationen und Benutzer identifizieren sich mit Hilfe von X.509-Zertifikaten. Hierbei wird das aus PKI bekannte Trust-Management, wie z. B. Listen von vertrauenswürdigen und zurückgezogenen Zertifikaten, genutzt. Es werden einerseits Vertraulichkeit und Unversehrtheit der Daten und andererseits die Authentifizierung von Applikationen und Anwendern sichergestellt.

Die OPC UA SDKs/Toolkits von Unified Automation unterstützen die definierten Sicherheitsprofile und Konfigurationen vollständig und stellen zudem APIs zum Erstellen, Ablegen und Validieren von Zertifikaten und vertrauenswürdigen Speichern zur Verfügung. Die Verwaltung von Zertifikaten und Trusts liegt außerhalb des OPC-UA-Standards und muss anwendungsspezifisch außerhalb des SDKs/Toolkits gelöst werden. Der Gerätehersteller muss hierbei den jeweiligen Anwendungsfall des Geräts und die vorhandene Infrastruktur berücksichtigen.

In einem gemeinsamen Projekt haben Wibu-Systems und Unified Automation eine Lösung entwickelt, die die Sicherheitsanforderungen von OPC UA mit einem einfach zu bedienenden PKI-Management und der sicheren Verwahrung von Geheimnissen kombiniert. Gerätehersteller können plattformübergreifend Schutz, Lizenzierung und Managementlösung in das OPC UA SDK integrieren.

Hersteller, die ihre Automatisierungssoftware auf dem OPC-UA-Standard basierend entwickeln, können ihre Maschinendaten schützen und ebenso ihr Geschäftsmodell abbilden. In einer Zeit, in der sich geistiges Eigentum in der Wertschöpfungskette von Hardware auf Software verschiebt, werden funktionalitäts-, laufzeit-, versions- oder pay-per-use-basierte Modelle den Marktanteil erhöhen und regelmäßige Einnahmen erzeugen.

Aufgabenstellung

Werden kryptografische Schlüssel und sensible Konfigurationsdateien im Dateisystem gespeichert, z. B. private RSA-Schlüssel und Trust-Listen, besteht die Gefahr von Diebstahl und Manipulation, insbesondere in einer Welt, in der cyberphysische Systeme mit offenen Netzwerken verbunden sind. Unter verschiedenen Methoden, ein System zu kompromittieren, benutzen Hacker Schwachstellen in Betriebssystemen, um Trojaner einzuschleusen und Zugang zum Dateisystem zu erlangen. Der Schutz von Geheimnissen und die Vereinfachung der Konfiguration von Vertrauensbeziehungen und Zertifikats-Rollout-Szenarien sind die größten Herausforderungen und zugleich die ausschlaggebenden Aspekte für ein hohes Schutzniveau.

CodeMeter Embedded von Wibu-Systems, eine modulare Laufzeitumgebung für eingebettete Systeme, z. B. Linux Embedded, VxWorks, QNX und Android, war der ideale Kandidat für die Integration in das ANSI-C-basierte OPC UA SDK.

Lösung

Die Sicherheitslösungen von Wibu-Systems wurden in das SDK integriert, ohne die Nutzerschnittstelle für Kunden zu verändern oder zu verkomplizieren. Die Entwickler können zwischen einer reinen Softwarelösung, die OpenSSL nutzt, und einer Hardwarelösung mit dem nahtlos integrierten CodeMeter Embedded wählen. Die OPC UA Security Extensions von Wibu-Systems bestehen aus einer Softwarebibliothek, der Engine von CodeMeter Embedded und Sicherungshardware. Die Speicherhardware, typischerweise USB-Dongles (aber ebenso ASICs oder sichere Speicherkarten im SD-, microSD-, CF- oder CFast-Kartenformat), sind mit den OPC-UA-Anwendungen des Endanwenders verbunden und bilden die sicheren Speicherorte für Kodierungsschlüssel und Softwarelizenzberechtigungsdetails. Zusätzlich zur sicheren Aufbewahrung bietet Wibu-Systems vereinfachte Konfigurations- und Verwaltungsfunktionalitäten.

Unified Automation GmbH
O'Brien Str. 2 • 91126 Schwabach • Germany
Tel: +49 911 495 25000 • Fax: +49 911 495 25009
info@unifiedautomation.com • www.unifiedautomation.com

OPC-UA-Hintergrund

CodeMeter fügt eine sichere Schlüsselverwahrung in einem Common-Criteria-EAL5+-zertifizierten Sicherheitscontroller hinzu. Symmetrische und asymmetrische Kryptografie werden innerhalb der Sicherungshardware ausgeführt, wodurch Kodierungsschlüssel und Lizenzinformationen vollständig geschützt bleiben. Container mit eingebettem Smartcardchip nutzen ihre zusätzlichen Verschlüsselungs- und Zertifizierungsbestandteile und sind in der Lage, Side-Channel- und Differential-Power-Analysis-Attacken (DPA) zu widerstehen. Diese proprietäre Technologie arbeitet automatisch völlig ohne Benutzereingriff und ist volltransparent für die OPC-UA-Schnittstellen. Mit einer zusätzlichen Softwarekomponente zur Integration in die OPC-UA-Serversoftware kann der Inhalt der Dongles auch ferngewartet werden: Softwareupdates und -upgrades können einfach und sicher verteilt werden und Lizenzen können vom Administrator erweitert, zurückgezogen und übertragen werden. Die Verwaltung und das Rollout von Zertifikaten sowie die Freigabe lizenzierter Produktfunktionalitäten können über die gleiche, schon vorhandene Wibu-Systems-Infrastruktur realisiert werden.

„Der Schutz von Geräte-Know-how in OPC Unified Architecture ist mit dem SDK von Unified Automation erweitert durch CodeMeter Embedded von Wibu-Systems einfacher, schneller und sicherer geworden“, sagt Dr. Sören Finster, Senior Software Developer bei Wibu-Systems.

Eingesetzte Produkte von Unified Automation

„Die Investition in sichere Lizenzierung bedeutet wirtschaftliche Stabilität, gute kommerzielle Reputation und es eröffnet neue Wertschöpfungsoptionen“, sagt Oliver Winzenried, Vorstand und Mitgründer von Wibu-Systems.

Die OPC UA SDKs von Unified Automation enthalten abstrakte Krypto- und PKI-Schnittstellen. Der Standard-Auslieferungszustand des SDKs erwartet, dass die Open-Source-Bibliothek OpenSSL installiert ist. Abgesehen von dieser reinen Softwarelösung bietet die Wibu-Systems Security Extension eine weitere Möglichkeit. Die Option einer Kombination aus Hardware-Dongle mit Crypto-Chip erhöht die Sicherheit und entlastet den Hauptprozessor. Wenn Gerätehersteller das OPC UA SDK von Unified Automation erwerben, können sie automatisch von den vollintegrierten Fähigkeiten des CodeMeter Embedded von Wibu-Systems profitieren. Das Paket an Sicherheitsfunktionalitäten ist für das ANSI-C-basierte und das High Perfomance OPC UA SDK erhältlich. Die Kombination aus sicherer Schlüsselverwahrung für Endpunkt-Zertifikate, private Schlüssel und Vertrauenslisten und zusätzlich das vielseitige Lizenz-Lebenszyklus-Management öffnet eine große Anzahl neuer Geschäftsmöglichkeiten für Anbieter von Automatisierungslösungen.

Über WIBU-SYSTEMS AG

WIBU-SYSTEMS AG ist ein innovativer Technologieführer im Bereich Sicherheit im weltweiten Markt für Softwarelizenzierung. Im Rahmen des Ziels, die sicherste, einzigartigste und vielseitigste Technologie anzubieten, hat Wibu-Systems CodeMeter® entwickelt, eine umfangreiche und ausgezeichnete Reihe von hardware- und softwarebasierten Lösungen für Computer, eingebettete Systeme, Mobilgeräte, SPSen und Mikrocontrollern, die international patentierte Prozesse zum Schutz der Integrität digitaler Ressourcen enthalten. Softwareanbieter und Hersteller intelligenter Geräte können das geistige Eigentum in ihren Anwendungen gegen unerlaubte oder missbräuchliche Nutzung, Reverse-Engineering und manipulative Eingriffe absichern und zudem neue digitale Geschäftsmodelle generieren, die vollständig in ERP-, CRM- und E-Commerce-Plattformen integrierbar sind.

Über Unified Automation

Als führender Anbieter von OPC-UA-Software vertreibt Unified Automation UA-fähige Produkte, Cross-Plattform-Toolkits und Entwicklerframeworks in unterschiedlichen Programmiersprachen (ANSI C, C++, JAVA und C# .NET) sowie für verschiedene Plattformen (Windows, Linux, VxWorks, QNX, RTOS, und viele Embedded-Betriebssysteme). Der Zielmarkt der OPC-UA-Produkte reicht von Herstellern eingebetteter Geräte bis hin zu Entwicklern von Unternehmensanwendungen.

Unified Automation sieht sich als Technologieanbieter im Bereich OPC-basierter Kommunikation. Die Software Development Kits (SDKs) werden weltweit als Basis für OPC-UA-Produkte nahezu aller großen und vieler kleiner Automatisierungshersteller eingesetzt.

Unified Automation GmbH
O‘Brien Str. 2 • 91126 Schwabach • Germany
Tel: +49 911 495 25000 • Fax: +49 911 495 25009
info@unifiedautomation.com • www.unifiedautomation.com