

Wibu-Systems AG: Verbessertes Codemeter genügt Anforderung im Embedded-Bereich

Dongle verhindert Produktpiraterie im Maschinenbau

Den Schutz vor Software-Piraterie hat sich die Wibu-Systems AG mit diversen Hardware-Lösungen auf die Fahnen geschrieben. Laut Wibu-Vorstand Oliver Winzenried gibt es aber »zwischen den im PC-Bereich existierenden Dongle-Lösungen und den Anforderungen an den Schutz im Maschinen- und Anlagenbau große Unterschiede«. Demzufolge wurde für die speziellen Anforderungen im Embedded-Bereich der Dongle Codemeter weiterentwickelt, der Smartcard-Chip im LGA-Package lässt sich jetzt auch »direkt in die Steuerung der Maschine oder Anlage einbauen«, zudem können neue Schnittstellen wie CF, CF-Card oder SD-Card verwendet werden.

Markt&Technik: Warum sollte der Maschinenbau seine Produkte schützen – betrifft Produktpiraterie nicht vorrangig die Konsumgüterindustrie?

Oliver Winzenried: Der Schutz vor Produktpiraterie gewinnt zunehmend auch im Investitionsgüterbereich an Bedeutung. Im Maschinen- und Anlagenbau geht es um den Schutz des technischen Know-hows verknüpft mit hohen Investitionen.

Die Praxis zeigt, dass Unternehmen unter gefälschten Ersatzteilen bis hin zu Nachbauten von komplexen Gesamtanlagen leiden. Sogar die Existenz von Unternehmen kann bedroht werden. Bisher sind effiziente Schutzverfahren im Bereich Embedded-Software kaum vorhanden. Software stellt bereits heute einen erheblichen Wirtschaftsfaktor dar. Grundsätzlich nimmt der Software-Anteil an Innovationen im Maschinen- und Anlagenbau stetig zu. Ein wirkungsvoller Schutz dieser Software ist folglich die Voraussetzung für den Schutz der Produkt-Innovationen. Gleichzeitig steigt mit zunehmender Digitalisierung der Produktion die Bedeutung des Schutzes von digitalen Produktionsdaten.

Reichen Gesetze, mit denen Unternehmen ihr geistiges Eigentum schützen können, nicht mehr aus?

Mit Urheberrecht, Gebrauchsmusterschutz und Patenten ver-

suchen Hersteller, ihre Rechte zu schützen, doch Produktpiraten beeindruckt das leider nur selten, im Gegenteil: Immer mehr Unternehmen verzichten laut Financial Times Deutschland darauf, Patente anzumelden, weil sie zu Recht befürchten, dass Piraten die Patente zum Nachbauen missbrauchen.

Technische Lösungen sollen Piraterie verhindern. Aber nur wenige standardisierte und herstellerübergreifende Maßnahmen zum Schutz von Produkten sind bislang bekannt: Hersteller kennzeichnen ihre Produkte mit Hologrammen oder Spezial-Etiketten wie RFID, schützen Software durch Lizenzschlüssel. Doch inzwischen haben die Angreifer ge-



Oliver Winzenried,
Wibu-Systems

» Die Praxis zeigt, dass Unternehmen unter gefälschten Ersatzteilen bis hin zu Nachbauten von komplexen Gesamtanlagen leiden. «

lernt, wie sie solche Schutzmaßnahmen umgehen, selbst gute Hologramme bieten heute keinen ausreichenden Schutz mehr.

Am Ende wird ein guter Schutz immer ein Mix aus rechtlichen und technischen Schutzmaßnahmen sein. Verbände wie VDMA und BITKOM oder diverse Initiativen zeigen verschiedene Maßnahmen.

Welche Problematik gibt es bei bisherigen Schutzstrategien im Maschinen- und Anlagenbau?

Es werden bisher zu wenig präventive Schutzmaßnahmen ergriffen. Mit der Standardisierung der Steuerungen und Schnittstellen wird das Erstellen von Plagiaten einfacher. Hier setzen unsere Lö-

sungen an, indem sie den Nachbau erschweren.

Womit wir bei Codemeter wären: Sind denn die hier gespeicherten Lizenzen sicher genug vor Missbrauch?

Ja, denn die Lizenzen werden nicht in einem gewöhnlichen EEPROM-Speicher gespeichert, sondern in einem EEPROM-Speicher in einem Smartcard-Chip. Dieser erfüllt besondere Sicherheitsanforderungen und ist auch nach Common Criteria EAL4+ zertifiziert, was bezüglich der Hardwaresicherheit mehr als ausreichend ist. Ergänzend kommen Codemeter-Technologien hinzu, die speziell für Embedded- und Real-Time-Betriebssysteme erwei-



Forschungsprojekt Pro-Protect

Digitales Maschinenbuch

Grundsätzliches Ziel des Forschungsprojekts Pro-Protect ist es, im Desktop-Computing existierende Lösungen zum Software-Schutz auf den Bereich der Produktion zu übertragen. F&E-Ziel Nr. 1 ist dabei die Entwicklung einer nicht manipulier- und kopierbaren Schutzhardware, die in die Maschine eingebaut werden kann, um den Nachbau von Maschinen und Komponenten, die mit komplexen Software-Funktionen ausgestattet sind, zu erschweren. F&E-Ziel Nr. 2 ist das Schützen von Produktionsdaten, um das Herstellen von Grau-

marktprodukten durch die eigenen Fertigungszulieferer zu verhindern. Zudem soll F&E-Ziel Nr. 3 ein »Digitales Maschinenbuch« schaffen, das den Service effizienter macht, dem autorisierten Servicetechniker alle Unterlagen an der Maschine bereitstellt und Serviceeinsätze auch nachweisbar dokumentiert.

Partner im Konsortium sind das FZI Forschungszentrum Informatik an der Universität Karlsruhe als Forschungspartner, HOMAG AG und ZSK Stickmaschinen GmbH als Anwender, GIS als Soft-

warehersteller und Wibu-Systems als Lösungsanbieter. Die Lösungen aus dem Forschungsprojekt werden nach und nach in die Produkte einfließen. Wibu-Chef Winzenried hofft, »bereits 2010 erste neue Lösungen in Produkten realisiert zu haben, ab 2011 soll ein zunehmender Umsatz mit neuen Verfahren erzielt werden«. Innerhalb des Konsortiums werden Pilotanwendungen entstehen und mit Unterstützung von Verbänden wie BITKOM und VDMA sowie der Initiative Conlmit weitere Anwender außerhalb des Konsortiums eingebunden. (es)

tert werden, um Programmcode und auch Produktionsdaten besonders wirkungsvoll zu schützen. Gerade wegen der Produktionsdaten ist es auch erforderlich, dass das Schutzsystem viele Lizenzen von unterschiedlichen Lizenzgebern speichern kann – beispielsweise Stickmuster von unterschiedlichen Auftraggebern in einer Stickmaschine.

Wie kommt die Lizenz denn auf den Codemeter-Stick?

Auf verschiedene Art und Weise: Der Hersteller der Maschine wird die Lizenzen für die erworbenen Funktionen der Maschine von Anfang an darauf speichern, bei späteren Erweiterungen wird dies dann aktualisiert. Bei geschützten Produktionsdaten werden die Lizenzen nachträglich gespeichert, ohne dass die Codemeter-Hardware von der Maschine entfernt wird. Dies könnte über das Internet geschehen, wird in Produktionsumgebungen aber eher dateibasiert zusammen mit der Übertragung der geschützten Produktionsdaten erfolgen.

Der bisherige Codemeter enthält zum Speichern von Daten auch einen Flash-Teil: Ist der überhaupt nötig im Anlagenbau?

Wenn es im Produktionsbereich nur um die Lizenzierung geht, dann ist der Flash-Speicher nicht erforderlich, dennoch kann er aber sehr nützlich sein. Eine bei Industrie-PCs sehr gebräuchliche Schnittstelle ist die CF-Card, deshalb wird die Codemeter-CF-Card mit Flash-Speicher in verschiedenen Größen von 1 bis 16 GByte verfügbar sein und zusätzlich zum Speicher auf derselben CF-Card die Schutz- und Lizenzierungsfunktionen bieten.

Ist es immer eine portable, leicht von außen einsteckbare Lösung oder ist auch daran gedacht, den Codemeter quasi nackt direkt auf ein Motherboard zu implementieren?

Technisch wäre es kein Problem, die Codemeter-Hardware direkt auf ein Motherboard zu bauen. Aber die praktische Durchsetzung ist sehr schwer: Einerseits ist der Preisdruck bei Steuerungshardware groß, andererseits gibt es unüberschaubar viele verschiedene Produkte und Varianten bei ein und demselben Hersteller – nicht zu vergessen all die, die bereits im Feld installiert sind. Vielleicht ergibt sich in Zukunft mit der eSD-Card (Embedded SD-Card, aktuell in der Standardisierung) einmal eine Chance. Heute setzen wir auf abnehmbare Formfaktoren: USB, Cardbus (PCMCIA), Expresscard und eine SD-Card (ab 2009), µSD-Card und CF-Card. Momentan unterstützen wir alle PC-Betriebssysteme wie Windows, Linux, Mac-OS und Sun Solaris, daneben auch Windows CE für Arm und Intel so-

Die Funktionen des Codemeter-Sticks werden für den Embedded-Bereich um die neuen Schnittstellen Compact-Flash, CF-Card und SD-Card erweitert.
Foto: Wibu-Systems



wie Realtime Linux (OSADL). In Zukunft werden mobile Devices mit Windows Mobile und Symbian folgen. Das sind anspruchsvolle Herausforderungen für unser Entwicklungsteam mit begrenzten Ressourcen.

Wenn der private User seinen CM-Stick verlegt oder dieser durch eigenes Verschulden oder auch sonstwie kaputt geht, sind die Programme erst wieder nutzbar, wenn Ersatzstick vorliegt. In der Industrie ist eine mehrstündige oder gar mehrtägige Auszeit nicht hinnehmbar . . .

Unser Konzept sieht Notfall-Dongles vor. Vorprogrammiert mit einer Nutzungszeit von X Tagen können diese Notfall-Dongles im Safe liegen. Kommt es zum Ausfall, wird dieser Dongle einfach aufgesteckt und die Maschine läuft unverzüglich weiter. Sobald der Standard-Dongle ausgetauscht wurde, kommt der Notfall-Dongle mit aktualisierter Nutzungszeit wieder in den Safe und der neue Standard-Dongle entschlüsselt wie gewohnt Software und Produktionsdaten. Der Notfall-Dongle kann so nicht dauerhaft als zusätzliche Lizenz genutzt werden. Alternativ können auch beide Dongles gleichzeitig angeschlossen sein, so dass ohne Benutzerinteraktion ein ausfallsicherer mehrkanaliger Betrieb möglich ist.

Haben Sie auch Konkurrenz unter Mitbewerbern wie Aladdin, die Dongles herstellen, oder ist Wibu-Systems als einziger Hardware-Hersteller im Boot?

Meines Wissens sind wir mit unseren intensiven Aktivitäten im industriellen Bereich derzeit einziger Anbieter. Unser in Europa, USA und Japan patentiertes Codemeter-System, das die unabhängige Verwaltung digitaler Rechte vieler Anbieter in einem Dongle ermöglicht, tut sein übriges dazu. Nichtsdestotrotz wird jede erfolgreiche Aktivität irgendwie von Wettbewerbern nachgemacht. (es)

Halle 10, Stand 310, www.wibu-systems.de