



Bundesministerium
für Bildung
und Forschung



HAUSANSCHRIFT Hannoversche Straße 28-30, 10115 Berlin
POSTANSCHRIFT 11055 Berlin

Presse- mitteilung

TEL 030 / 18 57-50 50

FAX 030 / 18 57-55 51

E-MAIL presse@bmbf.bund.de

HOME PAGE www.bmbf.de/

16. Juli 2010
131/2010

Bezahlen mit Chipkarte wird sicherer

BMBF startet neues Vorhaben zum Schutz von Chipkartentechnik

Ob Bezahlen für den Nahverkehr oder der Zugang zum Arbeitsplatz: Ohne Chipkarte geht heute gar nichts mehr. Doch die geheimen Schlüssel der Karten lassen sich mit etwas Aufwand ausforschen, selbst bei Einsatzgebieten mit hohen Sicherheitsanforderungen. Mit dem richtigen Werkzeug – Laptop, Lesegerät, entsprechende Software – können dann verhältnismäßig leicht gespeicherte Geldbeträge manipuliert oder Karten dupliziert werden. Diesen Gefahren will das Bundesministerium für Bildung und Forschung (BMBF) mit dem neu gestarteten Forschungsprojekt RESIST begegnen. Es fördert das Vorhaben mit insgesamt fast 2,8 Millionen Euro.

Wer sich Zugang zu den geheimen Kartenschlüsseln verschaffen will, nutzt häufig sogenannte „Seitenkanalangriffe“. Diese Technik macht sich zunutze, dass jede elektronische Schaltung auf einer Chipkarte verschiedenste Signale in ihre Umgebung abgibt, die sich auswerten lassen: elektromagnetische Strahlung, Wärme, Stromverbrauch sowie die Reaktionszeit für Berechnungen. Eigentlich werden Seitenkanalangriffe eingesetzt, um Verschlüsselungsgeräte zu überprüfen. In einigen Fällen lässt sich mit dieser Methode aber auch die Sicherheit von Chipkartensystemen aushebeln, deren Daten dann ohne großen Aufwand manipuliert werden können. Leidtragende sind weniger die einzelnen Nutzer der Karten, als vielmehr die Betreiber der Kartensysteme.

In RESIST werden neuartige Ansätze entwickelt, die Chipkarten resistent gegen Seitenkanalangriffe machen sollen. Vorstellbar ist es beispielsweise, die Systeme so

zu verpacken, dass keine leicht detektierbaren Signale mehr nach außen dringen können. Oder die eigentliche Datenverarbeitung wird zur Ablenkung gezielt mit „sinnlosen“ Aktionen überlagert, so dass die relevanten Informationen nicht so leicht herausgefiltert werden können.

Unter Führung des Fraunhofer-Instituts für Sichere Informationstechnologie SIT in Darmstadt arbeiten universitäre und industrielle Partner daran, sichere, einfache und kostengünstige Techniken hierfür zu entwickeln. Die Ergebnisse sollen auch zum Schutz und zur Qualitätssteigerung nationaler Produkte und Anwendungen beispielsweise im Zusammenhang mit dem elektronischen Personalausweis oder der digitalen Interaktion mit Bürgerämtern beitragen.

RESIST ist Teil des neuen Programms „IT-Sicherheitsforschung“, das gemeinsam vom BMBF und vom Bundesministerium des Inneren (BMI) aufgelegt wurde. Das BMBF fördert die IT-Sicherheitsforschung hierüber in den kommenden fünf Jahren mit insgesamt 30 Millionen Euro. Ziel ist es, das zuverlässige und sichere Funktionieren von Systemen der Informations- und Kommunikationstechnologie (IKT) zu gewährleisten. Weitere Projekte befassen sich beispielsweise mit der Sicherheit der elektronischen Komponenten im Auto oder von Selbstbedienungsautomaten in Banken und Geschäften. RESIST unterstützt sowohl innovative Entwicklungen von Hardwareherstellern als auch aus der IT-Sicherheitsbranche. So sollen neue, sicherere Produkte auf den Markt kommen, für die sich dann weitere Anwendungsfelder erschließen lassen.

RESIST wird auf der Internetseite <http://www.bmbf.de/de/14946.php> als aktuelles „Projekt des Monats“ vorgestellt.