Fraunhofer
AISEC

FRAUNHOFER RESEARCH INSTITUTION FOR
APPLIED AND INTEGRATED SECURITY

PRODUKTSCHUTZ
TECHNISCHE MASSNAHMEN GEGEN NACHAHMUNG UND REVERSE-ENGINEERING

Fraunhofer Research Institution for Applied and Integrated Security AISEC

Kontakt:
Bartol Filipovic
Parkring 4
85748 Garching b. München

Telefon 089 3229986-128
Fax 089 3229986-299
bartol.filipovic@aisec.fraunhofer.de
www.aisec.fraunhofer.de

Fälschungen und illegale Nachahmung von Produkten, Komponenten und Designs schädigen innovative Unternehmen und ganze Volkswirtschaften. Neben Verkaufseinbußen kann Produktpiraterie auch zu Image-Schäden führen, etwa wenn die Fälschungen beim Kunden Qualitätsmängel zeigen. Selbst Menschenleben können bedroht sein, falls im Automobilbau minderwertige Airbags oder Bremsteile zum Einsatz kommen. Ähnliches gilt für Marken, Technologien und Verfahren im industriellen Maschinen- und Anlagenbau – etwa sensible Mess- und Steuerungsgeräte.

Optimaler Schutz

Um Produktfälschungen sowie Technologiediebstahl durch Reverse Engineering (Nachvollzug der Konstruktion) zu verhindern, haben Entwickler am Fraunhofer AISEC für Partner aus der Investitionsgüterindustrie hocheffiziente, differenzierte Sicherheitstechniken für elektronische Komponenten und Software entwickelt. Diese für die Praxis entwickelten Systeme bieten einen optimalen Schutz, weil Sie zum Beispiel die Funktionalität eines Produktes verschleiern und so Reverse Engineering praktisch unmöglich machen. So hat Fraunhofer AISEC einen Scrambler realisiert, der digitale Signalströme verschleiert und eine fortlaufende Authentifizierung zwischen elektronischen Bauteilen und einer Firmware ermöglicht. Dies erschwert die Funktionsanalyse bzw. den Produktnachbau und lässt sich im Gegensatz zu komplexen Verschlüsselungsverfahren sehr einfach und ressourcenschonend anwenden.

Dort wo standardisierte Maßnahmen – wie Schutzrechte oder auch kommerziell verfügbare Security-Lösungen – nicht greifen, hat Fraunhofer AISEC maßgeschneiderte Lösungen entwickelt, die Produktgestaltung und Dienstleistungs-/Serviceprozesse zu einer unkopierbaren Einheit verbinden. Gleichzeitig lassen sich die Schutzmaßnahmen problemlos in bestehende Unternehmensprozesse und Fertigungsverfahren integrieren; das spart Kosten.

Lösungsbaukasten

Die Bandbreite an verfügbaren Schutzmaßnahmen und Verschlüsselungstechniken ermöglicht Lösungen für jede Preisklasse. Diese reichen von schützenden Hardware-Speicherbausteinen mit abgestimmter Software (FPGA oder Mikrocontroller), bis hin zu spezifischen Markierungstechniken. Die technischen Schutzmaßnahmen des Fraunhofer AISEC eignen sich insbesondere für den Maschinen- und Anlagenbau sowie den Automobilbereich.

Fraunhofer AISEC ist in der Lage, eingebettete Systeme auf Schwachstellen und Piraterierobustheit hin zu analysieren. Komplette Systemchecks sind dabei ebenso möglich wie Analysen einzelner Komponenten. Dabei kommen neben kommerziell erhältlichen Werkzeugen auch eigene Test-Tools zum Einsatz. Um die Wirksamkeit von Schutznahmen bewerten zu können, entwickelten Mitarbeiter zum Beispiel eine Software zur Prüfung von ausführbarem Binärcode. Damit lässt sich etwa analysieren, wie stark ein Programmcode durch Obfuskatoren oder andere Verschleierungsverfahren verkompliziert wurde.

08/2011

Fraunhofer
AISEC

FRAUNHOFER RESEARCH INSTITUTION FOR
APPLIED AND INTEGRATED SECURITY

PRODUCT PROTECTION

TECHNICAL MEASURES TO COMBAT PIRACY AND REVERSE ENGINEERING

Fraunhofer Research Institution for Applied and Integrated Security AISEC

Contact:
Bartol Filipovic
Parkring 4
85748 Garching (near Munich)
Germany

Phone +49 89 3229986-128
Fax +49 89 3229986-299
bartol.filipovic@aisec.fraunhofer.de
www.aisec.fraunhofer.de

Counterfeiting and piracy of products, components, and designs by unscrupulous competitors causes considerable harm to innovative companies and indeed whole national economies. In addition to lost sales, product piracy can also lead to reputational damage if customers notice quality deficiencies in the counterfeit articles. Human lives could even be at risk, for example if inferior airbags or brake parts are installed in a car. The same applies to the brands, technologies, and processes employed in industrial engineering – like sensitive measuring and control instruments.

Optimal protection

In an effort to eliminate product piracy and reverse engineering (the reproduction of systems and designs using stolen technology), Fraunhofer AISEC's developers have evolved highly efficient and subtly differentiated security techniques for electronic components and software on behalf of partners in the capital goods industry. These systems, which are offered in answer to practical needs, afford optimal protection by concealing a product's functionality and thus rendering reverse engineering virtually impossible. A scrambler designed by Fraunhofer AISEC, for instance, hides digital signal streams to facilitate continuous authentication between electronic components and firmware. This makes it much more difficult to analyze functionalities or reproduce products. In contrast to complex encryption procedures it is very easy to use and takes up comparatively few resources.

Wherever standardized mechanisms – such as property rights or commercially available security concepts – are inadequate, the Fraunhofer AISEC team develops made-to-measure solutions that inextricably link the product design and the services or service processes together to yield a unit that cannot be copied. At the same time, the protective measures integrate seamlessly into existing business and manufacturing processes, thus also cutting costs.

Solution kit

The broad spectrum of security measures and encryption techniques available on the market form the basis for solutions in all price categories. These range from protective hardware memory chips and matching software – whether in the form of field programmable gate arrays (FPGA) or as mechanisms for microcontrollers – to special methods for marking the materials used. The technical protection measures developed by Fraunhofer AISEC are specifically tailored to the needs of the engineering and automotive industries.

Fraunhofer AISEC has the capability to test embedded systems for weaknesses and robustness against piracy. Complete system checks can be carried out as well as analyses of selected components. Proprietary test tools are used alongside commercially available products. For instance, in order to evaluate the effectiveness of security measures, AISEC has developed software for testing executable binary codes. Among other things, it assesses the degree to which a program code has been complicated by obfuscators and obfuscation techniques.

08/2011