AUTUNNO 2013

KEYnote 26

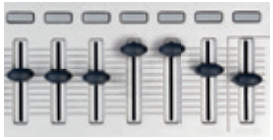
IL MAGAZINE DI WIBU

Semplice integrazione in software e processi

Indice

WIBU SYSTEMS

Contenuto



Cari Clienti e Partner di WIBU!

Non passa quasi giorno senza che vengano pubblicate notizie di PRISM, Tempora o XKeyscore. Questi acronimi hanno un minimo comun denominatore: la sicurezza dei dati privati dei cittadini. Al contempo anche lo spionaggio industriale prospera. Nel mondo del business, la sopravvivenza è strettamente legata al know-how, che può assumere diverse forme: algoritmi o processi software nell'IT, o parti e componenti di dispositivi e macchinari in ambito manifatturiero. I dati di produzione, i quali possono contenere essi stessi know-how inestimabile, sono una preda altrettanto ambita. In un mondo maggiormente interconnesso, la 'sicurezza' dei sistemi aperti è divenuta una priorità per eccellenza. I governi di tutto il mondo stanno investendo nella ricerca in questo settore, che si tratti dell'Europa con lo standard ISO62443, degli Stati Uniti con ISA99, o dell'Asia.

La protezione da queste minacce necessita di soluzioni maggiormente sofisticate. La gestione delle licenze ed il loro monitoraggio sta divenendo un elemento sempre più cruciale in ambiente IT, al fine di garantire agli utenti tutta la libertà di utilizzare i loro prodotti, pur preservando gli interi incassi degli editori. Nell'industria, l'introduzione di protezioni efficaci è divenuta essenziale nella lotta agli attacchi ciber-fisici e alla manipolazione illegale dei dati. Con CodeMeter i nostri sforzi in materia di ricerca e sviluppo coprono entrambi i versanti: i nuovi moduli di License Central vengono incontro alle esigenze espresse dalla vendita al dettaglio, con funzionalità di distribuzione controllata e reportistica. I nostri strumenti rendono la protezione dell'integrità più semplice ed efficace; e supportiamo anche un numero crescente di piattaforme e standard. L'obiettivo che ci siamo prefissi è quello di offrire agli utenti un sistema che cresca nel tempo e sia pertanto consono, tanto ai bisogni di oggi, quanto ai requisiti di domani.

Entro la fine di quest'anno, saremo presenti a molteplici eventi e conferenze internazionali. Venite a trovarci – i nostri specialisti ed io stesso non vediamo l'ora di conoscervi personalmente! Se la vostra agenda fosse troppo fitta, gradirei comunque cogliere l'occasione per augurarvi fin d'ora una chiusura d'anno estremamente positiva ed una piacevole stagione invernale.

Oliver Winzenried (CEO)

Wibu International Partner Summit 2013

L'assetto globale di Wibu-Systems

Wibu-Systems, fondata nel 1989 da Marcellus Buchheit e Oliver Winzenried, è diventata un punto di riferimento internazionale nel suo settore. Con filiali negli Stati Uniti e in Cina, rappresentanti commerciali in Belgio, Francia, Gran Bretagna, Paesi Bassi e Spagna, nonché numerosi distributori nel mondo, Wibu-Systems offre competenza e presenza capillare in loco.

A capitalizzazione interamente privata e gestita dai suoi stessi fondatori e proprietari, Wibu-Systems è impegnata a realizzare una visione a medio e lungo temine: fornire, alle software house e ai produttori di dispositivi high-tech di tutto il mondo, tanto soluzioni per il licenziamento del software e la protezione del prodotto, quanto strumenti efficaci per proteggere il know-how, combattere la manipolazione illegale e gli attacchi cibernetici.

Tutte le attività di ricerca e sviluppo sono accentrate nella nostra casa madre a Karlsruhe, Germania, ed includono anche un gran numero di compartecipazioni con partner tecnologici ed istituti di ricerca in Asia, Europa e Stati Uniti. Il nostro team di prodotto è strutturato in modo da potersi agilmente interfacciare con i diversi mercati. I brevetti internazionali che Wibu-Systems detiene sono una testimonianza della nostra professionalità e rafforzano il nostro posizionamento. La nostra azienda è conforme agli standard ISO 9001:2008 ed i nostri prodotti sono certificati in base ai criteri di Underwriters Laboratories (C-UL.US) validi negli Stati Uniti e in Canada, VDE e CE in Europa, FCC nelle Americhe, KCC in Corea, RCM in Australia e Nuova Zelanda e VCCI in Giappone.

Selezionando accuratamente i nostri fornitori e la componentistica, ci impegniamo ad adempiere ai numerosi requisiti dell'industria, quali ad esempio le norme relative a RoHS e REACH, atte a garantire una produzione libera da sostanze nocive, JIG, acronimo di Joint Industry Guide, ed altre misure atte ad evitare l'impiego di minerali di conflitto. Da ultimo, anche la regolamentazione delle operazioni di export è materia cui il nostro settore è particolarmente sensibile. Le soluzioni di Wibu-Systems per la protezione del know-how hanno ricevuto l'approvazione all'esportazione come merce non soggetta a restrizione alcuna, nella fattispecie AzG dalla Camera di Commercio tedesca, e EAR99 e NLR (No License Required) dall'ente BIS americano.

Tutti questi aspetti garantiscono un uso sicuro delle soluzioni di Wibu-Systems, suggellato dall'eccellente preparazione dei nostri dipendenti e dall'ineguagliabile supporto dei nostri rappresentanti ovunque nel mondo dislocati. Le nostre principali sedi propongono regolarmente seminari a clienti ed interessati affinché possiate trarre il massimo beneficio da contenuti esposti nella vostra stessa lingua. Non esitate a contattare i nostri team commerciali e tecnici, usufruendo dei molti servizi a vostra disposizione.

Scalabilità delle licenze con CodeMeter

"Chi ha bisogno di chiavi di protezione?" Posta anno dopo anno, questa domanda sta divenendo sempre più frequente ai giorni nostri con l'avvento di una crescente virtualizzazione. Ma partire direttamente dalla scelta della tecnologia o del dispositivo può non essere la via più oculata. Ciò cui l'utente finale è interessato sono flessibilità e sicurezza di accesso alle licenze, indipendentemente dalle condizioni nelle quali sta utilizzando il software in questione. Questo articolo esplora le molteplici e versatili opzioni offerte da CodeMeter.

Gli Independent Software Vendor (ISV) ed i loro utenti finali esprimono requisiti ed aspettative molto differenti in merito alla moderna gestione delle licenze. Quest'ultima deve essere sicura e mantenuta al passo con i più recenti progressi tecnologici al fine di prevenire la copia illegale, il reverse engineering e la manipolazione del software. Al contempo, ci si aspetta che la tecnologia fornisca modelli di licenza flessibili, quali licenze di rete, funzionalità on-demand, pagamento a consumo o altri modelli a tempo erogati in modo semplice e diretto.

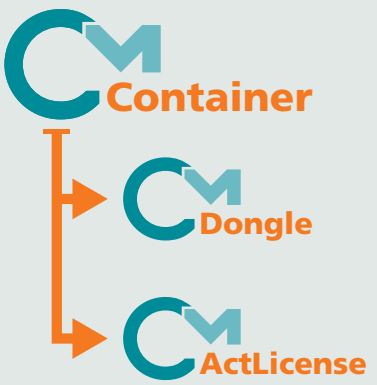
CodeMeter può fornire licenze in molteplici formati all'interno di una tecnologia unificata. Questa è la risposta a requisiti del mercato apparentemente in conflitto tra loro: chiavi di protezione (CmDongle) per la massima sicurezza e flessibilità, e codici di attivazione software (CmActLicense) con un collegamento intelligente al dispositivo utilizzato. Entrambe le opzioni possono trovare impiego localmente o in ambito di rete, offrendo tanto una pluralità di modelli di licenza, quanto solo la crittografia del software (protezione). La nuova soluzione CmWAN arriva a coprire anche le licenze sul cloud.

Ciò che l'utente finale desidera è poter utilizzare il modello di licenza dello sviluppatore in modo efficace ed efficiente all'interno dell'ambiente selezionato. Nessun software può avere successo senza questi requisiti. Il non plus ultra in fatto di sicurezza è garantito dalle chiavi CmDongle, nella loro intera gamma, capaci di memorizzare fino a 6000 licenze, anche di diversi vendor. A richiesta, l'ISV può ordinare l'opzione memoria flash addizionale, quale veicolo per distribuire il software ai suoi utenti finali.

Al contrario, CmActLicense non necessita di alcun hardware. La tecnologia SmartBind da noi brevettata consente un legame sicuro con il computer dell'utente finale e permette un uso sicuro anche in ambienti virtuali.

Chiavi di protezione o Attivazioni software?

CodeMeter rende questa domanda irrilevante. Indipendentemente dalla scelta effettuata, la soluzione di gestione licenze è integrata dall'ISV nel prodotto software. Lo sviluppo si fonda sui cosiddetti CmContainer, una sorta di ulteriore livello trasparente che si somma alla scelta di un contenitore fisico o virtuale per la licenza (CmDongle o CmActLicense).



Uso flessibile di licenze salvate in contenitori hardware e software

Una volta completata la compilazione del software, l'ISV può scegliere lo scenario di preferenza. Egli può distribuire l'applicativo mediante CmDongle o CmActLicense, o persino una combinazione di entrambi per garantire al vendor massima flessibilità in merito a come distribuire il software. Alla fin fine, la scelta del contenitore per la licenza viene effettuata presso la sede del cliente. Questo lascia spazio sufficiente, ad esempio, per rispondere alle varie restrizioni geografiche legate alla gestione delle licenze.

Questo approccio offre altri usi intelligenti per la manutenzione del software. Mentre il software stesso rimane attivamente protetto da CmActLicense, i processi ulteriori di manutenzione richiesti possono essere eseguiti collegando una chiave al sistema.

Licenze in reti locali (CmLAN)

Oltre alle funzionalità tipiche di una memorizzazione locale delle licenze, le licenze di rete promettono agli utenti finali una flessibilità ancora maggiore nell'uso del software. Le licenze flottanti (anche conosciute come licenze simultanee) vengono adottate in un'architettura all'interno della quale l'ISV fornisce all'utente finale un certo numero di licenze per uso su rete locale.

Le licenze di rete possono essere gestite da CmDongle o CmActLicense: è sufficiente collegare la chiave al server, o attivare la CmActLicense dal computer; quest'ultimo farà la funzione di server.

La Runtime di CodeMeter viene installata sul server licenze selezionato e su tutti i dispositivi scelti per l'uso con queste licenze. Questo permette un uso simultaneo delle licenze in rete, in numero massimo pari a quello consentito dal vendor. Richieste da PC addizionali verrebbero soddisfatte solo quando una licenza divenisse nuovamente disponibile.

Adottare le licenze di rete si rivela particolarmente efficace in reti miste, nelle quali computer con differenti sistemi operativi abbiano la necessità di accedere a un unico insieme di licenze condivise.

L'utente finale può anche gestire più di un server di licenze su una singola rete per far sì che tutte le licenze in suo possesso siano disponibili all'occorrenza. Questo diviene essenziale per permettere la distribuzione del carico ed l'alta affidabilità dei sistemi.

Licenze sul cloud (CmWAN)

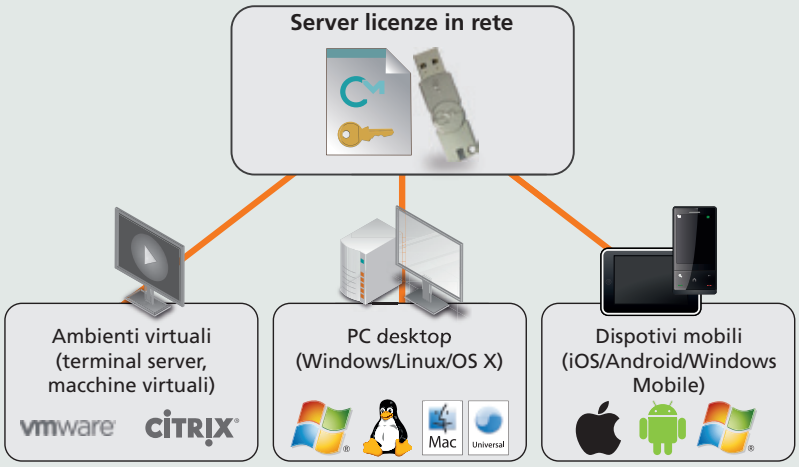
Wibu-Systems intraprende il passo logico successivo nell'evoluzione del concetto di CmLAN e lancia il nuovo prodotto CmWAN in abbinamento a CodeMeter 5.0. La tecnologia innovativa consente agli utenti di accedere alle licenze non solo sulle reti locali, ma anche su cloud mediante una connessione di rete Wide Area.

Le licenze non sono neppure limitate al software che viene eseguito localmente. Persino le applicazioni che risiedono su cloud possono essere eseguite attraverso licenze che si trovano sulla nuvola stessa. Tutte queste nuove opportunità hanno un minimo comun denominatore: lo stesso repertorio di modelli di licenza che gli utenti hanno imparato a conoscere ed apprezzare con la tecnologia CodeMeter. L'integrazione standard di CodeMeter rende le licenze locali e su cloud disponibili senza alcun bisogno che l'ISV modifichi il suo software.

Dal punto di vista del client, l'uso delle licenze via cloud è immediato: si include semplicemente l'indirizzo HTTPS del server licenze su cloud nell'elenco di ricerca del server. L'applicazione può poi direttamente accedere alle licenze presenti sul cloud.

Licenze – Sempre disponibili!

Esistono così tante possibilità attraverso le quali gli ISV forniscono le licenze agli utenti finali. Che siano basate su soluzioni hardware o software, conservate localmente o in rete o sul cloud, Wibu-Systems ha un'unica soluzione omnicomprensiva e scalabile. Nessun bisogno di scendere a compromessi: le licenze vengono messe a disposizione ovunque e comunque quando necessario.



Utilizzo delle licenze di rete in reti eterogenee

Boot Sicuro

I microcontrollori ed i controlli elettronici governano le nostre vite. Dagli impianti nucleari alle fabbriche e ai treni dei pendolari, sono ormai ovunque. Meno di un decennio fa, la maggior parte dei sistemi di controllo era costituita da innocue scatolette con hardware e software proprietario, completamente isolate dal mondo esterno. Quando il funzionamento di una di queste si interrompeva, un tecnico interveniva direttamente sul dispositivo. L'ottimizzazione di tempi e costi ha tuttavia portato online i sistemi di controllo; i tecnici possono così gestire molteplici incidenti remotamente, comodamente dalla propria scrivania. Ma questo comfort ha un prezzo: gli **attacchi ciber-fisici**.

Motivazioni di un attacco

Integrità: Per quale motivo vengono manipolati i sistemi di controllo delle macchine? Entriamo nella sfera dei servizi segreti e delle organizzazioni terroristiche? Può anche essere, come Stuxnet ha dimostrato al mondo. Sabotatori? Potrebbe sembrare improbabile, ma che cos'è l'hacking di sistemi di controllo non protetti se non sabotaggio? Quando i sistemi di controllo sono in funzione in modalità offline, il sabotatore deve essere fisicamente sul luogo per causare un danno. Deve guadagnarsi un accesso in loco e può essere catturato nel tentativo. Un sistema online minimizza il rischio per l'hacker che vuole lanciare un attacco. L'hacker sta tranquillamente seduto alla sua postazione con tutte le sue risorse a portata di mano, può agire nell'anonimato e aiutato da altri attori altrettanto disonesti. Che si tratti di un messaggio politico, di una tentata estorsione, o semplicemente di una "bravata", la motivazione è irrilevante.

Gli operatori di impianto potrebbero tentare "prodezze" con i macchinari, ma un uso delle apparecchiature di produzione al di fuori dei parametri consentiti ha spesso conseguenze rischiose, tra le quali l'usura è la meno preoccupante di tutte. I produttori originali di macchinari sono alla ricerca di modi per porre fine o almeno dimostrare la manipolazione, in modo da far valere diritti di garanzia e responsabilità.

Riservatezza: Lo spionaggio industriale rimane un rischio che viene troppo spesso sottovalutato. I parametri operativi o i concetti di controllo degli impianti manifatturieri sono infatti una preda ambita dalla concorrenza. Le connessioni remote rendono il furto dei dati più semplice. Il cinema può averci indotti a credere che sia sempre possibile scoprire chi accede ai dati e l'orario in cui ciò avviene, ma nella vita reale i sistemi spesso registrano le attività di login attraverso protocolli che sono fin troppo semplici da manipolare. La sottrazione di dati passa frequentemente inosservata, e il malfattore può analizzare il "bottino" con tutta calma offline.

Come posso proteggermi?

Molti dei moderni sistemi di controllo si basano su hardware standard, come PC industriali dotati di sistemi operativi standard, quali ad esempio VxWorks, QNX o Linux Embedded. Ambienti runtime in sistemi di controllo spesso adottano uno standard aperto (come CODESYS). Ogni rete remota va poi protetta da VPN e firewall, ma questi strumenti non offrono una protezione sufficiente per i sistemi di controllo. Una volta che l'hacker si è infiltrato, può agire liberamente in rete, e si dà il caso che numerosi tecnici salvino le password o le chiavi di accesso per la VPN dei propri clienti su laptop non protetti. Nessuna catena è più forte del suo anello più debole, ovvero una svista di un tecnico o una sola password debole possono compromettere la sicurezza di tutto il sistema.

I firewall e le VPN possono anche nascondere scappatoie e backdoor. Le chiavi crittografiche sono frequentemente troppo corte, specialmente quando si tratta di RSA. Fatti recenti hanno comprovato come la sicurezza promessa da tali sistemi sia stata poi violata. Il rovescio della medaglia delle rivelazioni dei media è che i potenziali hacker sono ora a conoscenza dei punti vulnerabili su cui fare breccia.

Una separazione fisica non corrisponde ad una protezione. In molti settori, svariate persone differenti possono accedere ai sistemi di controllo accessi. I tecnici manutentori accedono ai dispositivi in loco con i propri laptop. Un backup del software di controllo, ed i parametri di processo sono salvati anche altrove.

La protezione deve pertanto avere inizio dal sistema di controllo. Quest'ultimo può soltanto eseguire codice e far uso di configurazioni e parametri che siano stati garantiti da un soggetto autorizzato.

È possibile aggiornare la maggior parte dei sistemi di controllo sul campo. Si possono così aggiungere nuove funzioni e rimediare a malfunzionamenti. L'opzione di aggiornamento è però un tallone di Achille nell'armatura del sistema, che malintenzionati possono sfruttare per "iniettare" codice manipolato da remoto o direttamente nel dispositivo. Per impedire il suo verificarsi, il sistema deve essere avviato ed operato in un ambiente sicuro. Tutti i suoi componenti, dal bootloader in avanti, necessitano di un'autenticazione secondo i canoni crittografici per poterne garantire l'autenticità. Questo è quanto si definisce Boot Sicuro.

Come funziona il Boot Sicuro?

I componenti individuali dei sistemi di controllo sono firmati digitalmente dal produttore o dall'ingegnere di stabilimento. Ma chi verifica quali siano questi componenti? Quando e dove hanno luogo questi controlli? Un primo approccio consiste nel far sì che ogni stadio verifichi se quello successivo può essere avviato: il bootloader controlla il sistema operativo, il sistema operativo controlla l'ambiente runtime, l'ambiente runtime controlla l'applicazione, e così via. Affinché questa concatenazione sia efficace, la chiave pubblica non deve mai essere modificata nel primo stadio (deve cioè rimanere autentica). Ciò implica che il primo stadio debba perdurare immutabile. Rappresenta infatti l'ancoraggio dell'intera catena. L'optimum in fatto di sicurezza si raggiunge con un pre-bootloader, integrato fisicamente come SOC – system-on-chip. Un'alternativa meno onerosa è quella di utilizzare un dual bootloader, la cui prima parte non possa essere aggiornata, al fine di offrire almeno una protezione adeguata da minacce remote.

Il mio ambiente è sicuro?

Ulteriori requisiti di sicurezza prevedono che ciascuno stadio controlli se il precedente è stato eseguito correttamente. CodeMeter offre entrambi i tipi di controllo, in avanti e a ritroso. Il controllo a ritroso è gestito da un motore di stato a bordo della CmDongle e da una soluzione di crittografia abbinata a tale motore. Lo stadio successivo può essere decrittato solo se il precedente è stato eseguito correttamente e lo stato corretto è stato registrato nella chiave. Ciò impedisce che componenti individuali del software siano simulati nel laboratorio di un hacker, e preclude ogni possibile analisi del software nel suo ambiente. L'attività di spionaggio diventa impossibile, tanto quanto tentativi di fare leva su errori di implementazione. Il dispositivo viene protetto da uno scudo addizionale.

Conclusioni

Il boot sicuro e la protezione dell'integrità che facciano uso delle firme e della crittografia sono un pilastro su cui poggiano tutti i controlli di sicurezza. Essi complicano enormemente la riuscita degli attacchi fisici ed impediscono virtualmente tutti gli attacchi ciber-fisici. CodeMeter offre una soluzione concepita per infiltrarsi a fondo nel dispositivo, e richiede che tutti i componenti vengano eseguiti in concatenazione. I permessi possono essere definiti minuziosamente affinché incontrino le esigenze specifiche. CodeMeter protegge da spionaggio, manipolazione e sabotaggio.

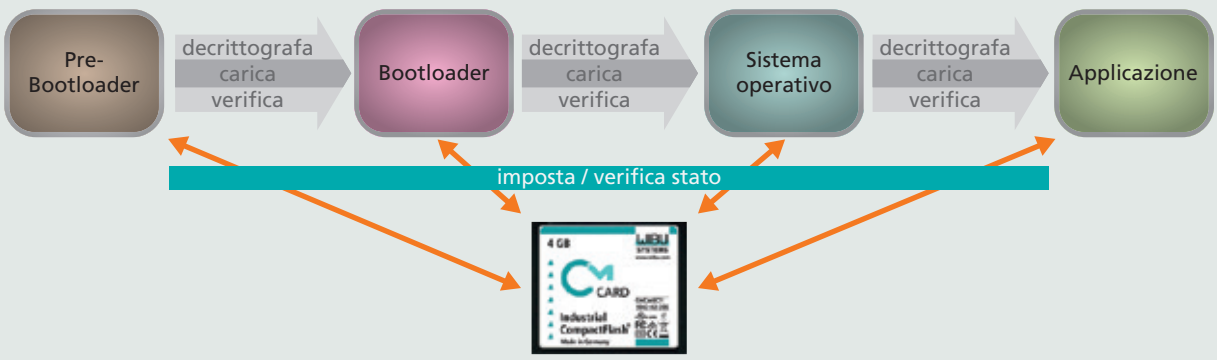
Perché così complicato? Perché non un semplice utilizzo di hash?

Qualsiasi algoritmo di crittografia asimmetrico, come l'ECC, si basa sull'uso di una chiave privata e di una pubblica. Questo rende il processo di decrittazione matematicamente impossibile – la chiave privata non può essere dedotta dalla chiave pubblica.

La chiave privata viene mantenuta al sicuro – in condizioni ideali, protetta in una chiave CodeMeter. Come il nome stesso lascia intuire, la chiave pubblica è disponibile a tutti.

Allora perché usare due chiavi? La chiave privata viene utilizzata per creare una firma, un'operazione che solo il detentore della chiave può attuare. La chiave pubblica verifica poi la validità della firma, ma non può essere impiegata per creare una firma valida di per se stessa.

Al contrario una funzione di hash, con o senza "sale casuale", utilizza la stessa chiave per creare e per verificare il valore di hash. Ciò implica che chiunque testi l'hash possa anche creare un hash valido. La firma non dovrebbe mai essere sostituita da hash. Ne risulterebbe soltanto un senso di sicurezza ingannevole.



AxProtector – Semplicemente più sicuro

La protezione del software dovrebbe essere un'operazione semplice e sicura. Trattasi di obiettivi inconciliabili? Non necessariamente. Con AxProtector di Wibu-Systems è possibile proteggere il software da contraffazione ed integrarlo con semplicità in processi esistenti.

Proteggere la proprietà intellettuale ed assicurare che solo i legittimi detentori delle licenze usufruiscano del prodotto sono due delle numerose sfide che gli sviluppatori di software ed i vendor affrontano quotidianamente. I prodotti software vengono distribuiti in molte forme e modalità, come eseguibili o librerie. Che il software sia stato predisposto per sistemi Windows, Mac o Linux, la risposta è la medesima e si chiama AxProtector.

Il termine AxProtector (Protezione Automatica degli Eseguibili) si riferisce agli strumenti per la protezione automatica dei programmi compilati. Essi comprendono svariate tipologie, dal puro codice binario, ad esempio, scritto in C/C++ o Delphi, al codice precompilato per .NET per Windows, o alle piattaforme miste a Java. Tutte queste tipologie possono essere protette con i metodi versatili offerti sotto il nome comune di AxProtector.

Un'interfaccia unificata

All'avvio di AxProtector, la prima scelta da operare sarà quella legata alla tipologia dell'applicativo. L'interfaccia guida poi l'utente attraverso il processo di conversione di un applicativo non protetto in un programma completamente crittografato. Solo pochi passi, niente istruzioni complesse o manuali. AxProtector supporta molteplici modelli di licenza, il che implica che un singolo programma può essere crittografato per un uso mediante licenze differentemente locate, ad esempio su chiavi di protezione CmDongle o codici di attivazione CmActLicense. Entrambe le opzioni possono essere consentite contemporaneamente, e il programma trova da sè la licenza corretta all'avvio. Una semplice configurazione determina come la licenza per il software protetto venga conteggiata, ad esempio ogni qualvolta il programma viene avviato o soltanto in base al numero di dispositivi. AxProtector propone una selezione di impostazioni pre-configurate per le svariate opzioni disponibili (quali ad esempio la frequenza con la quale la presenza della licenza debba essere verificata), impostazioni che possono essere ulteriormente personalizzate.

Protezione dagli attacchi

Il software protetto impara a riconoscere tentativi di manipolazione o di attacco provenienti da hacker. Questi incidenti conducono immediatamente al blocco della licenza in questione. La vostra proprietà intellettuale rimane al sicuro, protetta da eventuali attacchi futuri. AxProtector utilizza l'intera gamma di proprietà di CodeMeter per effettuare il processo crittografico. In aggiunta alle chiavi archiviate nelle licenze, esiste una chiave variabile lato software per rendere la crittografia imprevedibile. AxProtector verifica anche se il software sia stato manomesso da quando è stato originariamente crittografato e ne impedisce l'esecuzione nel caso in cui vengano rilevate manomissioni.

Maggiore protezione - IxProtector

L'elevato livello di sicurezza proposto dalla crittografia automatica può essere innalzato aggiungendo un'ulteriore protezione crittografica delle singole funzioni. Funzioni specificamente selezionate vengono crittografate individualmente e decrittate in codice eseguibile solo quando necessario. Tale tipologia di protezione viene definita

IxProtector ed è altrettanto semplice da integrare nel prodotto software. Selezionare la funzione interessata, aggiungere una semplice API per la richiesta di decrittazione, e contrassegnare la funzione nelle impostazioni è tutto quanto sia richiesto.

I differenti formati utilizzati dalle applicazioni in .NET e Java portano l'accento sul fatto che la protezione avvenga generalmente mediante metodi o classi crittografiche, che vengono decrittati automaticamente all'esecuzione dell'operazione.

Sono necessari pochi passi per includere una protezione modulare, la lettura e l'uso dei dettagli di licenza. L'interfaccia può definire licenze addizionali, ad esempio per moduli di licenza separati. L'Interfaccia Universale di Protezione Wibu (WUPI) può verificare se queste licenze addizionali siano disponibili mentre l'applicazione viene eseguita, e la crittografia agisce da scudo per il modulo in questione.

Semplici notifiche

Quando né licenze base né licenze addizionali siano disponibili, un sistema flessibile di gestione degli errori entra in azione. Le impostazioni di AxProtector e la cosiddetta libreria MessaggiUtente consente risposte e notifiche personalizzate per l'utente. L'applicazione può visualizzare il messaggio di errore o un servizio protetto può registrare l'incidente in un file di log sicuro.

Un facile processo di integrazione

La protezione dovrebbe essere implementata a livello profondo nei processi standardizzati per assicurare che il software sia già protetto durante la fase di test. La crittografia delle applicazioni o delle librerie può essere integrata prontamente nel processo di creazione. Tutti i parametri definiti mediante l'interfaccia AxProtector possono essere esportati in un file di configurazione con il semplice click di un tasto che consente la crittografia automatica mediante l'immissione di una linea di comando.

AxProtector protegge le seguenti tipologie di programmi:

- Applicativi Windows (32-bit, 64-bit)
- Librerie Windows (32-bit, 64-bit)
- Applicativi Mac OS X (32-bit, 64-bit)
- Librerie Mac OS X (32-bit, 64-bit)
- Applicativi Linux (32-bit, 64-bit)
- Librerie Linux (32-bit, 64-bit)
- .NET Assembly
- Applicativi Java
- Java Servlet

Proteggere il proprio investimento

Wibu-Systems rilascia regolarmente nuove versioni di AxProtector che introducono nuovi o migliorati meccanismi di sicurezza. Questi aggiornamenti gratuiti accrescono la sicurezza dei prodotti senza alcuno sforzo da parte vostra e mantengono il vostro vantaggio nella costante gara contro gli hacker. La protezione fornita da AxProtector non è soltanto semplice e immediata, ma cresce con voi. Non lasciatevi cogliere di sorpresa dal progresso tecnologico.

I sistemi embedded di AxProtector proteggono le applicazioni sulle seguenti piattaforme:

- Linux ARM
- Windows Embedded
- Android
- VxWorks

Semplice e sicuro

AxProtector offre la possibilità di distribuire le applicazioni e le librerie protette da un duplice scudo. In pochi semplici passi il software viene protetto sia dalla pirateria, sia da analisi del codice operate da malintenzionati. Proteggere il vostro fatturato e al contempo mettere al sicuro il know-how non ha prezzo.

SmartShelter PDF: Proteggere i documenti e saperli monetizzare

Tecnologie che proteggano dalla pirateria sono state da lungo tempo a disposizione degli sviluppatori di software e largamente impiegate. Qual è tuttavia la situazione relativa alla protezione e alla gestione dei documenti? Come è possibile garantire o addirittura moltiplicare i redditi derivanti dalla vendita o da un'accurata gestione dei documenti? È necessario un approccio differente che richiede un ulteriore grado di raffinazione del processo? L'articolo si addentra nelle similitudini dei due scenari e nelle peculiarità della gestione documentale sicura da un punto di vista orientato al profitto.

Lo scambio di informazioni è una componente essenziale della cultura attuale improntata alla comunicazione. Ciononostante, non dovrebbe sempre essere possibile duplicare informazioni o garantire un libero accesso alle fonti. Il know-how aziendale dovrebbe essere protetto, regolamentando l'accesso solo a particolari gruppi di utenti autorizzati, come nel caso dei tecnici manutentori verso la minaccia di spionaggio industriale. In un'era di sistemi interconnessi a livello globale, i manager devono considerare i documenti digitali sotto una nuova prospettiva ed implementare le misure necessarie per proteggerli. In linea con il motto "una stessa tecnologia per tutti", con CodeMeter®, Wibu-Systems offre una soluzione completa che non soddisfa soltanto i requisiti dei file documentali, ma anche quelli del tradizionale mercato dei PC, dei dispositivi industriali e delle infrastrutture basate sul cloud.

Semplicità nella protezione documentale

All'inizio degli anni Novanta l'azienda Adobe® introdusse il PDF, un formato per lo scambio di contenuti digitali. Al giorno d'oggi questo formato viene adottato come standard internazionale. Adobe® Acrobat® include di per sé un sistema di protezione documentale basato sull'assegnazione di password. Esistono tuttavia due problemi principali relativi all'impiego delle password; innanzitutto non vi è modo di impedire la loro circolazione incontrollata, e in secondo luogo sono spesso troppo corte ed ovvie, tanto da renderle suscettibili di attacco.

Il principio alla base delle password è fondamentalmente corretto, ma in pratica la sicurezza che esse offrono è minimale. Password lunghe e difficili da ricordare non sono la soluzione, in quanto risultano di complessa applicazione nell'uso quotidiano. Quale migliore soluzione allora se non generare tali password automaticamente e memorizzarle immediatamente in una chiave di protezione o in una chiave di licenza software?

Il plugin regolamenta la crittografia e la gestione licenze

L'approccio di Wibu-Systems alla soluzione si basa sull'impiego della tecnologia crittografica di Adobe Acrobat. Una volta installato, SmartShelter PDF® si annida nell'applicativo di Adobe come un vero e proprio plugin e fornisce all'utente un ventaglio di funzioni per generare documenti protetti. Il plugin è disponibile sia per Windows sia per Apple Macintosh. Un Codice Azienda univoco a livello globale generato direttamente per l'utente da Wibu-Systems ed un Codice Prodotto rappresentano lo scheletro del concetto di sicurezza. Insieme danno vita a una licenza d'uso per il documento che può essere archiviata in una chiave di protezione (CmDongle) o in una chiave di licenza software (CmActLicense).

Prima che il documento possa essere crittografato, è necessario avviare il plugin SmartShelter PDF. L'autore del documento inserisce il Codice Prodotto richiesto. Il plugin SmartShelter PDF entra in azione e crittografa il documento, generando una password

Il plugin SmartShelter PDF

estremamente sicura che viene archiviata nella chiave di protezione o nella chiave di licenza software. L'utente non verrà mai più in contatto con la password. Se tale procedura viene ripetuta intensivamente in un ambiente automatizzato, SmartShelter PDF può essere implementato come riga di comando.

Opzioni di uso documentale

Funzioni di utilizzo dei documenti, quali ad esempio stampa o modifica, possono essere regolamentate attivando o disattivando specifici diritti d'uso. È anche possibile limitare l'uso dei documenti soltanto ad Acrobat Reader. Il livello di protezione può essere ulteriormente innalzato; tra le opzioni disponibili, la disabilitazione della cattura schermate e un controllo anti-debugger per chiudere immediatamente il documento nel caso in cui venga rilevata una simile istanza.

Il cliente deve solo installare il plugin SmartShelter PDF per Acrobat Reader®. Se possiede una CmDongle o una CmActLicence con la corretta combinazione di codice azienda e codice prodotto, può ora aprire il documento crittografato.

Modelli di licenza flessibili facilitano la monetizzazione

La tecnologia di CodeMeter usata da SmartShelter PDF non fornisce soltanto funzionalità di sicurezza a protezione dei documenti, bensì anche modelli di licenza flessibili. La gamma include tra le varie alternative disponibili licenze a tempo, a consumo, di rete, ed ogni loro possibile combinazione.

È pertanto possibile definire nuovi modelli di vendita od uso documentale per generare introiti addizionali. Il concetto di codici di prodotto arbitrari permette di gestire i diritti d'uso alla base della protezione dei documenti.

Come semplificare la distribuzione delle licenze

Esistono svariate opzioni di distribuzione delle licenze. Nel caso di implementazione di un sistema di autorizzazioni, CmDongle e CmActLicense con i rispettivi diritti utente (licenze) possono essere preimpostate e spedite all'utente all'occorrenza.

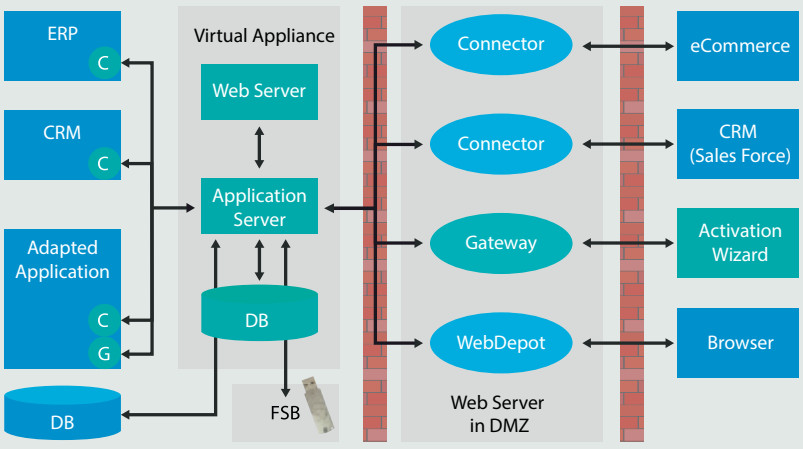
D'altro canto, l'attivazione online, come prevista da CodeMeter License Central Internet, offre un'ampia flessibilità sia al vendor sia all'utente. In questo scenario, le licenze non vengono generate anzi tempo, ma scaricate direttamente dall'utente dal server del vendor. Questo implica un negozio virtuale, per esempio, che venda e distribuisca licenze a livello globale, 24 ore al giorno, 7 giorni su 7.

Inizialmente il vendor archivia le licenze come articoli in vendita in CodeMeter License Central. Quando un utente acquista un particolare prodotto, il vendor gli trasmette un ticket per email. Il ticket può essere riscattato sul portale del vendor in cambio delle licenze effettive. Queste ultime vengono quindi trasferite in una CmDongle od attivate in una CmActLicense all'istante.

CodeMeter License Central Internet può essere integrato in processi esistenti del vendor, utilizzando interfacce web. In questo caso la connessione viene realizzata a sistemi esistenti interni od esterni di ERP o CRM che accettano direttamente gli ordini dei clienti e generano i ticket corrispondenti. In alternativa vi è la possibilità di integrare il negozio virtuale del vendor.

In conclusione

Se desiderate un sistema che protegga i vostri documenti e contemporaneamente vi aiuti ad implementare modelli di licenza idonei per i vostri utenti, SmartShelter PDF è la soluzione ideale. Non solo produce documenti protetti, ma permette anche di generare e distribuire licenze dei documenti stessi. SmartShelter PDF è da un lato la scelta ottimale per le case editrici, che desiderano essere ricompensate per ogni copia distribuita, e dall'altro per le aziende che veicolano contenuti a pagamento, o desiderano proteggere manualistica, documentazione brevettuale o documenti legali. Così facendo, SmartShelter PDF soddisfa tutti i requisiti tanto delle soluzioni per la piccola azienda quanto dei complessi sistemi di gestione documentale.



Integrazione flessibile di CodeMeter License Central Internet in processi esistenti

Portale clienti

In qualità di ISV – Independent Software Vendor, potreste chiedervi "Perché mai dovrei aver bisogno di un portale clienti?" La risposta è piuttosto semplice: "Perché volete avere la possibilità di **vendere maggiormente e contrarre i costi interni di processo**!" Potete conseguire questo risultato con una soluzione di sicurezza come CodeMeter che vi consente simultaneamente di proteggere e licenziare le vostre applicazioni. Il portale clienti è uno degli svariati strumenti per raggiungere l'obiettivo.

Che cos'è un portale clienti?

Un portale clienti è un'applicazione web che consente agli utenti di vedere e gestire le licenze per proprio conto. L'utente si logga al portale con il proprio nome e la propria password, o una chiave di licenza assegnatagli – il ticket. Una volta che ha avuto accesso, l'utente ottiene una panoramica di quali licenze è detentore e per quali prodotti. Può verificare quali licenze siano state riscattate ed attivate, attivare direttamente le licenze, e scaricare il software associato. Possono inoltre essere offerte opzioni per disattivare e riattivare le licenze. Il portale consente all'utente di registrare anche le licenze acquistate tramite rivenditore. In breve, voi ed i vostri utenti avete a disposizione un unico cruscotto per controllare le licenze comprate da ogni singolo cliente.

Come può aiutarmi ad aumentare il volume di affari?

Vendere licenze aggiuntive o tracciare i comportamenti degli utenti esistenti diventa estremamente più semplice e meno oneroso rispetto all'acquisizione di nuovi clienti. Prerequisito è conoscere di quali licenze il cliente è già entrato in possesso. I prodotti software e le loro licenze sono spesso venduti tramite rivenditore, e solo pochi ISV hanno il polso reale di chi siano i loro utenti finali.

Potete offrire ai vostri clienti l'opportunità di registrare tutte le loro licenze tramite il portale. Incentivi quali sconti o moduli addizionali o un accesso esclusivo a contenuti online possono motivarli a procedere in questa direzione.

I vantaggi sono sostanziali per voi e per i vostri clienti. Voi avete una completa visione delle licenze detenute dagli utenti e potete operare le migliori selezioni per loro. Il portale è anche un'ottima vetrina per proporre nuove offerte, che si tratti di aggiornamenti dei prodotti esistenti, versioni successive con funzioni aggiuntive, o nuovi prodotti che si confacciano ai bisogni ed ai gusti degli utenti. Inoltre, i dati raccolti consentono di personalizzare i messaggi inviati tramite le vostre newsletter.

E quali sono i benefici per gli utenti?

La registrazione mediante il portale clienti offre benefici non solo agli ISV, ma anche agli utenti finali. Che il tempo delle licenze smarrite abbia fine! Basta alla ricerca spasmodica delle chiavi di attivazione acquistate anni orsono, ogni qualvolta si renda necessario reinstallare il sistema operativo o il software debba essere migrato su un altro computer. Nessun utente ama dover abbandonare un software con cui ha familiarità. Con l'accesso al portale clienti, l'utente ha anche quello a tutte le licenze in suo possesso. Tutto ciò che dovrà tenere in un luogo sicuro è l'indirizzo email di registrazione, attraverso il quale potrà aggiornare la propria password di accesso, nel caso in cui sia andata dimenticata.

Da questa stessa piattaforma, l'utente avrà anche accesso a tutti gli aggiornamenti, in forma di note di servizio o di nuove versioni per i propri prodotti. L'aggiornamento di un software è sempre consigliato per garantirne la migliore funzionalità, specialmente quando si sia installato un nuovo sistema operativo.

Come posso contenere i costi?

In funzione del gruppo di utenti, si stima che il ricambio del computer o la reinstallazione del sistema operativo avvenga in un frangente di tempo compreso tra uno e cinque anni. Se le licenze vengono conservate su una chiave, come la CmStick, non è necessaria alcuna ulteriore attivazione dopo una tale modifica di sistema. Il caso è diverso nel momento in cui le licenze software, come una CmActLicense, richiedessero l'attivazione di un nuovo dispositivo. Secondo la legislazione vigente l'utente ha diritto all'uso della licenza. Generalmente, rimuovere il legame tra licenza e macchina quando quest'ultima raggiunge il termine del suo ciclo di vita non è consentito. Richiedendo una nuova attivazione, tuttavia, è l'utente finale a fare domanda e l'ISV a rilasciare il permesso.

È qui che il portale entra in gioco. Voi definite le regole per la disattivazione e la riattivazione che incontrino il vostro specifico gruppo di utenti per il vostro prodotto soltanto. Ad esempio, potete decidere che l'utente possa disattivare una licenza in un qualsiasi momento e riattivarla su una nuova macchina una volta che sia tornata disponibile. Nei casi in cui la disattivazione non fosse possibile, potete concedere un numero predefinito di riattivazioni, a distanza di un limite temporale dalla prima attivazione, ad esempio dopo un anno. Queste opzioni rendono possibile all'utente stesso operazioni di gestione e trasferimento delle licenze dal portale clienti, nella finestra temporale da voi impostata. Il servizio clienti dovrebbe intervenire solo in circostanze eccezionali. Voi restate nel pieno controllo delle licenze vendute, e minimizzate le risorse per l'assistenza tecnica in relazione a queste istanze.

Chi utilizza il mio software e per quanto a lungo?

Un ISV è per natura interessato a conoscere quanto spesso e per quanto tempo i suoi utenti utilizzino una specifica versione del suo software. Anche in questa evenienza, un portale clienti può essere la risposta: Grazie alla possibilità di registrarsi automaticamente insita nel software, il vostro portale clienti può raccogliere informazioni dettagliate in merito all'uso del software. Dare accesso a contenuti esclusivi online agli utenti può essere un incentivo per questo tipo di monitoraggio. Al tempo stesso, il sistema può verificare se la licenza dell'utente sia ancora valida. Anche senza registrazione automatica, il tracciamento del volume e della distribuzione di incidenti relativi ad operazioni di attivazione e riattivazione consente di stimare la vita media di un prodotto per il gruppo di riferimento.

Come può aiutarmi CmLicenseCentral?

CmLicenseCentral viene in aiuto nell'implementazione di un portale clienti. Con il suo Web Depot, CmLicenseCentral porta con sé una soluzione compatta ed indipendente pronta all'uso. Si adatta semplicemente l'aspetto grafico in modo che rifletta l'immagine aziendale e si definiscono le regole per disattivare e riattivare le licenze, in modo da sollevare immediatamente questo carico dalle incombenze del servizio di assistenza. Il Web Depot offre le seguenti funzionalità:

- Attivazione e disattivazione online delle licenze
- Attivazione e disattivazione offline delle licenze
- Riattivazione automatica

In funzione dell'infrastruttura prestabilita, il concetto modulare di Web Depot consente l'espansione dei suoi servizi e l'integrazione con i sistemi esistenti. I seguenti moduli sono sempre inclusi:

- Login cliente (stand-alone)
- Login cliente (integrato come Single Sign-On)
- Panoramica licenze
- Registrazione cliente
- Registrazione licenza / Ticket di registrazione
- Ordine e creazione di licenze demo
- Creazione di licenze per casi di emergenza

Con queste varianti a propria disposizione, è possibile personalizzare il portale clienti affinché incontri le vostre esigenze e si integri direttamente con i sistemi esistenti mediante servizi web (SOAP). CmLicenseCentral garantisce massima flessibilità ed un'integrazione totale.

Le ultimissime

Anteprima mondiale: CmCard/CFast

La carta CmCard/CFast coniuga il chip smart card di CodeMeter e l'elevata affidabilità della memoria flash SLC con un'interfacccia SATA II veloce. Il monitoraggio SMART, la protezione da interruzioni di tensione, una distinta base fissa sono alcuni dei tratti distintivi del prodotto (disponibile nei tagli da 2 a 16 GB).

Chiave CmStick/I interna

La chiave CmStick/I di Wibu-Systems si integra facilmente all'interno dei computer e di altri dispositivi, ed è così diventata un'opzione largamente impiegata. Concepita per schede madri dal design compatto, la nuova versione CmStick/IV (interna e verticale) completa la serie già composta da CmStick/I e CmStick/CI.

Inchiesta sulla soddisfazione clienti

In collaborazione con l'Istituto TNS Custom Research, abbiamo nuovamente interrogato i nostri clienti in merito alle loro opinioni sull'operato di Wibu-Systems. Desideriamo ringraziare tutti i clienti che hanno partecipato condividendo interessanti spunti di riflessione. In generale, l'inchiesta ha rivelato un'impellente necessità per misure di sicurezza straordinarie, anche se questo implica mettere seriamente mano al portafogli. I nostri clienti hanno dimostrato di apprezzare le nostre soluzioni a supporto incrociato, come CmActLicense per l'attivazione software, o la linea CmDongle dalla spiccata versatilità, o ancora CmLicenseCentral, estremamente flessibile a livello di integrazione backend con i processi di vendita.

Congratulazioni a Jens Kopf, il Product Manager di Pilz GmbH & Co. KG! È il vincitore estratto per una speciale "Cena per due".

La nuova CmStick/M

Le innumerevoli funzionalità di CodeMeter, la crittografia AES hardware, e la massima flessibilità di archiviazione sono i caratteri distintivi della chiave CmStick/M 1011-03. Il nuovo modello sarà commercializzato a partire dal I trimestre del 2014 e provvisto di memoria flash SLC (nei tagli da 128 MB a 16 GB) per uso industriale grazie all'ampio intervallo di temperatura certificato, o di memoria MLC (nella gamma da 8 a 128 GB).

Certificazione WHQL

Nella prima metà dell'anno, la carta CmCard/SD (4 GB) e la chiave CmStick con interfaccia USB hanno superato i controlli di qualità hardware per Windows effettuati dai laboratori Microsoft. Il risultato garantisce ai nostri clienti un'operatività fluida senza inconvenienti.

Microsoft Partner
Gold OEM

Marchio RCM ottenuto

Wibu-Systems ha aderito al piano di qualità delle autorità australiane. Tutti i nostri prodotti hanno ottenuto il marchio di conformità radio (RCM).

Oliver Winzenried confermato nelle associazioni industriali di categoria

Wibu-Systems è impegnata in prima linea nelle associazioni industriali; ciò permette all'azienda di raccogliere importanti segnali dal mercato, ed in particolare i requisiti di editori di software ed utenti industriali. Oliver Winzenried è orgoglioso di essere stato confermato quale membro del consiglio direzionale di BITKOM ed eletto Presidente del gruppo di lavoro "Protect-ing" di VDMA.

Aumentano i controlli di qualità

Abbiamo introdotto un nuovo controllo di qualità cui sottoponiamo l'hardware di CodeMeter; si tratta di una speciale camera climatica dove vengono eseguiti test di temperatura ed umidità.

I webinar spopolano

Ai già richiestissimi workshop e seminari, abbiamo da qualche tempo aggiunto un fitto calendario di webinar che stanno registrando un'ampia popolarità tra i nostri clienti e coloro che sono interessati ad esplorare la tecnologia di Wibu-Systems. Questi appuntamenti virtuali ospitano spesso anche partner illustri del settore, come Wind River, 3S-Smart Software Solutions e charismathics, i quali offrono ulteriori spunti e prospettive personali. Prenotatevi ora – da non perdere!

CodeMeter SDK 5.10

La nuova runtime 5.10 consente una rapida integrazione degli aggiornamenti remoti nelle chiavi CmDongle, specialmente per i casi ove coesistano codici prodotto multipli. È stata anche sviluppata una nuova interfaccia per utilizzare i browser senza l'intervento di Java. AxProtector .NET 9.0 può inoltre offuscare metodi, fare uso di trappole, e configurare le operazioni di caching per i metodi non crittografati. Per ulteriori dettagli, fare riferimento alle note tecniche sulla nuova versione.

Propellerhead – una storia di successo

propellerhead

Fondata nel 1994, Propellerhead Software è un'azienda a capitale privato con sede a Stoccolma, Svezia. Rinomata per la propria verticalizzazione in ambito musicale, Propellerhead ha creato alcuni degli applicativi software, delle applicazioni per telefonia mobile e degli standard tecnologici più innovativi al mondo.

Musicisti, produttori e i media stessi hanno elogiato Reason, ReCycle e ReBirth, per l'ispirazione, la qualità del suono e la performance di alto livello. L'app Figure per iOS nata per creare propri contenuti musicali ha vinto il premio App dell'Anno messo in palio da Apple in svariate categorie nel 2012. Tecnologie come ReWire ed il formato file REX sono divenuti standard internazionali nel settore, implementati da tutti i maggiori software musicali.

Al giorno d'oggi i prodotti di Properllehead sono utilizzati in tutto il mondo da centinaia di migliaia di professionisti ed appassionati artisti di ogni genere musicale.

La sfida

"La nostra sfida consisteva nell'individuare una soluzione sicura e dal costo contenuto, supportata da una solida infrastruttura che ci permettesse una sua integrazione con i nostri sistemi di gestione e distribuzione licenze; il prodotto avrebbe al contempo dovuto essere sufficientemente aperto, tanto da non creare un legame di dipendenza a lungo termine."

La soluzione

"CodeMeter ci consente di mettere a disposizione degli utenti finali molteplici opzioni di licenza, che essi dimostrano apprezzare in virtù dei loro bisogni diversificati. Nella fattispecie, possiamo dare vita alla stessa soluzione tanto per singoli clienti privati quanto per aziende, uno scenario questo che comporta centinaia di postazioni. Le API vengono inoltre in aiuto ai nostri ingegneri rendendo possibile un'integrazione di basso livello tra i meccanismi crittografici ed il nostro software, e garantendoci così una sicurezza senza eguali.

Il successo

"Fino ad oggi Wibu-Systems ci ha fornito una soluzione estremamente affidabile, sia in termini tecnologici che di supporto. In particolare, una chiave CmStick personalizzata come "Chiave di avvio", la variante CmStick/CI integrata e la soluzione CmActLicense basata sull'attivazione software ci regalano la massima flessibilità e maggiore adattabilità."

Ernst Nathorst-Böös

CEO Propellerhead:
AD Propellerhead:

"Utilizzando la tecnologia di prim'ordine di protezione del software di Wibu-Systems, Properllerhead si è assicurata la possibilità di creare soluzioni di gestione licenze in linea con le aspettative degli utenti finali e che non proteggono soltanto i nostri interessi ma anche quelli dei nostri partner, i quali generano prodotti addizionali per la nostra piattaforma. Senza questo sistema, dubito che le Rack Extensions avrebbero mai raggiunto il successo che hanno ottenuto."

Eventi

WIND RIVER

Developer Conference China

05 novembre – Shenzhen, JW Marriott Hotel
06 novembre – Shanghai, Sheraton Pudong Hotel
08 novembre – Beijing, Marriott Northeast Hotel

MEDICA 2013
ore 11-1, TechForum Hall 12
22 novembre 2013
Duesseldorf, Germania

Bits & Chips 2013 Embedded Systems
07 novembre, 2013
Stand 22
Brabanthallen 's-Hertogenbosch, NL

SPS IPC Drives 2013
26-28 novembre, 2013
Hall 7, Pad. 640
Norimberga, Germania

WIBU-SYSTEMS AG (WIBU®) è stata fondata nel 1989 da Oliver Winzenried e Marcellus Buchheit. Fin dai suoi esordi Wibu-Systems ha rivoluzionato la scena globale con innovazioni tecnologiche legate al mondo della sicurezza. I suoi prodotti, coperti da numerosi brevetti, offrono protezione dei contenuti digitali, della proprietà intellettuale e dell'integrità contro pirateria, reverse-engineering e code-tampering. L'ampia gamma delle soluzioni Wibu-Systems, più volte accreditate internazionalmente, è unica nel suo genere e copre ambiti applicativi che si estendono dai computer, alla telefonia mobile, dall'automazione industriale al cloud computing, dai modelli SaaS a quelli virtuali.

Attraverso il motto "Perfection in Protection", Wibu-Systems ha generato nuovi modelli di business; produttori di software attivi tanto nel settore consumer o corporate, quanto con i sistemi embedded, possono monetizzare i propri investimenti attraverso un'intera sinfonia di schemi di licenza applicabili.

Con sede a Karlsruhe. Germania, Wibu-Systems ha filiali a Seattle, USA così come a Shanghai e Pechino, Cina; l'azienda gestisce inoltre uffici di rappresentanza in Belgio, Olanda, Portogallo, Regno Unito e Spagna, ed una rete capillare di distribuzione a livello globale.

www.wibu.it

Imprint
KEYnote
26th edition, Fall 2013

Publisher:
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

Responsible for the content:
Oliver Winzenried

Editors:
Stefan Bamberg
Marco Blume
Rüdiger Kügler
Wolfgang Völker
Oliver Winzenried

Design
Markus Quintus

Print
E&B engelhardt und bauer,
Karlsruhe, Germany, EMAS III &
ISO 14001 certified

Letters are always welcome. We will protect the confidentiality of sources. Third party articles do not necessarily reflect the opinion of the editorial office. Write us at global-marketing@wibu.com

MEDIA
ACCESS
PERFECTION IN SOFTWARE PROTECTION
DOCUMENT

WIBU SYSTEMS