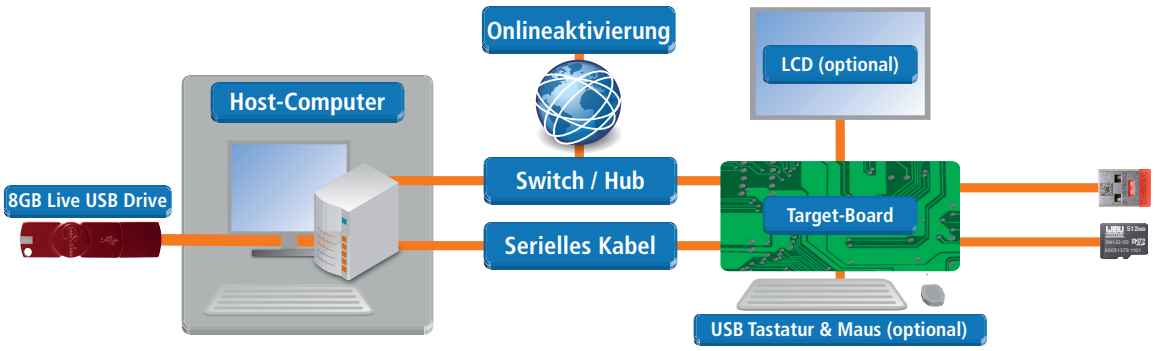
VxWorks EDK mit WindRiver

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 Piraterie, 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.

Der AxProtector als Eclipse-Plug-in schützt verschiedene Projekte wie VxWorks Image (VIP), Downloadable Kernel Modules (DKM) und Real-Time-Processes (RTP). Alle Einstellungen erfolgen innerhalb der Wind River Workbench: Schutz gegen Reverse Engineering und Lizenzmanagement und/oder Schutz gegen Verändern durch Codesignaturen, Parameter für das Lizenzmanagement und die Codeverschlüsselung sowie Schlüsselquelle für den privaten Schlüssel zur Codesignatur.



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 Verändern des Programmcodes, z.B. durch Cyberangriffe
- 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 Computer gestartet. Die 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.

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.

WIBU SYSTEMS

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:

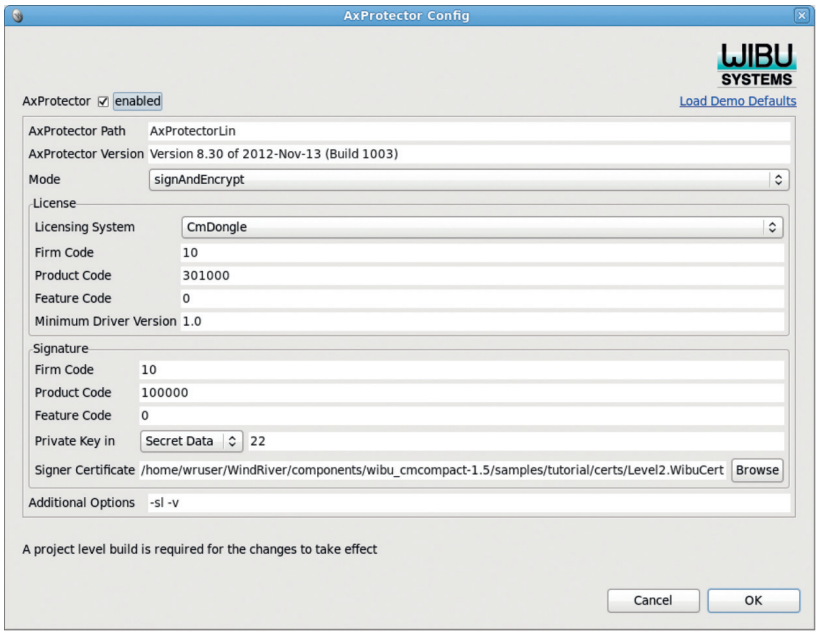
1. Die Einstellungen des AxProtectors erlauben dem Entwickler, ein Integritätszertifikat zu definieren, bestehend aus einem Hash-Wert, der Signatur und des Public-Keys.
2. Sobald das VxWorks-Projekt geladen wird, berechnet der VxWorks-Loader binär einen Hash-Wert und vergleicht diesen mit dem Hash-Wert, 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.



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

WIBU SYSTEMS