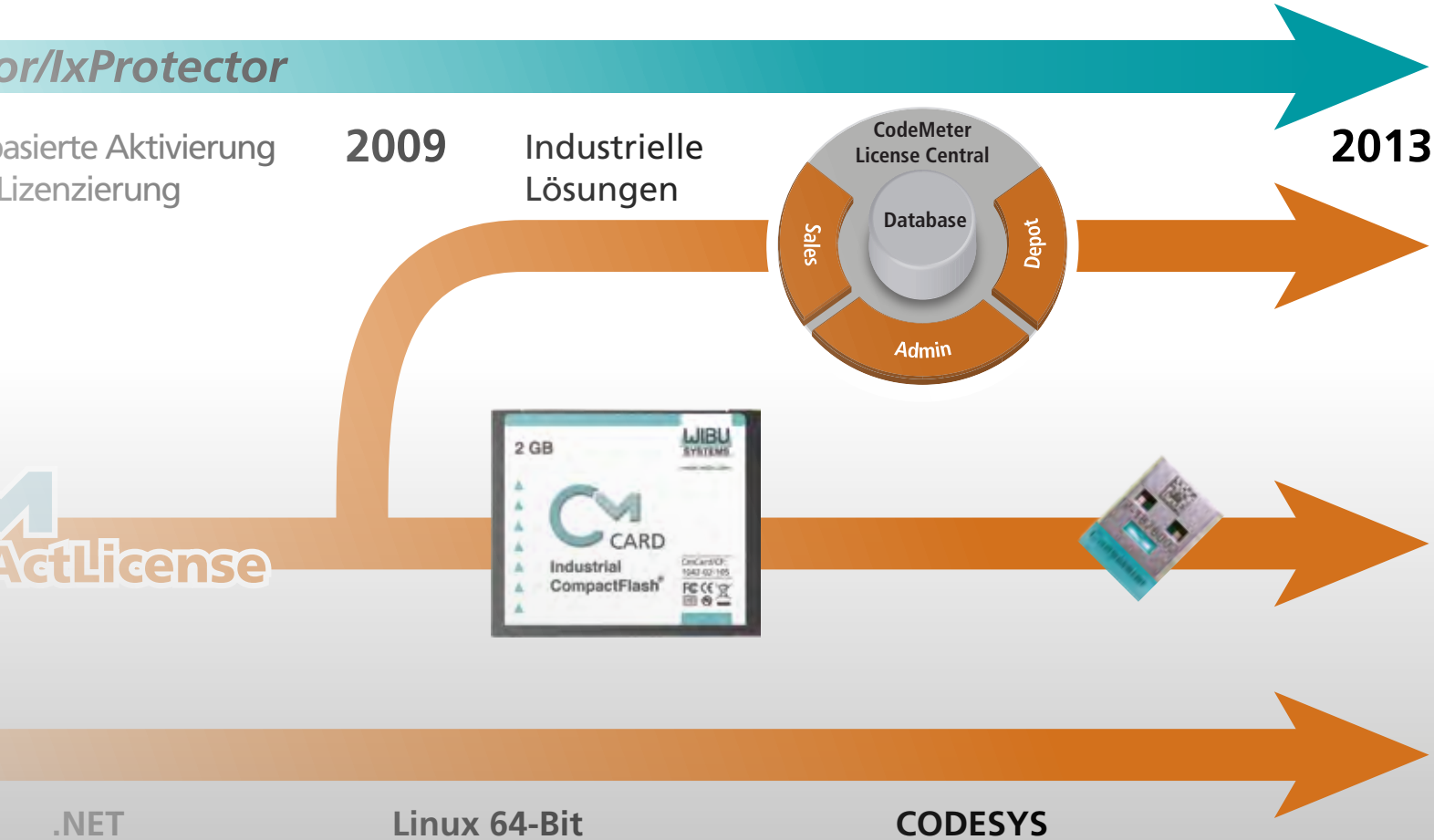
FRÜHJAHR 2013



.NET Linux 64-Bit CODESYS

Embedded OS VxWorks

KEYnote 25

DAS WIBU-MAGAZIN

Innovation und Kontinuität @ Wibu-Systems

Themen

- VxWorks EDK mit CodeMeter
- Fallen gegen Hacker
- License Central Reporting

WIBU SYSTEMS

Inhalt

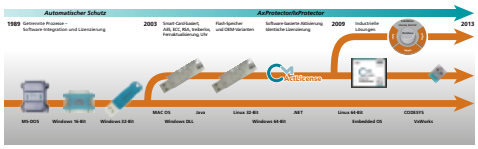
PRODUKT
Studio 5000 Projektschutz 3

PRODUKT
VxWorks EDK mit CodeMeter 4



KNOW-HOW
Fallen gegen Hacker 6

INFORMATION
Innovation und Kontinuität @ Wibu-Systems 8



PRODUKT
License Central Reporting 10

PRODUKT
Hosting und Support 12



HIGHLIGHTS
Aktuelles in Kürze 14

CASE STORY
Erfolgsgeschichte Glaser 15

INFORMATION
Wibu-Systems informiert 16

Sehr geehrte Kunden und Partner,



Politik, Verbände und Unternehmen widmen sich der Industrie 4.0, der vierten industriellen Revolution. Die Skaleneffekte der Serienproduktion sollen mit Individualisierung bis zur Losgröße 1 herunter in einem Konzept kombiniert werden. In der Produktion entstehen sog. Cyber-Physical-Production-Systems mit intelligenten Maschinen, die eigenständig Informationen austauschen und sich steuern. Sie schaffen Smart Factories mit einer völlig neuen Produktionslogik: horizontale Integration über die Wertschöpfungskette, vertikale Integration und vernetzte Produktionssysteme sowie eine Durchgängigkeit des Engineerings über den gesamten Lebenszyklus. Schutz vor Produktpiraterie und Know-how-Schutz sind dabei wichtiger denn je. Ferner sind ganzheitliche Sicherheitskonzepte nötig, die sowohl Cloud Security als auch Industrial Security adressieren. Wir bieten hier Lösungen, arbeiten in der Arbeitsgruppe „Security in der Industrie 4.0" in Deutschland und integrieren unsere Lösungen in OPC UA der amerikanischen OPC Foundation, der wir im Dezember 2012 beigetreten sind.

Hier zeigt sich, wie wichtig Kontinuität und Innovation sind. Unsere neuesten Tools unterstützen WibuKey; gleichzeitig bauen wir CodeMeter aus: vom softwarebasierten CmActLicense über CmDongles für industrielle Umgebungsbedingungen bis zur Cloud-Lösung für das Ausrollen der Lizenzen und die Integration in Vertriebs- und Fertigungsprozesse. Viele Eigenschaften, die Marktbegleiter heute „neu und unique" nennen, erfüllen unsere Produkte schon seit über zehn Jahren.

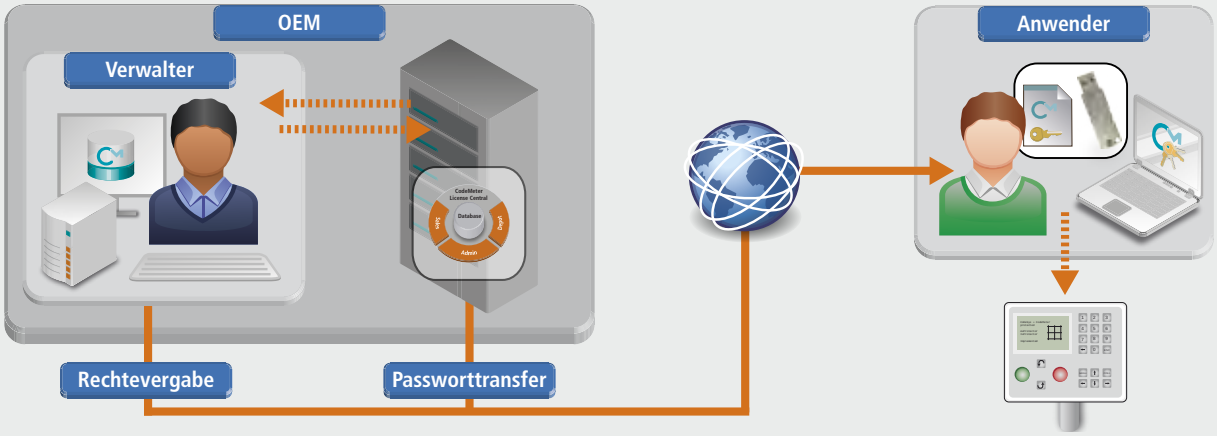
Lesen Sie über spannende Themen: eine Zeitreise durch die Wibu-Produkte, Beispiele zum Know-how-Schutz in Rockwells RS Logix 5000, verbesserter Schutz durch Fallen gegen Hacker, unser EDK für Wind Rivers VxWorks, Interessantes zur Cloud-basierten Hostinglösung für die CodeMeter License Central, die Erfolgsgeschichte unseres Kunden Glaser-ISB und weitere Neuigkeiten.

Im Frühjahr stellen wir auf vielen Messen aus. Besuchen Sie uns – ich freue mich auf ein persönliches Gespräch mit Ihnen

Oliver Winzenried (Vorstand)

Rockwell Automation

Studio 5000 Projektschutz



Rockwells Studio 5000 Entwicklungsumgebung – jetzt neu mit CodeMeter zur Rechteverwaltung zum Schutz geistigen Eigentums



Früher wurde der Zugriff auf den Quellcode einfach über Passwörter geregelt. Passwörter sind an sich nicht besonders sicher und mit dem Menschen kommt ein weiterer Unsicherheitsfaktor hinzu. Passwörter sind oft schwach und daher leicht zu knacken. Ferner können sie absichtlich oder unabsichtlich weitergegeben werden und gestatten dauerhaft Zugriff, wenn sie nicht zeitlich begrenzt sind.

Aufwendig entwickelte und teure eingebettete Systeme verdienen den bestmöglichen Schutz. Gewährt ein Passwort Zugriff auf den Quellcode, so sollte es besonders sicher und zuverlässig gespeichert werden.

Der „Studio 5000 Logix Designer" von Rockwell ist eine anwenderfreundliche Entwicklungsumgebung zum Design und zur Konfiguration von Automatisierungssystemen, geeignet für unterschiedliche Einsatzgebiete von OEM-Herstellern, Systemintegratoren und Anwendern.

Der Quellcode zur Steuerung der Controller-Hardware von Rockwell wird vom Studio 5000 aus verwaltet. Dank der neuen Technologie von Wibu-Systems werden Passwörter nicht mehr unverschlüsselt lokal in einer Datei gespeichert, sondern verschlüsselt in einem „CmContainer". Dieser ist entweder ein „CmDongle" (eine Smart-Card-basierte Schutzhardware, z.B. der USB CmStick) oder eine Aktivierungsdatei „CmActLicence". Der CmContainer kann darüberhinaus selbst noch über ein Kennwort geschützt werden. Dadurch wird eine Zwei-Faktor-Authentifizierung erreicht, da sowohl der Besitz des passenden CmContainers als auch die Kenntnis dessen Kennworts erforderlich ist.

Der „CodeMeter Source Protection Provider" CSPP ist eine Anwendung zur zentralen Verwaltung dieser Passwörter in CodeMeter, speziell für den Unternehmensbereich. Mit dem „CSPP Manager" werden Benutzerrechte verwaltet. Die „CodeMeter License Central" läuft auf einem zentralen Rechner und sorgt für die Verteilung der Benutzerrechte an die Rechner der Anwender, auf denen der „CSPP Client" und die Entwicklungsumgebung Studio 5000 laufen. Wann, wie lange und welche Funktionen von Studio 5000 der Anwender nutzen kann, hängt von den zuvor zugeteilten Nutzungsrechten ab.

Über das sichere Speichern der Benutzerrechte hinaus, bietet die neue CodeMeter-Technologie von Wibu-Systems weitere Vorteile wie kryptographisch starke Authentifizierung und Aktualisierung aus der Ferne, entweder über das Internet oder Dateiaustausch. Damit ist das Zuweisen von Benutzerrechten auch über unsichere Übertragungswege sicher und einfach möglich. Die Rechte können dabei zeitbegrenzt sein, die Anzahl der Zugriffe begrenzen oder einfach dauerhaft vergeben werden. Darüber hinaus kann ein CmDongle mit Flash-Disk verwendet werden, der rückwärtskompatibel auch eine sichere Speicherung der „Rockwell Source Protection Keys" in der bisherigen Passwortdatei ermöglicht.

Dank Wibu-Systems CodeMeter-Technologie ist Logix Studio 5000 nicht nur eine der effizientesten und benutzerfreundlichsten Entwicklungsumgebungen, sondern auch eine der sichersten – geschützt vor beabsichtigten oder unabsichtlichen Manipulationen. Hersteller ernten selbst die Früchte ihres Entwicklungsaufwands für ihr geistiges Eigentum und machen Plagiatoren das Leben schwer.



VxWorks EDK mit CodeMeter

Das Embedded Development Kit für VxWorks ist das Ergebnis der Zusammenarbeit von Wind River, Emerson und Wibu-Systems. Entwickler schützen ihr Know-how und Produkt gegen Pir aterie, Reverse Engineering und Angriffe. Dabei verhindern sie Manipulationen ihres Codes , booten sicher das Betriebssystem und führen ihre Anwendungen sicher aus. Flexible Abrechnungsmodelle wie Pay-per-Use oder Feature-on-Demand ermöglichen neue Geschäftsmodelle.

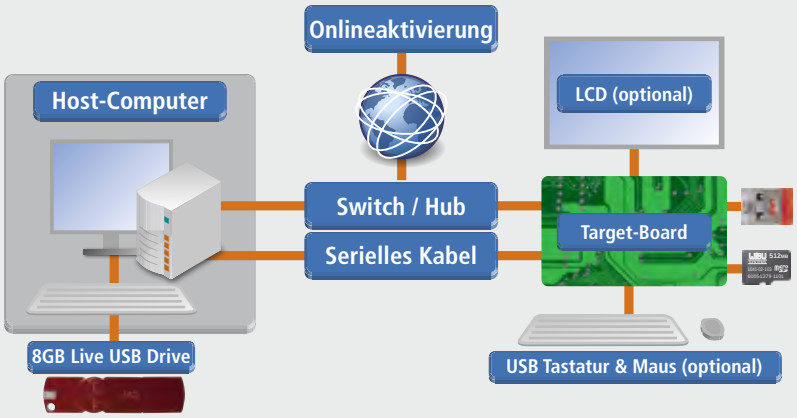
CodeMeter wurde für VxWorks erweitert und so in die Eclipse basierte Wind River Workbench integriert, dass Anwender ohne externe Tools ihren Code schützen können.

Die Schritt-für -Schritt-Anleitung und vorbereitete Beispiele zeigen dem Entwickler die unterschiedlichen Einsatzmöglichkeiten:

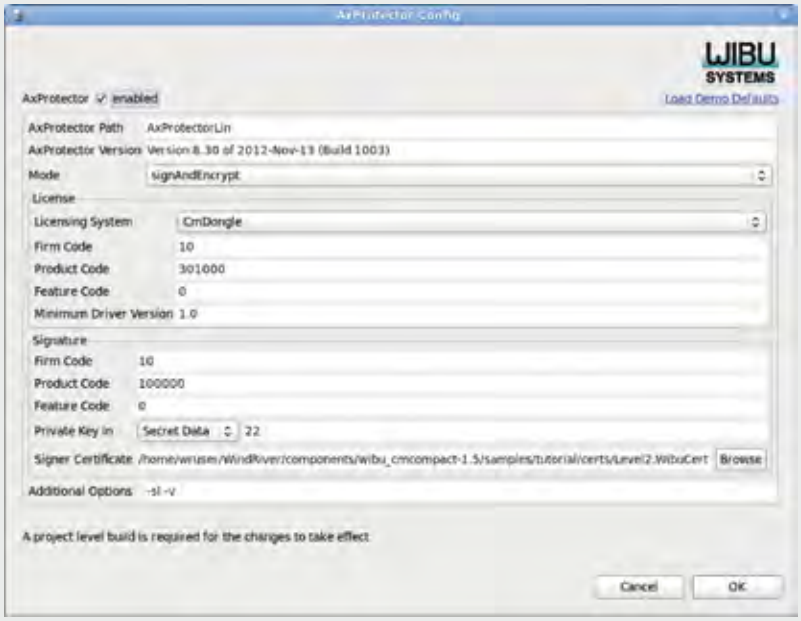
- Softwareschutz gegen Kopieren der Software durch Verschlüsselung des Programmcodes
- Know-how-Schutz gegen Reverse Engineering der implementierten vorteilhaften Algorithmen
- Integritätsschutz gegen unberechtigtes Ver-ändern des Progr ammcodes, z.B. durch Cy-berangriffe
- Feature-on-Demand als Business Enabler für neue Geschäftsmodelle

Zum Lieferumfang des Wind River EDK gehören ein Emerson NITX-315-Board mit Intel Atom-Prozessor und drei CmDongles . Die VxWorks-Entwicklungsumgebung wird direkt vom CmStick/M am Host C omputer ges tartet. Di e CmCard/µSD wird ins Target-Board gesteckt und enthält das VxWorks-Boot-Image sowie die dazu notwendigen CodeMeter -Lizenzen. Der CmStick/C wird am Target-Board angeschlossen und enthält eine Lizenz, um weitere Features der Software, die bereits im Image enthalten sind, nutzen zu können.

Der AxProtector als Eclipse-Plug-in schützt verschiedene Projekte wie VxWorks Image (VIP), Downloadable K ernel Modules (DKM) und Real-T ime-Processes (RTP). Alle Einstellungen erfolgen innerhalb der Wind River Workbench: Schutz gegen Reverse Engineering und Lizenzmanagement und/oder



So werden die CodeMeter Dongles, der Entwicklungsrechner und das Target-Board verbunden



Alle Einstellungen des Wibu-Systems AxProtector erfolgen über ein Plug-in in der Wind River Workbench

Schutz gegen Verändern durch Codesignaturen, Parameter für das Lizenzmanagement und die Codeverschlüsselung sowie Schlüsselquelle für den privaten Schlüssel zur Codesignatur.

Um die Sicherheits- und Lizenzmanagementfunktionen nutzen zu können, wird der Standard VxWorks-Loader durch den CodeMeter-VxWorks-Loader ersetzt. Dies stellt sicher, dass nur korrekt signierte Projekte auf dem Zielsystem ausgeführt und entschlüsselt werden.

Signaturen und Zertifikate

Beim Start des geschützten VxWorks-Projekts auf dem Zielsystem prüft CodeMeter die Integrität. Der AxProtector nutzt für Signaturen asymmetrische Kryptografie mit elliptischen Kurven (ECDSA Elliptic Curve Digital Signature Algorithm) in drei Schritten:

1. Der AxProtector signiert eine Prüfsumme, genau genommen einen Hash-Wert über das Projekt oder den Programmcode, mit dem privaten Schlüssel. Der signierte Hash-Wert wird Signatur genannt und entspricht einem digitalen Fingerabdruck für dieses Projekt.
2. Gleichfalls errechnet der modifizierte VxWorks-Loader den Hash-Wert, um diesen mit der digitalen Signatur abzugleichen. Dabei wird der Public-Key benutzt, um den digitalen Fingerabdruck durch den Vergleich beider Hash-Werte zu prüfen.
3. Nach erfolgreicher Prüfung gilt das VxWorks-Projekt als unverändert, d.h. es wurde nicht verändert, seit es mit dem richtigen Private-Key signiert wurde.

Mit Hilfe von Zertifikaten wird sichergestellt, dass bei der Prüfung der richtige Public-Key verwendet wird. Zertifikate sind digitale Äquivalente zu Ausweisdokumenten im realen Leben. Sie ermöglichen die Prüfung, ob der gespeicherte Public-Key wirklich zum passenden Private-Key gehört.

Zertifikatskette

Zur Prüfung der Authentizität nutzt Wibu-Systems eine Kette an Zertifikaten, auch „Chain of Trust" genannt, welche die Richtigkeit des öffentlichen Schlüssels garantiert. Dieses Verfahren beruht auf dem Root-Zertifikat als „Anchor of Trust" in einer Reihe verschiedener Zertifikatsabfragen, wobei das Vertrauen an die darüber liegende Schicht vererbt wird. Der Schlüsselwert liegt im jeweiligen Public-Key. Im Detail sieht eine Zertifikatskette wie folgt aus:

1. Die Einstellungen des AxProtectors erlauben dem Entwickler, ein Integritätszertifikat zu definieren, bestehend aus einem Hash-Wert, der Signatur und des Public-Keys.
2. Sobald das VxWorks-Projekt geladen wird, berechnet der VxWorks-Loader binär einen Hash-Wert und vergleicht diesen mit dem Hash-Wert, der vom AxProtector als Integritätszertifikat erzeugt wurde. Stimmen diese Werte nicht überein, wird das VxWorks-Projekt nicht geladen.
3. Sind beide Hash-Werte gleich, dann beginnt die Signatur-Prüfung über die Zertifikate. Bei jeder Ebene benutzt die Signatur-Prüfung den Public-Key der darunter liegenden Ebene, bis zum Root-Zertifikat.

Dieses auf den ersten Blick sehr komplex aussehende Verfahren ist so integriert, dass es für den Entwickler einfach zu handhaben ist. Es bietet den großen Vorteil, dass das wichtigste Geheimnis, nämlich der private Schlüssel des Root-Zertifikats, nur einmal zur Signatur der untergeordneten Zertifikate benötigt wird und dann im Safe verschwinden kann. Selbst wenn ein Zertifikat einmal kompromittiert sein sollte, kann dieses über einen „Revocation-Mechanismus", der jetzt hier nicht weiter ausgeführt werden soll, zurückgerufen werden. Dadurch bleibt die Sicherheit und Integrität des Gesamtsystems erhalten und die ausgerollten Systeme müssen auch dann nicht getauscht werden.

Erstellen, Verwalten und Ausrollen der Lizenzen

Neben den Sicherheitsfunktionen ist es auch wichtig, die Erstellung und Verteilung der Lizenzen und Schlüssel in die Vertriebs- und Herstellungsprozesse zu integrieren. Die CodeMeter License Central ist die Lösung dafür. Sie wird über einen Browser oder eine Webschnittstelle bedient und lässt sich leicht in bestehende ERP-Systeme wie SAP oder MS Dynamics, CRM-Systeme wie Sales Force oder Online-Shops integrieren. Die License Central kann beim Hersteller betrieben werden oder als Wibu-Cloud-Lösung genutzt werden.

Mit dem Wind River EDK sieht der Entwickler, wie verschiedene Funktionen in einer Anwendung unterschiedlich geschützt werden, sodass zu deren Ausführung später eine individuelle Lizenz erforderlich ist. Dies kann sinnvoll sein, um Gerätefunktionen separat zu verkaufen, auch Aftersales, oder um bestimmten Personen, z.B. Servicetechnikern, die Nutzung spezieller Funktionen zu ermöglichen.



Fallen gegen Hacker

Vielleicht haben Sie bereits meinen Artikel „Softwareschutz aus der Sicht eines Hackers" in der vorletzten KEYnote gelesen. Dort habe ich mir die Zähne an der Emulation eines CodeMeter -Dongles ausgebissen. Die verschlüsselte Kommunikation zwischen Dongle und Software ist zwar nur „State-Of-The-Art", aber die im Datenstrom versteckten P-RID-Pakete stellen eine komplett neue Qualitätsstufe im Softwareschutz dar. Die in diesem Artikel beschriebene Art des Angriffs durch Emulation des Dongles habe ich vor allem in Russland gesehen. Daher nenne ich dies auch gerne den „Russischen Hack". Gegen den „Russischen Hack" kann sich CodeMeter erfolgreich wehren, aber was ist mit dem „Chinesischen Hack"?.

Der Chinesische Hack

Während der russische Hacker die Software nahezu unverändert lässt, patcht der chinesische Hacker die Software und ersetzt verschlüsselte Stellen durch den unverschlüsselten Code. Damit sind natürlich der Aufwand und die Gefahr von Risiken und Nebenwirkungen deutlich höher als beim russischen Pendant.

Der Aufwand des „Chinesischen Hacks" hängt dabei natürlich davon ab, ob die Software überhaupt verschlüsselt ist oder reine API-Aufrufe absetzt. Falls sie verschlüsselt ist, ist es natürlich ein deutlicher Unterschied, ob es wie bei den meisten Produkten ein großer Block mit einem Schlüssel ist oder ob es wie bei CodeMeter viele kleine Puzzlesteine, evtl. sogar mit unterschiedlichen Schlüsseln, sind.

Auch hier zeigt sich CodeMeter als „Best-of-Breed". Bei CodeMeter wird die Software mit AxProtector und IxProtector in viele kleine Puzzlesteine zerlegt und erst zur Laufzeit dynamisch wieder zusammengesetzt. Dabei werden, sogar bei der gleichen Lizenz, unterschiedliche Schlüssel verwendet. Aber wie gut ist dies gegen den „Chinesischen Hack"?

Dynamisch vs. Statisch

Prinzipiell gibt es zwei Vorgehensweisen beim Reverse Engineering. Entweder analysiert der Hacker die Software ohne diese auszuführen durch Disassemblieren und manuelles Entschlüsseln (statische Analyse) oder er führt die Software in einem Debugger aus und beobachtet und modifiziert sie dabei (dynamische Analyse).

Bei einer HelloWorld-Anwendung ist beides mehr oder weniger trivial. Bei der dynamischen Analyse besteht natürlich die Gefahr, dass die geschützte Software Anti-Debug-Maßnahmen implementiert hat und ich als Hacker in eine Debugger-Erkennung tappe.

Bei einer richtigen Anwendung stellt sich dies natürlich anders dar. Im Falle der statischen Analyse muss ich als Hacker alle Teile finden und wieder zusammensetzen. Dies ist ein großer Aufwand, den ich natürlich als Hacker gerne automatisieren möchte.

Die dynamische Analyse

Bei der dynamischen Analyse höre ich oft von angehenden Jung-Hackern, dass „man doch nur warten müsse, bis alle verschlüsselten Methoden einmal aufgerufen wurden und damit entschlüsselt im Speicher liegen". Ich bin seit den ersten Yellow Point und Yellow Star CDs 1996 in den Bereichen Softwareentwicklung, Softwaretest und Reverse Engineering tätig. Und aus meiner Erfahrung kann ich eins ganz sicher sagen: Wer es schafft, eine fremde Software

nahezu komplett zu durchlaufen, d.h. fast jede Codestelle einmal auszuführen, der hat den Stein der Weisen und den Heiligen Gral zugleich gefunden. Wer dies kann, der verdient viel Geld mit seinen Testwerkzeugen und genießt seine Schirmchen-Drinks auf seiner „eigenen" Insel in der Südsee.

Betrachten Sie zum Beispiel eine Software wie MS Word. Selbst ein Poweruser nutzt weniger als 10% der Funktionalität. Wäre diese Software so geschützt, welcher Hacker würde es schaffen, dann 100% des Codes zu durchlaufen?

Zusammengefasst kann man sagen, dass eine dynamische Analyse bei einer mit dem IxProtector geschützten Anwendung bis auf wenige Ausnahmen, die meist die Komplexität einer HelloWorld-Anwendung nicht übersteigen oder den IxProtector nur rudimentär nutzen, nicht erfolgreich sein wird.

Ein kurzer Rückblick

Die Yellow Point CD ist übrigens ein wunderbares Beispiel, wie man es nicht machen sollte. Eine reine Marketingfirma hat von einem Ingenieur-Büro (ohne vorherige Erfahrung in Bereich Softwareschutz) eine Freischalt-CD entwickeln lassen. Das Ergebnis war in weniger als einer Woche nach Veröffentlichung geknackt. Der Grund war ein fataler Implementierungsfehler, der den verwendeten Schlüssel stark verkürzt hat. Wenn man davon ausgehen kann, dass in jedem verschlüsselten Archiv am Anfang eine exe liegt, was bei 95% der Produkte der Fall war, musste man nur die wenigen Schlüssel durchprobieren und auf „MZ" (die Kennung einer exe") triggern. Schon war der Hack fertig. Die Entschlüsselungsroutinen wurden mit der Software ja gleich mitgeliefert. Beim Nachfolger Yellow Star hat man dann auf eine Firma mit jahrelanger Erfahrung in diesem Bereich gesetzt. Diese CDs wurden übrigens nie gekrackt. Die Firma Yellow Point, die alles selbst hat machen lassen, war schnell vom Markt verschwunden. Die Firma hinter Yellow Star, die das Know-how und die Lösung eingekauft hatt, wurde zu einem jahrelangen Erfolg.

Die statische Analyse

Was ist, wenn ich als Hacker also die Anwendung statisch analysiere? Ich nehme mir jede einzelne Methode und entschlüssle diese separat. Dann füge ich die ganze Anwendung wieder zusammen. Und ähnlich wie bei der Yellow Point CD wird der Code zum Entschlüsseln ja gleich mitgeliefert. Ich muss mir diese Routine noch nicht einmal selber schreiben. Wobei das CodeMeter-API so gut zu benutzen ist, dass dies auch kein großer Aufwand für mich wäre. Die Theorie ist klar, also mache ich mich an die Praxis. Und hier kommt eine große Gemeinheit von CodeMeter. Die verschlüsselte Anwendung ist mit Fallen für meine statische Analyse gespickt und ich habe mir ähnlich wie bei der Debugger-Erkennung bei der dynamischen Analyse schon wieder meine Lizenz gesperrt.

Was ist geschehen? In der Anwendung liegt Code, der eigentlich nie ausgeführt wird, also auch nie entschlüsselt wird. Bei meiner statischen Analyse finde ich natürlich alle verschlüsselten Stellen, was gar nicht so einfach war. Wenn ich alle diese Stellen nacheinander entschlüssele, dann wird auch eine solche Falle entschlüsselt. In dem Augenblick, in dem eine solche Falle entschlüsselt wird, sperrt sich der CodeMeter-Dongle intern automatisch. Aufgrund der vielen unterschiedlichen Schlüssel bei CodeMeter ist es mir unmöglich, eine Falle vorher zu erkennen. Ich merke es erst, wenn es zu spät ist. Aber dann ist die Lizenz gesperrt und ich kann es vergessen, die nächsten Stellen zu entschlüsseln. Die Lizenz ist ja gesperrt.

Diese Art der Fallen durch verschlüsselte Methoden, die beim Entschlüsseln automatisch die Lizenz sperren, ist ein weiterer Quantensprung, der CodeMeter von anderen Schutz- und Lizenzierungssystemen abhebt.

Ablaufdiagramm

Einen Versuch habe ich mir noch gegeben. Ich fange mit der Entschlüsselung der Main-Funktion an und hangle mich durch den Programmablauf. Ich suche, welche Methoden von hier aus aufgerufen werden (natürlich schreibe ich mir dafür ein Tool), entschlüssele diese und suche dort wieder . D. h. ich baue mir ein Ablaufdiagramm der Software auf und finde auf diese Weise heraus, welche Methoden aufgerufen werden und welche nicht. Übrigens, am Namen kann man dies nicht erkennen. Die Jungs von CodeMeter sind eben Profis.

Wenn ich dieses Ablaufdiagramm habe, dann – so dachte ich zumindest – kenne ich alle guten Stellen und kann die anderen als Fallen einstufen. Aber auch hier hat CodeMeter natürlich die Antwort parat. Erwähnte ich schon, dass ich als Hacker an CodeMeter verzweifle? Einige Methoden werden durch Reflection aufgerufen (natürlich sind die Methodennamen verschlüsselt) und können so nicht automatisch als gute Funktionen erkannt werden. Aber noch schlimmer; es sieht so aus, als wenn einige der Fallen in meinem Ablaufdiagramm auftauchen. Durch Verzweigungen, die nach der Logik des Programmes nie zutreffen, werden diese nie aufgerufen, tauchen aber als Verzweigung bei meiner Analyse als „gut" auf Und schon wieder sitze ich in der Falle.

Mein Fazit

Und wieder bin ich von CodeMeter beeindruckt. CodeMeter kannte wieder einmal die Antwort auf alle Fragen, die mir eingefallen sind. Die Unterschiede von CodeMeter zu anderen Produkten sind auf den ersten Blick zwar nur gering: fast alle bieten einen Wrapper. Aber die Funktionen unter der Haube, sorgen dafür, dass CodeMeter dem Hacker den entscheidenden Schritt voraus ist.

Natürlich ist der Schutzlevel stark von der Integration in die Software abhängig. CodeMeter kann Fallen automatisch hinzufügen, aber die volle Wirksamkeit entfaltet sich erst, wenn ich als Entwickler der Software die Fallen hinter meiner Geschäftslogik verstecke. Als Entwickler weiß ich, dass eine Böschung nie mehr als 90% geneigt ist, dass mein Kartensatz immer eine gerade Anzahl an Karten enthalten muss, dass mein Motor nie mehr als 19.000 Umdrehungen macht oder der Spitzensteuersatz nie mehr als 100% sein kann. Aber der Hacker weiß dies in der Regel nicht und wird daher in diese Fallen tappen. Und ein Hacker mit einer gesperrten Lizenz ist all seiner Waffen beraubt, CodeMeter sei Dank.

Wibu-Systems Professional Services Team

Unser Team unterstützt Sie, um Ihre Anforderungen schnell und kostengünstig umzusetzen. Dies umfasst Konzepte und deren Implementierung, so dass Sie wertvolle Zeit sparen. Nutzen Sie unser Wissen und unsere Erfahrung und fordern Sie uns: sales@wibu.com, Tel. +49-(0)721/93172-17



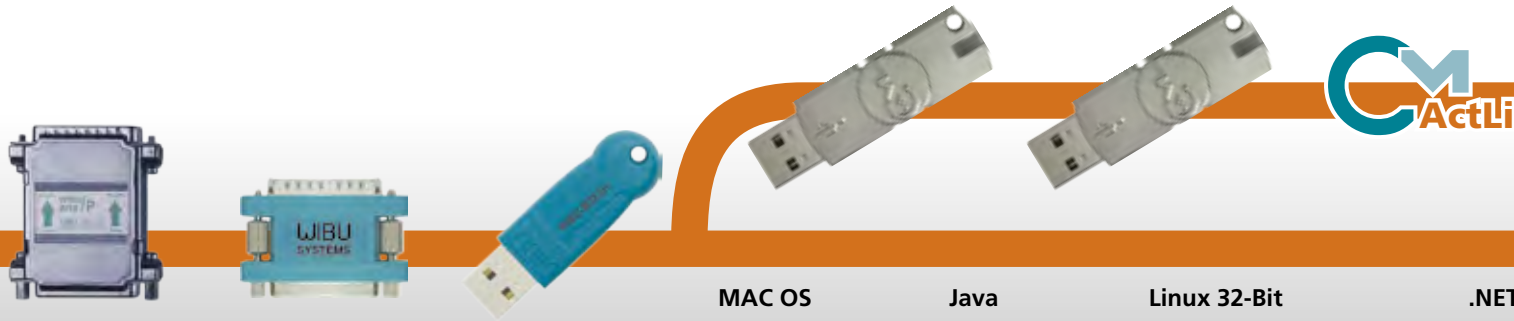
Automatischer Schutz *AxProtector/IxP*

1989 Getrennte Prozesse –
Software-Integration und Lizenzierung

2003 Smart-Card-basiert,
AES, ECC, RSA, treiberlos,
Fernaktualisierung, Uhr

Flash-Speicher
und OEM-Varianten

Software-basierte A
Identische Lizenzier



Innovation und Kontinuität @ Wibu-Systems

Wibu-Systems wurde 1989 gegründet um, ein einfach handhabbares Softwareschutzsystem anzubieten. Ziele waren Know-how-Schutz gegen Reverse Engineering, Schutz vor Produktpiraterie, also Kopierschutz und Umsetzung neuer Geschäftsmodelle. WibuKey hatte schon damals Eigenschaften, die heute noch nicht selbstverständlich sind: ein Dongle für Netzwerk und Einzelplatz, Programme auf Funktionsebene unterschiedlich verschlüsseln oder eine geschützte Software erstellen, die von verschiedenen Kunden individuell je nach Lizenzen genutzt wird.

Die Verbindung aus Kontinuität und Innovation hat Wibu-Systems heute, 24 J ahre später, zu einem Anbieter mit einer weltweit einzigartigen Palette an Lösungen gemacht:

- Softwarebasierte Aktivierung
- Smart-Card-basierte Dongles für viele Schnittstellen
- Web- und cloud-basiertes Ausrollen der Lizenzen mit Integration in Vertriebsprozesse.

Die Einsatzgebiete reichen von mobilen Systemen über industrielle Anwendungen in Embedded-Systemen und SPS bis zu Desktop-PCs, Servern und zur Cloud. Kein Marktbegleiter hat eine so vollständige Palette in der Breite.

Was versteht Wibu-Systems unter Kontinuität?

- **Unternehmen:** inhabergeführt, finanziell unabhängig, Festhalten an Visionen, partnerschaftliche Philosophie in der Zusammenarbeit mit Mitarbeitern, Lieferanten und Kunden
- **Mitarbeiter:** konstante Ansprechpartner über viele Jahre, ständige Weiterbildung und Schulungen in allen Bereichen, hohe Identifikation mit Unternehmen, Produkten und Zielen
- **Entwicklungsprozesse:** integriert in das QM-System nach ISO 9001:2008, Codemetriken, Versionskontrolle, Daily Builds, Test Driven Development, teilweise Scrum, professionelles Produktmanagement, kein Outsourcing; Design, Development & Produktion „Made in Germany“
- **Kooperationen:** Forschungs- und Entwicklungsprojekte mit Hochschulen, Forschungseinrichtungen und Partnern, Standardisierungsgremien wie USB IF, SDA, OPC, intensive Arbeit in Verbänden
- **Produkte:** langfristig verfügbar, hohe Zuverlässigkeit, kontrollierte Stückliste (BOM), rückwärts kompatibel, aktualisierbar im Feld, Made in Germany

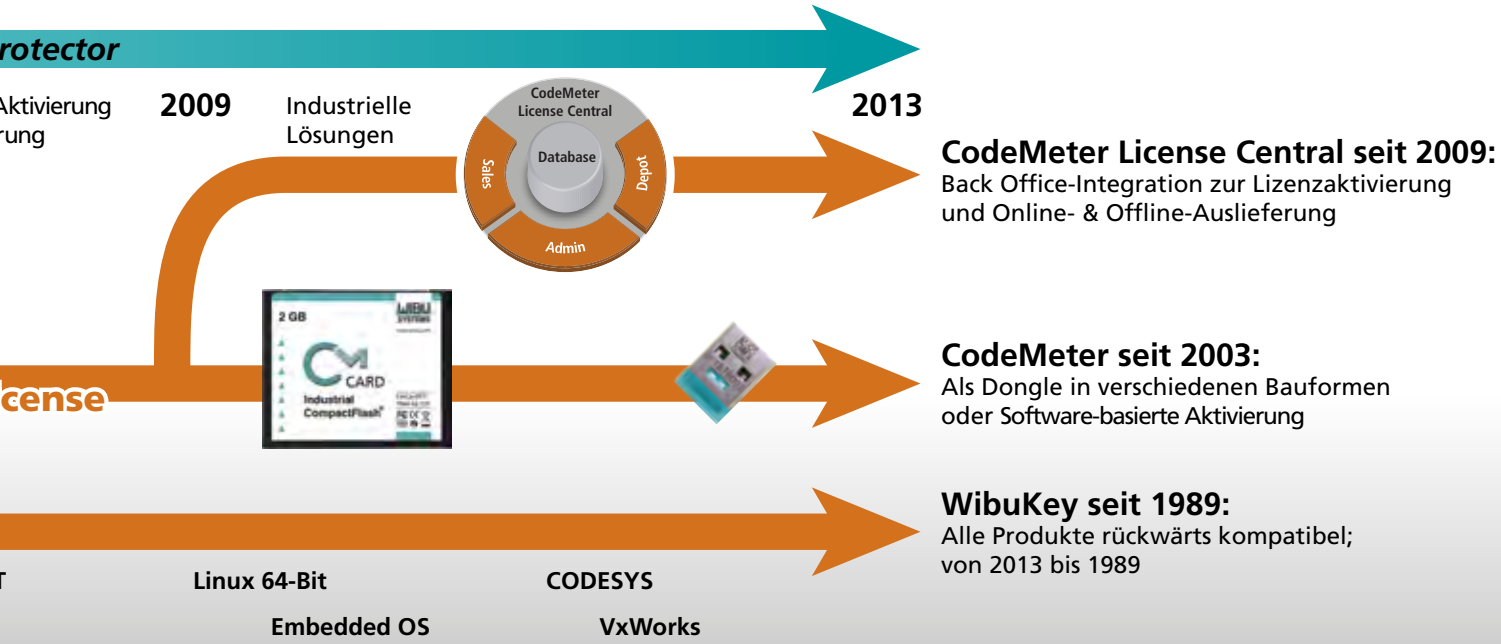
Zeitreise zu den wichtigen Innovationen von Wibu-Systems:

1989:

- WibuKey: ein Dongle für Einzelplatz und Netzwerk, auch 2013 noch verfügbar
- 240 Softwarefunktionen individuell lizenzieren mit einem Dongle
- Software einmal verschlüsseln und für alle Kunden individuell lizenzieren
- WibuKey als ASIC erhältlich

1990:

- WibuKey für serielle Schnittstelle und als Steckkarte
- Automatischer Schutz fürWindows- und DOS-Anwendungen, ohne Quellcodemodifikation
- WibuKey-Dongles mit FEAL-Algorithmus von NTT, Japan, rückwärts kompatibel mit V1 von 1989
- 4 Milliarden Verschlüsselungsvarianten pro Lizenzeintrag



CodeMeter License Central seit 2009:
Back Office-Integration zur Lizenzaktivierung und Online- & Offline-Auslieferung

CodeMeter seit 2003:
Als Dongle in verschiedenen Bauformen oder Software-basierte Aktivierung

WibuKey seit 1989:
Alle Produkte rückwärts kompatibel; von 2013 bis 1989

1993:
- WibuBox/M als PCMCIA-Karte

1994:
- Neues prämiertes WibuBox/P-Gehäuse
- Verschlüsselung einzelner Funktionen (AXAN, heute IxProtector genannt)

1997:
- Wibu-Systems ISO 9001 zertifiziert

1998:
- WibuBox/U für die USB-Schnittstelle

2001:
- Erstes CodeMeter-Patent angemeldet

2003:
Markteinführung von CodeMeter mit wegweisenden Eigenschaften:
- Höchste Sicherheit mit Smart-Card-Chip als Herzstück
- Verwendung von Standard-Verschlüsselungsverfahren AES-128, ECC-224, RSA-1024, SHA-256, alle per API nutzbar
- Großer Lizenz- und Datenspeicher von 64 kByte, ausreichend für mehr als 1000 individuell lizenzierbare Funktionen
- Interne manipulationssichere Uhr im CodeMeter-Dongle
- Treiberlos: Mass-Storage-Kommunikation
- Möglichkeit des Firmware-Updates, d.h. Verbesserungen und neue Funktionen ohne Hardwaretausch beim Kunden nutzbar
- Entwicklungstools unterstützen WibuKey und CodeMeter gleichzeitig

2004:
- AxProtector für automatischen Schutz von Software ohne Quellcodeänderung für native Code unter Windows, Mac OS X und Linux sowie Java und .NET für CodeMeter und WibuKey in einer geschützten Anwendung
- Alle WibuBoxen mit 16 kByte Speicher und FEAL-32 mit 64-Bit Schlüsseln (Erleichterung Exportbeschränkungen, kompatibel mit V1 von 1989 und V2 von 1990)
- Preisgekröntes Design des CmSticks bei iF-Design Award
- Erster CmStick/M, Dongle kombiniert mit Flash-Disk

2008:
- Markteinführung CmActLicense, softwarebasiertes Lizenzierungsverfahren

2009:
- Markteinführung CodeMeter License Central zur Erstellung, Verwaltung und Auslieferung von Lizenzen
- Flexibles Ausleihen von Lizenzen (Borrowing) in allen Kombinationen von Dongle und CmActLicense.

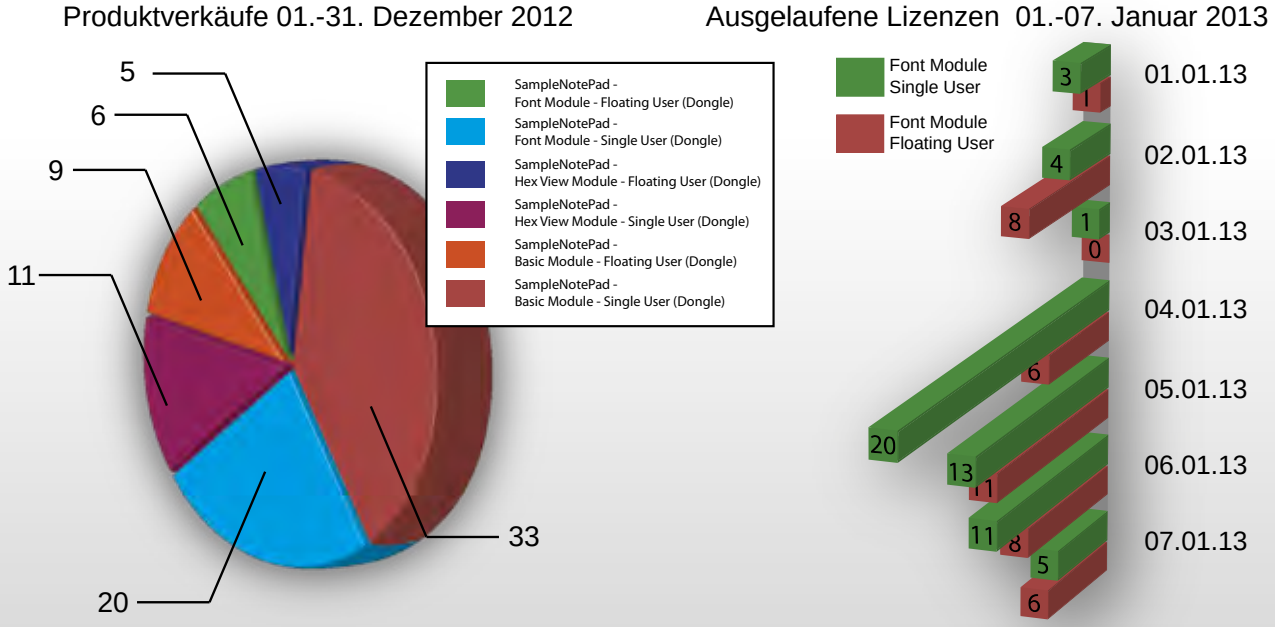
2010:
- Größerer Lizenz- und Datenspeicher von 384 KByte für bis zu 6000 individuell lizenzierbare Funktionen
- CmCards als µSD-, SD- und CF-Card für industrielle Anwendungen mit bis zu 16 GByte Flash Memory
- Unterstützung für Embedded-Betriebssysteme, z.B. Wind River VxWorks

2011:
- Markteinführung CmStick/C als weltkleinster USB-CodeMeter-Stick
- Markteinführung CmStick/T mit unterbrechungsfreier Uhr

2012:
- 2048-Bit RSA-Schlüssel
- CmSticks für USB umschaltbar zwischen HID- und Mass Storage Kommunikation
- Unterstützung für CODESYS IEC61131 Entwicklungsumgebung

Marktbegleiter stellen heute, im Jahr 2013, einige unserer Innovationen von 1989 als neue „einzigartige Funktionen" dar. Vergleichen Sie selbst, wenn Sie sich jetzt für eine neue Lizenzierungslösung entscheiden.

Partnerschaft mit Wibu-Systems, Ihr Nutzen:
- **Investitionssicher:** Schutzlösung langfristig verfügbar
- **Zukunftssicher:** kontinuierliche Innovationen in Hard- und Software, nachrüst- und aktualisierbar
- **Fokussiert auf Softwarelizenzierung und Schutz:** klare Ausrichtung auf die Nische in der Breite, vom mobilen System, über Embedded-Systeme, SPS, Industrie-PC, Desktop-PC, Server bis zur Cloud
- **Vertrauen:** langjährig gleiche Ansprechpartner im inhabergeführten, finanziell unabhängigen Unternehmen, das an Visionen und Zielen festhält
- **Partnerschaft:** Zusammenarbeit in F&E und ein offenes Ohr für neue Ideen
- **Made in Germany:** Standort Deutschland bei Design, Entwicklung und Produktion mit Partnern und lokalem Support weltweit

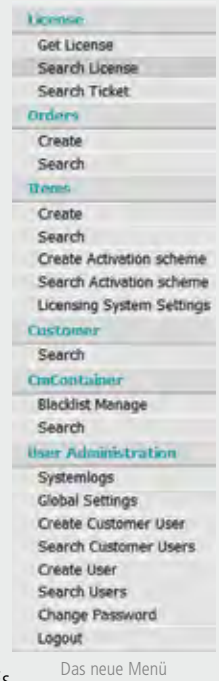


License Central Reporting

Schnell eine Übersicht über verkaufte Lizenzen und auslaufende Lizenzen zu erhalten hilft dem Vertrieb, Nachfolgegeschäft anzukurbeln. Diese und viele andere Auswertungsmöglichkeiten liefert das neue License Central Reporting.

Was bietet das neue Reporting?

Das neue Reporting baut auf einer neu entwickelten, vielfältigen und komfortablen Suche auf. Dabei liefert die Suche zu einer Anfrage nicht nur statische Ergebnisse. Vielmehr können auf den erhaltenen Suchergebnissen weitere, flexible und in die Tiefe gehende Suchen ausgeführt werden, um sich Detailinformationen zu bestimmten Ergebnissen anzeigen zu lassen. Ein einzelner Report umfasst eine Suchmaske, eine Übersichtsansicht und eine Detailansicht. Es stehen fünf Reports zur Verfügung. Sie umfassen die Reports für Lizenzen, Tickets, Aufträge, Kunden und CmContainer.



Das neue Menü

Durch die neue Menüstruktur ist ein schneller Aufruf der Reports möglich. Bei Auswahl eines der genannten Menüpunkte wird das Suchfenster des ausgewählten Reports angezeigt. Die Suchmasken sind einheitlich für alle Reports und vereinfachen damit die Nutzung.

Die Suchmaske

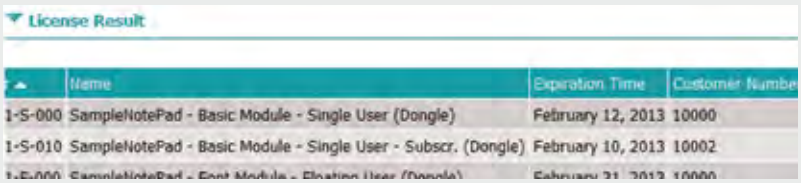
Die Suchmaske ist das A und O, um die benötigten Ergebnisse schnell und einfach zu erhalten. Design und Layout der Suchmasken wurden darauf ausgerichtet, eine vielfältige und trotzdem komfortabel zu bedienende Suche zu bieten. Dazu wurden die Suchfelder in Standardsuchfelder und optionale Suchfelder unterteilt.

Die Standardsuchfelder im oberen Bereich der Suchmaske enthalten für alle Reports die gleichen Suchfelder. Mit den optionalen Suchfeldern können Vergleichskriterien für Daten hinzugefügt werden. Beispielsweise kann eine Gruppe von Items, das sind Produkte, gewählt werden oder nach bestimmten Begriffen, die in einem Informationsfeld zu den Lizenzen hineingeschrieben wurden, um nur zwei zu nennen.

Nach der Definition der Suche, kann diese gestartet werden. Die Ergebnisse werden aus der Datenbank geladen und in der Übersichtsansicht angezeigt.

Die Übersichtsansicht

Die Übersichtsansicht zeigt einerseits die Ergebnisse der Suchanfrage, andererseits ist sie der Ausgangspunkt, um Detailinformationen zu bestimmten Ergebnissen anzuzeigen.



Die Übersichtsansicht als Ausgangspunkt für weitere Detailinformationen

Die Übersichtsansicht öffnet sich direkt unterhalb der Suchmaske, so dass die Suchkriterien immer noch sichtbar sind und leicht verfeinert werden können. Es können Kriterien her ausgenommen werden, indem einfach der zu dem

Feld gehörende Haken entfernt wird. Genauso kann die Suche weiter eingeschränkt werden durch zusätzliche Suchkriterien.

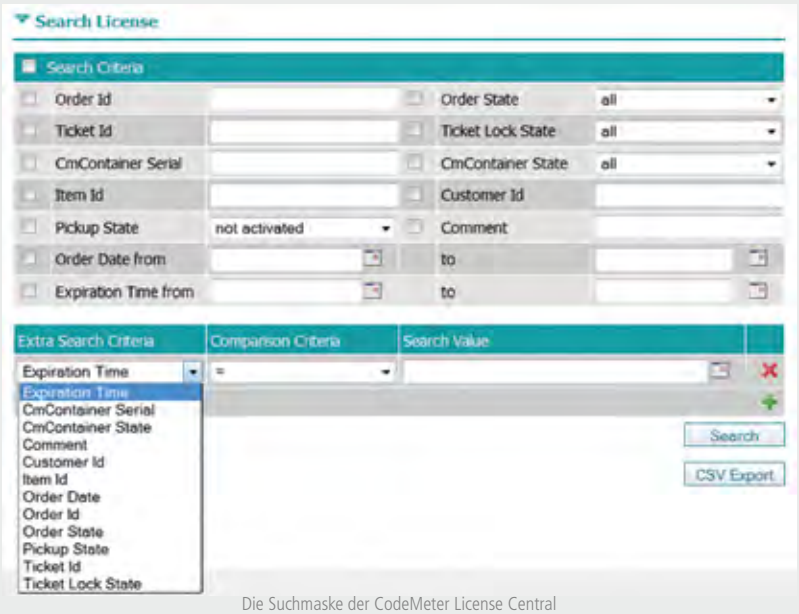
Die Übersichtsansicht bietet einen schnellen Überblick über das Suchergebnis. Die Ansichten sind individuell für den gewählten Report.Beispielhaft wird hier die Übersichtsansicht des Lizenzreports erläutert. Diese setzt sich aus den Informationen zu den Feldern *letztes Aktivierungsdatum, Artikelnummer, Lizenzname, Lizenzstatus, Lizenzanzahl, Nutzungszeitraum, Verfallsdatum, Wartungszeitraum, Anzahl der Aktivierungen, Auftragsdatum, Auftragsnummer, Ticketnummer, Kundennummer* und der *CmContainer-Seriennummer* zusammen. Zusätzlich gibt es Icons für folgende Merkmale: *Nicht aktiviert|genau einmal aktiviert|mehrmals aktiviert; Zurückgegeben|verschoben|splitted* sowie *Enthält Abholfehler|Quittierung steht aus.* In der Grafik ist ein Ausschnitt einer Suche zu sehen. Dieser zeigt die Artikelnummer, den Namen, das Ablaufdatum und die Kundennummer zu den Lizenzen, die in einem bestimmten Zeitraum ablaufen.

Die Übersicht kann alsAusgangspunkt genutzt werden, um weitere Details zu dem gezeigten Suchergebnis anzuzeigen. Möglicherweise soll ermittelt werden, welche weitere Lizenzen mit dem Auftrag verkauft wurden, oder falls die Lizenz mehrfach aktiviert wurde , in welche CmContainer sie übertragen wurde.

Durch eine automatisch zu den Übersichtsergebnissen hinterlegte Verlinkung ist es möglich, schnell Details anzeigen zu lassen.Ein Klick auf den Lizenznamen in der Spalte *Name* genügt und es öffnet sich eine neue Detailansicht

Die Detailansicht

Die Detailansicht zeigt weitere Informationen zu einer einzelnen Lizenz, einem CmContainer, einem Auftrag, einem Kunden oder einem Ticket. Bei der Detailansicht handelt es sich jedoch nicht um eine Sackgasse , sie ist also nicht das Ende der Suchmöglichkeit. In der Detailansicht haben Sie genauso wie in der Übersichtsansicht die Möglichkeit, sich schnell durch einen Klick auf manche Ergebniswerte weitere detaillierte Informationen dazu anzeigen zu lassen. Z.B. werden in der Detailansicht des Lizenzreports Informationen zur Lizenz, zu den Aufträgen, in denen die Lizenz enthalten ist, zu den dazugehörenden Tickets und den CmContainer, in welchen die Lizenz aktiviert wurde, angezeigt. Durch einen Klick auf die Kundennummer, welche beimAuftrag hinterlegt wurde, werden detaillierte Informationen zu dem Kunden angezeigt. Damit kann man sofort



Die Suchmaske der CodeMeter License Central

sehen, welche Lizenzen der Kunde erhalten hat. Daraus lässt sich ableiten, welche Lizenzen dem Kunden noch fehlen, wo also noch Bedarf von Seiten des Kunden bestehen könnte.

Integration des Reportings

Wie können Sie die Suchergebnisse entsprechend aufbereiten oder Diagramme dazu erstellen? Dafür bietet das neue Reporting die Möglichkeit, die Suchergebnisse als CSV-Datei zu exportieren. CSV-Dateien können dann mit externen Programmen, wie z.B. Excel, geöffnet werden. Mit Hilfe dieser Programme können die aus der Suchabfrage gewonnenen Ergebnisse aufbereitet und dazu unterschiedliche Diagramme erstellt werden.

Wie kann das Reporting in andere Anwendungen eingebunden werden?

Die Struktur der License Central gliedert sich in die drei Komponenten Datenbank, Webservice und Oberfläche.

Entsprechend dieser Struktur wurde viel Wert bei der Programmierung des Reporting auf die Erstellung des Webservice gelegt. Es wurde Sorge getragen, dass ein einfaches Anbinden des neu erstellten Web Service an Ihre Anwendungen möglich ist. Dafür wurde ein Webservice geschaffen, welcher für jeden der oben erwähnten Reports eine Methode enthält.

Ein Aufruf der Methode für den Auftragsreport kann beispielhaft folgendermaßen umgesetzt werden:

```
public WSReporting2.OrderReport
QueryOrderByCustomer(int count, int page, string
customerNumber, out long numberOfFoundItems)
{
WSReporting2.Message message = null;
WSReporting2.OrderReport[] report = null;

WSReporting2.SearchCondition searchCondition =
new WSReporting2.SearchCondition;
searchCondition.licenseActivationDateFrom = new
DateTime(2012, 10, 01);
searchCondition.licenseActivationDateTo = new
DateTime(2012, 12, 01);
searchCondition.customerNumber = customerNumber;

WSReporting2.OrderBy orderBy = new WSReporting2.
OrderBy[1];
orderBy[0] = new WSReporting2.OrderBy();
orderBy[0].field = „OrderId“;
orderBy[0].direction = WSReporting2.Direction.
Ascending;

orderReport = mReporting2.
queryOrder(GetSecurity(), GetMessageId(),
GetAction(„queryOrder“),
        GetTo(), GetReplyTo(), GetClientIp-
        Address(),
        searchCondition, orderBy, count, page,
out
        numberOfFoundItems, out message);

CheckMessage(message);
return report;
}
```

Weiterhin werden die Ergebnisfelder durch Complex Types in den Web Service abgebildet. Damit ist eine optimale Unterstützung bei der Anbindung mit Entwicklungsumgebungen, z.B. durch Nutzung von IntelliSense im Microsoft Visual Studio, möglich.

Gerne unterstützt Sie bei der Anbindung auch unser **WIBU Professional Services Team!**



Hosting und Support

Ihre Software ist fertig. Softwareschutz und Lizenzmanagement von Wibu-Systems sind erfolgreich integriert. Wie kommen die Lizenzen nun zum Kunden? Auch diese Herausforderung ist schon gelöst, denn Sie werden die CodeMeter License Central Internet einsetzen. Dafür fehlt Ihnen die nötige Infrastruktur? Sie haben keine Zeit oder gerade keine Experten an der Hand, die das System nach aktuellen Maßstäben sicher aufsetzen? Scheuen Sie die internen Aufwände und Betriebskosten? Kein Problem! Lassen Sie einfach Wibu-Systems die Arbeit für Sie erledigen!

Die CodeMeter License Central Internet ermöglicht es Ihnen, Lizenzen zu verwalten, zu verkaufen und an Kunden zu verteilen. Das mächtige Werkzeug lässt sich aber auch auf vielfältige Art erweitern und in unternehmensinterne Prozesse einbinden.

Um diese Funktionalitäten nutzen zu können, wird die CodeMeter License Central auf einem Server installiert und entsprechend administriert. Dabei sind natürlich netzwerk- und sicherheitsrelevante Anforderungen des entsprechenden Rechenzentrums zu berücksichtigen. Nachdem der initiale Schritt durchgeführt ist, müssen vor Inbetriebnahme noch geeignete Backup- und Desaster-Recovery- Maßnahmen definiert sein, um im Falle eines Falles schnell und zuverlässig reagieren zu können. Während des gesamten Betriebs muss kontinuierlich darauf geachtet werden, dass Sicherheitsupdates für die verschiedenen Bereiche (angefangen beim Betriebssystem bis hin zu den Applikationen) zeitnah eingespielt werden.

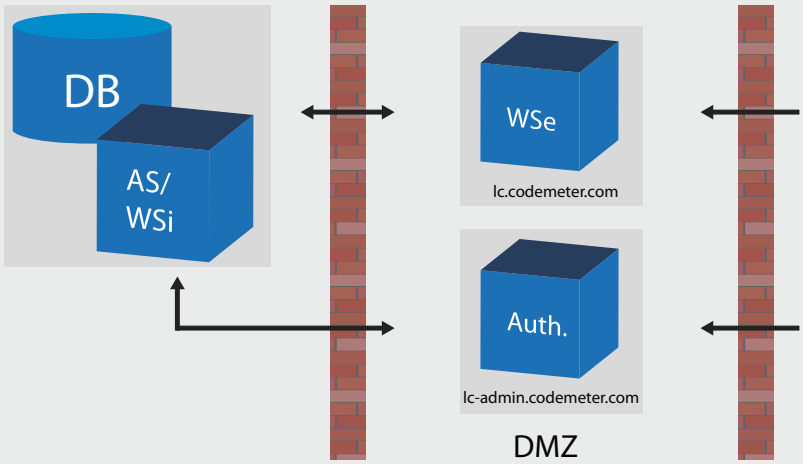
Aus Zeit- und Kostengründen kann es deswegen sehr attraktiv sein, ein solches System nicht im eigenen Unternehmen zu betreiben, sondern es im Rechenzentrum von Wibu-Systems hosten zu lassen. In vielen Fällen hat sich diese Investition bei den nicht zu vernachlässigenden internen Kosten für Hardware und Personal sehr schnell amortisiert.

Die Architektur

Grundsätzlich gibt es zwei Zugangswege zur CodeMeter License Central. Einerseits werden der Verkauf von Produkten und die Administration des Systems über Sie als Anbieter durchgeführt, auf der anderen Seite benötigen Ihre Kunden einen Zugang zur Abholung von Lizenzen. Aus diesem Grund sieht die Architektur der gehosteten Lösung wie in der Abbildung dargestellt aus. Es wird zwischen dem internen Webserver (WSi) und dem externen Webserver (WSe) unterschieden. Beide greifen über den Application Server (AS) auf die Datenbank (DB) zu. Es gibt nun jeweils für Sie als Anbieter und Ihre Kunden getrennte Zugänge auf das System.

Ihr Kunde greift über lc.codemeter.com auf die Abholseiten (Depot) der CodeMeter License Central zu. Diese Seiten können an Ihr Corporate-Design und Ihre Abläufe einfach angepasst werden.

Als Anbieter greifen Sie über einen geschützten Zugang (per https) auf lc-admin.codemeter.com zu. Hier haben Sie vollen Zugriff auf den internen Webserver und können alle Tätigkeiten ausführen, die Sie bei einer eigenen inhouse CodeMeter License Central auch ausführen können. Der Zugriff wird durch ein Clientzertifikat geregelt, das Ihren Rechner gegenüber der CodeMeter License Central authentifiziert.



Zugangsarchitektur der CodeMeter License Central für Kunden und Administratoren

Gegen Angriffe von außen ist die gehostete CodeMeter License Central durch eine zweistufige Architektur geschützt. Der externe Webserver steht in einer DMZ; die Datenbank, der interne Webserver und der Applikationsserver sind nach außen vollständig abgeschirmt. Gekoppelt mit dem internen Frühwarnsystem bietet damit eine State-Of-The-Art Sicherheit.

Aufbau und Betrieb des Systems

Entscheiden Sie sich für eine gehostete CodeMeter License Central, so erhalten Sie neben einem Server auch die Dienstleistung der vollständigen Installation und Konfiguration des Pakets. Einer der wichtigsten Punkte ist dabei der kontinuierliche Betrieb der Lösung, der folgende Punkte umfasst:

- Einspielen von Betriebssystem-Updates
- Einspielen von Updates der CodeMeter License Central
- Überwachen der Verfügbarkeit
- Überwachen und Gegenmaßnahmen bei Angriffen
- Tägliches Backup der Datenbank

Leistung	Data Center Edition	Dedizierter Server
Bereitstellung Server	✓	✓
Installation und Konfiguration der CodeMeter License Central	✓	✓
Einspielen von Updates für das Betriebssystem	✓	✓
Einspielen von Updates für die CodeMeter License Central	✓	✓
Überwachung Verfügbarkeit	✓	✓
Überwachung Sicherheit und Gegenmaßnahmen bei Angriffen	✓	✓
Tägliches Backup	✓	✓
Anbindung an das Internet	✓	✓
Zugriff auf Webserver intern (Clientzertifikat)	✓	✓
Zugriff auf Connectoren und Gateways	✓	✓
Depot-Seiten anpassbar	✓	✓
Zugriff auf alle Webservices		✓
Eigene Erweiterungen der CodeMeter License Central (Extensions)		✓
Administrationsrecht in der CodeMeter License Central		✓
Anzahl Accounts inkl. Clientzertifikate	3	10
Verfügbarkeit	99,9 %	99,9 %

Integration in eigene Prozesse

Auch bei der gehosteten Variante der CodeMeter License Central stehen Ihnen alle Schnittstellen für die Integration in eigene interne Prozessabläufe wie gewohnt zur Verfügung. Für die Erzeugung von Tickets existieren geeignete Connectoren; für die Abholung der Lizenzen auf Basis der Tickets stehen entsprechende Gateways zur Verfügung. Über die Connectoren lassen sich CRM-Systeme wie SAP® oder Salesforce.com anbinden oder direkt eine Verbindung zu einem Shopsystem realisieren, wie z.B. Digital River, element5, share*it! und Cleverbridge.

Varianten des Hostings

Wibu-Systems bietet das Hosting in zwei Varianten an, einer kostengünstigen Einstiegslösung und einer individuellen Variante, die Ihre speziellen Anforderungen an eine individuelle Lösung berücksichtigt.

- Datacenter Edition: In dieser Variante teilen Sie sich einen Server mit anderen Anbietern, verfügen aber aus Sicherheitsgründen über eine eigene, separate Datenbank. Ebenso können die HTML-Seiten des WebDepots zur Abholung der Lizenzen durch Ihre Kunden an Ihr Corporate Design angepasst werden.
- Dedizierter Server: Bei diesem Paket verfügen Sie über eine eigene virtuelle Maschine mit Ihrer CodeMeter License Central. Alle Connectoren und Gateways können an Ihre Anforderungen angepasst und zusätzlich spezielle Erweiterungen nach Ihren Vorstellungen entwickelt werden.

Beide Pakete werden mit einer Server-Verfügbarkeit von 99,9 % angeboten, geplante Wartungszeiten sind davon ausgenommen.

Mit einem Hostingmodell von Wibu-Systems sparen Sie nicht nur Zeit und Geld bei der Einrichtung einer CodeMeter License Central, sondern auch bei der intensiven Betreuung des Systems während des Betriebs. Und mit einem Supportvertrag „Silver" oder „Gold" können Sie sich auch auf die garantierten Reaktionszeiten und einen persönlichen Ansprechpartner verlassen. Einfacher geht es nicht!

Aktuelles in Kürze

CmSticks HID-konform

Seit 2003, der Markteinführung von CodeMeter, mussten niemals zusätzliche Treiber installiert werden: Es wurde der „Mass Stor age"-Treiber des Betriebssystems genutzt. Mit der neuen CodeMeter Firmw are 2.02 und dem Runtime 5.0 können die USB-CmSticks auch als HID-k onformes Gerät eingestellt werden. Somit erscheint der CmStick nicht im Windows-Explorer mit einem Laufwerksbuchstaben.

CodeMeter SDK 5.0

Das CodeMeter SDK 5.0 bringt eine ganze Reihe von Verbesserungen: den neuen AxProtector 8.50, HID-Support beim CodeMeter Runtime und viele kleine Verbesserungen. Mit CmWAN wird zudem eine optionale Kommunikationsart über https eingeführt; bei Einsatz entsprechender Infrastruktur können Lizenzen damit über das Internet belegt werden, erfolgreiche Authentifizierung vorausgesetzt.

B&R entscheidet sich für CodeMeter

„Perfection in Automation" – das ist B&R, so steht es auf der Firmenseite. Innovation und Trends in der Automatisierung bilden wichtige Teile der langfristigen Strategie und Philosophie. Wir sind stolz und freuen uns, dass B&R künftig zur Lizenzierung seines Automation-Studios und für Runtime-Komponenten auf CodeMeter setzt und auch seinen Kunden die Nutzung der CodeMeter -Know-how- und Produktschutzfunktionen ermöglicht.

Automation Award für CodeMeter

Zur SPS IPC Drives 2012 wurde CodeMeter von der Jury für den Automation Award nominiert und von den Messebesuchern auf Platz 4 gewählt. Am 22.01.2013 fand die Preisverleihung in Stuttgart statt.



Wir freuen uns , diese Auszeichnung und Anerkennung für unser Engagement mit CodeMeter in der Automatisierungsindustrie zu erhalten.

Kooperation mit OPC Foundation

Wibu-Systems ist Ende 2012 der OPC-Foundation beigetreten. Das Ziel ist, C odeMeter a ls O PC U A k onforme Lösung zur Authentifizierung industrieller Steuerungskomponenten z u v erwenden, m it sicheren a ber d ennoch b enutzerfreundlichen Mechanismen zum Ausrollen der Zertifikate. Teil der Wibu-Systems-Strategie ist es, Industrie 4.0, Cyber-Physical-Systeme und die gesamte Automatisierungsbranche zu unterstützen.

CSSI 5.0 verfügbar

charismathics
the middleware company

CSSI 5.0 von charismathics, einem führenden Anbieter von Plattform- und Token-übergreifender Middleware, unterstützt jetzt das Speichern von X.509-Zertifikaten mit 1024-Bit oder 2048-Bit RSA-Schlüsseln sicher im CmDongle. Die Lösung ist PKCS#11 und Microsoft CSP k ompatibel und nutzbar unter Windows, Mac OS X und Linux.

Erfolgreiche Webinarserie gestartet



Ergänzend zu Workshops und Seminaren führen wir Webinare durch: Z.B. war Software Monetization das Thema im Dezember 2012 und Embedded-Software-Security im J anuar 2013 – beide mit F rost & Sulliv an. Am 1. Februar fand ein CodeMeter Webinar statt und am 19. Februar das Webinar „Secure Development of Connected Applications w ith Out of the Box Complete IP Protection" zusammen mit Wind River und Emerson Network Power. Aufgrund der großen Resonanz werden wir die Webinarserien ausbauen. Probieren Sie es aus.

Newsflash

+++ Firefox 19 CodeMeter PasswordManager Plug-in verfügbar +++ Firefox 19 CmIdentity-Plug-in +++ License Centr al 2.0 mit ausgefeiltem Reporting kurz vor Fertigstellung +++ CodeMeter Runtime und SDK 5.0 verfügbar +++ Wibu-Systems + Emerson + WindRiver: EDK jetzt lieferbar +++ Whitepaper zu Integritätsschutz mit CodeMeter +++

Aktuelle Software-Versionen:

- CodeMeter SDK 5.0, März 2013
- CodeMeter License Central 2.0, März 2013
- CmIdentity 4.50, 2011-12-20
- WibuKey SDK 6.10a, 2012-12-21
- AxProtector 8.40, März 2013
- SmartShelter PDF 11, 2013-01-09

Aktuelle Firmware:

- CmStick 1001-02: 2.02
- CmStick/M 1011-02: 2.0
- CmCard/µSD, /SD, /CF 104x-02: 2.01

Mit der neuesten Softw are profitieren Sie von letzten Verbesserungen; die neueste Fi rmware b ietet h öchste Stabilität und neue Funktionalität. Bitte stets aktualisieren.



www.wibu.com/de/cs25.html

GLASER -isb cad-
a NEMETSCHEK Company

Erfolgsgeschichte -isb cad-

-isb cad- 2013

Bauingenieure und Architekten benötigen für die Planung und Bearbeitung ihrer Projekte spezielle Software-Werkzeuge. -isb cad- ist ein hoch spezialisiertes, sorgfältig auf die Aufgaben in der Bauplanung abgestimmtes CAD-Programm. Zeitsparend und im Ergebnis hochwertig werden damit alle Konstruktionsarbeiten erledigt. Mit durchdachten Detaillösungen hebt es sich von unspezifischen und daher für die Anforderungen der Planer weniger gut geeigneten CAD-Programmen ab.

Ingenieure nutzen -isb cad- außerdem zur Bewehrungsplanung. Aus Bewehrungsplänen geht hervor, wie viel und wo Betonstahl in Fundamenten, Decken- und Bodenplatten, Wänden und anderen Bauteilen aus Stahlbeton eingebracht wird. Aus den Plänen erzeugt -isb cad- Stahllisten. Diese beinhalten die genauen Mengen und Biegeformen des Stahls, die sich aus den Berechnungsergebnissen der Tragwerksplanung und anderen konstruktiven Bedingungen ergeben.

Alle Programme von -isb cad- vereinen einfachste Bedienung und hohe Effizienz.

Die Herausforderung

Die in moderner .NET-Technologie entwickelte CAD-Software -isb cad- 2013 soll zuverlässig und sicher gegen Kopieren und Reverse Engineering geschützt werden. Sie soll flexibel lizenziert werden, um dem Kunden eine optimale Skalierbarkeit der Programmpakete sowie bedarfsorientierte Nutzungsmodelle anbieten zu können. Die Lizenzerzeugung und Verteilung soll in die Vertriebsprozesse integriert werden. Der Umstieg vom bisherigen Schutzsystem muss im Einklang mit dem Produkt-Release-Zyklus vollzogen werden. Vor dem Release von -isb cad- 2013 müssen die Bestandsdongles mehrerer tausend Anwender ausgetauscht werden.

Die Lösung

Die Verschlüsselung der Methoden in unterschiedlichen Modulen ist steuerbar mit Attributen im Quellcode. Die Einarbeitung in die einfach zu nutzenden und leistungsfähigen Tools



Die PGE-Arena in Danzig ist ein Beispiel für die vielen Projekte, die weltweit mit GLASER -isb cad- realisiert werden

AxProtector und CodeMeter Softwareschutz-API ging schnell. Der Wibu-Support begleitete alle Schritte hervorragend.

Der Erfolg

Optimierte Prozesse und breiter Funktionsumfang des Wibu-CodeMeter-Systems senken die Vertriebskosten und erleichtern die Entwicklung neuer Vertriebskonzepte. Die CmSticks im edlen lasermarkierten Metallgehäuse oder die superkleinen CmStick/C unterstützen die Marke GLASER -isb cad- bei den Kunden.



Dipl.-Ing. (FH) Matthias Glaser,
Geschäftsführer der Firma GLASER -isb cad- Programmsysteme GmbH



„Durch den Einsatz von CodeMeter sind wir in der Lage, -isb cad- maßgeschneidert und zuverlässig zu lizenzieren. Mit Hilfe von Remote Updates haben wir Vertriebswege verkürzt, wodurch unsere Produkte schneller beim Kunden sind. Auch hinsichtlich neuer Herausforderungen bezüglich der IT-Landschaft unserer Kunden, Stichwort Virtualisierung und Terminalserver-Lösungen, sind wir mit CodeMeter sehr gut positioniert. Die umfassende und engagierte Unterstützung durch das Wibu-Team während aller Projektphasen der Umstellung war vorbildlich und hat dazu beigetragen, die Projektziele innerhalb des engen Zeitplans zu erreichen."

Secure Code Webinare .NET

Sicherer Schutz von .NET-Assemblies gegen Raubkopieren und Reverse Engineeringinklusive Lizenzmanagement.

Unser erfolgreiches Secure Code Seminar wird jetzt als Webinar angeboten. Erfahren Sie online, wie Sie Ihre .NET-Anwendungen innerhalb von wenigen Minuten sicher gegen Raubkopieren und Reverse Engineering schützen.

Das Secure Code Webinar .NET richtet sich sowohl an den Produktmanager, der erfahren möchte, wie seine Lizenzmodelle mit CodeMeter realisiert werden, als auch an den Entwickler, der erfahren möchte, wie CodeMeter in .NET-Assemblies integriert wird.

Unser Webinar ist in einen Vormittags- und einen Nachmittags-Block unterteilt.

Teil 1, 9:30 Uhr bis 11:30 Uhr (Dauer 1:30h, danach 30 Minuten für Fragen und Antworten)

- Einführung in die Basistechnologie von CodeMeter
- Sichere Integration in Ihre Software durch intelligente Werkzeuge
- Fragen und Antworten

Teil 2, 14:00 Uhr - 16:00 Uhr (Dauer 1:30h, danach 30 Minuten für Fragen und Antworten)

- Einführung in die Lizenzverwaltung von CodeMeter
- Lizenzverwaltung mit der CodeMeter License Central
- Integration der License Central in Ihre Prozesse
- Fragen und Antworten

Besuchen Sie uns auf folgenden Messen:

Deutschland

embedded world 2013 Exhibition&Conference ... it's a smarter world

Halle 5 | Stand 340
26. – 28. Februar 2013
Nürnberg, Deutschland

BASTA! .NET, WINDOWS, VISUAL STUDIO

Vortrag - Reverse Engineering
27. Februar 2013
Mainz, Deutschland

CeBIT

Halle 12 | Stand D82
05. – 09. März 2013
Hannover, Deutschland

HANNOVER MESSE 8.-12. APRIL 2013

Halle 8 | Stand D5
08. – 12. April 2013
Hannover, Deutschland

Weltweit

05. – 07. März 2013
Antwerpen, Belgien

Stand 28
07. – 08. März
Den Haag, Niederlande

tech days 2013

04. – 06. März
Guangzhou, China

SIAF GUANGZHOU
SPS – Industrial Automation Fair Guangzhou
中国广州国际工业自动化技术及装备展览会

5060-002-01/20130206

Impressum
KEYnote
25. Ausgabe, Frühjahr 2013

Herausgeber:
WIBU-SYSTEMS AG
Rüppurrer Straße 52-54
76137 Karlsruhe
Tel. +49 721 93172-0
Fax +49 721 93172-22
info@wibu.com
www.wibu.com

Verantwortlich für den Inhalt:
Oliver Winzenried

Redaktion:
Stefan Bamberg
Daniel Eichhorn
Rüdiger Kügler
Oliver Winzenried

Design
Markus Quintus

Druck
E&B engelhardt und bauer, Karlsruhe

Zuschriften sind jederzeit willkommen. Schreiben Sie uns an: global-marketing@wibu.com.
Sie sind durch das Redaktionsgeheimnis geschützt. Namentlich gekennzeichnete Artikel geben nicht unbedingt die Meinung der Redaktion wieder.
Wibu®, CodeMeter®, SmartShelter® und SmartBind® sind Warenzeichen von Wibu-Systems. Alle anderen Firmen- und Produktnamen sind eingetragene Marken der jeweiligen Eigentümer. Copyright ©2013 Wibu-Systems. Alle Rechte vorbehalten.

Bildernachweis:
Seite 6:
©iStockphoto.com/perrygerenday
Alle nicht gekennzeichneten Bilder/Grafiken liegen bei dem jeweiligen Urheber

MEDIA ACCESS
PERFECTION IN SOFTWARE PROTECTION
DOCUMENT

WIBU SYSTEMS