stiftung secure information and communication

Jahresbericht 2017

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 2017 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 4. Juni 2018

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 2017 stellt die Leistungen der Stiftung nach dem Stiftungszweck im Zeitraum 1.1. – 31.12.2017 dar. Der Bericht behält die Struktur der bisherigen Berichte.

2017 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 zu einem Drittel und einer Assistentinnen-Stelle zu zwei Drittel finanziert.
- Zur Professur „*Kryptographie*" von Prof. Christian Rechberger wurde ab Mitte 2017 eine Assistentinnenstelle zu zwei Drittel finanziert.
- Sechs Studierende wurden mit einem Research Excellence Award ausgezeichnet.
- Die Stiftung hat zum EU Forschungsprojekt CREDENTIAL beigetragen.
- 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 2017 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 23. Mai 2018 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 2017 über die Stiftungsprofessur Cloud Computing, die Stiftungsprofessur Kryptographie, sowie Research Excellence 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 Projekt „CREDENTIAL“ engagiert, womit sie auch in internationalen Forschungsaktivitäten verankert ist.

Der Hilfsbetrieb „*JCE Toolkit*“ konnte einen Gewinn erwirtschaften, der gänzlich dem gemeinnützigen Stiftungszweck zufließt. Der Personalstand in der Stiftung ist um eine Person gestiegen.

Es bestehen also Reserven, um die Leistungen der Stiftung weiterhin auf hohem Niveau halten zu können.

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.

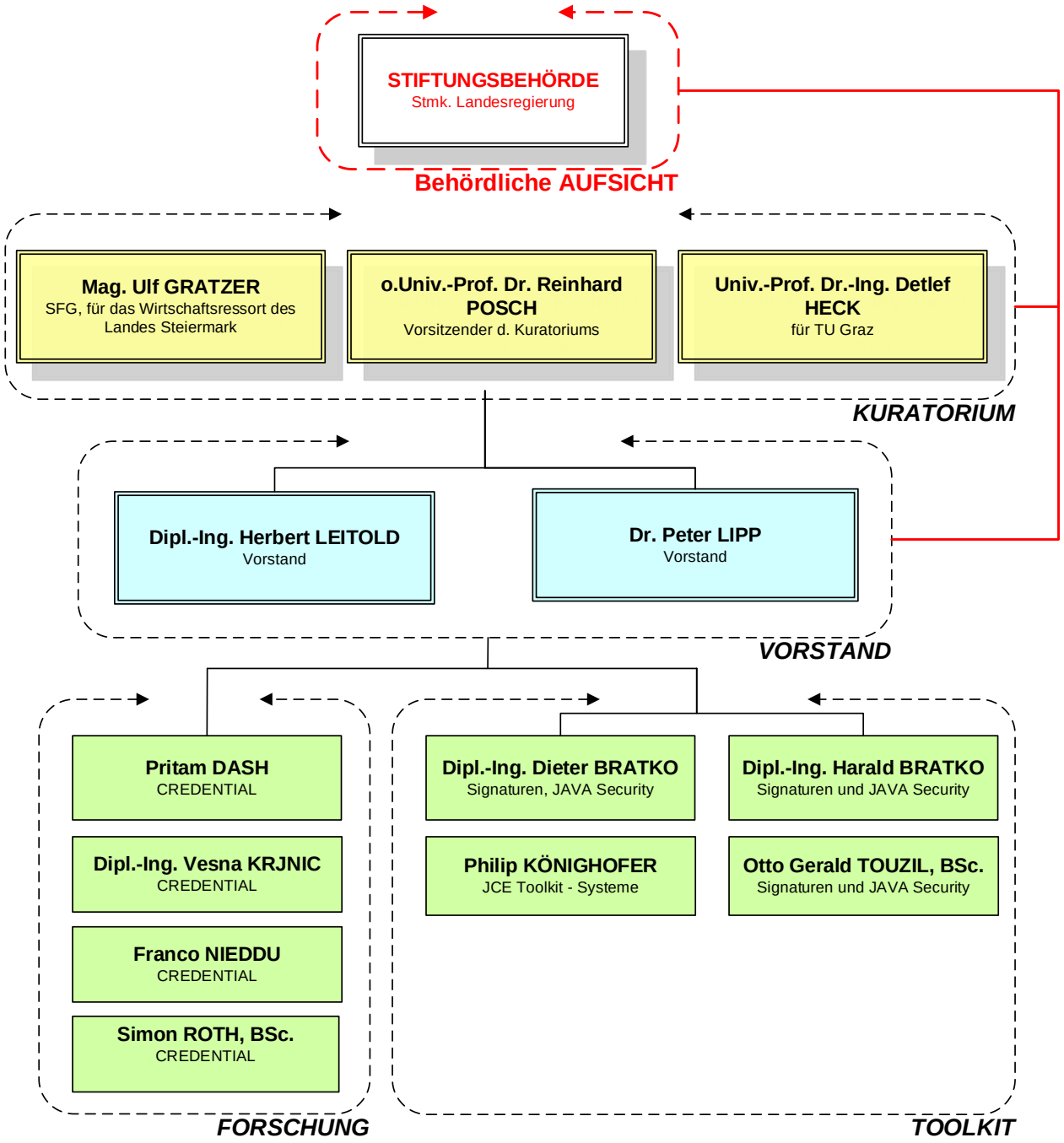
Die Abgrenzung zwischen gemeinnützigem und gewerblichem Bereich erfolgt über getrennte Kostenrechnung der Bereiche „Forschung“ (gemeinnützige Aktivitäten), „Toolkit“ (gewerblicher Hilfsbetrieb) und „Overheads“ (Gemeinkosten, die anteilig den Bereichen Toolkit und Forschung zugeordnet werden).

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 2017 waren dies:
    - Mag. Ulf Gratzer (für das Wirtschaftsressort des Landes Steiermark)
    - Univ.-Prof. Dr.-Ing. Detlef Heck (für die TU Graz)
    - 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 31.12.2017 dargestellt. Administration und technische Infrastruktur wird gegen Kostenersatz vom IAIK der TU Graz gestellt.



Organigramm und Personalstand per 31.12.2017

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 Kryptographie

Diese Stiftungsprofessur wurde 2004 eingerichtet und von der Stiftung durchgängig co-finanziert. Nach Wechsel von Prof. Vincent Rijmen 2012 nach Leuven wurde als Überbrückung eine Gastprofessur von Florian Mendel finanziert. Seit 2016 ist die Professur mit Prof. Christian Rechberger besetzt. Die Stiftung hat eine vorgezogene Bestellung 2016 mit einer Überbrückungsfinanzierung unterstützt.

Die Stiftung bekennt sich weiter zu der von ihr 2004 initiierten Professur, es besteht die Finanzierungszusage einer AssistentInnenstelle. Diese wurde Mitte 2017 besetzt.

Die Gruppe um Prof. Rechberger konnte 2017 ihre Ergebnisse an namhaften und auch erstklassigen wissenschaftlichen Tagungen und Journalen veröffentlichen:

1. A new structural-differential property of 5-round AES; Grassi, L., Rechberger, C. & Rønjom, EUROCRYPT 2017

2. Chameleon-Hashes with Ephemeral Trapdoors and Applications to Invisible Sanitizable Signatures; Camenisch, J., Derler, D., Krenn, S., Pöhls, H., Samelin, K. & Slamanig, D., PKC 2017

3. Collisions and Semi-Free-Start Collisions for Round-Reduced RIPEMD-160; Liu, F., Mendel, F. & Wang, G., ASIACRYPT 2017

4. Cryptanalysis of Simpira v1; Eichlseder, M., Dobraunig, C. E. & Mendel, F., Selected Areas in Cryptography - SAC 2016

5. Homomorphic Proxy Re-Authenticators and Applications to Verifiable Multi-User Data Aggregation; Derler, D., Ramacher, S. & Slamanig, D. Financial Cryptography and Data Security - 21st International Conference, FC 2017

6. Impossible-Differential and Boomerang Cryptanalysis of Round-Reduced Kiasu-BC; Dobraunig, C. E. & List, E., CT-RSA 2017

7. ISAP - Towards Side-Channel Secure Authenticated Encryption; Dobraunig, C. E., Eichlseder, M., Mangard, S., Mendel, F. & Unterluggauer, T., IACR Transactions on Symmetric Cryptology. 2017

8. Post-Quantum Zero-Knowledge and Signatures from Symmetric-Key Primitives; Chase, M., Derler, D., Goldfeder, S., Orlandi, C., Ramacher, S., Rechberger, C., Slamanig, D. & Zaverucha, G.; ACM SIGSAC 2017

9. Practical Strongly Invisible and Strongly Accountable Sanitizable Signatures; Beck, M. T., Camenisch, J., Derler, D., Krenn, S., Pöhls, H. C., Samelin, K. & Slamanig, D., ACISP 2017

10. To BLISS-B or not to be - Attacking strongSwan's Implementation of Post-Quantum Signatures; Peßl, P., Groot Bruinderink, L. & Yarom, Y., CCS 2017

In der Lehre wurden von der Gruppe unter anderem die Vorlesungen „*IT Security*“, „*Applied Cryptography*“, „*Applied Cryptography 2*“ und „*Modern Public Key Cryptography*“ gehalten, wie auch Seminare, Bakkalaureats- und Master-Arbeiten, sowie Dissertationen betreut werden.

2.1.2 Stiftungsprofessur Cloud Computing Security

Die Stiftungsprofessur *Cloud Computing* wurde mit November 2014 mit Prof. Stefan Mangard besetzt. Die Stiftung hat diese Professur auf drei Jahre bis November 2016 zu 67% finanziert, sowie wird diese auf weitere drei Jahre zu 33% finanzieren. Zusätzlich übernimmt die Stiftung 67% der Stelle einer Universitätsassistentin auf sechs Jahre.

Darüber hinaus konnte die Gruppe um Prof. Mangard 2017 wieder an teils erstklassigen Konferenzen und Journalen veröffentlichen:

1. An Efficient Side-Channel Protected AES Implementation with Arbitrary Protection Order; Groß, H., Mangard, S. & Korak, T., CT-RSA 2017

2. An IoT Endpoint System-on-Chip for Secure and Energy-Efficient Near-Sensor Analytics; Conti, F., Schilling, R., Schiavone, P. D., Pullini, A., Rossi, D., Gürkaynak, F. K., Mühlberghuber, M., Gautschi, M., Loi, I., Haugou, G., Mangard, S. & Benini, L., IEEE Transactions on Circuits and Systems 2017

3. Automated Detection, Exploitation, and Elimination of Double-Fetch Bugs using Modern CPU Features; Schwarz, M., Gruss, D., Lipp, M., Maurice, C., Schuster, T., Fogh, A. & Mangard, S., arXiv.org e-Print archive 2017

4. Dependable Internet of Things for Networked Cars; Großwindhager, B., Rupp, A., Tappler, M., Tranninger, M., Weiser, S., Aichernig, B., Boano, C. A., Horn, M., Kubin, G., Mangard, S., Steinberger, M. & Römer, K. U.m International Journal of Computing 2017

5. Higher-Order Side-Channel Protected Implementations of KECCAK; Groß, H., Schaffenrath, D. & Mangard, S., DSD 2017

6. KASLR is Dead: Long Live KASLR; Gruss, D., Lipp, M., Schwarz, M., Fellner, R., Maurice, C. & Mangard, S., ESSoS 2017

7. Malware guard extension: Using SGX to conceal cache attacks; Schwarz, M., Weiser, S., Gruss, D., Maurice, C. & Mangard, S., DIMVA 2017

8. Multi-core Data Analytics SoC with a flexible 1.76 Gbit/s AES-XTS Cryptographic Accelerator in 65 nm CMOS; Gürkaynak, F. K., Schilling, R., Mühlberghuber, M., Conti, F., Mangard, S. & Benini, L., CS2 '17

9. Practical Keystroke Timing Attacks in Sandboxed JavaScript; Lipp, M., Gruss, D., Schwarz, M., Bidner, D., Maurice, C. & Mangard, S., ESORICS 2017

10. Reconciling d+1 Masking in Hardware and Software; Groß, H. & Mangard, S., CHES 2017

11. Securing Memory Encryption and Authentication Against Side-Channel Attacks Using Unprotected Primitives; Unterluggauer, T., Werner, M. & Mangard, S., ASIACCS'17

12. SGXIO: Generic Trusted I/O Path for Intel SGX; Weiser, S. & Werner, M., Seventh ACM Conference on Data and Application Security and Privacy 2017

13. Side-Channel Plaintext-Recovery Attacks on Leakage-Resilient Encryption; Unterluggauer, T., Werner, M. & Mangard, S., DATE 2017

14. Single-Trace Side-Channel Attacks on Masked Lattice-Based Encryption; Primas, R., Peßl, P. & Mangard, S., CHES 2017

15. Strong and Efficient Cache Side-Channel Protection using Hardware Transactional Memory; Gruss, D., Lettner, J., Schuster, F., Ohrimenko, O., Haller, I. & Costa, M., 26th USENIX Security Symposium 2017

16. Transparent Memory Encryption and Authentication; Werner, M., Unterluggauer, T. & Mangard, S., FPL 2017

In der Lehre wurden von der Gruppe unter anderem die Vorlesungen „*Introduction to Information Security*“, „*IT Security*“, „*Digital System Design*“, „*Embedded Security*“ und „*System on Chip*“ betreut. Das Angebot wird mit Seminaren, Bakkalaureats- und Master-Arbeiten, sowie Dissertationsbetreuungen ergänzt.

Die beiden von der Stiftung mit-finanzierten Professuren „Cloud Computing Security“ und „Kryptographie“ sind also Quelle erstklassiger Forschung im Bereich der Kryptographie und Informationssicherheit. Es hat sich daraus eine Gruppe an Forschern in der Steiermark etabliert, die internationales Ansehen genießt.

2.1.2 Research Excellence Awards

Die Prämierung ausgezeichneter studentischer Leistungen wurde 2008 begonnen und seither jährlich fortgeführt. 2017 wurden Preise an sechs Studierende der TU Graz vergeben, die bereits im Zuge ihrer studentischen Tätigkeiten Ergebnisse wissenschaftlich veröffentlichen konnten. Es waren dies:

- Lukas Alber für „Towards Cross-Domain eID by using Agile Mobile Authentication“
- David Bidner für „Practical Keystroke Timing Attacks in Sandboxed JavaScript“
- Richard Fellner für „KASLR is Dead: Long Live KASLR “
- Lukas Giner für „Hello from the Other Side: SSH over Robust Cache Covert Channels in the Cloud “
- Robert Primas für „Single-Trace Side-Channel Attacks on Masked Lattice-Based Encryption “
- Davis Schaffenrath für „Higher-Order Side-Channel Protected Implementations of KECCAK “

Die prämierten Studierenden erhielten jeweils moderne Streaming-Lautsprecher.

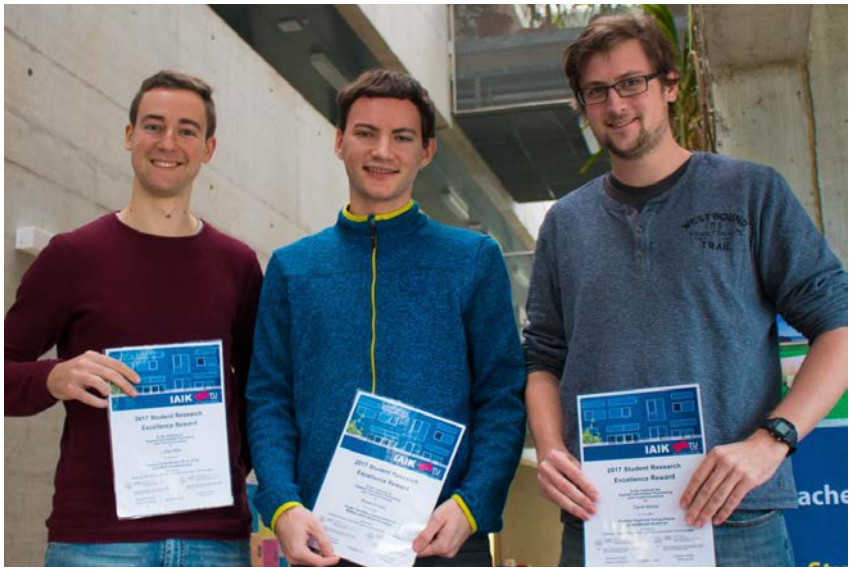


Bild © Karl Christian Posch

2.1.3 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.

2.1.4 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.

2.1.5 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 hinaus gehend 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 2017 sehr gut. Dies wurde über Aufträge im ETSI Standardisierungsmandat zu elektronischen Signaturen ergänzt.