

Press release**Fraunhofer-Gesellschaft****Dr. Johannes Ehrlenspiel**

03/09/2001

<http://idw-online.de/en/news31101>Research projects
Information technology, Media and communication sciences
transregional, national**Sicherheit für Computernetze****Hacker-Angriffe oder Virus-Attacken sorgen weltweit immer wieder für Furore und legen Unternehmen lahm. Ein neues Sicherheits-System kann den Missbrauch sensibler Informationen verhindern und die Verletzung von Urheberrechten aufklären.**

Hacker-Angriffe gegen Konzerne wie Microsoft, Forschungslabors oder das Pentagon sorgen immer wieder für Schlagzeilen. Doch Gefahren drohen Unternehmen nicht nur von Viren oder Trojanischen Pferden aus dem Internet, sondern auch von den eigenen Mitarbeitern: Nicht genehmigte Software, eingeschleuste Viren, Missbrauch der Netzzugangsrechte oder Datendiebstahl sind - beabsichtigt oder unbeabsichtigt - leider keine Seltenheit. Im Projekt CIPRESS (Cryptographic Intellectual Property Rights Enforcement SyStem) wurde im Auftrag der Mitsubishi Corporation, Tokyo, Japan, ein System für Datensicherheit entwickelt, das unter dem Namen »ReEncryption System« nun von der Mitsubishi Corporation kommerziell angeboten wird. Das System wird auf der CeBIT in Halle 16, Stand B23/2 vorgestellt.

»Ziel unserer Forschungsarbeiten war ein umfassendes Sicherheitskonzept, das den Missbrauch sensibler Informationen und die Verletzung von Urheberrechten verhindert - nach innen und außen«, berichtet Dr. Christoph Busch vom IGD. Das Besondere: Die Verschlüsselung erfolgt für jedes Dokument automatisch, ohne dass der Nutzer es bemerkt oder verhindern kann. Er gibt seine Daten ein, bearbeitet die Dokumente wie gewohnt. Sobald er sie speichert, laufen im Hintergrund komplexe Vorgänge ab. Bleiben die Daten innerhalb des gesicherten Bereichs, sind die Verschlüsselungsmechanismen für den Nutzer unsichtbar. »Will jemand jedoch ein verschlüsseltes Dokument an einem nicht mit dem Sicherheitssystem verbundenen, also fremden PC oder Laptop öffnen, oder verfügt er nicht über hinreichende Zugriffsrechte, so wird er nur »Rauschen«, d.h. verschlüsselte Daten sehen«, erklärt Dr. Busch. Selbst in ausgedruckten Daten sind unsichtbare Wasserzeichen verborgen. Sie geben Aufschluss über den letzten Nutzer des Dokuments und über den rechtmäßigen Besitzer. Auch wenn komplette Datenträger oder Rechner entwendet werden, ist die Sicherheit der dort gespeicherten Daten gewährleistet. Sie sind jederzeit verschlüsselt gehalten.

Verantwortlich für den hohen Sicherheitsstandard ist die Verknüpfung von zwei Technologien: das von Mitsubishi Corporation patentierte ReEncryption™ Verfahren und die vom IGD patentierten Digitalen Wasserzeichen. Sie können wie Viren-Scanner direkt in das Betriebssystem eingebettet werden und somit sämtliche auf dem Betriebssystem verfügbaren Anwendungen umfassend absichern. Die aktuelle Version des Systems unterstützt Microsoft® Windows® NT 4.0. Versionen für Microsoft® Windows® 2000 sowie für führende Unix® Varianten wie Sun® Solaris® sind derzeit in der Entwicklung.

Ansprechpartner:
Dr. Christoph Busch
Telefon: 0 61 51/1 55-1 47
Fax: 0 61 51/1 55-4 99
christoph.busch@igd.fhg.de

URL for press release: <http://www.igd.fhg.de/igd-a8/projects/cipress/index-d.html>

URL for press release: <http://www.fraunhofer.de/german/press/md/index.html>

