Protection coat for embedded systems

Not every thief needs a crusher bar - for some a drill, just few micrometers thick, is enough to reach the prey: Information and data on a chip. A successful attack can have serious consequences, especially in security-sensitive areas such as critical infrastructures, banking and finance, or the healthcare sector. Companies and criminal hackers have been having a fierce race for a long time, and technological tricks are becoming increasingly sophisticated.

“Against this backdrop, it is no longer enough to protect data from manipulation on the software level alone”, says Martin König from Fraunhofer EMFT. In a cooperation between the Fraunhofer Institutes EMFT, AISEC and IMS, the competences in the fields of foil development, security and microelectronics complement each other in order to protect chips from unwanted attacks at system level: The innovative solution consists of a manipulation protection foil with an electrically conductive grid structure wrapped around the entire circuit board. „After the start, individual production fluctuations in the foil are measured as Physical Unclonable Function (PUF) to check the integrity from the inside,” explains Matthias Hiller, scientist at Fraunhofer AISEC. „Stored data can only be decrypted if the foil is completely intact.“ If the grid is damaged during operation, this automatically initiates the deletion of critical information such as cryptographic keys. The system provides reliable protection against drilling attacks up to a diameter of 300 µm. However, approaches already exist to further optimize this protection in the future. Already during the development phase, industry customers have shown keen interest in the protection foil. „The feedback from potential customers who have already taken a closer look at our solution helps us a lot to tailor our protective foil even more to the needs of future users”, says König. To further prepare the protective film for practical use, the research team will also extensively test it for security gaps in complex attack scenarios. „In order to maintain the protective effect of our foil, the integrity of the integrated measuring circuits must also be extensively tested,“ says Alexander Stanitzki from Fraunhofer IMS.
It will thus be more difficult for the criminal data thieves to access the coveted information inside the chips in the future. At this year’s electronica trade fair from November 13-16, interested visitors will have the opportunity to take a closer look at the protection foil at the Fraunhofer joint stand in Hall C5, booth 426.
The Fraunhofer Institute for Applied and Integrated Security AISEC is one of the leading international institutions for applied research in the field of IT security. The competence spectrum ranges from embedded and hardware security, automotive and mobile security to security solutions for industry and automation. In addition, Fraunhofer AISEC provides the possibility to evaluate the security of networked and embedded systems, hardware and software products as well as web-based services and cloud offerings in its modern test laboratories. Fraunhofer AISEC developed the security architecture to harness the physical uniqueness of each foil and at the same time detect attacks as well as confirm practical reliability and attack tests. In addition, novel error correction algorithms and a software connection to the system to be protected were developed.

Contact person: Dr.-Ing. Matthias Hiller | Phone +49 89 32299 86-162 | matthias.hiller@aisec.fraunhofer.de

The Fraunhofer Research Institution for Microsystems and Solid State Technologies EMFT contributes to the project with its expertise in printed flexible electronics. In the project, a capacitive foil with electrically conductive grid structure with line and space of 100 µm was developed. Wrapping the protective foil around the electronic system sets high requirements on the flexibility of the electrodes on the front- and backside of the foil. The evaluation chip was integrated in the foil with flip-chip technology, using the infrastructure and equipment available at Fraunhofer EMFT.

Contact person: Martin König | Phone +49 889 56795 -140 | martin.koenig@emft.fraunhofer.de

For more than three decades, the Fraunhofer Institute for Microelectronic Circuits and Systems IMS has been an innovation driver for integrated sensor systems and CMOS-based semiconductor manufacturing processes. For applications in automation, eHealth and eMobility, the IMS develops integrated circuits and post-CMOS sensor elements with special requirements for failure and cyber safety. The IMS accompanies partners from concept and technology development through to pre-production, drawing on the best external manufacturing partners and its own CMOS and microsystems technology manufacturing facilities. The Fraunhofer IMS developed the integrated sensor circuit, which makes the minimum production fluctuations in the film measurable. In addition, industry-compatible technologies for the secure identification of silicon chips were developed and protective measures against reverse engineering were integrated into the CMOS chips.

Contact person: Dipl.-Ing. Alexander Stanitzki | Phone +49 203 3783-239 | alexander.stanitzki@ims.fraunhofer.de