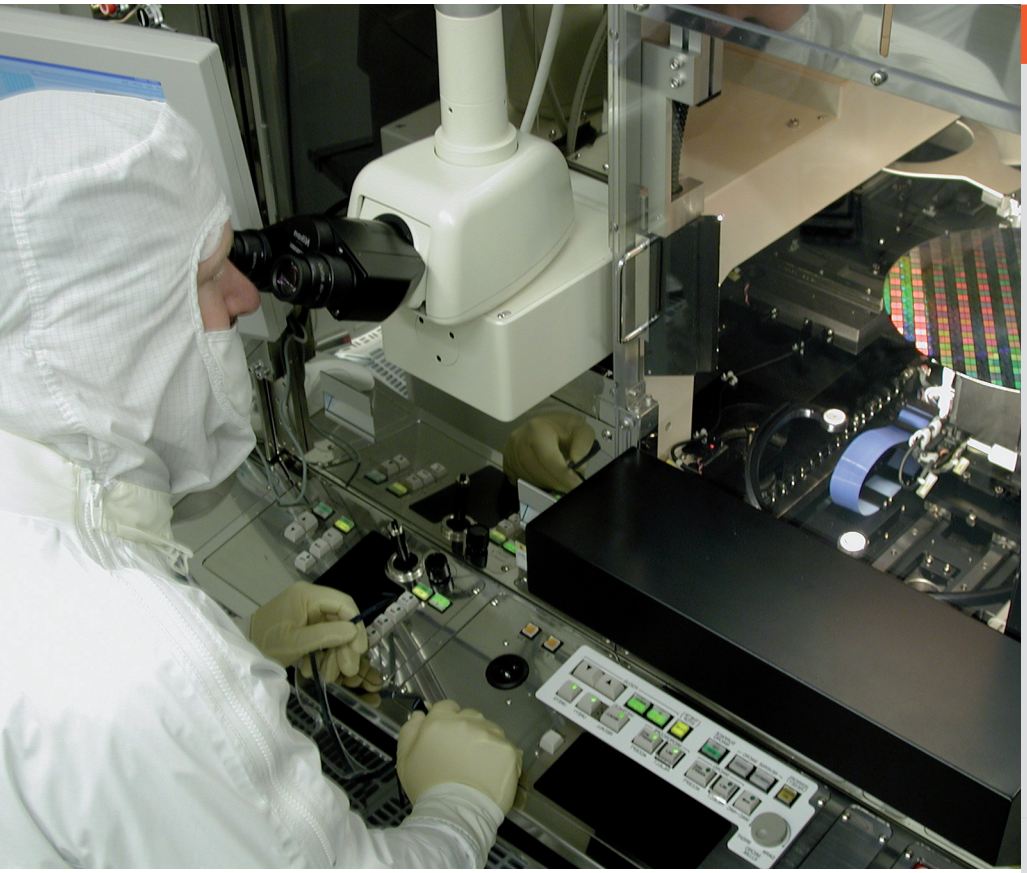
Fälschungssicherheit von Hardware

COMPUTER MIT ECHTHEITSZERTIFIKAT



UNIQUE

Foundations for Forgery-Resistant Security Hardware

Programm: 7. EU-Rahmenprogramm für Forschung, technologische Entwicklung und Demonstration

Förderlinie: Informations- und Kommunikationstechnologien

Projekttyp: STREP

Projektkosten: 4,215.026 Euro, davon 2,954.221 Euro EU-Förderung

Laufzeit: 1.9.2009 - 31.08.2012

Projektkoordinator: Technikon Forschungs- und Planungsgesellschaft mbH

Projektwebsite: www.unique-project.eu

Computerbauteile werden immer komplexer und daher anfälliger für Manipulationen und Fälschungen. Im Projekt UNIQUE sollen Technologien entwickelt werden, die die Echtheit und Fälschungssicherheit der Hardware von der Produktion bis zum Einsatz garantieren.

Hardware wird immer komplexer und benötigt daher stärkere Sicherheitsmechanismen, um gegen unautorisierte Angriffe geschützt zu sein. Solche bösartigen Attacken werden allgemein als „Fälschen“ bezeichnet. Unter diesem Begriff versteht man einerseits die unerlaubte Entwicklung und Produktion entsprechender Imitate bzw. Nachbauten, wenn Urheberrechte nicht entsprechend berücksichtigt werden oder andererseits die Manipulation von bestehenden Produkten.
Der Wert an gefälschten Gütern betrug im Jahre 2002 über 200 Mrd. $ und stieg 2006 sogar auf 450 Mrd. $ an. Um den Anteil an Fälschungen am Weltmarkt zu verringern bzw. die Möglichkeit eines Angriffs zu unterbinden, erforscht und entwickelt das UNIQUE Projekt innovative Chip Eigenschaften, um die eindeutige Markierung und Identifizierung von IT Produkten zu ermöglichen.
UNIQUE hat es sich zum Ziel gesetzt, die dringend geforderte Glaubwürdigkeit der Authentifizierung von Produkten, sowie die sichere Erzeugung von Hardware sicherzustellen. Das Vertrauen in Hardware Produkte konnte bislang leider nicht hergestellt werden, da in der Vergangenheit immer nur die Sicherheitsanalyse und nicht die Entwicklung von Sicherheitsmechanismen im Vordergrund stand.
Die im UNIQUE Projekt nun neu entwickelten Technologien sollen hingegen Funktionalitäten aufweisen, die es ermöglichen, gegen Fälschungen, Klonen, Verfälschungen, Reverse Engineering und die Einbindung von schädlichen Codes in Produkte zu agieren und somit jeglicher unautorisierten Modifikation entgegenzuwirken. Dabei wird aber nicht nur auf neue Sicherheitshardware, sondern auch auf die in die Hardware integrierten Sicherheitsfunktionen und Evaluierungsmethoden der Hardware und Software Wert gelegt.
Das Projekt versucht, dem Problem der bislang ursprünglichen Fälschungssicherung vom Level der Applikation bis

SERVICE

Ihr Wegweiser durch die Europäischen und Internationalen Programme: Information, Beratung, Coaching von der Projektidee bis zum Projektabschluss bieten Ihnen die ExpertInnen der FFG.

Profitieren Sie vom umfassenden Service und optimieren Sie damit Ihre Erfolgschancen im „Match“ um europäische Forschungsgelder.

FFG

Projektkoordinator Klaus-Michael Koch

Fotos: Intel, fellex/Pixelio, beigestellt

hin zur direkten Integration auf den Computerchips entgegenzuwirken. Jedoch muss dies schon beim Design der Sicherheitsarchitektur, welche die Sicherheitsprotokolle und Designprinzipien enthält, berücksichtigt werden. Kryptographische Bausteine werden dazu verwendet, um eindeutige Eigenschaften der vorhandenen Hardware auszuwerten und das Sicherheitsprotokoll zu generieren. In jedem Designschritt müssen diese Technologien durch geeignete Mechanismen abgesichert werden; zusätzlich muss für eine sichere Kommunikation und konsistente Schnittstellen von der Applikationsebene bis hin zur Hardware-Schicht gesorgt sein.

Die Hauptaufgabe des Projekts ist die Entwicklung von innovativen sicheren Technologien, die kosteneffizient und effektiv einsetzbar sind. Für die Realisierung der gesicherten Hardware Komponenten werden integrierte Schaltkreise verwendet, um vor allem die Sicherheit in der Elektronik-, Automobil-, Flugzeug- und Pharmaindustrie sowie kritische Infrastrukturen und behördliche Anwendungen wesentlich zu erhöhen.

PROJEKTPARTNER

Organisation	Land
Technikon Forschungs- und Planungsgesellschaft mbH (Projekt Koordinator)	Österreich
Ruhr-University-Bochum	Deutschland
Katholieke Universiteit Leuven	Belgien
Technische Universität Darmstadt	Deutschland
Thales Communications SA	Frankreich
Sirrix AG	Deutschland
Intrinsic ID B.V.	Niederlande
Intel Performance Learning Solutions Limited	Irland

Aktivitäten der FFG im Bereich Europäische und Internationale Programme werden von der Republik Österreich und der Wirtschaftskammer Österreich finanziert.