

Software-Schutz:

CompactFlash-Karte gegen Produktpiraterie

Wibu Systems baut seine Software-Kopierschutzlösung Codemeter so aus, dass sich damit auch Maschinen-Software schützen lässt. Ziel ist eine universelle Lösung, die für viele Arten von Maschinen einsetzbar ist.

Der Maschinen- und Anlagenbau sieht sich zunehmend mit Produktpiraterie konfrontiert. Piraterie kann in mehreren Erscheinungsformen auftreten. Am gefährlichsten dürfte für Hersteller die Produktfälschung sein, bei der ein Gerät sklavisch nachgeahmt und der

gefährdet sind, erst dann zur Kenntnis, wenn es zu spät ist und eine Fälschung auftaucht. Dann ist der Schaden jedoch schon eingetreten. Auch was die Gegenmaßnahmen betrifft, denken viele zuerst an den Rechtsanwalt. Einen bereits eingetretenen Schaden zu begrenzen, ist jedoch schwierig und langwierig. Aus diesem Grund haben sich einige Hersteller zur Initiative „Pro-Protect“ zusammengeschlossen, die auch vom BMBF gefördert wird. Ziele von Pro-Protect sind:

- ▶ Die Entwicklung einer nicht manipulier- und kopierbaren Schutz-Hardware zum Einbau in Maschinen. Dies erschwert den Nachbau von Maschinen sowie Komponenten, die komplexe Software-Funktionen enthalten.
- ▶ Schutz von Produktionsdaten und Prävention gegen Graumarkt-Produkte durch Fertigungszulieferer.
- ▶ Einführung eines „digitalen Maschinentagebuchs“ zur Effizienzsteigerung im Service.

Möglichst maschinenunabhängige Lösung

Bei der Entwicklung von Schutz-Hardware hat sich Pro-Protect die Nutzung von Standard-Schnittstellen auf die Fahnen geschrieben. Da zur Steuerung von Maschinen heute vielfach PC-gestützte Systeme oder andere Mikroprozessor-Hardware mit Standard-Schnittstellen zum Einsatz kommen, sollen diese Schnittstellen auch genutzt werden, um die Kopierschutz-Hardware anzuschließen. Damit ist die Integrationsfähigkeit in möglichst viele Maschinenumgebungen gesichert. Auf dem Gebiet der Kopierschutz-Hardware ist die Karlsruher Firma Wibu Systems ein sehr aktiver Treiber von Pro-Protect, da Wibu schon lange mit Kopierschutz-Dongles im Geschäft ist. Das bisherige Geschäftsmodell von

Wibu zielte allerdings auf den Schutz klassischer PC-Software ab. Doch im Rahmen von Pro-Protect will Wibu die Schutz-Funktionen auch auf Embedded-Software ausdehnen. Wibu bringt dazu sein Codemeter-System (www.codemeter.de) in die Initiative ein.

Codemeter ist eine Familie von Kopierschutz-Dongles, die mit einem Smartcard-Chip und Flash-Speicher ausgestattet sind. Der SmartCard-Chip regelt die verschlüsselte Übertragung und Speicherung von Lizenzierungs-Informationen. Die Codemeter-Dongles gibt es in mehreren Bauformen. Am populärsten dürfte sicherlich der USB-Stick sein. Er ist gut für „portable“ Lizenzen geeignet, also z.B. für die Nutzung einer Software durch eine Person auf verschiedenen PCs. Der Stick fungiert dann wie ein Schlüssel: An dem PC, an dem er eingesteckt ist, lässt sich die Software nutzen. Genau dieser Effekt ist bei Maschinen-Software allerdings nicht gewollt. Ein USB-Stick, der „Beine bekommen“ kann, ist hier denkbar ungeeignet. Deshalb hat Wibu auf der CeBIT 2009 Codemeter auch als CompactFlash-Karte vorgestellt. Diese Bauform lässt sich gut in Maschinen einbauen, da viele Industrie-Computer einen mitunter sogar innen liegenden CompactFlash-Steckplatz haben und die Karte hier unverlierbar eingebaut ist.

Die Software muss mitspielen

Mit dem Einbau der CompactFlash-Karte allein ist es allerdings nicht getan, damit die Maschinen-Software geschützt ist – auch die Software muss passen. Hier ist es das Bemühen der Initiative Pro-Protect, Kopierschutzlösungen zu entwickeln, die sich möglichst universell auf vielen Maschinen einsetzen lassen. Das bedeutet im Klartext: Die Codemeter-Bibliotheken müssen auf die Betriebssysteme der Maschine portiert werden. Auf der Hannover-Messe hat Wibu bereits eine Industriesteuerung von Beckhoff mit Codemeter-Schutz gezeigt. Dieser Fall war allerdings noch vergleichsweise einfach, weil diese Steuerung mit Windows XP Embedded arbeitet und hierfür keine Änderungen nötig sind. Al-

lerdings sind auch Lösungen für Windows CE 5.0 und 6.0 einsatzfertig. Ebenfalls in Arbeit ist die Unterstützung für OSADL-Linux (www.os-adl.org) – ein im Maschinenbau weit verbreitetes Linux. Noch nicht realisiert, aber auf der Agenda, ist eine Codemeter-Portierung auf das Echtzeit-Betriebssystem VxWorks von Wind River.

Die Initiative Pro-Protect besteht hauptsächlich aus Maschinenbauern, die die Anforderungen für die zu entwickelnde Software vorgeben. Wibu ist momentan der einzige kommerzielle Anbieter, der eine universelle, maschinenunabhängige Schutzlösung anbietet. Das einzige Pro-Protect-Mitglied, das sich ebenfalls mit Software-Entwicklung beschäftigt, ist das FZI Karlsruhe. Hier liegt der Schwerpunkt der Arbeiten auf dem Schutz von FPGAs und der Anwendung von Trusted Platform Modules für den Maschinenbau. Allerdings befinden sich diese Arbeiten noch im Forschungsstadium und sind zur kommerziellen Nutzung noch nicht verfügbar.

Neben dem Schutz von Embedded-Software auf Steuer-PCs steht noch eine weitere Anforderung auf dem Wunschzettel der Pro-Protect-Mitglieder: der Schutz von SPS-Programmen. Hier besteht das Bedürfnis, Teile der Software offen zu lassen, damit der Maschinenbetreiber Änderungen vornehmen kann, und wichtige Algorithmen als geschützte „black box“ auszuliefern, die vor Manipulation und Vervielfältigung geschützt ist. Oliver Winzenried, Mitgründer und Geschäftsführer von Wibu Systems, sieht hierfür aber noch keine Lösung: „SPS-Systeme von Siemens oder Allen Bradley oder wie sie alle heißen sind doch recht geschlossene Systeme, und die Hersteller haben bis jetzt noch wenig Interesse daran, ihre Systeme so weit zu öffnen, dass hier eine systemübergreifende Lösung für alle Steuerungen möglich wird. Zwar bieten die Hersteller einfache Passwort-Schutzmechanismen an, aber da braucht man nur mal zu googeln, und schon findet man Schritt-für-Schritt-Anleitungen, wie man diesen Schutz umgeht.“ *jk*



CompactFlash-Karte mit Codemeter-Smartcard-Chip. Auf der gehäuselosen Karte ist der CompactFlash-Controller von Hyperstone zu sehen, der so angepasst wurde, dass er mit dem SmartCard-Chip zusammenarbeitet. Dieser wird als Die direkt auf die rechte obere Ecke der Leiterplatte geklebt, gebondet und dann vergossen.

(Bild: Wibu Systems)

Markenname des Originalherstellers verwendet wird. Damit wird dem Originalhersteller die Urheberschaft der minderwertigen Kopie unterstellt. Die mit Fälschungen geprellten Kunden wenden sich bei Gewährleistungsansprüchen an den Originalhersteller, was neben Kosten auch noch einen erheblichen Imageverlust bedeutet. Aber auch echte Originalware kann auf dubiose Weise auf Abwege gelangen, sei es als Grauimport oder indem der beauftragte Fertigungsdienstleister in der Nacht oder am Wochenende eine „Sonderschicht“ einlegt und die zusätzlich produzierte Ware über Hehler verkauft. Viele Unternehmen nehmen die Tatsache, dass Know-how, Maschinen-Software oder Produktionsdaten diebstahl-