Mit DVD!

Ausgabe 1.06

Deutschland € 5,50 Österreich € 6,00 Schweiz sFr 10,80

S&S

entwickler magazin

Enterprise Technologies & Business Solutions

WinFX SDK
Entwickeln für Windows Vista

Delphi 2006
Arbeiten mit dem neuen Delphi

MediaWiki
Websites mit dem Open-Source-Projekt

Schutz vor Spam
99,95 % Treffsicherheit mit DSPAM

Firebird 2.0
Stabile Datenbank in neuer Version

SQL-Tuning
Beschleunigung von Select-Abfragen

V-Modell XT
Dokumentenorientierte Systementwicklung

Enterprise Service Bus
Komplexität einfach gestalten

VoiceXML
Die wichtigsten Neuerungen der Version 2.1

XForms
Die neue Benutzerschnittstelle im Web

UML-Tools
Architekturen besser modellieren

USB-Sticks im Linux-Einsatz
Die wichtigsten Produkte im Test

www.entwickler-magazin.de

DVD-Inhalt

TurboDB 5
Firebird 1.5.2
ADS 8.0

Python 2.4.2
FormFaces Alpha
X-Hive/DB 7.0

Castor 0.9.9.1
DSPAM 3.6.1
Ubuntu 5.10

Enterprise Architect 5.0
Eclipse SDK 3.1.1
Poseidon 3.2.1 Community Edition

D31141F

4 194156 605502 01

Der große Report – Teil 2

Die richtige Taktik

In der letzten Ausgabe des *Entwickler Magazins* wurden einige Möglichkeiten zur Realisierung von Kopierschutz- und auch Lizenzierungssystemen sowie die Meinungen einiger Firmenvertreter vorgestellt. In der aktuellen Ausgabe folgt nun der zweite Teil des Reports.

von Malte Kollakowski

Die Einstellungen der einzelnen Beteiligten – seien es Anwender oder Anbieter von Software – könnten nicht unterschiedlicher sein. Selbst innerhalb der Meinungen der Herstellervertreter lassen sich deutliche Unterschiede in den Ansichten ausmachen. Einige sind dabei durchaus in der Lage, die strategisch erfolgreiche Planung (Kritiker nennen es puren Zufall, Glück oder Planlosigkeit) Microsofts zu würdigen, seine Software anfangs gänzlich ohne Kopierschutz auszuliefern. Andere fordern unverhohlen härtere Gesetze und noch mehr Verbote. Fast kommen einem die Werbespots der Musik- und Filmindustrie aus Film und Fernsehen in den Sinn, die Benutzer von illegalen Softwarekopien, Filmen und Musikstücken virtuell und wahrscheinlich auch in Realität mit Mördern, Schlägern und Vergewaltigern auf eine Stufe stellen wollen.

Die aktuell verfügbaren Kopierschutzsysteme lassen sich bei richtiger und maßvoller Anwendung zu einer einfachen und sicheren Lösung zur Sicherung der mit viel Aufwand und finanziellen Mitteln entwickelten Produkte nutzen und schrecken somit das Gros der illegalen Nutzer ab, die sich „mal eben eine Kopie ziehen wollen". Gegen wirklich kriminelle und mit dem entsprechenden Willen und Mitteln ausgestattete Gestalten ist jedoch kein Kraut gewachsen. Kein Schutz ist 100-prozentig sicher und irgendwann wird er geknackt. Nun sagt zwar die Theorie, dass man das Spiel beliebig weit treiben kann, wenn man den Schutz so weit wie möglich unvorhersagbar in die Software einbaut, dass er nicht, oder zumindest nicht vollständig, umgangen werden kann. Aber wer möchte schon jede Funktion des Programms verdonglen und verschlüsseln? Natürlich kann man die Prüfroutine an jedem zweiten Dienstag an Monaten im Herbst nach Vollmond zwischen 14.32 Uhr und 15.22 Uhr beim Aufrufen der Funktion *Datei Speichern* einbauen. Aber wer möchte das testen? Wer gibt die Garantie, dass das nicht zu Problemen führen kann und vor allem: Wer leistet Support und haftet, wenn der Kopierschutz mal aus irgendwelchen Gründen Amok läuft? Der Einsatz der vorhandenen Technik kann helfen, die sauer verdienten Gewinne zu sichern und vielleicht sogar zu erhöhen, aber es geht auch ein großes Stück Verantwortung an die Hersteller über.

Letztendlich könnte die Frage also lauten, ob man sich mit seiner eventuell falschen Kopierschutztaktik vor den Nutzern illegaler Softwarekopien oder doch eher vor den ehrlichen Käufern schützt …

SafeNet Deutschland GmbH

- sales@de.safenet-inc.com
- www.safenet-inc.com/products/tokens/iKey1000.asp
- www.safenet-inc.com/products/tokens/iKey2032.asp
- www.safenet-inc.com/products/sentinel/ultraPro.asp

Das Unternehmen

SafeNet, Inc. ist seit 1983 ein führender Anbieter von Sicherheitslösungen für private und öffentliche Netzwerke. Die Produktpalette von SafeNet umfasst Hardware-, Software- und On-Chip-Lösungen. Geliefert werden Produkte aus den Bereichen WAN-, VPN-, SSL-VPN-, PKI-, zweistufige Authentifizierungs-, Wireless-VPN-, Softwareschutz- und Digital-Rights-Management-Technologien sowie -Dienstleistungen an.

Produkte

- iKey (1000 und 2032)
- Sentinel UltraPro

Produktbeschreibung

iKey: Die USB-Stick-ähnlichen iKeys dienen beide der persönlichen Authentifizierung dem System gegenüber. Da die Hardware normalerweise am Schlüsselbund getragen wird, ist eine Authentifizierung durch den Besitz des Schlüssels gegeben – natürlich vorausgesetzt, man kennt das Passwort. Mit beiden Systemen (1000/1032 – letzteres hat 32 KB Speicher statt 8 KB – und 2032) können Anmeldeverfahren gesichert und E-Mails verschlüsselt werden. Zusätzlich ist durch den internen Speicher ein Anwendungslizenzierungsmanagement möglich. Der iKey 2032 bietet als das jüngere Produkt bessere Leistungsdaten, so zum Beispiel auch eine 2048 Bit RSA-Verschlüsselung.

Sentinel UltraPro: Der Sentinel UltraPro – die SuperPro-Version wird nur noch für bestehende Kunden unterstützt – das Hardwaremodul beinhaltet Verschlüsselungsalgorithmen (AES-Standard) sowie einen programmierbaren Schreib-/Lesespeicher. Die normale Version bietet 128 Byte Speicherplatz, die XM-Version bietet 464 Byte. Sowohl die parallele Schnittstelle – auf Wunsch in der 797-Version mit sehr kleinen Modulabmessungen, die auch Notebookbesitzer nicht zur Verzweiflung bringen sollten – als auch der USB-Port wird unterstützt. Die Verschlüsselungsengine wird über ein API angesprochen, womit sich alle relevanten Funktionen des Dongles aufrufen lassen. Hierbei wurde die Unterstützung einer Multiplattformumgebung berücksichtigt. Auch die Funktion in heterogenen Netzwerken ist gewährleistet, wobei mehrere Anwendungen eines Herstellers gegebenenfalls durch ein einziges Modul unterstützt und verwaltet werden können.

Das Lizenzmanagement von Sentinel UltraPro ist auf jede erdenkliche Situation vorbereitet, so werden folgende Szenarien unterstützt: Evaluation (quasi Probebetrieb ohne Dongle), Pay-per-Use, Standalone (gebunden an eine Maschine), Network (Lizenzen werden über einen zentralen Server verwaltet), Feature-based (der User zahlt für die Freischaltung bestimmter Funktionen oder Funktionsgruppen). Zur Lizenzverwaltung kann bei Bedarf „remote" aktualisiert werden, etwa wenn neue Features eingekauft, die Nutzungsdauer/Anzahl ausgelesen oder die Anzahl der Lizenzen geändert wurden. Über das Einspielen von neuen Keys kann so aus einer Demoversion eine voll funktionsfähige Version werden oder zusätzliche Features einer Premiumversion aktiviert werden.

Hardware- oder Softwarelösung?

- **iKey:** Hardware
- **Sentinel UltraPro:** Hardware

Betriebssysteme: Windows, Linux, Mac OS

Preise: Auf Anfrage

SG Intec Ltd & Co KG

- info@sg-intec.de
- www.sg-lock.de

Das Unternehmen

Das Unternehmen SG Intec Ltd & Co KG und sein Vorgänger S. Goers IT-Solutions ist seit 1996 im Bereich Software-Security/Kopierschutz tätig. Das in dieser Zeit erarbeitete Know-how ermöglicht es dem Unternehmen, innovative Lösungen im Bereich Kopierschutz und Datensicherheit anzubieten. Ziele der eigenen Produktentwicklung sind sowohl für Entwickler als auch für Anwender einfach zu handhabende Lösungen zu erhalten, ohne auf Sicherheit verzichten zu müssen. Eines der Hauptanliegen der Produkte – neben der erhöhten Sicherheit vor illegaler Softwarenutzung – ist der Versuch, die Komplexität der Entwicklung der Software nicht zu erhöhen.

Produkte

- SG-Lock (2er-, 3er- und 4er-Modell)

Produktbeschreibung

SG-Lock: SG-Lock ist ein flexibles Hardware-basiertes Kopierschutz- und Cryptosystem, das unter allen aktuellen Windows-Betriebssystemen eingesetzt werden kann. Es wird sowohl für die USB- als auch für die LPT-Schnittstelle angeboten, wobei die Module jeweils gegeneinander austauschbar sind (also USB- gegen LPT-Modul und umgekehrt) und keinerlei Treiber benötigen, was ein Vorteil ist, wenn man keine Administratorenrechte auf der jeweiligen Maschine hat. Bei LPT-Modulen werden angeschlossene Drucker natürlich nicht beeinflusst. Jedes Modul besitzt neben einer Verschlüsselungs-Engine eine individuell auslesbare Seriennummer und bis zu 1.024 Byte frei nutzbaren Speicher, auf den zum Beispiel Lizenzierungsinformationen und programminterne Variablen verschlüsselt (128-Bit-Verschlüsselung, bis zu 16 frei wählbare Schlüssel) ab-

Interview mit Sven Görs

„Massenprodukte mit Kopierschutz zu versehen lässt Anwender auf andere Produkte ausweichen“

Sven Görs, Geschäftsführer der SG Intec Ltd & Co KG, hat an der Universität Kiel Geographie, Geologie und Informatik studiert. Über den Weg der geowissenschaftlichen Umweltforschung, bei der Herr Görs computergestützte Modelle im Bereich der Klimaforschung entwickelte, kam er zur industriellen Anwendung der Informatik. Die mathematisch-naturwissenschaftliche Basis der Kryptographie hat ihn dabei in den Bereich der Sicherheitstechnik gebracht.

Entwickler Magazin: Seit wie vielen Jahren beschäftigen Sie sich mit Kopierschutzsystemen?

Sven Görs: Mein erstes Kopierschutzprojekt habe ich vor zehn Jahren durchgeführt. Die Kryptographie war für mich der besonders reizvolle Teil des Kopierschutzprojektes. Für mich geht tatsächlich eine gewisse Faszination von diesem Thema aus, weil die Kryptographie eine sehr mächtige Technik ist, die nur auf Wissen beruht und zu vielen Zeitpunkten Einfluss auf den Lauf der Weltgeschichte hatte. Wer wusste, wie man die eigenen Informationen geheim hält und die der anderen entschlüsselt, konnte den Lauf der Geschichte mitbestimmen – nur durch Zahlenspiele – das ist etwas Besonderes.

EM: Wo sehen Sie die Hauptanwendungsgebiete Ihrer Produkte?

Görs: Die Hauptanwendung von SG-Lock liegt zurzeit im Kopierschutz von Software. Immer mehr rückt aber auch der Dokumentenschutz durch Signierung und Verschlüsselung von Daten in den Vordergrund. Der Bedarf nach Datensicherheit, Know-how-Schutz und Authentifizierungsmöglichkeiten wächst nach unseren Erkenntnissen überproportional. SG-Lock ist auch in die Richtung entwickelt worden, dass zum Beispiel die Weitergabe von wertvollen oder geheimen Daten unter Kontrolle bleibt, die Authentizität eines Nutzers oder einer Information überprüfbar ist.

EM: Wo macht Kopierschutz Ihrer Meinung nach Sinn?

Görs: Wo Kopierschutz für Software Sinn macht, zeigt der Markt selbst. Ich denke, dass viele Softwarehersteller sich sehr gründlich Gedanken gemacht haben, ob ein Kopierschutz für sie eine Alternative darstellt oder nicht. Hier gilt es, die sich teilweise widersprechende Argumente abzuwägen. Entwicklungsintensive und dadurch teure, aber nur für kleine Märkte entwickelte Produkte sind prädestiniert für Kopierschutz – dort sind Sie auch überwiegend zu finden. Massenprodukte mit Kopierschutz zu versehen kann möglicherweise dazu führen, dass die Anwender auf andere Produkte ausweichen, weil die große Auswahl an sich wenig unterscheidenden Produkten in diesem Marktsegment dies einfach macht – denn er sieht für sich im Kopierschutz keinen Nutzen. Dieser Erkenntnis muss man sich stellen. Einen gewissen Nachholbedarf sehen wir in der Nutzung alternativer Vertriebsmodelle, wie Pay-per-Use, Leasing, Vermietung von Software. Hier bietet der Kopierschutz, der dann mehr als reiner Kopierschutz wird, viele Lösungen.

EM: Inwieweit hat sich die Art der von Ihnen angebotenen Produkte im Laufe der Jahre entwickelt?

Görs: SG-Lock ist von Anfang an sowohl für Programmierer als auch Nutzer besonders anwenderfreundlich konzipiert worden. Da unsere USB-Modelle unter den aktuellen Betriebssystemen ohne Treiberinstallation arbeiten, entspricht die „gefühlte Installationsart“, wie ein Kunde einmal formulierte, um seine Zufriedenheit auszudrücken, der einer reinen Softwareinstallation. Der Anwender hat nicht das Gefühl, eine lästige Hardwareinstallation mit fragwürdigem Ausgang für die Stabilität seines Systems durchführen zu müssen, nur um eine neue Software zu nutzen. Dies erhöht die Akzeptanz und macht Anwender und Softwarehersteller zufriedener.

EM: Wie wichtig erachten Sie das Internet als Möglichkeit für die Realisierung von (neuen) Kopierschutzverfahren?

Görs: Grundsätzlich neue Kopierschutzverfahren im engeren Sinne sehe ich kurz- bis mittelfristig nicht durch das Internet ermöglicht, da immer noch ein großer Teil der weltweit installierten PC-Basis nicht dauerhaft online betrieben wird. Eine große Erleichterung für Remote-Update, Leasing und Mietlösungen stellt das Internet allerdings dar. Die Möglichkeiten der Automatisierung dieser Lösungen sind immens. Das gleiche gilt auch für den Bereich Zugangskontrolle zu Webinhalten. Hier wird sich sicherlich viel in der näheren Zukunft tun.

EM: Wo stellen sich hier die Probleme in Bezug auf Angreifbarkeit von Internet-basierten Verfahren?

Görs: Es gibt viele sichere und bewährte Verfahren, Informationen über einen unsicheren Kanal zu übertragen. Das eigentliche Problem dürfte die direkte Absicherung des Rechners des einfachen Anwenders sein, wenn keine Kopierschutzhardware verwendet wird. An den Endpunkten der Übertragung sind Passwörter, Zugangscodes und Schlüssel zu finden. Wenn man zum Beispiel bedenkt, wie viel private und auch gewerbliche WLAN-Netze aus Unkenntnis völlig offen betrieben werden, braucht sich kein Hacker die Mühe zu machen, das Netz selber anzugreifen – er holt sich alles was er braucht direkt an der Quelle. Wenn es möglich ist, massenhaft per gefälschter E-Mail PIN und TAN eines Online-Banking-Zugangs beim Kontoinhaber schlicht zu erfragen, dann steht und fällt die Sicherheit internetbasierter Verfahren mit der Kompetenz der Anwender.

EM: Wie werden sich Kopierschutzsysteme Ihrer Meinung nach entwickeln?

Görs: Ich sehe zum einen anwenderfreundlichere Systeme, was den klassischen Kopierschutz betrifft. Das schon länger nicht mehr zutreffende Image des „Dongles, den keiner will und der nur Ärger macht“ wird sich zu einem zwar nicht geliebten, aber immerhin akzeptierten Teil von Software wandeln. Pay-per-Use, Leasing und Vermietung von Software gehört die Zukunft – hier wird die Entwicklung am schnellsten fortschreiten. Eine andere Frage ist, ob die Industrie es schafft, DRM-fähige Systeme direkt in die PC-Architektur zu integrieren. Nach einer Phase, in der viel darüber geredet wurde, ist es um dieses Thema etwas leiser geworden – da wird wohl noch etwas Zeit vergehen, bis sich konkrete Lösungen abzeichnen werden. Wenn diese dann verfügbar sind, muss noch die Hardwarebasis ausgetauscht werden, was noch einmal Jahre dauert. Der Kulminationspunkt der Verbreitung von Hardwarekopierschutz ist unserer Meinung noch lange nicht erreicht.

EM: Vielen Dank für das Gespräch.

gelegt werden können, was zusätzliche Programmsicherheit bietet. Darüber hinaus bietet jedes Modul bis zu 64 frei programmierbare Zählerzellen zur einfachen Erfassung zählbarer Ereignisse, was die Realisierung von Pay-per-Use-Systemen erleichtert. Die Programmanbindung geschieht über ein API, das die notwendigen Funktionen realisiert – zur Installation und Nutzung genügt das Kopieren einer DLL. Bei der Sicherheit hat SG-Lock einige Besonderheiten zu bieten, so wird das API selbst „geschützt", d.h. die API-Funktionen sind nicht sofort uneingeschränkt verwendbar. Jede Anwendung muss sich gegenüber dem SG-Lock-API authentifizieren, um Zugriff auf SG-Lock-Module zu bekommen. Somit ist ein Angriff von nicht authorisierten Programmen (zum Beispiel um Schwachstellen der API-Funktionen auszutesten) nicht möglich. Außerdem hat das zu schützende Programm die Möglichkeit, das API selbst zu verifizieren und eine gefälschte Bibliothek zu erkennen und entsprechend zu reagieren.

Die verschiedenen Modellreihen (2er, 3er und 4er) unterscheiden sich in einigen Punkten voneinander: So haben die Module der 2er-Reihe keinen Speicher und keine Zählerfunktion, wodurch sie lediglich für einfache und kostengünstige Kopierschutzmechanismen auf Hardwarebasis ausreichend sind. Der enthaltene fest programmierte und nicht änderbare Schlüssel hat eine Stärke von 128 Bit. Die 3er-Reihe kommt mit 256 Byte Speicher, 16 frei programmierbaren 32-Bit-Zählern und zwei frei programmierbaren 128-Bit-Schlüsseln, während die 4er-Reihe 16 frei programmierbare Schlüssel, 1 KB Speicher und 64 32-Bit-Zähler besitzt.

SG-Lock hat bei der Sicherheit Besonderheiten zu bieten

Hardware- oder Softwarelösung?

SG-Lock: Hardware

Betriebssysteme: Windows, Linux, Mac OS

Preise: 2er-Modul: 23,90 Euro/Stück, 3er-Modul: 29,90 Euro/Stück, 4er-Modul: 34,90 Euro/Stück, Demo Kit Single: 29 bis 39 Euro/Stück (jeweils 2er- bis 4er-Module, USB oder LPT), Demo Kit Double: 44 bis 54 Euro/Stück (jeweils 2er- bis 4er-Module, USB und LPT)

Für die Module bestehen gestaffelte Preisreduktionen für Chargen ab 10, 25, 100, 250, 500, 1.000 und 2.500 Stück.

WIBU-SYSTEMS AG

- info@wibu.de
- www.wibu.de

Das Unternehmen

Die WIBU-SYSTEMS AG wurde 1989 von Oliver Winzenried und Marcellus Buchheit gegründet und hat sich auf die Bereiche Digital-Rights-Management, Kopierschutz, Lizenzmanagement, Dokumentenschutz und Zugangsschutz spezialisiert. Das Karlsruher Unternehmen ist weltweit über Distributoren und eine Niederlassung in Seattle (USA) sowie eine Repräsentanz in Shanghai (China) vertreten.

Produkte

- WIBU-KEY
- SmartShelter
- SecuriKey
- CodeMeter

Produktbeschreibung

WIBU-KEY: Das WIBU-KEY-Lizenzmanagement ermöglicht Softwareherstellern sowohl den Schutz der Software als auch die Kontrolle der Lizenzen im Netzwerk, wofür nur eine WIBU-BOX in heterogenen Netzwerken (also mit angeschlossenen Windows-, Mac- und Linux-Rechnern) benötigt wird. Dabei werden verschiedenste Schnittstellen – von COM über LPT und PCMCIA bis USB – unterstützt. Bei Installation auf einem (gesicherten) Server ist die Möglichkeit eines „Verlusts" des Dongles somit auch beschränkt. Eine Fernwartung des Anwendungssystems, also das Aufstocken von Lizenzen, Pay-per-Use oder spezielles Freischalten von Funktionen für bestimmte Anwender ist auf diese Weise möglich. Zur Nutzung und Realisierung des Schutzes bietet WIBU-KEY eine API-Schnittstelle an.

SmartShelter: Mit SmartShelter können verschiedenste Dokumente von einfachen Textdokumenten über HTML, PDF, PowerPoint, Grafiken, Flash-Animationen, Video-/Audio-Dateien und JavaScript verschlüsselt werden. Die Daten werden auf „unsicherem" Weg zum Anwender gebracht, können jedoch nur von berechtigten Personen, also Besitzern der passenden WIBU-BOX entschlüsselt und im Internet Explorer gelesen werden. SmartShelter bietet sich – neben der Sicherung vertraulicher Dokumente – deshalb besonders für Abonnentensysteme an, wo zum Beispiel Normen und Dokumentationen bisher in teurer und meist wenig aktueller Form als Papierversion gehandhabt werden mussten. Einer Versorgung des Abonnenten mit aktuellsten Daten über das Internet steht somit nichts mehr im Wege.

SecuriKey: Für Windows 2000 und Windows XP kann ein sicherer Zugangsschutz für die USB-Schnittstelle mit dem SecuriKey erreicht werden. Dabei können Dateien oder Verzeichnisse verschlüsselt gespeichert werden. SecuriKey ist für Unternehmen mit Netzwerken als Enterprise Edition (zum Beispiel Verwaltung der Clients über Netzwerk möglich, etc.) und auch für Einzelunternehmen oder Privat-

Interview mit Oliver Winzenried

„Das Internet ist das ideale Vertriebsmedium für digitale Güter aller Art"

Oliver Winzenried, heutiger Vorstand der WIBU-SYSTEMS AG, hat 1989 zusammen mit Marcellus Buchheit die Firma WIBU-SYSTEMS in Karlsruhe gegründet. Er blickt auf über 25 Jahre Entwicklungserfahrung in den Bereichen Industrieelektronik, Automotive und Consumer Elektronik zurück. Oliver Winzenried studierte Elektrotechnik an der Universität Karlsruhe und ist heute aktiv in Standardisierungsgremien und Verbänden wie VDE, IEEE, BITKOM, SIIA, PCMCIA und USB, um nur einige zu nennen..

Entwickler Magazin: Seit wie vielen Jahren beschäftigen Sie sich mit Kopierschutzsystemen?

Oliver Winzenried: Bevor mein Partner und ich 1989 WIBU-SYSTEMS gegründet haben, durchleuchteten wir den Markt. Unsere Erfahrung war, dass keine optimalen Produkte zum Schutz von Software auf dem Markt verfügbar waren. Deswegen hatten wir das Ziel, die vielfältigen Schwächen der damaligen Produkte in ein flexibles, effektives und sicheres Produkt umzuwandeln – und schon war WIBU-KEY geboren. Natürlich entwickelt sich die Softwareindustrie weiter und fordert inzwischen Lösungen für die geänderten Bedürfnisse – beispielsweise noch stärkere Schutzmechanismen gegen Hackerangriffe. Deswegen bieten wir stets verbesserte aber kompatible Softwareschutzlösungen mit ausgereiften Sicherheitskonzepten für Softwarehersteller an. Faszinierend daran ist, dass wir unsere Produkte ständig in jeder Richtung verbessern müssen, um den Wettlauf mit Hackern aus Russland, den Wettbewerbern mit Low-cost-Produkten aus China und der stetigen Umsetzung neuester Technologien gewinnen können. Nur dies gibt uns die Chance, in einem Hochlohnland wie Deutschland langfristig erfolgreich zu sein und weiter zu wachsen.

EM: Wo sehen Sie die Hauptanwendungsgebiete Ihrer Produkte? Welche Branchen und Kunden wenden Ihre Produkte an?

Winzenried: Heute wird der Löwenanteil unserer Produkte zum Schutz von Software eingesetzt. Meist ist dies hochpreisige Software, bei der der Softwarepreis wesentlich den Preis der WIBU-BOX oder des CM-Sticks übersteigt.

personen mit Einzelplätzen als Professional Edition verfügbar. Die Verwendung dieses hardwarebasierten Authentifizierungssystems steigert die Sicherheit von Systemen – vor allem von Laptops mit sensiblen Daten. Da das SecuriKey Token am Schlüsselbund befestigt werden kann, ist die Wahrscheinlichkeit, dass es irgendwo vergessen wird oder liegen bleibt, minimiert. Bekannte und seit Kindheit antrainierte Verhaltensweisen helfen so, die Sicherheit des IT-Systems zu verbessern.

CodeMeter: CodeMeter ist eine Digital-Rights-Management-Lösung, die sicheren Schutz, Nutzungsmessung und vollautomatische Verkaufsabwicklung unter Einbindung des Handels ermöglicht. Verwendet wird hierbei ein USB-Stick, der so genannte CM-Stick. Auf ihm können bis zu 1.000 Lizenzen für verschiedene Produkte von unterschiedlichen Herstellern sicher (AES- und ECC-Algorithmen mit 128, bzw. 224 Bit Schlüssellänge und eigene Verschlüsselungsengine auf dem Stick selbst) gespeichert und verwaltet werden. Die Nutzungsmöglichkeiten des Systems gehen damit von Lizenz- und Kopierschutz über Pay-per-Use-Unterstützung bis hin zu einem sicheren Authentifizierungsverfahren, mit dem man seinen PC abschließen (bzw. erst den notwendigen Zugang erhält) oder E-Mails verschicken kann. Darüber hinaus ist der CM-Stick ein Memory-Stick, auf dem sich eigene Daten wie zum Beispiel PINs, TANs, Passwörter und beliebige andere Daten speichern lassen.

Hardware- oder Softwarelösung?

WIBU-KEY: Hardware

SmartShelter: Hardware

SecuriKey: Hardware

CodeMeter: Hardware

Betriebssysteme:

WIBU-KEY: Windows 95/98/2000/Me/XP/NT/Server 2003, Mac OS, UNIX, Linux, DOS

SmartShelter: Windows 95/98/Me/2000/XP

SecuriKey: Windows 2000 und Windows XP

Code Meter: Windows 98/2000/Me/XP, Mac OS, Linux

Preise: Auf Anfrage

Neben dem reinen Schutz werden Lizenzmanagement im Netzwerk sowie Logistikvorteile durch modulare Lizenzierung genutzt.
Die Hauptanwendungen liegen bei Software im CAD/CAE-Bereich, aber auch CRM-Lösungen und Software im industriellen Bereich, zum Beispiel Prozessvisualisierung oder auch Maschinensteuerungen.
Hinzu kommen Anwendungen im Konsumerbereich, die erstmals mit CodeMeter bedient werden können, da der Softwarehersteller den „Dongle" nicht kaufen muss: zum Beispiel „WISO Mein Geld" oder „Tax2005" oder Produkte im Spielebereich und Software für Musiker.

EM: Wo macht Kopierschutz Ihrer Meinung nach Sinn?

Winzenried: Kopierschutz passt für alle Arten von „Intellectual Property". Kopierschutz oder Digital-Rights-Management (DRM) ist für Anbieter und Nutzer von Vorteil gegenüber Pauschalabgabensystemen wie beispielsweise GEMA oder VG Wort. Warum? Pauschalabgabensysteme verteuern PCs, CD-Laufwerke, Drucker auch dann, wenn sie überhaupt nicht zum Kopieren urheberrechtlich geschützter Werke genutzt werden. Als nationale Lösung stellen sie außerdem Wettbewerbsnachteile für Deutschland dar. Anderseits werden die Urheber nicht angemessen entlohnt. DRM-Systeme wie CodeMeter bieten Flexibilität für den Anwender, der nur für das bezahlt, was er nutzen möchte, und dies aber mobil überall nutzen kann. Solche DRM-Systeme stellen sicher, dass der Urheber individuell den Preis seiner „Leistung" festlegen kann. Der Gesetzgeber hat sich schon in Richtung technische DRM-Systeme bewegt, jedoch die Pauschalabgabensysteme immer noch zu weit anerkannt. Sie sollten auf Analogkopien, zum Beispiel Fotokopierer oder analoge Audio/Videoaufnahme, beschränkt werden; hier sind diese bewährt und meines Erachtens in Ordnung. Bei digitalen Gütern passen sie aber nicht, da die Kopie keinen Qualitätsverlust gegenüber dem Original hat.

EM: Inwieweit hat sich die Art der von Ihnen angebotenen Produkte im Laufe der Jahre entwickelt?

Winzenried: 1989 war der Kopierschutz wirklich reiner Kopierschutz: Wenn der „Dongle"

Fortsetzung von Seite 78: Interview mit Oliver Winzenried

am PC angeschlossen wurde, konnte man die Software nutzen und sonst nicht. In der Zwischenzeit hat sich viel verändert: Neue Schnittstellen wie PCCard und USB, Multiplattformfähigkeit für Windows, Linux und Mac OS sowie die Unterstützung gemischter Netzwerke und neue Lizenzmodelle wie Pay-per-Use, Try-before-Buy kamen hinzu. Darüber hinaus ist es möglich, nachträglich Lizenzen in eine WIBU-BOX auf einfache und sichere Weise zu übertragen, die bereits an den Anwender geliefert wurde.

Durch harte Verschlüsselung und Technologien ausführbare Programme zu verändern, erreichen wir heute einen sehr hohen Sicherheitslevel. WIBU-SYSTEMS bewies dies durch drei Hacker's Contests. Das Ziel, eine geschützte Funktion zu knacken und ein geheimes Berechnungsergebnis dieser Funktion zu ermitteln, wurde nicht erreicht.

Mit CodeMeter bieten wir heute ein einzigartiges Produkt an: Der CM-Stick bietet DRM für Tausende von Lizenzen von unterschiedlichen Herstellern und gleichzeitig bis zu 2 GB sichere Flash Disk. Durch Verwendung von ECC- und AES-Verschlüsselung bieten wir anerkannte harte Verfahren und höchste Sicherheit durch einen vom Anbieter definierbaren Private oder Secret Key. Damit könnte selbst WIBU-SYSTEMS als Erfinder und Hersteller des Schutzsystems den Schutz nicht umgehen.

Bei CodeMeter erhält auch der Anwender einzigartige Vorteile: Zum Betrieb müssen keine Treiber mehr installiert werden, und jeder CM-Stick bringt persönliche Sicherheitsfunktionen wie den CM Password Manager, Steganos Safe zur Dateiverschlüsselung und Zugangsschutz mit SecuriKey Lite mit. Wichtig für die Akzeptanz im Konsumermarkt sind: CodeMeter wurde mehrfach ausgezeichnet, zum Beispiel mit dem iF Design Award, der Nominierung zum Designpreis 2006 der Bundesrepublik Deutschland und der Wahl zum Finalist bei der Software and Information Industry Association in den USA in der Rubrik „Best Digital Rights Management Solution: Software".

EM: Wie wichtig erachten Sie das Internet als Möglichkeit für die Realisierung von (neuen) Kopierschutzverfahren?

Winzenried: Gerade durch das Internet werden sichere Kopierschutzverfahren immer wichtiger. Das Internet ist das ideale und kostengünstigste Vertriebsmedium für digitale Güter aller Art wie Software, Studien, Standards, Dokumente, Musik und Videos. Die Einfachheit ermöglicht auch die Distribution illegaler angefertigter Kopien von Standorten, die keine Urheberrechte kennen.

Sind die Anwender „always online", so könnte man meinen, ein Kopierschutz wäre nicht mehr nötig, da der Anbieter ständigen Kontakt zur Anwendung hat. In den meisten Fällen funktioniert dies aber nicht, da erstens die Anwender auch „offline" die Software nutzen wollen und andererseits durch Programmpatches die Verbindung unterbrochen werden kann.

Produktaktivierung ist eine beliebte Lizenzierungsart in Massenmärkten. Sie hat den Vorteil, dass vor Nutzung der Software ein Kontakt zum Anbieter aufgebaut werden muss und der Anbieter durch eine Registrierung die Anwenderdaten erhält. Dies kann auch für den Anwender nützlich sein, wenn er über nützliche Tipps, Upgrades oder Updates informiert wird. Produktaktivierung bedeutet aber meist auch Bindung an einen bestimmten PC. Dies ist unbequem für den Anwender, wenn er wegen eines Defekts oder des Alters eines PCs auf einen neuen PC wechseln möchte, denn er muss alle Aktivierungen wiederholen. Der Anbieter auf der anderen Seite weiß nicht, wenn er die x-te Aktivierung durchführt, ob der Kunde tatsächlich einen neuen PC hat oder nur ein zusätzliche „Gratis-Lizenz" möchte.

Aktivierung mit CodeMeter bietet dagegen viele Vorteile: Ein CM-Stick kann nahezu unbegrenzt Lizenzen für viele Produkte speichern. Der CM-Stick wird durch Verwendung von Public-Key-Verfahren vom Licenseserver des Anbieters sicher authentifiziert. Der Anwender behält seine Mobilität. Lediglich der CM-Stick, der weitere Vorteile bietet, muss vom Anwender einmalig erworben werden. Dies ist eine Investition, die sich mehrfach auszahlt.

Für Pay-per-Use-Verfahren benötigt man sichere Hardware, um die Nutzung zu messen. Im Mobilfunkbereich ist dies die SIM-Karte im Handy. Aber was kann man beim PC nutzen? Solange TPM nicht verbreitet ist und neue Betriebssysteme dies unterstützen, benötigt man in jedem Fall sichere „Dongles". Bei CodeMeter kann ein Dongle viele Lizenzen speichern und mit unbegrenzten Attributen wie die Anzahl der Benutzer im Netzwerk, Pay-per-Use-Messungen, Ablaufdatum, Modulfreischaltung ausgestattet sein und diese beliebig kombinieren. Der Anwender benötigt also nicht spezielle Dongles für Netzwerksupport oder Zähler oder die Nutzung von Datumsinformationen.

EM: Wo stellen sich hier die Probleme in Bezug auf Angreifbarkeit von Internet-basierten Verfahren?

Winzenried: Wir bevorzugen heute stets Lösungen, die nur zur Übertragung von Lizenzen – also beim Kauf, Verkauf oder Update – eine Internetverbindung benötigen. Der Anwender kann seine Systeme unabhängig offline nutzen.

Die Lizenzübertragung über das Internet haben wir mehrfach mit Public Key Kryptographie abgesichert: Zum einen authentifiziert sich der CM-Stick beim Server des Anbieters. Dies verhindert, dass eine Softwaresimulation vortäuschen kann, ein CM-Stick zu sein. Die weiteren Schritte sind bei CM-Talk, unserem SOAP-basierten Protokoll zur Übertragung der Lizenzen übers Internet, ebenfalls abgesichert gegen alle möglichen Man-in-the-Middle-Angriffe.

Das Risiko beim Anwender besteht höchstens darin, dass der CM-Stick selbst ausfällt. Für diesen Fall kann der Anwender einen „Reserve-CM-Stick" haben, der die Lizenzen begrenzt für einen kurzen Zeitraum enthält. Dies gibt dem Anwender höchste Verfügbarkeit zu minimalen Kosten.

EM: Wie werden sich Kopierschutzsysteme Ihrer Meinung nach entwickeln?

Winzenried: Kopierschutz und Digital-Rights-Management-Systeme werden zusammenwachsen. Die Anwendungen werden erweitert: Von hochpreisiger Software heute zu Low-Cost-Software morgen, genauso wie für Dokumente, Online-Zeitschriften, Video On Demand, HDTV, DVB-H, Musik, Anwendungen im mobilen Bereich, zum Beispiel Navigation und Kartenmaterial. Dazu kommen neue gesetzliche Anforderung an eCommerce, zum Beispiel Altersverifikation beim Online-Weinhändler oder für Erotikangebote.

Mit CodeMeter arbeiten wir an Lösungen in diesen Bereichen. Neben den PC-Plattformen mit USB-Schnittstelle (Windows, Linux, Mac OS, Mediacenter und Settopboxen) werden wir das DRM mit CodeMeter auf PDAs und High End Mobile Phones, die heute meist einen SD/MMC Slot bieten, ausdehnen.

Natürlich können wir als mittelständisches Unternehmen keine weltweiten Standards festlegen. Wir setzen an dieser Stelle auf Kooperationen mit den Big-Playern und versuchen, wo immer es geht, Interoperabilität mit den am Markt bestehenden Systemen herzustellen. Durch Patente rund um CodeMeter stellen wir sicher, dass wir in solchen Kooperationen langfristig am Erfolg teilhaben können.

EM: Vielen Dank für das Gespräch.