Fingerprint makes chips counterfeit-proof

February 8 2011

Digital fingerprint makes chips conterfeit-proof. Credit: Fraunhofer SIT

Product counterfeiters are increasingly targeting chips and electronic components, with attacks on hardware modules becoming commonplace. Tailor-made security technology utilizes a component‘s individual material properties to generate a digital key. This provides components with an identity – since their unique structure cannot be copied. Fraunhofer researchers will be presenting a prototype at the embedded world Exhibition & Conference in Nuremberg from March 1 to 3.

Product piracy long ago ceased to be limited exclusively to the consumer goods sector. Industry, too, is increasingly having to combat this problem. Cheap fakes cost business dear: The German mechanical and plant engineering sector alone lost 6.4 billion euros of revenue in 2010, according to a survey by the German Engineering Federation (VDMA). Sales losses aside, low-quality counterfeits can also damage a company‘s

brand image. Worse, they can even put people‘s lives at risk if they are used in areas where safety is paramount, such as automobile or aircraft manufacture. Patent rights or organizational provisions such as confidentiality agreements are no longer sufficient to prevent product piracy. Today’s commercially available anti-piracy technology provides a degree of protection, but it no longer constitutes an insurmountable obstacle for the product counterfeiters: Criminals are using scanning electron microscopes, focused ion beams or laser bolts to intercept security keys – and adopting increasingly sophisticated methods.

No two chips are the same

At embedded world, researchers from the Fraunhofer Institute for Secure Information Technology SIT will be demonstrating how electronic components or chips can be made counterfeit-proof using physical unclonable functions (PUFs). ”Every component has a kind of individual fingerprint since small differences inevitably arise between components during production”, explains Dominik Merli, a scientist at Fraunhofer SIT in Garching near Munich. Printed circuits, for instance, end up with minimal variations in thickness or length during the manufacturing process. While these variations do not affect functionality, they can be used to generate a unique code.

Invasive attacks destroy the structure

A PUF module is integrated directly into a chip – a setup that is feasible not only in a large number of programmable semiconductors known as FPGAs (field programmable gate arrays) but equally in hardware components such as microchips and smartcards. “At its heart is a measuring circuit, for instance a ring oscillator. This oscillator generates a characteristic clock signal which allows the chip‘s precise material properties to be determined. Special electronic circuits then read these

measurement data and generate the component-specific key from the data", explains Merli. Unlike conventional cryptographic processes, the secret key is not stored on the hardware but is regenerated as and when required. Since the code relates directly to the system properties at any given point in time, it is virtually impossible to extract and clone it. Invasive attacks on the chip would alter physical parameters, thus distorting or destroying the unique structure.

The Garching-based researchers have already developed two prototypes: A butterfly PUF and a ring oscillator PUF. At present, these modules are being optimized for practical applications. The experts will be at embedded world in Nuremberg (hall 11, stand 203) from March 1-3 to showcase FPGA boards that can generate an individual cryptographic key using a ring oscillator PUF. These allow attack-resistant security solutions to be rolled out in embedded systems.

Provided by Fraunhofer-Gesellschaft

Citation: Fingerprint makes chips counterfeit-proof (2011, February 8) retrieved 25 April 2024 from https://phys.org/news/2011-02-fingerprint-chips-counterfeit-proof.html

This document is subject to copyright. Apart from any fair dealing for the purpose of private study or research, no part may be reproduced without the written permission. The content is provided for information purposes only.