O.Univ.-Prof. Dipl.-Ing. Dr.techn. Reinhard Posch
Institut für Angewandte Informationsverarbeitung und Kommunikationstechnologie
E-Mail: Reinhard.Posch@iaik.at
Tel.: 0316 873 5510

Forschung an der Fakultät für Informatik

Privatsphäre und Identifikation: ein Gegensatz?

Privacy and Identification: Contradicting Principles?

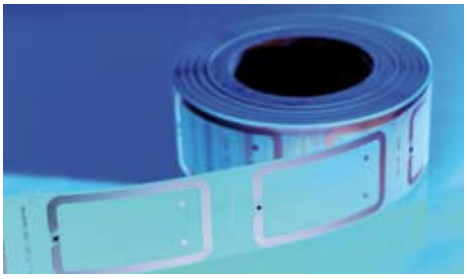
Geldabheben, Zufahrt zum Parkplatz, Zutritt zum Arbeitsbereich, elektronische Unterschrift auf der Steuererklärung, eCard beim Arztbesuch, aber auch ein einfaches Telefongespräch mit dem Mobiltelefon: Immer öfter verwenden wir Chipkarten im täglichen Leben. Wir hoffen, dass einerseits beim eigenen Bankkonto alles richtig läuft, gleichzeitig bangen wir über den Verlust von Privatsphäre. Wer speichert welche Datenspuren von mir wie lange und zu welchem Zweck?

Bei der Verwendung von Chipkarten haben wir uns einigermaßen an die Problematik gewöhnt. Die Benützung der Chipkarte lässt sich oft angesichts des Komforts, den sie bietet, nicht vermeiden. Aber es handelt sich noch immer um einen bewussten Akt: Man nimmt die Karte aus der Tasche und bringt sie mit dem Lesegerät in Verbindung.

E-Government-Basistechnologie Chipkarten (Photonachweis: IAIK)

Doch bereits jetzt sprechen alle von Alltagsgegenständen, welche demnächst mit Funkchips, sogenannten RFID-Chips ausgestattet werden. Die Kommunikation mit diesen Chips ist über die menschlichen Sinne nicht wahrnehmbar.

Sollte man solche RFID-Chips am Körper tragen, etwa innerhalb der mitgeführten elektronischen Geräte, aber vielleicht auch als Marken auf Kleidungsstücken, dann besteht die Gefahr der unbemerkten Kommunikation mit diesen Funkchips und die damit verbundene Möglichkeit des unbemerkten Hinterlassens einer Datenspur. Die Praxis geht noch viel weiter; in den USA werden Patienten – auf deren Wunsch – heute schon Chips eingepflanzt, damit Falschmedikation über medizinische Einrichtungen hinweg vermieden werden kann.



Smart Labels verbinden die Welt der Dinge mit der Welt der Logistik und Administration (Photonachweis: NXP)

Die Erforschung von technischen Methoden zum Schutz solcher sensiblen Daten gehört zum wissenschaftlichen Kerngebiet des Institutes für Angewandte Informationsverarbeitung und Kommunikationstechnologie (IAIK) an der Fakultät für Informatik.

Die langjährige intensive Beschäftigung mit diesem Thema, sei es aus Sicht der manches Mal notwendigen Identifikation und Authentifikation von Personen oder Daten, aber auch aus Sicht des Schutzes der Privatsphäre, hat das Institut zum internationalen Hotspot im Bereich Informationssicherheit gemacht. Das Institut beschäftigt sich sowohl mit Grundlagenthemen wie etwa Kryptografie oder Kryptoanalyse – Vincent Rijmen ist mit seiner Krypto-Gruppe auf mehreren Themen hier weltweit führend – , als auch in der angewandten Forschung, wo sowohl Netzwerk-, Software- und auch Hardwarethemen bearbeitet werden. Mit dem am Institut ansässigen E-Government-Innovationszentrum werden zudem auch die aus der Sicherheitsproblematik abgeleiteten organisatorischen Fragen des Umbaus der österreichischen Bundes- und Regionalverwaltung in ein „digitales Österreich" beforscht.

Die in der jüngeren Vergangenheit daraus entstandenen Forschungsergebnisse sind etwa mit dem Konzept „Bürgerkarte" im europäischen Umfeld mit großem Interesse aufgenommen worden. Der dem Bürgerkartenkonzept zu Grunde liegende sensible Umgang mit Identifikation einerseits und der Schutz der Privatsphäre andererseits haben nicht zuletzt zu mehreren internationalen Preisen für das österreichische E-Government-Modell geführt. Zudem wurde 2006 im jährlich stattfindenden von der Kommission durchgeführten europaweiten Ranking das österreichische E-Government-Modell auf den 1. Platz gereiht.

Als Leiter des IAIK und gleichzeitiger langjähriger Chief Information Officer des Bundes freut es mich zu sehen, wie die Spannbreite von universitärer Grundlagenforschung über angewandte Forschung bis hin zur Transformation der Organisation eines Staates wie Österreich unter dem gemeinsamen Thema Informationssicherheit zu gegenseitiger Befruchtung der einzelnen Arbeitsschwerpunkte geführt hat.

Auch die jüngste Anerkennung des „ID Community Award" am Weltkongress für automatische Identifikationstechnologien in Mailand betrachte ich als Ergebnis des vielfältigen und exzellenten Hintergrunds nicht zuletzt auf der TU Graz, auf Basis dessen es für mich sehr angenehm zu arbeiten ist. Diese Auszeichnung wurde auf Grund der langjährigen Bemühungen, digitale Sicherheitsstandards innerhalb der Europäischen Union zu schaffen, ausgestellt.

Wenn es nunmehr darum geht, das österreichische Bürgerkartenkonzept auf kontaktlosen Chipkarten zu testen oder der aufkommenden Sicherheitsproblematik bei RFID-Chips mit neuen Forschungsergebnissen aus dem Bereich Kryptografie zu begegnen, so sehe ich das Gebiet Informationssicherheit noch lange als für unsere Gesellschaft extrem relevant an. Hinzu kommen Fragen nach der Sicherheit der sogenannten „kritischen Informationsinfrastrukturen" eines Landes. Die Stärke unseres Institutes liegt nahezu in allen Fällen im ganzheitlichen Forschungsansatz und im Abdecken an sich unterschiedlicher Fachgebiete, die in der Anwendung zusammenspielen. Das kann Hardware und Software sein, wie im Fall der effizienten Umsetzung von Krypto-Algorithmen in Chips; das kann aber auch Datenschutz und RFID sein wie im konkreten Fall der kontaktlosen Bürgerkarte.

Bei all diesen Themen hat Österreich bereits jetzt eine über die Größe des Landes hinausgehende internationale Bedeutung.

Privacy and Identification: Contradicting Principles?

Privacy and identification are the cornerstones in many of today's activities in business or as a citizen: Be it banking, access to parking lots, a visit to the doctor, issuing an electronic signature or just a call with the mobile phone. Smart cards are everywhere. The next technology generation will most likely introduce a massive amount of similar devices, so called RFID chips, for even more aspects of our lives. Then, many items will be equipped with such radio frequency identification chips, and their communication with the environment will not be apparent to the bearer as in the case of smart cards. In both cases, smart cards and RFID chips, the topics privacy as well as identification and authentication need to be addressed with appropriate technology, but also with suitable processes and a regulatory framework.

With the Citizen Card Framework, Austria's eGovernment has been ranked number 1 in the EU in 2006. Research at the Institute for Applied Information Processing and Communications has provided a substantial base for this success.