Dipl.-Ing. Herbert Leitold
A-SIT, Zentrum für sichere Informationstechnologie Austria
E-Mail: Herbert.Leitold@a-sit.at
Tel.: 0316 873 5521

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

Die TU Graz als Leuchtturm für Netzwerk- und Informationssicherheit

A Beacon in Network- and Information-Security

Das Institut für Angewandte Informationsverarbeitung und Kommunikationstechnologie (IAIK) der Fakultät für Informatik setzt seit jeher in seiner Forschung den Schwerpunkt auf die Informationssicherheit. In diesem in einer Informationsgesellschaft immens an Bedeutung gewinnenden Bereich deckt das IAIK mit seinen nun nahezu 50 Mitarbeiterinnen und Mitarbeitern ein breites Feld ab — in vielen Bereichen genießt das IAIK dabei internationales Renommee und liefert herausragende Spitzenleistungen. Diese Kompetenz wurde jüngst auch dadurch anerkannt, dass der Institutsvorstand Prof. Reinhard Posch im März 2007 zum Vorsitzenden des Verwaltungsrates der European Network and Information Security Agency (ENISA) bestellt wurde. In diesem Artikel beschreiben wir kurz diese europäische Agentur und die Funktion, die Prof. Reinhard Posch nun dort innehat. Wir stellen danach Highlights der Forschungsbereiche des IAIK vor, um den Zusammenhang mit der Forschung in der Netzwerk- und Informationssicherheit an der TU Graz darzustellen.

Informationssicherheit hat viele Erscheinungsformen (Photo: IAIK)

ENISA wurde von der Europäischen Union (EU) im Jahr 2004 als Europäische Agentur für Netz- und Informationssicherheit gegründet. Sie ist damit eine der bisher 22 Gemeinschaftsagenturen der EU. Die EU unterstreicht mit der Einrichtung von ENISA den Stellenwert für die Gesellschaft, den sie Fragen der Sicherheit in Informations- und Kommunikationssystemen beimisst. Nach einem interimistischen Sitz in Brüssel ist die Agentur seit August 2005 an ihrem von der griechischen Regierung gewählten Standort in Heraklion in Kreta eingerichtet. Mit der Übersiedlung wurde auch der operative Personalstand weitgehend erreicht, sodass ENISA den Vollbetrieb aufnehmen konnte. Ende 2006 war der Personalstand bei 37 Personen, dieser soll 2007 auf 44 Mitarbeiterinnen und Mitarbeiter anwachsen. Eigene Aktivitäten von ENISA werden ergänzt durch Ad-Hoc-Arbeitsgruppen, die zu ausgewählten Themen mit internationalen Experten besetzt werden.

ENISA Gebäude in Heraklion, Kreta (Photo: ENISA)

Das jährliche Budget der Agentur umfasst etwa 8 Millionen Euro. Zu den Aufgaben von ENISA zählt unter anderem die Unterstützung der EU-Institutionen und der Mitgliedsstaaten in Fragen der Netzwerk- und Informationssicherheit, die Förderung der Zusammenarbeit der verschiedenen Akteurinnen und Akteure in diesem Bereich oder die Beratung in Bezug auf Forschungsarbeiten. Die organisatorische Struktur umfasst einen Direktor, eine beratende ständige Gruppe der Interessensvertreterinnen und Interessensvertreter sowie einen Verwaltungsrat. Die ständige Gruppe umfasst 30 Mitglieder aus Industrie, Verbrauchergruppen und wissenschaftlichen Sachverständigen. Sie berät bei der Ausarbeitung des Arbeitsprogramms von ENISA und in der Pflege von Kontakten zu interessierten Kreisen. Der Verwaltungsrat wird von einem Vertreter/einer Vertreterin jedes EU Mitgliedsstaats, drei VertreterInnen der Europäischen Kommission sowie je einem Experten/einer Expertin aus der Industrie, der Verbrauchergruppen und der Wissenschaft gebildet. Zu den Aufgaben des Verwaltungsrats zählt unter anderem die Bestellung des Direktors/der Direktorin der Agentur, die Annahme des Arbeitsprogramms oder die Annahme des Budgets. Nachdem Prof. Reinhard Posch bereits seit der Einrichtung von ENISA Österreichs Vertreter im Verwaltungsrat war, wurde er nun für eine Funktionsperiode von zweieinhalb Jahren zu dessen Vorsitzenden ernannt.

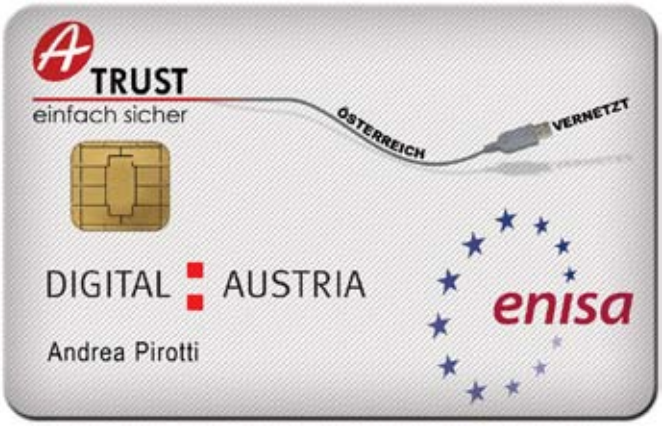
Diese Bestellung sehen wir auch als Anerkennung der Forschungsleistungen, die die Mitarbeiterinnen und Mitarbeiter des IAIK seit der Gründung 1986 an der TU Graz erbracht haben. Dabei ist auch die Netzwerk- und Informationssicherheit selbst ein breites Feld, das weit über die Sicherheit von PCs oder im Internet hinausgeht. Leert jemand die Taschen, so wird er oder sie dabei einiges an Informationstechnologie finden, wo Sicherheit über Anwendungen im Internet hinausgehend eine Rolle spielt. Dies können Zutrittssysteme zu Gebäuden, elektronische Autoschlüssel, Mobiltelefone, die E-Mail empfangen oder mit dem gemeinsamen Kalender der Organisationseinheit synchronisieren, Bankomat- und Kreditkarten oder die Chipkarte als Krankenscheinersatz für den Arztbesuch sein. Dies sind nur einige Beispiele, in denen die Informationssicherheit zum Funktionieren der Anwendung essentiell ist. Das IAIK setzt sich in dieser breiten Landschaft das ehrgeizige Ziel, in einigen ausgewählten Bereichen Exzellenz zu erreichen.

Ein wesentlicher Bereich ist Chip-Design und sichere Hardware. Dabei entwickeln wir effiziente Umsetzungen kryptographischer Verfahren, die je nach Anforderungen in der Leistungsaufnahme, im Durchsatz oder im Chipflächenbedarf optimiert sind. Aus diesen Aktivitäten entstand die Initiative PROACT, in der gefördert von NXP (vormals Philips) zusammen mit mehreren Instituten der TU Graz fakultätsübergreifend zu Radio Frequency Identification (RFID) Lehre angeboten und Forschung durchgeführt wird. In der sicheren Hardware wurde auch herausragende Kompetenz im Bereich so genannter Seitenkanalattacken sowie deren Gegenmaßnahmen erreicht. Es handelt sich dabei um Verfahren, bei denen über Messung des Verlaufs von

Stromverbrauch oder elektromagnetischer Abstrahlung Annahmen zu internen Verarbeitungen getroffen und damit Rückschlüsse auf die kryptographischen Schlüssel gezogen werden. Ähnlich wird untersucht, wie über bewusstes Induzieren von Fehlersituationen über die Umgebungsbedingungen, etwa über die Versorgungsspannung oder über gezielte Lichtblitze Chipkarten kompromittiert werden können.
In der Netzwerksicherheit beschäftigt sich das IAIK mit dem Erkennen von Angriffen auf Netzwerke oder Betriebssysteme über Wahrscheinlichkeitstheorie, mit Public-Key-Infrastrukturen (PKI) und deren Anwendungen wie in elektronischen Signaturen. Ein zunehmend an Bedeutung gewinnender Bereich ist Trusted Computing. Hier werden über — in aktuellen PCs oder Laptops bereits standardmäßig mitgelieferten low-cost Kryptokomponenten — gesicherte Systemzustände und Umgebungen möglich. Neben der Integration in Betriebssysteme stellen sich hier wissenschaftlich vor allem Fragen zu geeigneten Vertrauensinfrastrukturen.
Mit der Stiftungsprofessur von Prof. Vincent Rijmen konnte das IAIK seine Aktivitäten um die Forschung in der Kryptographie und der Kryptoanalyse erweitern. Die Schwerpunkte liegen in der Analyse von kryptographischen Hash-Funktionen, bei der die derzeit effizientesten Methoden zum Finden von Kollisionen bei SHA-1 an der TU Graz entwickelt wurden, und in der Analyse von effizienten Umsetzungen des von Prof. Rijmen zusammen mit Joan Daemen entwickelten Algorithmus Rijndael, der 2000 in einem mehrjährigen kompetitiven Verfahren vom amerikanischen National Institute of Standards and Technology (NIST) als Advanced Encryption Standard (AES) ausgewählt wurde.
Herausragende Ergebnisse des IAIK werden auch vermarktet: In der vom IAIK gegründeten gemeinnützigen Stiftung Secure Information and Communication Technologies (SIC) wird mit dem JCE Toolkit eine JAVA-Kryptographiebibliothek vertrieben; die Gewinne daraus fördern gänzlich Forschung und Lehre in der Informationssicherheit an der TU Graz.
Die Forschung am IAIK ist anwendungsorientiert und bemüht, Ergebnisse unmittelbar in konkrete Umsetzungen einfließen zu lassen. Dazu ist das IAIK in langfristigen Kooperationen, über die Wissenschaft direkt in die Anwenderbereiche und Benutzerkreise getragen worden: Das Zentrum für sichere Informationstechnologie — Austria (A-SIT) — ist ein Verein, in dem die TU Graz neben dem Bundesministerium für Finanzen und der Österreichischen Nationalbank seit 1999 Mitglied ist. A-SIT betreibt im Rahmen seiner Technologiebeobachtung Forschung an der TU Graz vor allem im Bereich der elektronischen Signatur, der Bürgerkarte und des E-Governments. Eine weitere Kooperation ist das E-Government Innovationszentrum (EGIZ), eine gemeinsame Initiative des Bundeskanzleramts und der TU Graz, in der Forschung zur Unterstützung der Vorreiterrolle Österreichs im E-Government betrieben wird. Ergebnisse daraus kommen seit kurzem Studierenden der TU Graz direkt zugute: In Zusammenarbeit mit dem Zentralen Informatikdienst (ZID) wurden der Zugang zu TUGonline über die Bürgerkarte und elektronisch signierte Studienerfolgsnachweise umgesetzt.

Webseiten

ENISA:	http://www.enisa.europa.eu
IAIK:	http://www.iaik.tugraz.at
PROACT:	http://proact.tugraz.at
A-SIT:	http://www.a-sit.at
EGIZ:	http://www.egiz.gv.at
Stiftung SIC:	http://sic.iaik.tugraz.at



Sichere Hardware: Die österreichische Bürgerkarte des ENISA Direktors (Photo: A-Trust)

A Beacon in Network- and Information-Security

In March 2007 Prof. Reinhard Posch, head of the Institute for Applied Information Processing and Communications (IAIK) has been elected Chairman of the Management Board of the European Network and Information Security Agency (ENISA). We see this responsible position as recognition of IAIK's scientific achievements. Therefore, this article briefly describes ENISA and then discusses information security research at TU Graz.
ENISA has been established in 2004 as one of EU's meanwhile 22 Community agencies. Installing an own agency of network and information security emphasizes the importance of this field in an information society. After an interim location in Brussels, ENISA moved to its seat in Heraklion, Crete, in August 2005. Meanwhile, ENISA is fully operational with about 40 person staff and a yearly budget of about € 8 million. ENISA's tasks are inter alia support of the EU institutions and the Member States, to enhance cooperation between different actors operating in the field, or to advise the Commission on research in the area of network and information security. The organizational structure consists of an Executive Director, an advising Permanent Stakeholder Group, and the Management Board – a body now chaired by Prof. Posch for two and a half years.
IAIK's research is directed towards information security. As this is already a broad field, we aim for achieving excellence in selected fields. We research on secure hardware design and side channel analysis where we achieved international reputation. Prof. Vincent Rijmen has established a renowned research group that works on cryptanalysis of hash functions and efficient implementations of block ciphers. Further fields are intrusion detection, public key cryptography and trusted computing. Research areas gaining increasing importance at IAIK are electronic signatures and E-Government. There we have long-term co-operations such as the Secure Information Technology Center Austria (A-SIT) inter alia carrying out research on the Austrian Citizen Card. A further important initiative is the E-Government Innovation Center, a joint effort of the Austrian Federal Chancellery and the Graz University of Technology the has been established to advance the Austrian leadership in E-Government by scientific research.