

Wegfahrsperrung für die Maschine: Hardware schützt vor Produktpiraterie

VON OLIVER WINZENRIED

Durch Schutz der Software im PC- oder Embedded-Bereich und den Schutz von digitalen Maschinentagebüchern und Serviceunterlagen kann der Nachbau von Maschinen erheblich erschwert werden. Im Verbundprojekt Pro-Protect arbeitet ein Konsortium an verbesserten Lösungen. Erstes Resultat ist die neuentwickelte Sicherheitshardware „CmCard/CF“.

Der Softwareanteil im Maschinen- und Anlagenbau steigt stetig. Gleichzeitig fallen mit zunehmender Digitalisierung der Produktion immer mehr Produktionsdaten an. Klassische Schutzmaßnahmen reichen nicht, um das geistige Eigentum zu schützen, das in diesen digitalen Inhalten steckt. Hier setzt das vom BMBF geförderte Forschungsprojekt Pro-Protect an und überträgt Erfahrungen und Lösungen aus dem Software-schutzbereich in den Maschinen- und Anlagenbau.

Die an Pro-Protect beteiligten Unternehmen nutzen ihr vorhandenes Know-how aus den Bereichen CAD-Software, Maschinenbau und Digital-Rights-Management, um die speziellen Schutzbedürfnisse im Maschinen- und Anlagenbau zu berücksichtigen und ein durchgehendes Konzept zum Schutz vor Produktpiraterie zu erstellen. Dabei geht es sowohl um das Erschweren des Nachbaus von Maschinen und Komponenten, die mit komplexen Software-Funktionen ausgestattet sind, als auch um die Abwehr von Methoden, die auf das nicht autorisierte Kopieren und die Nutzung von Daten zur Herstellung von geklonten Produkten abzielen.

Pro-Protect geht folgende Wege:

- Nachbau von Maschinen und Anlagen präventiv erschweren durch wirkungsvollen Schutz der Embedded Software.
- Know-how-Schutz für Maschinendaten und technische Spezifikationen und 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 Graumarkt produzieren können.



Stickmaschine von ZSK mit CmCard/CF

FOTOS: WIBU SYSTEMS

Diebstahlsicherung für die Industrie

Um eine Lösung entwickeln und anbieten zu können, die im Maschinen- und Anlagenbau akzeptiert wird, hat das Pro-Protect-Konsortium verschiedene Unternehmen gefragt, welche Einsatzbedingungen bei ihnen vorherrschen und welche Anforderungen sie an ein Schutzsystem stellen. Das Interesse war sehr groß; Unternehmen aus den unterschiedlichsten Branchen haben sich an der Umfrage beteiligt oder am Industriearbeitskreis teilgenommen. Heraus kam Folgendes: Die Unternehmen legen Wert auf eine Lösung,

- die sie mit vorhandenen Maschinen und Anlagen nutzen können, die also nachrüstbar ist,
- die zuverlässig im harten Fabrikalltag funktioniert und
- die sicheren Schutz vor Produktpiraten bietet.

Die neu entwickelte und auf Wibu-Systems' CodeMeter-Technologie basierende CompactFlash-Karte „CmCard/CF“ erfüllt diese Anforderungen:

- Als CompactFlash-Karte ist sie auf den meisten vorhandenen Maschinen und Anlagen einsetzbar. Insbesondere auf SPS-Maschinen und Industrie-PCs, egal ob unter Windows CE, Realtime Linux oder anderen Echtzeitsystemen.
- Sie funktioniert zuverlässig auch bei extremen Temperaturen von -25° bis $+85^{\circ}$ Celsius, verwendet hochzuverlässige und schnelle Speicher und ist robust geschützt vor Staub, Feuchtigkeit oder starken elektrischen und magnetischen Feldern.
- Sie ist sicher wie jede auf CodeMeter basierende Schutztechnik – das haben ein weltweit veranstalteter Hacker-Wettbewerb und die Zeit bewiesen.

Sicherheit durch Verschlüsselung

Das Herz der patentierten CodeMeter-Technologie und der CmCard/CF ist ein Smart-Card-Chip. Der Chip ist so programmiert, dass er tausende digitale Rechte speichern kann, um beispielsweise Funktionen der Maschinensoftware modular

freizuschalten oder digitale Produktionsdaten zu schützen und deren Nutzung zu verfolgen. Er funktioniert mit Embedded Software und bietet mit seinem zusätzlichen, mehrere Gigabyte großen Speicher genügend Platz, um Maschinen- und Produktionsdaten abzulegen – natürlich ebenfalls verschlüsselt. Zur Laufzeit entschlüsselt die CmCard/CF die gerade benötigten Programmteile oder Daten. Nicht benötigte Bereiche bleiben weiterhin verschlüsselt, um ein Auslesen zu verhindern. Ausgefeilte Schutzverfahren, die sich bei Desktop-PCs bewährt haben, wurden übertragen: Polymorphe Verschlüsselung von Programmcode und Ressourcen, Obfuskierung, Anti-Debugging-Techniken, Angriffserkennung. Zum Einsatz kommen aber auch Redundanz, Techniken des Cold- und Hot-Standby, um höchste Zuverlässigkeit und Verfügbarkeit zu gewährleisten. CodeMeter nutzt anerkannte sichere Verschlüsselungsverfahren wie AES für symmetrische Verschlüsselung und Elliptic Curve Cryptography, für asymmetrische Verschlüsselung ebenso wie sichere Hardware, die Standards wie Common Criteria EAL 4 erfüllt.

Einsatz in der Industrie

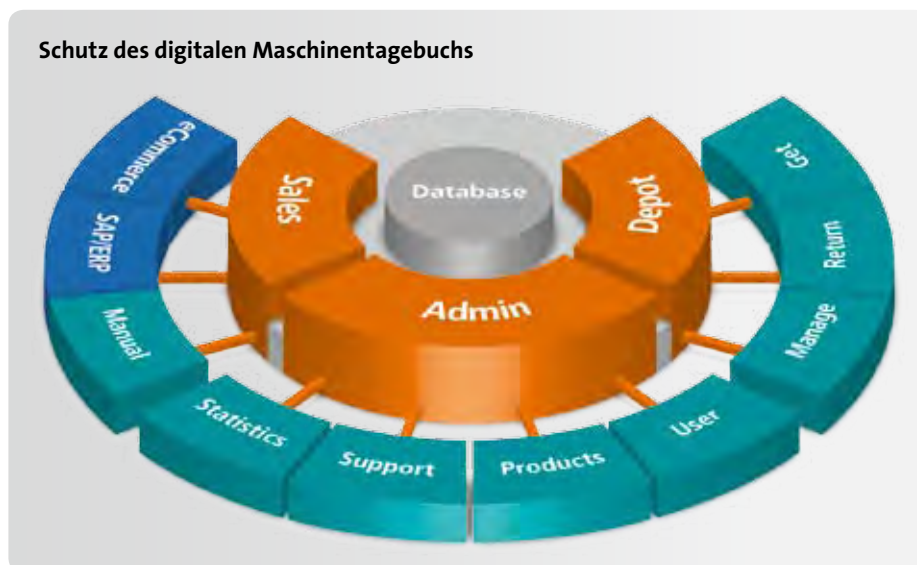
Praxisnah setzt Pro-Protect die erarbeiteten Schutzstrategien bei seinen beiden Konsortial-Partnern um: der HOMAG Holzbearbeitungssysteme AG, weltweit führender Hersteller bei der Format- und Kantenbearbeitung, und der ZSK Stickmaschinen GmbH, weltweit einer der führenden Hersteller von Stickmaschinen.

Der Schutz des digitalen Maschinentagebuchs 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.

Zukunftsaussicht

Die bei der Erprobung durch die HOMAG AG und ZSK Stickmaschinen GmbH gewonnenen Erkenntnisse fließen in die weitere Entwicklung ein. Unabhängig vom Pro-Protect-Konsortium können unterschiedlichste Maschinen- und Anlagenbauer von den



HOMAG untersucht die Nutzung der CodeMeter License Central, um Lizenzen zu erstellen, zu verwalten und weltweit auszuliefern.

INFORMATIONEN

Pro-Protect

Das Pro-Protect-Konsortium besteht aus den Forschungs- und Entwicklungspartnern FZI Forschungszentrum Informatik am Karlsruher Institut für Technologie 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. Interessierte Unternehmen können sich auf der Webseite über die Ergebnisse informieren, ihre Anforderungen und Wünsche einbringen und an Test und Evaluierung teilnehmen.

www.pro-protect.de

Ergebnissen profitieren. Weitere Unternehmen wie beispielsweise Beckhoff, CodeSys, Rockwell oder Windriver evaluieren die entwickelten Lösungen.

Zukünftige Lösungen decken eine noch weitere Bandbreite von Geräten ab. Vom Mobiltelefon und Embedded-Systemen, die eine µSD-Card nutzen können, über Netbooks, Notebooks mit SD-Card, Industrie-PCs mit CF-Card und normale Desktop-PCs und Server mit USB-Sticks geht die Unterstützung bis zum Cloud Computing im Internet, um Programme und Daten umfassend in der kompletten Wertschöpfungskette und über alle Beteiligte schützen zu können.

Dipl.-Ing. Oliver Winzenried
 Vorstand und Gründer
 WIBU-SYSTEMS AG
 Telefon +49 721 931720
 info@wibu.com