Fraunhofer

Machines with built-in copy protection

The annual cost to industry of illegal copies of branded products is estimated at a staggering 650 billion U.S. dollars worldwide, and German machine tool manufacturers are becoming an increasingly popular target for pirating operations. Around one third of all companies have seen their business eroded by cheap imitations of their products, especially manufacturers of textile machines, compressors and plastics processing equipment. "Most companies have absolutely no idea just how easily their products can be copied," says Bartol Filipovic, head of the Product Protection department at the Fraunhofer Research Institution for Applied and Integrated Security AISEC in Garching near Munich. The AISEC advises companies on how best to protect their products and IT services from unlawful attacks on their proprietary rights (overview of product protection: http://ais.ec/psinfo).

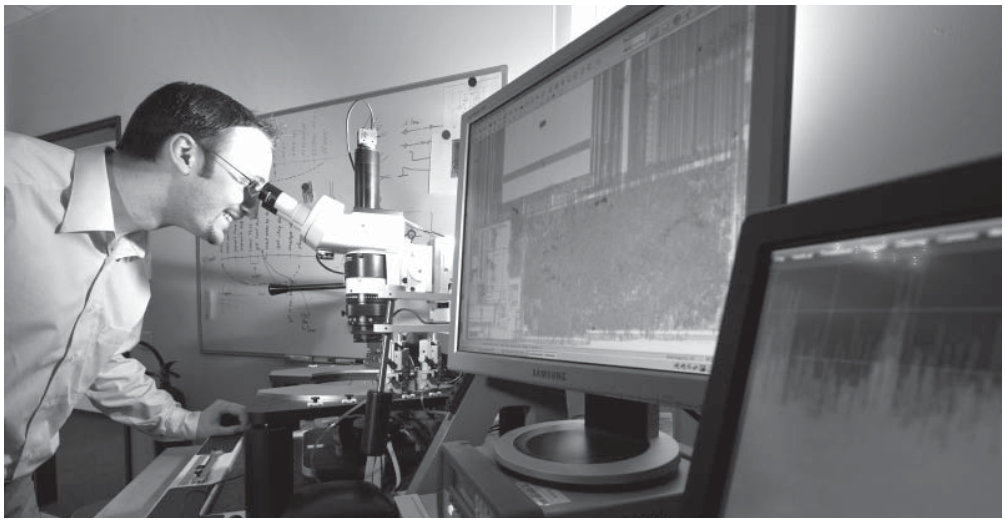
In the world of industrial machines, there are forgeries of almost everything that can be copied, from housing design to instruction manuals. The most critical elements are those that give a product its "intrinsic value": electronic circuits and software that constitute its distinctive characteristics. This makes embedded systems with measurement, control, or signal processing functions prime targets for forgers. Product pirates tend to steer clear of getting their own hands dirty, preferring to engage the services of those offering "reverse engineering". This involves performing the same development process only in the opposite direction, which begins by analyzing exactly how the hardware is put together and creating circuit diagrams of the original product. Reverse engineers can then rip the software and reconstruct the machine's control system and functions, thereby gaining access to the manufacturer's key know-how.

In addition to conducting research, AISEC's most important role is instructive. Many companies react only once counterfeits of their own products have surfaced on the market. Although it is then too late to prevent fake copies, it is possible to tag the original so that it can be distinguished from imitations. The aviation industry marks safety-critical spare parts with copy-resistant holograms; it is also possible to build a kind of indelible electronic fingerprint into the circuit. But taking any number of safety precautions is not going to be enough to deter manufacturers of fake products, and trade in them can only be stopped when customs officers, distributors and customers are all equipped with the devices needed to read and decode the markings. As this is often not the case, companies should see to it that suitable protection mechanisms are placed deep within the hardware when developing each new product range. The optimum scenario is for clients to consult AISEC before completing this phase, and have their developers share the proposed hardware setup, circuit diagrams and software with AISEC's product protection team – in strictest confidence, of course. AISEC's researchers analyze this information to identify any weaknesses and offer suggestions for making the product more secure.

Targeted technical methods guard against forgery

One option is to install cryptographic devices that encrypt the data stored within the machine. These devices generate the corresponding decryption key based on the duration of electrical signals on the microchip. The signals emitted by other chips, even those from the same production batch, will be of a slightly different duration, rendering the key unusable. Another option is to use hardwired control units. These purpose-built chips make it extremely difficult for offenders to rip the software and run it using standard chips built into product imitations. However, it is possible for companies to safeguard computer programs without the need for special hardware; for instance by adopting obfuscation techniques. It is definitely worthwhile for companies to analyze and develop suitable technical safeguards, says Bartol Filipovic. "The service we provide is less costly than the damages inflicted by product piracy." The cost of such services varies according to the scope of analysis and the extent of the protection required.

Through its advice, AISEC aims to buy companies as much time as possible. Companies that have implemented AISEC recommendations enjoy at least five to ten years relief from attacks by product counterfeiters. This time lead is crucial for companies to protect their expensive investments. The technological know-how required to manufacture industrial goods does not go out of date as quickly as that for consumer goods, making it thoroughly worthwhile for forgers to copy a machine even if it has already been on the market for five years. Equipping goods with the latest protection methods means that forgers would simply be wasting their time. "I'm not aware of a single case where someone has successfully broken through our safeguards," says Filipovic.



Researchers are developing technical safeguards. (© Volker Steger) | Picture in color and printing quality: www.fraunhofer.de/press

Fraunhofer Research Institution for Applied and Integrated Security AISEC | Parkring 4 | 85748 Garching b. München | www.aisec.fraunhofer.de
Contact: Dipl.-Inf. Bartol Filipovic | Phone +49 89 3229986-128 | bartol.filipovic@aisec.fraunhofer.de
Press: Viktor Deleski | Phone +49 89 3229986-169 | viktor.deleski@aisec.fraunhofer.de