IT-Security

★★★★★ 1 BEWERTUNG

RAUBKOPIEN VERMEIDEN

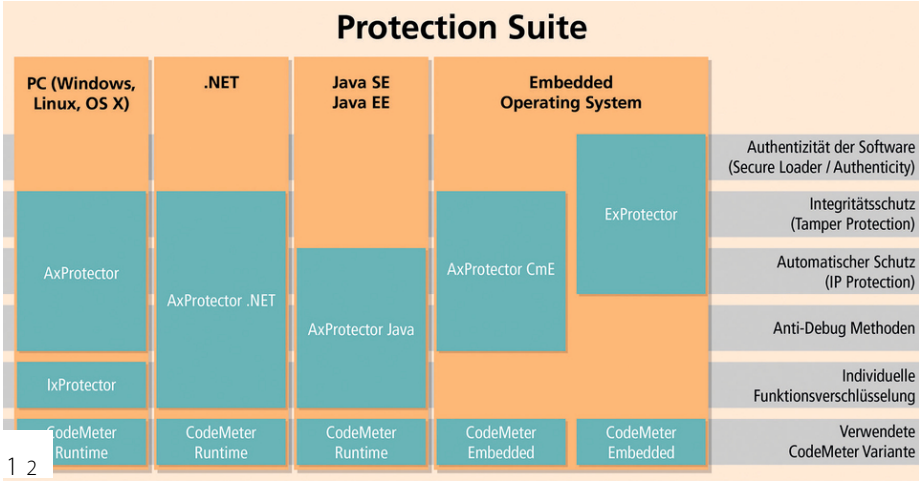
TEXT: OLIVER WINZENRIED, WIBU-SYSTEMS

TAGS EMBEDDED-SYSTEME & BAUGRUPPEN EMBEDDED-PC BETRIEBSSYSTEME WIBU-SYSTEMS AG FÄLSCHUNGEN RAUBKOPIEN SICHERHEIT SCHUTZ IT-SECURITY CODEMETER AXPROTECTOR

Wibu-Systems, Spezialist für IT-Security, hat für Software-Hersteller die Schutztechnologie CodeMeter entwickelt. Das Schutzkonzept dahinter soll sich intuitiv erfassen lassen. Außerdem wird das Tool CodeMeter Protection Suite regelmäßig aktualisiert und lässt sich für verschiedene Plattformen einsetzen: vom Server und PC bis zu Embedded-Systemen. In nur kurzer Zeit können Softwarehersteller laut Anbieter diese Suite bedienen und die für sie wichtigen Schutzmaßnahmen integrieren, ohne den Quellcode ihrer Programme ändern zu müssen. Aktuelle Anti-Debugging- und Anti-Reverse-Engineering-Maßnahmen werden automatisch integriert. Alternativ haben Softwareentwickler die Möglichkeit, flexibel aus ihrem Quellcode Funktionen des CodeMeter-API aufzurufen.

CodeMeter Protection Suite vereint die Verschlüsselungstools AxProtector und IxProtector für nativen Programmcode sowie AxProtector .NET für .NET- und AxProtector Java für Java-Anwendungen. Auch AxProtector CmE und ExProtector für eingebundene Geräte der Embedded-Welt gehören dazu: Hersteller sollen immer passendes Werkzeug zur Hand haben.

BILDERGALERIE



1 2

Übersicht zur CodeMeter Protection Suite

Bild: Wibu Systems

Alle AxProtectoren erzeugen eine Art geschütztes selbst entpackendes Archiv von der Software, das unkompliziert startet, wenn eine passende Lizenz, beispielsweise durch Aktivierung oder einen Dongle, auf dem Zielsystem vorhanden ist. Das Betriebssystem muss nicht angepasst werden. Anders der ExProtector: Er erzeugt ein geschütztes Programm, das vom Betriebssystem beim Laden entschlüsselt wird, wenn die passende Lizenz vorhanden ist. Dazu muss der Lademechanismus des Betriebssystems angepasst sein, wie es standardmäßig bei VxWorks sowie einigen verbreiteten SPS-Steuerungssystemen der Fall ist.

Native Anwendungen

Native Anwendungen für Windows, OS X oder Linux, die beispielsweise in C++ oder Delphi entstanden, lassen sich mit dem AxProtector schützen. Dieser verschlüsselt den Binärcode in großen Teilen automatisch, Sprünge werden umgebogen oder ersetzt sowie Sicherheits- und Bibliotheksfunktionen hinzugefügt. Diese verschlüsselte Datei oder Bibliothek enthält eine Schutzschale, die die komplette Software umgibt, was sie für Angreifer unbrauchbar macht. Nur mit passender Lizenz in der Schutzhardware CmDongle oder der Aktivierungsdatei CmActLicense ist es möglich, sie zu verwenden. Ohne Quellcodeänderung kann der Schutz in kurzer Zeit und mit minimalem Aufwand eingebaut werden.

Durch zusätzliche, individuell festgelegte Verschlüsselung einzelner Funktionen, die vor der Verwendung per API-Aufruf entschlüsselt werden, erhöht sich die Sicherheit deutlich. Die mit dem IxProtector verschlüsselten Funktionen verbleiben selbst nach dem Laden der Software verschlüsselt im Speicher. Erst bei Benutzung werden sie für kurze Zeit entschlüsselt. Der IxProtector ermöglicht den Einbau von Fallen und Maßnahmen gegen Crack-Methoden wie Memory-Dumps, Patchen oder Emulation der Software. Der IxProtector ist im AxProtector integriert und lässt sich zusätzlich oder alternativ zum AxProtector benutzen.

Darüber hinaus signiert der AxProtector Programme digital. Verschiedene Programmteile, beispielsweise eine Exe-Datei und zehn DLLs, können gegenseitig die Signatur und damit die Integrität prüfen. Dies verhindert, dass ein Angreifer oder Virus das Programm unbemerkt verändert.

.NET-Anwendungen bestehen aus vor- übersetztem Code und sind daher besonders einfach zu dekompilieren. Der AxProtector .NET extrahiert den Inhalt aller zu verschlüsselnden Methoden und legt diesen verschlüsselt im Datenbereich ab. Zur Laufzeit werden diese Inhalte bei Bedarf automatisch entschlüsselt und dynamisch zur Verfügung gestellt. Das verschlüsselte .NET-Assembly ist weiterhin gültiger reiner .NET-Code (managed Code), enthält aber eigentlich nur Rümpfe. Gepaart mit der integrierten Obfuskierung von privaten und internen Methoden geben diese Reste nur wenige Hinweise auf die Funktionalität.

.NET-Assemblies und Java

Ähnlich verhält es sich bei Java. Der kompilierte Byte-Code lässt sich mit zahlreichen Tools wieder zurückübersetzen. Besondere Herausforderungen sind die eingebauten Debug-Schnittstellen und die Möglichkeit, die Java Virtual Machine selbst neu zu bauen. Der AxProtector verschlüsselt Java-Klassen. Zur Laufzeit werden diese Klassen in nativem Code wieder entschlüsselt und direkt der Java Virtual Machine zur Verfügung gestellt.

Heutzutage ist es besonders im Umfeld von Applikationsservern wie GlassFish oder WebSphere notwendig, Klassen in Teilen vorab auszulesen, damit vorhandene Optimierungen funktionieren. Mit dem IxProtector können die Klassen selbst unverschlüsselt bleiben und innerhalb der Klasse eine, mehrere oder auch alle Methoden verschlüsselt werden. Über Annotationen lassen sich diese Konfigurationen dann im Quellcode vornehmen. Die Entschlüsselung zur Laufzeit erfolgt daran anschließend auto- matisch.

Embedded-Systeme schützen

Gerade in der Industrie werden Embedded-Systeme in Maschinen, Anlagen und Geräte eingebaut. Anstatt eines PC-Betriebssystems laufen auf diesen Systemen spezielle Systeme wie Linux, Windows Embedded, VxWorks, Android oder QNX. Embedded-Systeme stecken beispielsweise in Routern, Ampelsteuerungen, Gebäudeleitsystemen oder in Steuerungen von Maschinen. Da aufgrund der wachsenden Vernetzung der einzelnen Systeme diese nicht mehr als proprietäre Insellösung betrieben werden können, müssen die Embedded-Systeme besonders vor Angriffen und Manipulationen geschützt werden.

Bei speicherprogrammierbaren Steuerungen, SPS, arbeitet man mit Entwicklungsumgebungen wie CODESYS, B&R Automation Studio oder Studio 5000 von Rockwell Automation.

Anders als PCs sind Embedded-Systeme von kleinen, resourcensparenden Architekturen geprägt, sie zeichnen sich also durch höhere Anforderungen an die Echtzeitfähigkeit, schlanke Arbeitsspei-

cher und geringe Rechenleistung aus. Embedded-Systeme passt man auf jeweilige Anforderungen hin an. So wurde die CodeMeter Protection Suite mit dem AxProtector CmE und dem ExProtector speziell auf diese Anforderungen hin optimiert. Die kleinste Implementierung von CodeMeter MicroEmbedded wurde entwickelt für Mikrocontroller wie den XMC4000 von Infineon und der dazugehörige AxProtector wurde in die Eclipse- basierte Entwicklungsumgebung DAVE von Infineon integriert. Ähnlich verhält es sich mit der Workbench von VxWorks und dem AxProtector.

AxProtector CmE und ExProtector

Der AxProtector CmE erzeugt ein automatisch verschlüsseltes Archiv mit dem Original-Programmcode. Erweiterungen sind eine Selfextraction-Funktion und Lizenzparameter, mit denen sich die Entschlüsselung durch die CodeMeter Runtime autorisieren lässt. Das verschlüsselte Programm vergrößert sich nur um einige Kilobyte. Nachdem sich das Archiv beim Programmaufruf autorisiert und entpackt hat, überprüft es seine Integrität selbst.

Mithilfe des ExProtectors wird ein Programm, eine Bibliothek oder ein Datenfile für ein Embedded-System verschlüsselt und optional tief ins Embedded-System integriert. Die verschlüsselte Datei wächst nur um ein paar zusätzliche Bytes für die für die Entschlüsselung notwendigen Lizenzparameter sowie einen signierten Hash (Prüfsumme) im Header. Alle kryptographischen Funktionen sind bereits ins Betriebssystem integriert. Auch der Treiber für den Zugriff auf die Lizenzen im CmDongle oder die softwarebasierte CmActLicense befindet sich als nativer Code direkt im Loader des Betriebssystems.

Wind River bietet bereits eine komplette Integration des CodeMeter Loaders in VxWorks an. Durch die Möglichkeit der Modifikation des Betriebssystems ist eine Integration in Linux und Android ebenfalls leicht möglich. Die tiefe Verankerung im Betriebssystem erhöht Effizienz wie Sicherheit. Der Loader überprüft die Integrität des mit dem ExProtector gesicherten Programms oder der Daten anhand des Hashes und der Signatur, nachdem er es autorisiert und entpackt hat. In Kombination mit Secure-Boot-Prozeduren, die sich ebenfalls mit der CodeMeter-Technologie abbilden lassen, erhält der Hersteller ohne weitere zusätzliche Software ein gegen Kopieren und Manipulation geschütztes System.

Die Vielfalt an Programmiersprachen, Entwicklungsumgebungen und Betriebssystemen fordert unterschiedliche Werkzeuge für Schutz und Lizenzierung. Die CodeMeter Protection Suite unterstützt dies und ist einfach anzuwenden. Dies ermöglicht Softwareentwicklern, die komplexen kryptographischen Schutzmechanismen fehlerfrei zu nutzen.

Firmen zu diesem Artikel

WIBU-SYSTEMS AG

KARLSRUHE, DEUTSCHLAND 19

BEWERTEN 4,9 ●●●●● (1)