Fraunhofer
SIT

FRAUNHOFER-INSTITUT FÜR
SICHERE INFORMATIONSTECHNOLOGIE

PIRATERIESCHUTZ
FÜR BEWEGUNGSSTEUERUNGS-ANWENDUNGEN

Fraunhofer-Institut für Sichere Informationstechnologie SIT

Kontakt:
Dr. Kpatcha Bayarou
Rheinstraße 75
64295 Darmstadt

Telefon 06151 869-274
Fax 06151 869-224
kpatcha.bayarou@sit.fraunhofer.de

Der deutsche Maschinenbau ist Weltspitze. Fraunhofer SIT unterstützt Anlagenbauer und Komponentenhersteller beim aktiven Know-how-Schutz und bietet einsatzfertige Lösungen für den Kampf gegen Produktfälscher und Industriespione.

In wirtschaftlich aufstrebenden Ländern erzielen Anlagenbauer hohe Gewinne. Gleichzeitig ist das Risiko für Produktpiraterie dort am höchsten. Der illegale Nachbau von Anlagen, Systemen oder Komponenten stellt für die Industrie eine zunehmende Bedrohung dar und verursacht große wirtschaftliche Schäden. Allein deutschen Unternehmen entstehen dadurch laut Verband Deutscher Maschinen- und Anlagenbau e.V. (VDMA) jährlich Schäden von ca. 7,9 Milliarden Euro. Maschinen werden dabei nicht nur nachgebaut, sondern mitunter auch als angebliche Originalprodukte anerkannter Markenfirmen vertrieben. Darüber hinaus bieten Produktpiraten auch Reparatur- und Wartungsdienste mit gefälschten Bauteilen an. Solche Servicearbeiten sind insbesondere bei größeren Maschinenanlagen notwendig, die mehrere Bewegungsabläufe koordiniert durchführen. Allein aufgrund von Abnutzung muss der Betreiber solcher Anlagen Komponenten von Zeit zu Zeit austauschen und seine Anlage regelmäßig warten. Deshalb ist es gerade im Anwendungsbereich von Bewegungssteuerungen wichtig, auch einzelne, nachträglich eingebaute Komponenten eindeutig als Originalprodukt zu kennzeichnen.

Bisherige Konzepte basieren häufig auf Verschleierungsmechanismen (z. B. Code Obfuscation) oder unflexiblen physischen Absicherungsmaßnahmen (z. B. Hardware-Dongle). Code Obfuscation zielt darauf ab, die Logik des Programmablaufs unverständlich erscheinen zu lassen. Es erhöht jedoch lediglich den Aufwand beim Nachbau, bietet aber keinen wirksamen Schutz vor illegalen Kopien. Eine Kombination mit einem Hardware-Modul (Dongle) schützt lediglich die Software in der Steuerungseinheit, kann aber einen Nachbau der Hardware nicht verhindern. Anders die am Fraunhofer SIT entwickelten Schutzkonzepte. Sie schützen sowohl die Maschinendaten und Software vor unerlaubter Weitergabe als auch die Bauteile vor erfolgreichem Nachbau nach Reverse-Engineering-Angriffen auf einzelne Komponenten oder das Gesamtsystem.

Schutz für Anlagenbauer und Komponentenhersteller

Die Sicherheit der von Fraunhofer SIT angebotenen Lösungskonzepte basiert auf der Erkennung von Systemkomponenten mittels geheimer Schlüssel und der Implementierung von State-of-the-Art-Krypto-Verfahren. Konkret handelt es sich um eine Kombination aus Software- und Hardware-Elementen. Selbst Insider aus dem Unternehmen, welche das System genau kennen und an der Konstruktion beteiligt sind, können ohne Zugriff auf die für eine Maschine genutzten geheimen Schlüssel weder einzelne Bauteile noch die zentrale Steuereinheit fälschen. Das am Fraunhofer SIT entwickelte Grundkonzept orientiert sich an den Richtlinien des Bundesamts für Sichere Informationstechnik und lässt sich besonders kosteneffizient in bestehende Anlagen integrieren – ohne Änderung von Fertigungsprozessen oder Betriebs- und Wartungsabläufen. Außerdem lässt sich das Schutzniveau so anpassen, dass Störungen durch versehentliche oder kurzfristige Änderungen an einzelnen Originalkomponenten unterbleiben.

Fälschungen erkennen

Grundlage für die Komponentenerkennung bildet die Verkettung individueller kryptographischer Identitäten mit vorhandenen Systemkomponenten. Zum Zwecke eines ordnungsgemäßen Betriebs der Maschine müssen gewünschte Komponenten vorab lizensiert sein und anschließend ihre Autorisierung gegenüber einer zentralen Steuereinheit nachweisen. Dabei kann der Piraterieschutz gemeinsam von Komponentenhersteller und Anlagenbauer oder separat verwirklicht werden. Das System des Fraunhofer SIT sichert einzelne Komponenten sowie die daraus zusammengesetzten Anlagen. Die Sicherheitskonzepte werden auf die individuellen Wünsche des Anwenders abgestimmt und berücksichtigen die für den jeweiligen Anwendungsfall relevanten Parameter (z. B. Umfang und Sicherheitskritikalität anfallender Daten).

Die Fälschung einzelner Systemkomponenten wird sofort erkannt. Dementsprechend funktionieren Anlagen nur einwandfrei, wenn die eingesetzten Komponenten echt und entsprechend vom Hersteller lizensiert sind. Fallen einzelne Systemkomponenten aus, so können sie jederzeit durch neue, ordnungsgemäß lizensierte Komponenten ersetzt werden, ohne dass es einer Neuinitialisierung des Gesamtsystems bedarf. Dabei ist das System offen und flexibel. Insbesondere können auch Unterlizenzen (in Form von zertifizierten Schlüsseln) an fremde Komponentenhersteller vergeben werden, welche auf diese Weise ihre Produkte integrieren können, ohne dass der Piraterieschutz des Gesamtsystems beeinträchtigt wird. Die Hardware- und Software-Bausteine werden auf die Bedürfnisse des Anwendungskontexts angepasst, indem lediglich die konkret gewünschten bzw. benötigten Funktionalitäten implementiert werden. Unnötig komplizierte und kostenintensive (für den konkreten Anwendungsfall ggf. nicht angebrachte) Sicherheitsbausteine werden vermieden. So lassen sich Exportchancen nutzen und das Know-how von Hersteller und Anlagenbauer wirksam schützen.

Unser Angebot

Fraunhofer SIT unterstützt Anlagenbetreiber und Komponentenhersteller bei der Absicherung von Bauteilen und Anlagen.

Konkret bieten wir

- Beratung zum technischen Piraterieschutz
- Entwicklung von individuellen Sicherheitskonzepten
- Entwicklung von Bedrohungsmodellen und Testszenarien
- Pilotierung und Machbarkeitsstudien
- Prüfung und Weiterentwicklung existierender Schutzkonzepte