



1 Neue Hardware der CodeMeter-Technologie schützt Industrie-PCs und erfüllt industrielle Anforderungen.

## Schutz von Embedded-Software

# Sicherung gegen Produktpiraterie

*Die Embedded-Software steuert moderne Maschinen und Anlagen, definiert deren Funktionalität und enthält immer mehr wichtiges Know-how des Herstellers. Produktpiraten, die vom Erfolg des Herstellers profitieren wollen, vermeiden die aufwändigen Entwicklungskosten, indem sie sich eine Maschine oder Anlage organisieren und dann bis ins letzte Detail auseinander nehmen: sie analysieren sowohl die einzelnen Komponenten als auch die dazugehörige Software. Ist die Maschine oder Anlage des Herstellers schlecht geschützt, ist es für Piraten ein leichtes, ein Plagiat zu erstellen. Dann wird nicht nur der Umsatz des Herstellers gemindert oder sogar dessen Existenz bedroht, sondern auch dessen Ruf aufgrund mangelnder Qualität geschädigt.*

*Autor: Oliver Winzenried, Gründer und Vorstand der Wibu-Systems AG*

Um die Bedrohung der deutschen Unternehmen durch Produktpiraterie zu reduzieren, fördert das Bundesministerium für Bildung und Forschung (BMBF) in verschiedenen Projekten die Entwicklung von Abwehrmaßnahmen. Zusätzlich kämpfen Verbände gegen Pro-

duktpiraterie. Die Zahlen der aktuellen Studie des VDMA Verband Deutscher Maschinen- und Anlagebau e.V. verdeutlichen die Problematik der Produktpiraterie: Der jährliche Schaden für den Maschinen- und Anlagebau betrug im Jahr 2009 6,4 Milliarden Euro, wobei mit 45 Prozent der

größte Schaden durch den Nachbau ganzer Maschinen und Komponenten entsteht. Ansatzpunkt des Plagiatschutzes ist der Schutz der Maschinen und Anlagen durch die Software. Bisher sind im Bereich Embedded-Software effiziente Schutzverfahren kaum vorhanden.



Forschungsprojekt Pro-Protect entwickelt für Maschinen und Anlagen eine wirkungsvolle Diebstahlsicherung gegen Produktpiraterie.

2

## Forschungsprojekt Pro-Protect im Überblick

Das Pro-Protect-Konsortium besteht aus den Forschungs- und Entwicklungspartnern FZI Forschungszentrum Informatik am Karlsruher Institut für Technologie (KIT) und der Wibu-Systems AG sowie den industriellen Anwender-Unternehmen GIS Gesellschaft für Informatik und Steuerungstechnik mbH, HOMAG Holzbearbeitungssysteme AG und ZSK Stickmaschinen GmbH. Mit dem Know-how der verschiedenen Partner werden existierende Lösungen zum Softwareschutz auf die Produktion übertragen und so weiterentwickelt, dass sie problemlos und branchenübergreifend eingesetzt werden können. Mehr Informationen über die Webseite [www.pro-protect.de](http://www.pro-protect.de).

### Pro-Protect entwickelt Diebstahlsicherung für Maschinen und Anlagen

Vier deutsche Unternehmen aus den Bereichen CAD-Software, Maschinenbau und Digital-Rights-Management und ein Forschungszentrum entwickeln seit 2008 gemeinsam beim Forschungsprojekt Pro-Protect eine Art Wegfahrsperrung für Maschinen und Anlagen. Ihr Ziel ist, eine effektive Lösung zum Schutz vor Produktpiraterie zu finden. Die existierenden Lösungen zum Softwareschutz werden dabei auf die Produktion übertragen und die speziellen Anforderungen der Industrie berücksichtigt: das sind Sicherheit, Nachrüstbarkeit, Flexibilität und Robustheit im Fabrikalltag. Pro-Protect erlaubt verschiedene Sicherheitsstrategien:

- Der Nachbau von Maschinen und Anlagen wird präventiv erschwert durch den wirkungsvollen Schutz der Embedded-Software.
- Know-how-Schutz für Maschinendaten und technische Spezifikationen und der Schutz von Maschinentagebüchern zur

Effizienzsteigerung im Service und rechtssicheren Dokumentation.

- Schutz von Produktionsdaten und deren Kontrolle, um so zu verhindern, dass Piraten mit Originaldaten geklonte Produkte oder mit „Sonderschichten“ weitere Originalprodukte ohne Wissen des Herstellers für den Graumarkt produziert werden können.

### Schutz der Embedded- Software mit CodeMeter

Pro-Protect nutzt als Grundlage die bewährte Softwareschutzlösung CodeMeter. Um auch die Embedded-Software in industriellen Anwendungen zu schützen, wurde CodeMeter erweitert. Wibu-Systems hat im Projekt Pro-Protect spezielle Schutzhardwarevarianten entwickelt: als Mikro-SD-Karte, als SD-Karte und als CompactFlash-Karte. Sie erfüllen industrielle Anforderungen wie einen erweiterten Temperaturbereich von -25 Grad C bis +85 Grad C und erhöhte EMV-Festigkeit. Sie können nachträglich auf einfache Weise für bestehende Embedded-Systeme eingesetzt werden. Die Karten werden auf den in der Industrie gebräuchlichen

Schnittstellen aufgesteckt und können unter harten Umgebungsbedingungen betrieben werden. Durch den Flash-Speicher auf jeder Karte wird kein zusätzlicher Steckplatz benötigt, denn Schutzsystem und Speicher sind auf einer einzigen Karte. Damit diese Karten auch mit denen im Industriebereich üblichen Betriebssystemen wie Windows Embedded, Windows CE oder OSADL Real-Time Linux funktionieren, wurde sowohl die notwendige Laufzeitsoftware als auch die Tools entwickelt, die die Embedded-Software auf hohem Level schützen. Einen hohen Sicherheitslevel erreicht CodeMeter mit wirkungsvollen Verfahren im SmartCard-Chip. Die Verschlüsselung im SmartCard-Chip erfolgt mit anerkannten Algorithmen wie AES für symmetrische Verschlüsselung und ECC (Elliptic Curve Cryptography) für asymmetrische Verschlüsselung. Diese Smart Card Chips schützen auch gegen Hardwareangriffe wie DPA (Differential Power Analysis) oder Betrieb außerhalb zulässiger Betriebsbedingungen durch Tem-



3

CodeMeter als Schutz für die CompactFlash-Schnittstelle und die USB-Schnittstelle im Industrie-PC.

peratur-, Spannungs- und Frequenz-Überwachung.

### *Integration des Schutzes in die Software*

Wichtig ist die Integration des Schutzes in die Software: der Prozessor im Embedded-System oder im IPC muss den Code lesen, verstehen und ihn ausführen. Keinesfalls liegen der gesamte Code und die Ressourcen zu irgendeinem Zeitpunkt unverschlüsselt im Arbeitsspeicher. Gleichfalls ist die Codeanalyse durch Obfuskation erschwert und Anti-Debugging- und Crack-Detection-Techniken greifen, sobald ein Angriff durch Produktpiraten erkannt wird. Dann wird bei CodeMeter die Lizenz gesperrt und der Angreifer kann nicht beliebig oft versuchen, den Schutz aus-

zuhebeln. Dabei dürfen die Betriebssicherheit, die Integrität, das Echtzeitverhalten und die gesamte Zuverlässigkeit nicht leiden. Produktionsdaten, mit denen eine Maschine arbeitet, können so geschützt werden, dass im Schutzsystem der Maschine die Produktionszahl „mitgezählt“ wird: der Auftraggeber hat einen Zähler, der die produzierte Stückzahl erfasst und bei Erreichen der Auftragsmenge die Verwendung der geschützten Produktionsdaten stoppt und somit unbemerkte „Mehrproduktionen“ nicht mehr möglich sind. Gleichzeitig werden die digitalen Maschinenakten gesichert, das sind beispielsweise Servicedokumente, Zeichnungen, Teilelisten oder auch die Dokumentation von Serviceeinsätzen. Ähnlich wie beim Softwareschutz werden diese Dokumente geschützt und die verschiedenen Serviceeinsätze durch eine elektronische Signatur manipulationssicher dokumentiert.

### *Einsatz in der Industrie*

Praxisnah setzt Pro-Protect die erarbeiteten Schutzstrategien bei seinen beiden Konsortial-Partnern um: der Homag Holzbearbeitungssysteme AG, Hersteller bei der Format- und Kantenbearbeitung, und der ZSK Stickmaschinen GmbH, Hersteller von Stickmaschinen. Der Schutz des digitalen Maschinengebuchs mit den Detaildaten der Anlage und allen Serviceinformationen steht bei Homag AG im Mittelpunkt. Daneben ist die Integration der Rechteverwaltung in

die ERP-Systeme und Logistik ein wichtiger Faktor. Im Rahmen des Projekts wurde das datenbankbasierte System CodeMeter License Central so weiterentwickelt, dass Lizenzen über eine SOAP-Schnittstelle aus beliebigen ERP-Systemen erstellt und diese über ein Gateway direkt auf die Maschine übertragen werden können. Stickmaschinen bieten Produktpiraten besonders viel Angriffsfläche: Sie wollen die Vorlagen der Designer für die Stickereien stehlen, die Software zur Steuerung der Maschine oder Maschinenteile kopieren. ZSK Stickmaschinen GmbH benötigt ein „elektronisches Typenschild“ mit allen maschinenspezifischen Informationen: es soll die Maschinensoftware gegen Raubkopien schützen, die Funktionen auf die durch den Kunden erworbene begrenzen und zur Zeitlimitierung der Nutzung gemäß der vereinbarten Ratenzahlungen dienen. Die Verarbeitung geschützter Produktionsdaten einschließlich der Überwachung der Produktionsstückzahlen ist eine weitere wichtige Funktion.

### *Für weitere Betriebssysteme*

Damit der Schutz wirkungsvoll mit den verschiedenen Embedded-Systemen eingesetzt werden kann, wird CodeMeter demnächst mit weiteren auf Embedded-Systemen verbreiteten Betriebssystemen wie VxWorks und QNX funktionieren sowie mit SoftSPS-Lösungen wie CoDeSys. Denn nur ein ausgefeiltes Konzept sichert die Investitionen des Herstellers - egal, bei welchem Produktionsprozess - und erlaubt Verbesserungen ohne Austausch der Schutzhardware. ■

[www.wibu.de](http://www.wibu.de)