stiftung secure information and communication

Jahresbericht 2015

Zusammenfassender Bericht über die Aktivitäten der
Stiftung Secure Information and Communication Technologies SIC

Die *Stiftung Secure Information and Communication Technologies SIC* wurde vom Institut für Angewandte Informationsverarbeitung und Kommunikationstechnologie (IAIK) der Technischen Universität Graz (TU Graz) als gemeinnützige Stiftung gegründet und mit Bescheid der Stiftungsbehörde vom 5. Februar 2003 für zulässig erklärt. In diesem Jahresbericht werden die Aktivitäten der Stiftung im Geschäftsjahr 2015 dargestellt.

Inhaltsverzeichnis

Auskünfte

Stiftung Secure Information and Communication Technologies SIC
Inffeldgasse 16a
8010 Graz
Tel.: (0316) 873-5513 / 5521 Fax.: (0316) 873-5520

Impressum

Medieninhaber, Herausgeber und Verleger
Stiftung Secure Information and Communication Technologies SIC, Inffeldgasse 16a, 8010 Graz

Redaktion und für den Inhalt verantwortlich
Dipl.-Ing. Herbert Leitold, Dr. Peter Lipp *(Vorstand der Stiftung)* Graz, am 24/ Juni 2016

Executive Summary

Die **Stiftung Secure Information and Communication Technologies SIC** wurde im Februar 2003 gegründet und mit einem Stammvermögen von € 2.320.000 ausgestattet. Der Zweck der Stiftung ist „*die Förderung und eigenständige Durchführung von wissenschaftlicher Forschung und Entwicklung sowie der Lehre und des Wissenstransfers in den Bereichen Angewandte Informationsverarbeitung und Kommunikationstechnologie sowie Informationssicherheit*“. Satzungsgemäß kann dies durch „*…eigenständige Durchführung von Forschungsaufgaben und -projekten, Förderung anderer Einrichtungen, Personen und Institutionen, die zur Erreichung des Stiftungszweckes beitragen, Vergabe von Forschungsaufträgen, Vergabe von Beiträgen für wissenschaftliche Arbeiten, Durchführung von Veranstaltungen zur Bekanntmachung der Forschungsergebnisse, Publikation und Dokumentation der im Rahmen des Stiftungszwecks durchgeführten Forschungstätigkeiten*“ erfolgen.

Dieser Jahresbericht 2015 stellt die Leistungen der Stiftung nach dem Stiftungszweck im Zeitraum 1.1. – 31.12.2015 dar. Der Bericht behält die Struktur der bisherigen Berichte.

2015 konnte die Stiftung in allen Bereichen des Stiftungszwecks Beiträge leisten:

- Die Stiftungsprofessur „*Cloud Computing Security*“ – besetzt mit Prof. Mangard – wurde weiter mit Beteiligung an den Kosten der Professur und einer Assistentinnen-Stelle zu jeweils zwei Drittel finanziert.
  Besonders bemerkenswert ist, dass Prof. Mangard einen *ERC Consolidator Grant* mit etwa € 2 Mio. an die TU Graz holen konnte.

- Die Personalkosten der Vorlesung „*Kritische Informationsinfrastrukturen*“ an der TU Graz wurden finanziert.

- Vier Studierenden wurde für beste Ferial-, Bakkalaureats- und Master-Arbeiten ein Best@IAIK Award gestiftet.

- Die Stiftung hat sich im EU Projekt STORK 2.0 beteiligt. Es ist dies ein Large Scale Pilot zur Interoperabilität elektronischer Identität.

- Als weiteres EU Forschungsprojekt ist CREDENTIAL Ende 2015 gestartet.

- Der Hilfsbetrieb JCE Toolkit hat wiederum Gewinne erwirtschaftet, die dem gemeinnützigen Forschungsbereich zufließen.

1 Einleitung

Die „*Stiftung Secure Information and Communication Technologies SIC*“ – in diesem Bericht in Folge als „*die Stiftung*“ bezeichnet – wurde vom Institut für Angewandte Informationsverarbeitung und Kommunikationstechnologie (IAIK) der Technischen Universität Graz (TU Graz) im Jahr 2003 gegründet. Rechtliche Grundlage ist das *Steiermärkische Stiftungs- und Fondsgesetz, LGBl. Nr. 69/1988* – in Folge als *StSFG* abgekürzt. Mit Bescheid der Stiftungsbehörde vom 5. Februar 2003 wurde die Stiftung für zulässig erklärt. In diesem Jahresbericht wird die Tätigkeit der Stiftung im Jahr 2015 dargestellt. Es stellt dies auch den Bericht über die im Sinne des Stiftungszwecks erbrachten Leistungen gemäß StSFG § 14 (3) dar (Abschnitt 2 „Leistungen im Sinne des Stiftungszwecks“). In den Anhängen sind die weiteren nach StSFG § 14 (3) definierten Berichte an die Aufsichtsbehörde angefügt.

Entsprechend einem Beschluss des Kuratoriums vom 18. Mai 2016 ist dieser Bericht im Internet zu veröffentlichen (ohne Finanzdaten, Bilanz und Rechnungsabschluss).

In diesem einleitenden Abschnitt werden die Grundlagen der Stiftung zusammengefasst.

1.1 Stiftungszweck

Der gemeinnützige Stiftungszweck ist in Artikel III. der Satzung (aktuelle Version vom 7.11.2013) wie folgt definiert:

> *Zweck der Stiftung, die nicht auf Gewinn gerichtet ist, ist die Förderung und eigenständige Durchführung von wissenschaftlicher Forschung und Entwicklung sowie der Lehre und des Wissenstransfers in den Bereichen Angewandte Informationsverarbeitung und Kommunikationstechnologie sowie Informationssicherheit.*
>
> *Das Ziel der Stiftung ist die Erweiterung des menschlichen Wissens in den oben genannten Bereichen im Interesse der österreichischen Allgemeinheit.*

Die gesamte Satzung ist in der Willbriefsammlung des Steiermärkischen Landesarchivs unter LReg. Vertrag Nr. 5509 hinterlegt bzw. auch im Internet unter der Adresse http://sic.iaik.tugraz.at/sic/about_us/stiftung/satzung veröffentlicht.

1.2 Forschungsschwerpunkte

Die allgemeine Formulierung des Stiftungszwecks soll dem in der Informationsverarbeitung, der Kommunikationstechnologie und der Informationssicherheit immens schnelllebigen technologischen Fortschritt begegnen, wo einzelne Forschungsgebiete sich laufend wandeln, jedoch in der auf Dauer eingerichteten Stiftung auf lange Sicht ein entsprechend vitales Betätigungsfeld anzunehmen ist.

Um die Leistungen der Stiftung dennoch der aktuellen technologischen und wissenschaftlichen Situation angepasst gestalten zu können, wurden Schwerpunkte definiert.

Als aktuelle Forschungsschwerpunkte sind festgelegt:

- Sicherheitsaspekte der Informationsgesellschaft, insbesondere E-Commerce und E-Government
- Kryptographie und Kryptoanalyse
- Hardware- und Software-Umsetzung kryptographischer Verfahren
- Public Key Infrastrukturen und elektronische Signaturen

- Netzwerksicherheit
- Radio Frequency Identification – RFID
- Cloud Computing
- Beiträge zur Standardisierung in obgenannten Bereichen

Diese Forschungsschwerpunkte schließen andere im Rahmen des Stiftungszwecks rechtfertigbare Leistungen nicht aus, sondern geben eine grobe Richtlinie zu besonders förderungswürdigen Themen. Die Schwerpunkte sollen auch laufend an aktuelle Gegebenheiten angepasst werden.

1.3 Zur Lage der Stiftung

Seit Bestehen der Stiftung wurde über Forschungsförderungen, Zuwendungen, Kooperationen und Gewinne des Hilfsbetriebs Toolkit ein Vermögensstand aufgebaut, der über das gewidmete Stammkapital hinausgeht. Trotz seit längerem anhaltend geringen Zinsniveaus konnten die Leistungen vor allem über Rücklagen uneingeschränkt beibehalten werden. Es ist in absehbarer Zukunft nicht damit zu rechnen, dass für Leistungen auf das Stammvermögen zurückgegriffen werden wird müssen.

Die gemeinnützigen Leistungen kamen im Berichtszeitraum 2015 über die Stiftungsprofessur Cloud Computing, die Lehrveranstaltung kritische Informations-infrastrukturen, sowie Best Project Awards vor allem Studierenden der Technischen Universität Graz zugute und stärken damit Ausbildung im Wirkungsbereich der Stiftung.

Über die beiden Stiftungsprofessuren „*Kryptographie*“ und „*Cloud Computing Security*“ werden exzellente, international beachtete Forschungsleistungen in der Steiermark unterstützt.

Die Stiftung war im EU Large Scale Pilot „STORK 2.0“ engagiert, das 2015 abgeschlossen wurde. Mit „CREDENTIAL“ ist 2015 ein weiteres EU Forschungsprojekt gestartet.

Der Hilfsbetrieb „*JCE Toolkit*“ konnte einen Gewinn erwirtschaften, der gänzlich dem gemeinnützigen Stiftungszweck zufließt. Der Personalstand in der Stiftung ist gleich geblieben.

1.4 Hilfsbetrieb JCE Toolkit

Mit Übertragung des „*JCE Toolkit*“ durch das IAIK Ende 2003 besteht ein Hilfsbetrieb, über den die Stiftung Zuflüsse über die Erträgnisse aus dem pekuniären Stammvermögen bzw. aus der Veranlagung der Rücklagen hinausgehend erzielen kann.

Mit Bescheid der Finanzlandesdirektion aus 2003 wurde festgestellt, dass der Vertrieb des JCE Toolkit keine Begünstigung auf abgaberechtlichem Gebiet zukommt, jedoch die Begünstigung in den gemeinnützigen Bereichen weiterhin erhalten bleibt. Es wurde hier die Auflage erteilt, die Gewinne aus der kommerziellen Verwertung den gemeinnützigen Aktivitäten zuzuführen. Diese auch im Übertragungsvertrag des IAIK gegebene Maßgabe ist seit 2004 in der Satzung verankert.

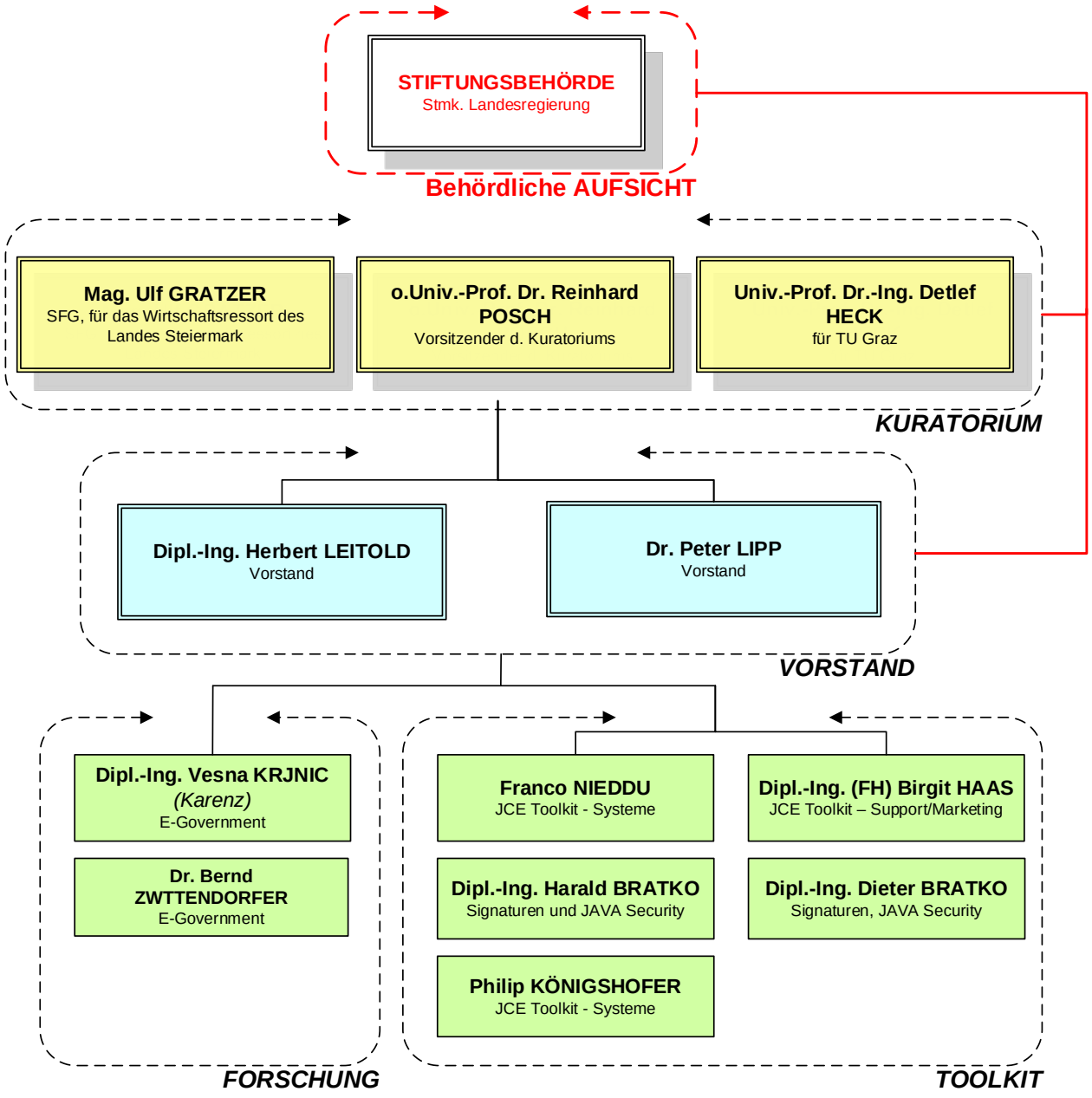
Die Abgrenzung zwischen gemeinnützigem und gewerblichem Bereich erfolgt über getrennte Kostenrechnung der Bereiche „Forschung“ (gemeinnützige Aktivitäten), „Toolkit“ (gewerblicher Hilfsbetrieb) und „Overheads“ (Gemeinkosten, die anteilig den Bereichen Toolkit und Forschung zugeordnet werden).

1.5 Stiftungsorgane und Organisationsstruktur

Die Organisationsstruktur der Stiftung teilt sich in drei Ebenen:

- Die Kontrollebene wird durch das Kuratorium und die staatliche Aufsicht gebildet.
  - Das Kuratorium besteht aus drei Personen. Im Geschäftsjahr 2015 waren dies:
    - Mag. Ulf Gratzer (für das Wirtschaftsressort des Landes Steiermark)
    - o.Univ.-Prof. Dr.techn. Dr.h.c. Harald Kainz (für die TU Graz, bis 30.9.2015)
    - Univ.-Prof. Dr.-Ing. Detlef Heck (für die TU Graz ab 1.10.2015)
    - o.Univ.-Prof. Dr. Reinhard Posch (Vorsitzender des Kuratoriums)
  - Staatliche Aufsicht ist die Stiftungsbehörde FA7C der Steiermärkischen Landesregierung
- Die Führungsebene bildet der Vorstand
  - Dipl.-Ing. Herbert Leitold
  - Dr. Peter Lipp
- Die operative Ebene wird durch zwei Säulen gebildet:
  - Der Bereich *Forschung* umfasst die mit eigenständiger Durchführung von Forschung und Entwicklung befassten MitarbeiterInnen der Stiftung.
  - Der Bereich *Toolkit* ist als Hilfsbetrieb vom gemeinnützigen Bereich *Forschung* abgegrenzt, unterstützt diesen jedoch über Gewinne und in der nicht-kommerziellen Forschung kostenlos verwendbare Werkzeuge.

Diese Struktur ist im folgenden Organigramm dargestellt. Dabei wird der Stand an Mitarbeiterinnen und Mitarbeitern der Stiftung per 31.12.2015 dargestellt. Administration und technische Infrastruktur wird gegen Kostenersatz vom IAIK der TU Graz gestellt.



Organigramm und Personalstand per 31.12.2015

2 Leistungen im Sinne des Stiftungszwecks

Über die Leistungen der Stiftung wird dem in der Satzung der Stiftung definierten Stiftungszweck entsprechend in „Förderung von Forschung und Lehre“ berichtet.

2.1 Förderung von Forschung und Lehre, Wissenstransfer

2.1.1 Stiftungsprofessur Informationssicherheit

Diese Stiftungsprofessur wurde 2004 eingerichtet und von der Stiftung durchgängig bis 2013 co-finanziert. Nach Wechsel von Prof. Vincent Rijmen 2012 nach Leuven wurde als Überbrückung bis zur Nachbesetzung eine mit Florian Mendel besetzte Gastprofessur unterstützt. Die Nachbesetzung erfolgte 2015 mit Prof. Christian Rechberger.

Die Stiftung bekennt sich weiter zu der von ihr 2004 initiierten Professur, und hat eine Finanzierungszusage einer AssistentInnenstelle abgegeben. Diese wurde allerdings 2015 noch nicht besetzt.

2.1.2 Stiftungsprofessur Cloud Computing Security

Eine Stiftungsprofessur *Cloud Computing* wurde mit November 2014 mit Prof. Stefan Mangard besetzt. Die Stiftung wird diese Professur auf drei Jahre zu 67% finanzieren sowie auf weitere drei Jahre zu 33%. Zusätzlich finanziert die Stiftung 67% einer Stelle eines/einer UniversitätsassistentIn auf sechs Jahre.

Als High-Light 2015 dieser Professur ist der Zuschlag eines ERC Consolidator Grants für das Projekt „Securing Software against Physical Attacks“ (SOPHIA) anzusehen. Diese mit etwa € 2 Mio. dotierte Forschungsförderung erstreckt sich über fünf Jahre. Mit dem Anstoß der Professur durch die Förderung der Stiftung ist damit ein wesentlicher Impuls zur Forschung in der Informationssicherheit in der Steiermark gelungen.

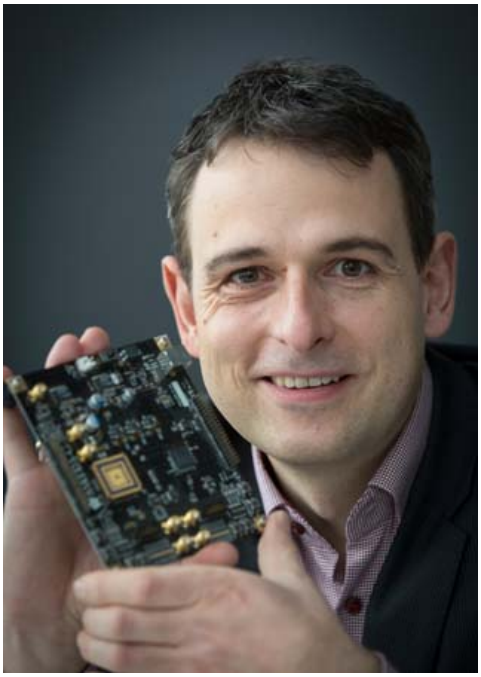


Bild © Lunghammer - TU Graz

Darüber hinaus konnte die Gruppe um Prof. Mangard 2015 wieder an teils erstklassigen Konferenzen und Journalen veröffentlichen:

1. Christoph Erwin Dobraunig, Maria Eichlseder, Florian Mendel, Martin Schläffer - "Cryptanalysis of Ascon" - Topics in Cryptology - CT-RSA 2015

2. Hannes Groß - "Sharing is Caring–On the Protection of Arithmetic Logic Units against Passive Physical Attacks" - Workshop on RFID Security - RFIDsec 2015, 11th Workshop, New York, USA, June 22 - 23, 2014, Proceedings.

3. Daniel Gruß, David Bidner, Stefan Mangard - "Practical Memory Deduplication Attacks in Sandboxed Javascript"

4. Christoph Erwin Dobraunig, Maria Eichlseder, Florian Mendel - "Higher-Order Cryptanalysis of LowMC" - Information Security and Cryptology - ICISC 2015

5. Christoph Erwin Dobraunig, Maria Eichlseder, Florian Mendel - "Analysis of SHA-512/224 and SHA-512/256" - Advances in Cryptology - ASIACRYPT 2015

6. Christoph Erwin Dobraunig, Maria Eichlseder, Florian Mendel - "Forgery Attacks on round-reduced ICEPOLE-128" - Selected Areas in Cryptography

7. Christoph Erwin Dobraunig, Maria Eichlseder, Florian Mendel - "Heuristic Tool for Linear Cryptanalysis with Applications to CAESAR Candidates" - Advances in Cryptology - ASIACRYPT 2015

8. Daniel Gruß, Raphael Spreitzer, Stefan Mangard - "Cache Template Attacks: Automating Attacks on Inclusive Last-Level Caches" - 24th USENIX Security Symposium, Washington, D.C., USA, August 12-14, 2015

9. Christoph Erwin Dobraunig, Francois Koeune, Stefan Mangard, Florian Mendel, Francois-Xavier Standaert - "Towards Fresh and Hybrid Re-Keying Schemes with Beyond Birthday Security" - CARDIS

10. Christoph Erwin Dobraunig, Maria Eichlseder, Florian Mendel - "Related-Key Forgeries for Proest-OTR" - Fast Software Encryption

11. Hannes Groß, Erich Wenger, Christoph Erwin Dobraunig, Christoph Ehrenhöfer - "Suit up! Made-to-Measure Hardware Implementations of ASCON" - 18th Euromicro Conference on Digital Systems Design

12. Michael Muehlberghuber, Thomas Korak, Michael Hutter, Philipp Dunst - "Towards Evaluating DPA Countermeasures for Keccak on a Real ASIC" - , The sixth International Workshop on Constructive Side-Channel Analysis and Secure Design

13. 2015 Hannes Groß, Marko Hölbl, Daniel Slamanig, Raphael Spreitzer - "Privacy-Aware Authentication in the Internet of Things" - 14th International Conference on Cryptology and Network Security (CANS 2015) 10-12 December 2015, Marrakesh, Morocco. (Full version Cryptology ePrint Archive Report 2015/1110)

14. Mario Lamberger, Florian Mendel, Christian Rechberger, Vincent Rijmen, Martin Schläffer - "The Rebound Attack and Subspace Distinguishers: Application to Whirlpool" - Journal of cryptology (Volume: 28)

In der Lehre wurden von der Gruppe unter anderem die Vorlesungen „*Einführung in die Informationssicherheit*“, „*Applied Cryptography*“ und „*Applied Cryptography 2*“, „*IT Security*“, „*System on Chip*“ und „*VLSI Design*“ betreut. Das Angebot wird mit Seminaren, Bakkalaureats- und Master-Arbeiten, sowie Dissertationsbetreuungen ergänzt.

Die von der Stiftung mit-finanzierte Professur ist also Quelle erstklassischer Forschung im Bereich der Kryptographie und Informationssicherheit. Es hat sich daraus eine Gruppe an Forschern in der Steiermark etabliert, die internationales Ansehen genießt.

2.1.3 Best Project Awards

Die Prämierung ausgezeichneter studentischer Leistungen wurde 2008 begonnen und seither jährlich fortgeführt. 2015 wurden Preise an vier Studierende der TU Graz vergeben:

1. Beste Ferialarbeit: Patrick Klampfl für die Arbeit „Implementation, Optimisation, and Evaluation of a Soft-Error Analysis Tool “

2. Beste Bakkalaureats-Arbeit: David Bidner für die Arbeit „Timing Attacks on Memory Deduplication“

3. Beste Bakkalaureats-Arbeit: Dominik Wieser für die Arbeit „Electronic Signatures Integrated Into Google Docs“

4. Beste Masterarbeit: Johannes Feichtner für die Arbeit „Crypto-Slice: Static Analysis of Cryptography in Android Applications“

Die prämierten Studierenden erhielten jeweils moderne Streaming-Lautsprecher.

Bild © Florian Reimair

2.1.4 STORK 2.0

Die Stiftung nahm am EU Projekt STORK 2.0 teil. Es war dies ein von der Europäischen Kommission geförderter Large Scale Pilot zur Interoperabilität elektronischer Identität. Die Teilnahme der Stiftung erfolgte über eine Arbeitsgemeinschaft „ARGE STORK.AT“ zusammen mit dem Bundeskanzleramt, dem Bundesministerium für Gesundheit, der TU Graz, der ELGA GmbH und A-SIT. 2015 wurde das Projekt erfolgreich abgeschlossen, wobei die Beteiligung der Stiftung 2015 nur mehr gering war, die wesentlichen Beiträge der Stiftung konnten bereits davor abgeschlossen werden.

2.1.5 CREDENTIAL

Als EU Forschungsprojekt mit Beteiligung der Stiftung ist im Oktober 2015 das Projekt Secure Cloud Identity Wallet „CREDENTAL“ gestartet. Ziel dieses ambitionierten Projekts mit zwölf Partnern in sieben Ländern ist es, Lösungen zu sicherer Identität in Cloud-Umgebungen über fortgeschrittene kryptographische Protokolle zu erforschen.

2.1.6 Vorlesung Kritische Informationsinfrastrukturen

Die Vorlesung über kritische Informationsinfrastrukturen an der TU Graz wurde von der Stiftung zum neuten Mal finanziert. Die Vorlesung wurde wieder von Dr. Otto Hellwig gehalten.

2.1.7 E-Government

MitarbeiterInnen des Bereichs Forschung der Stiftung unterstützen das E-Government Innovationszentrum (EGIZ). EGIZ ist eine Initiative des Bundeskanzleramts und der TU Graz zur wissenschaftlichen Weiterentwicklung des E-Government in Österreich. Experten der Stiftung werden zu Projekten beigezogen.

2.1.8 Eigene Forschungsleistungen

Mitarbeiter der Stiftung haben eigenständige Forschung im Bereich elektronischer Identität und Signaturen fortgesetzt.

2.2 Organisatorisches und Sonstiges

In diesem Abschnitt werden Aktivitäten berichtet, die zwar nicht in ursächlichem Zusammenhang mit dem gemeinnützigen Stiftungszweck stehen, jedoch als Hilfsbetrieb den gemeinnützigen Bereich fördern, oder als administrative und organisatorische Infrastruktur erforderlich sind, um die Stiftungsaktivitäten effizient durchzuführen.

2.2.1 Technische Infrastruktur

Die technische Infrastruktur der Stiftung wurde weiterhin vor allem vom IAIK der TU Graz getragen. Darüber hinausgehend wurde keine Infrastruktur angeschafft, da hier die qualitativ hochwertigen Ressourcen des IAIK die Anschaffung eigener teurer Anlagen nicht rechtfertigt. Die Nutzung der Infrastruktur wird an das IAIK abgegolten.

2.2.2 Entwicklungsaktivitäten JCE Toolkit

Die Umsatzerlöse aus dem Verkauf des JCE Toolkits im Hilfsbetrieb waren 2015 sehr gut. Dies wurde über Aufträge im ETSI Standardisierungsmandat zu elektronischen Signaturen ergänzt.