Fraunhofer

Maschine mit Kopierschutz

650 Milliarden US-Dollar pro Jahr – so hoch wird weltweit der Schaden durch die illegale Nachahmung von Produkten geschätzt. Immer häufiger ist der deutsche Maschinenbau von Produktpiraterie betroffen. Etwa zwei Drittel aller Unternehmen werden durch Produktpiraterie belastet, vor allem Hersteller von Textilmaschinen, Kompressoren und Anlagen für die Kunststoffverarbeitung. »Die meisten Unternehmen wissen gar nicht, wie leicht ihre Produkte kopiert werden können«, sagt Bartol Filipovic, Leiter der Abteilung für Produktschutz an der Fraunhofer-Einrichtung für Angewandte und Integrierte Sicherheit AISEC in Garching bei München. Das AISEC berät Unternehmen, wie sie ihre Produkte und IT-Dienstleistungen gegen Angriffe und Plagiatsversuche schützen können (Übersicht zum Produktschutz: http://ais.ec/psinfo).

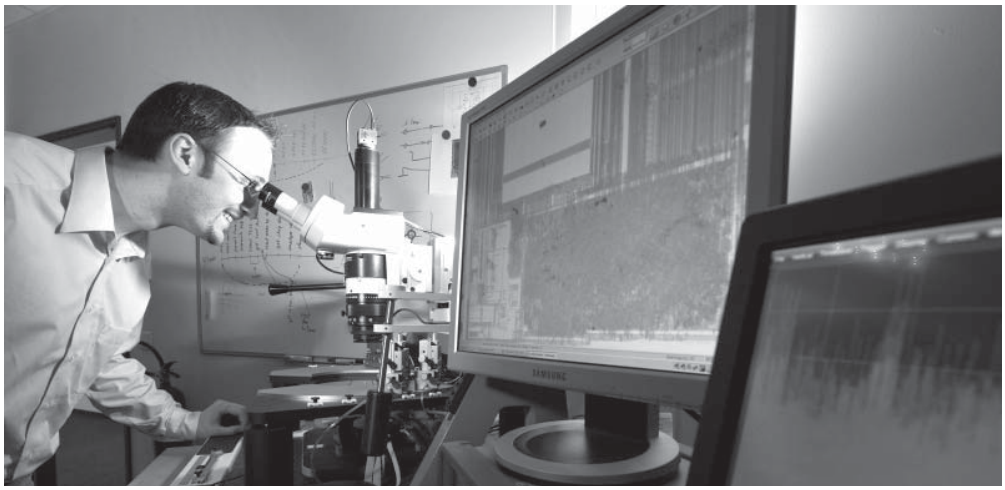
Gefälscht wird im Maschinenbau alles – vom Gehäusedesign bis zur Bedienungsanleitung. Und vor allem die »inneren Werte«: elektronische Schaltungen und Software, welche der Maschine erst ihre unverwechselbaren Eigenschaften verleihen. Eingebettete Systeme, die zum Messen, Steuern, Regeln und zur Signalverarbeitung dienen, sind deshalb ein bevorzugtes Ziel für Angriffe von Fälschern. Meist machen sich die Produktpiraten die Hände gar nicht mehr selbst schmutzig. Es gibt Dienstleister, die »Reverse Engineering« anbieten. Dabei spielen sie den Entwicklungsprozess in umgekehrter Reihenfolge nach. Zunächst analysieren sie den Aufbau der Hardware und fertigen Schaltpläne des Originalprodukts an. Dann lesen sie die Software aus und rekonstruieren daraus die Steuerung und die Funktionen der Maschine – und damit das Kern-Know-how des Herstellers.

Die wichtigste Aufgabe des AISEC ist neben der Forschung die Aufklärung. Denn viele Firmen reagieren erst, wenn Fälschungen der eigenen Produkte aufgetaucht sind. Der Nachbau lässt sich dann nicht mehr verhindern, man kann aber das Original so markieren, dass es sich eindeutig von der Fälschung unterscheidet. Sicherheitskritische Ersatzteile etwa in der Luftfahrtindustrie werden mit nicht kopierbaren Hologrammen gekennzeichnet. Oder man baut eine Art elektronischen Fingerabdruck in die Schaltkreise ein, der sich nicht verändern lässt. Doch trotz aller Vorsichtsmaßnahmen: Einen Nachbau verhindert das nicht, und auch der Handel damit lässt sich nur stoppen, wenn Zoll, Händler und Kunden die technischen Möglichkeiten haben, die Markierung auszulesen. Weil das häufig nicht der Fall ist, sollten Unternehmen bereits bei der Entwicklung einer neuen Produktgeneration geeignete Schutzmechanismen tief in der Hardware verankern. Im günstigsten Fall nimmt der Kunde bereits in der Entwicklungsphase für eine neue Produktgeneration mit dem Produktschutz-Team am AISEC Kontakt auf. Die Entwickler des Klienten zeigen den geplanten Hardwareaufbau, Schaltpläne und Software – absolute Diskretion ist da natürlich Pflicht. Die AISEC-Forscher analysieren diese Informationen auf Schwachstellen hin und geben Empfehlungen dazu, wie man das Produkt sicherer machen kann.

Gezielte technische Maßnahmen schützen vor Nachahmung

Eine Möglichkeit ist es, Kryptochips einzubauen, welche die Daten in der Maschine verschlüsseln. Sie erzeugen den Schlüssel aus den Laufzeiten elektrischer Signale auf dem Mikrochip. Bei einem anderen Chip – sogar aus derselben Produktion – sind die Laufzeiten etwas anders, und der Schlüssel lässt sich nicht nutzen. Eine weitere Option besteht darin, das Steuerungsprogramm fest in der Hardware zu verdrahten. Diese eigens entworfenen Chips machen es dem Angreifer sehr schwer, die Software auszulesen und in einem kopierten Produkt auf Standardchips laufen zu lassen. Aber auch ohne spezielle Hardware können Computerprogramme geschützt werden, indem Unternehmen beispielsweise Verschleierungsverfahren nutzen. Eine Analyse und die Entwicklung entsprechender technischer Schutzmaßnahmen lohne sich für das Unternehmen auf jeden Fall, sagt Bartol Filipovic. »Unsere Dienstleistung ist viel billiger als die durch Produktpiraterie entstehenden Kosten.« Die Kosten variieren je nach Umfang der Analyse und je nach Ausmaß der Schutzverfahren.

Ziel der Beratung durch das AISEC ist es, dem Unternehmen einen möglichst großen Zeitvorteil zu verschaffen. Wenigstens fünf bis zehn Jahre Ruhe vor Produktfälschern haben Kunden, wenn sie die AISEC-Empfehlungen umsetzen. Diese Zeitspanne ist nötig, um die teuren Investitionen zu schützen. Anders als bei Konsumgütern veraltet das technologische Know-how bei Investitionsgütern wie Maschinen nicht so schnell. Für einen Fälscher kann es sich also durchaus auszahlen, eine Maschine zu kopieren, die seit fünf Jahren auf dem Markt ist. Sind die Waren mit den neuesten Schutzvorkehrungen ausgerüstet, beißen die Fälscher jedoch auf Granit. Bartol Filipovic: »Mir ist kein Fall bekannt, wo unsere Schutzmaßnahmen erfolgreich umgangen wurden«.



Forscher entwickeln technische Schutzmaßnahmen. (© Volker Steger) | Bild in Farbe und Druckqualität: www.fraunhofer.de/presse

Fraunhofer-Institut für Angewandte und Integrierte Sicherheit AISEC | Parkring 4 | 85748 Garching b. München | www.aisec.fraunhofer.de
Kontakt: Dipl.-Inf. Bartol Filipovic | Telefon +49 89 3229986-128 | bartol.filipovic@aisec.fraunhofer.de
Presse: Viktor Deleski | Telefon +49 89 3229986-169 | viktor.deleski@aisec.fraunhofer.de