stiftung secure information and communication

Jahresbericht 2016

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 2016 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 04/ Mai 2017

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 2016 stellt die Leistungen der Stiftung nach dem Stiftungszweck im Zeitraum 1.1. – 31.12.2016 dar. Der Bericht behält die Struktur der bisherigen Berichte.

2016 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.
- Eine Überbrückungsfinanzierung der Professur „*Kryptographie*“ erlaubte deren frühere Besetzung mit Prof. Christian Rechberger. Die Finanzierung einer AssistentInnenstelle wurde zugesagt, allerdings erst 2017 ausgeschrieben.
- Die Personalkosten der Vorlesung „*Kritische Informationsinfrastrukturen*“ an der TU Graz wurden finanziert.
- Sieben 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 2016 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 3. Mai 2017 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 2016 über die Stiftungsprofessur Cloud Computing, die Stiftungsprofessur Kryptographie, die Lehrveranstaltung kritische Informationsinfrastrukturen, 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 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.

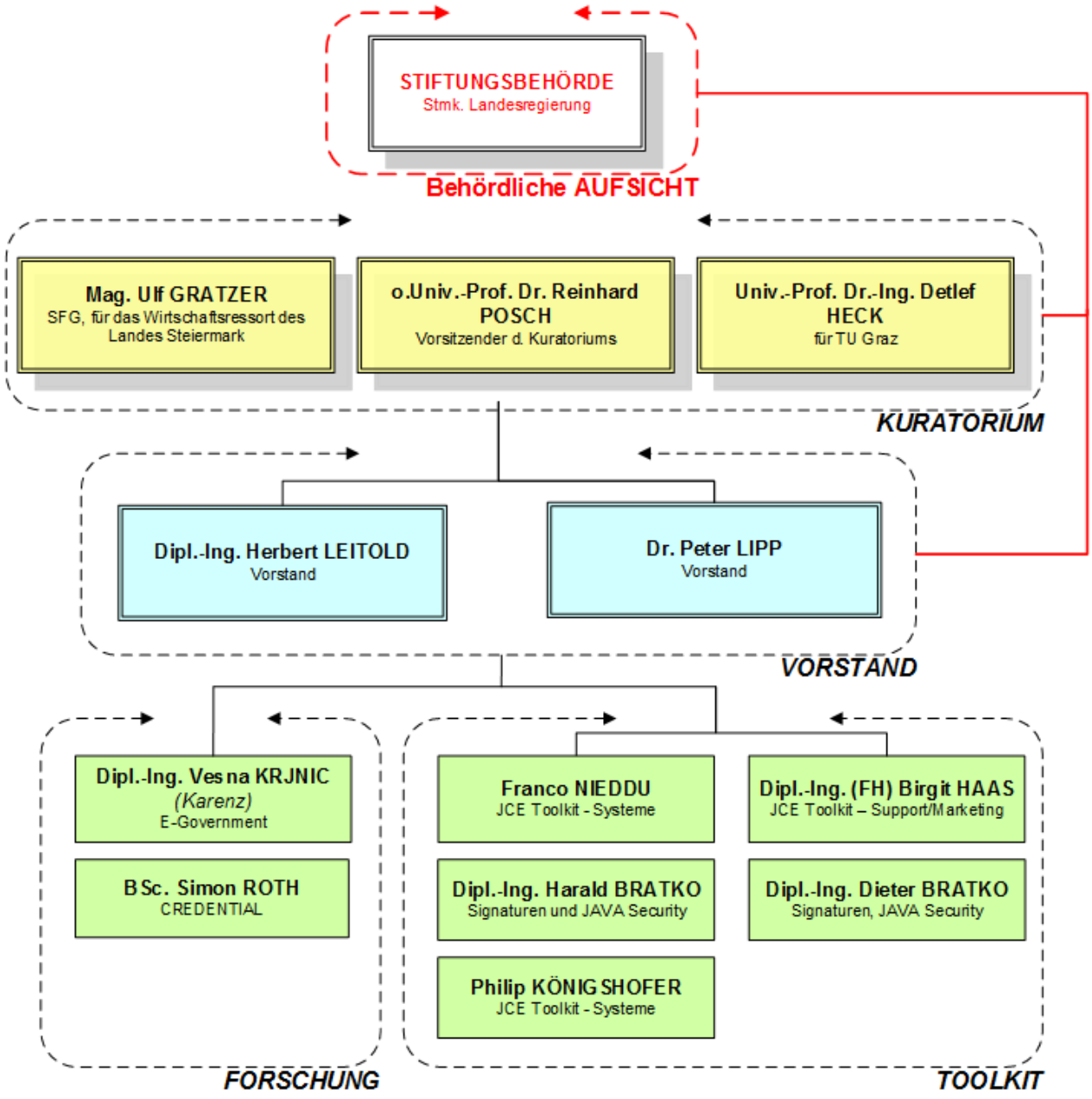
Die Abgrenzung zwischen gemeinnützigem und gewerblichem Bereich erfolgt über getrennte Kostenrechnung der Bereiche „Forschung“ (gemeinnützige Aktivitäten), „Toolkit“ (gewerblicher Hilfsbetrieb) und „Overheads“ (Gemeinkosten, die anteilig den Bereichen Toolkit und Forschung zugeordnet werden).

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 2016 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 31.12.2016 dargestellt. Administration und technische Infrastruktur wird gegen Kostenersatz vom IAIK der TU Graz gestellt.



Organigramm und Personalstand per 31.12.2016

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 2015 ist die Professur mit Prof. Christian Rechberger besetzt. Die Stiftung hat eine vorgezogene Bestellung 2015 mit einer Überbrückungsfinanzierung unterstützt.

Die Stiftung bekennt sich weiter zu der von ihr 2004 initiierten Professur, es besteht die Finanzierungszusage einer AssistentInnenstelle. Diese wurde allerdings noch nicht besetzt, eine Ausschreibung ist Anfang 2017 erfolgt.

Die Gruppe um Prof. Rechberger konnte 2016 ihre Ergebnisse an namhaften und auch erstklassigen wissenschaftlichen Tagungen und Journalen veröffentlichen:

1. Signer-Anonymous Designated-Verifier Redactable Signatures for Cloud-Based Data Sharing; Derler, D., Krenn, S. & Slamanig, D.; CANS 2016

2. Signatures for Privacy, Trust and Accountability in the Cloud: Applications and Requirements; Alaqra, A., Fischer-Hübner, S., Groß, T., Lorünser, T. & Slamanig, D.; 10th International IFIP Summer School on Privacy and Identity Management

3. Towards Authenticity and Privacy Preserving Accountable Workflows; Derler, D., Hanser, C., Pöhls, H. C. & Slamanig, D.; 10th International IFIP Summer School on Privacy and Identity Management

4. A New Architecture for Developing Cryptographic Cloud Services; Lorünser, T., Slamanig, D., Länger, T. & Pöhls, H. C.; ERCIM news

5. Practical Round-Optimal Blind Signatures in the Standard Model from Weaker Assumptions; Fuchsbauer, G., Hanser, C., Kamath, C. & Slamanig, D.; 10th Conference on Security and Cryptography for Networks

6. Analysis of the Kupyna-256 Hash Function; Dobraunig, C. E., Eichlseder, M. & Mendel, F.; Fast Software Encryption 2016

7. Cryptanalysis of Reduced NORX; Bagheri, N., Huang, T., Jia, K., Mendel, F. & Sasaki; Fast Software Encryption 2016

8. Cryptanalysis of Simpira; Eichlseder, M., Dobraunig, C. E. & Mendel, F.; Selected Areas in Cryptography

9. Haraka v2 - Efficient Short-Input Hashing for Post-Quantum Applications; Kölbl, S., Lauridsen, M., Mendel, F. & Rechberger, C.; IACR Transactions on Symmetric Cryptology, 2016

10. Improved Rebound Attacks on AESQ: Core Permutation of CAESAR Candidate PAEQ; Bagheri, N., Mendel, F. & Sasaki, Y.; ACISP 2016

11. Linking-Based Revocation for Group Signatures: A Pragmatic Approach for Efficient Revocation Checks; Slamanig, D., Spreitzer, R. & Unterluggauer, T.; Mycrypt 2016

12. MiMC: Efficient Encryption and Cryptographic Hashing with Minimal Multiplicative Complexity; Albrecht, M. R., Grassi, L., Rechberger, C., Roy, A. & Tiessen, T.; Advances in Cryptology - ASIACRYPT 2016

13. MPC-Friendly Symmetric Key Primitives; Grassi, L., Rechberger, C., Rotaru, D., Scholl, P. & Smart, N. P. Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security

14. Non-Interactive Plaintext (In-)Equality Proofs and Group Signatures with Verifiable Controllable Linkability; Blazy, O., Derler, D., Slamanig, D. & Spreitzer, R. 2016 Topics in Cryptology - CT-RSA 2016

15. Practical Key Recovery Attack on MANTIS-5; Dobraunig, C. E., Eichlseder, M., Kales, D. & Mendel, F. 2016 In : IACR Transactions on Symmetric Cryptology

16. Practical Low Data-Complexity Subspace-Trail Cryptanalysis of Round-Reduced PRINCE; Grassi, L. & Rechberger, C.; Progress in Cryptology – INDOCRYPT 2016

17. Square Attack on 7-Round Kiasu-BC; Dobraunig, C. E., Eichlseder, M. & Mendel, F.; ACNS 2016

18. Statistical Fault Attacks on Nonce-Based Authenticated Encryption Schemes; Dobraunig, C. E., Eichlseder, M., Korak, T., Lomné, V. & Mendel, F. Advances in Cryptology - ASIACRYPT 2016

19. Subspace Trail Cryptanalysis and its Applications to AES; Grassi, L., Rechberger, C. & Rønjom, S. 2016 FSE 2017

In der Lehre wurden von der Gruppe unter anderem die Vorlesungen „*IT Sicherheit*“, „*Cryptography*“, „*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 2016 wieder an teils erstklassigen Konferenzen und Journalen veröffentlichen:

1. Concealing Secrets in Embedded Processors Designs; Groß, H., Jelinek, M., Mangard, S., Unterluggauer, T. & Werner, M.; 15th Smart Card Research and Advanced Application Conference - CARDIS 2016

2. 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 Cryptography and Security in Computing Systems

3. Ascon hardware implementations and side-channel evaluation; Groß, H., Wenger, E., Dobraunig, C. E. & Ehrenhöfer, C.; Microprocessors and microsystems (Accepted, in press)

4. Analyzing the Shuffling Side-Channel Countermeasure for Lattice-Based Signatures; Peßl, P.; Progress in Cryptology – INDOCRYPT 2016

5. Domain-Oriented Masking: Compact Masked Hardware Implementations with Arbitrary Protection Order; Groß, H., Mangard, S. & Korak, T.; ACM Workshop on Theory of Implementation Security 2016

6. Prefetch Side-Channel Attacks: Bypassing SMAP and kernel ASLR; Gruss, D., Maurice, C., Fogh, A., Lipp, M. & Mangard, S.; CCS 2016

7. Microarchitectural Incontinence: You would leak too if you were so fast!; Gruß, D.; 13th Hacktivity conference 2016

8. Using Undocumented CPU Behavior to See into Kernel Mode and Break KASLR in the Process; Fogh, A. & Gruß, D.; BlackHat USA 2016

9. Exploiting Data-Usage Statistics for Website Fingerprinting Attacks on Android; Spreitzer, R., Griesmayr, S., Korak, T. & Mangard, S.; ACM Conference on Security and Privacy in Wireless and Mobile Networks (WiSec 2016)

10. Rowhammer.js: A Remote Software-Induced Fault Attack in JavaScript Gruss, D., Maurice, C. & Mangard, S.; Detection of Intrusions and Malware, and Vulnerability Assessment (DIMVA) 2016

11. Cache Side-Channel Attacks and the case of Rowhammer; Gruß, D.; RuhrSec

12. Protecting the Control Flow of Embedded Processors against Fault Attacks; Werner, M., Wenger, E. & Mangard, S.; 14th International Conference CARDIS

13. ARMageddon: How Your Smartphone CPU breaks software-level Security and Privacy; Lipp, M. & Maurice, C. L. N.; Black Hat Europe 2016

14. ARMageddon: Last-Level Cache Attacks on Mobile Devices; Lipp, M., Gruss, D., Spreitzer, R., Maurice, C. & Mangard, S.; 25th USENIX Security Symposium

15. DRAMA: Exploiting DRAM Addressing for Cross-CPU Attacks; Peßl, P., Gruß, D., Maurice, C. L. N., Schwarz, M. & Mangard, S.; 25th USENIX Security Symposium

16. Enhancing Side-Channel Analysis of Binary-Field Multiplication with Bit Reliability; Peßl, P. & Mangard, S.; Topics in Cryptology - CT-RSA 2016

17. Exploiting the Physical Disparity: Side-Channel Attacks on Memory Encryption; Unterluggauer, T. & Mangard, S.; Constructive Side-Channel Analysis and Secure Design - COSADE 2016

18. Flush+Flush: A fast and stealthy cache attack; Gruss, D., Maurice, C., Wagner, K. & Mangard, S.; 13th International Conference, DIMVA 2016

19. What could possibly go wrong with <insert x86 instruction here>?; Maurice, C. L. N. & Lipp, M.; 33. Chaos Communication Congress

In der Lehre wurden von der Gruppe unter anderem die Vorlesungen „*Einführung in die Informationssicherheit*“, „*IT Security*“, „*Digital System Design*“, „*Embedded Security*“; „*System on Chip*“ und „*VLSI Design*“ 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. 2016 wurden Preise an sieben Studierende der TU Graz vergeben, die bereits im Zuge ihrer studentischen Tätigkeiten Ergebnisse wissenschaftlich veröffentlichen konnten. Es waren dies:

- Christian Ertler für „Applied Dynamic Policy Selection“
- Manuel Jelinek für „Concealing Secrets in Embedded Processors Designs“
- Daniel Kales für „Practical Key Recovery Attack on MANTIS-5“
- Christian Kollmann für „Emulating U2F authenticator devices“
- Moritz Lipp für „ARMageddon: Cache Attacks on Mobile Devices“
- Michael Schwarz für „DRAMA: Exploiting DRAM Addressing for Cross-CPU Attacks“
- Klaus Wagner für „Flush+Flush: A Fast and Stealthy Cache Attack“

Die prämierten Studierenden erhielten jeweils moderne Streaming-Lautsprecher.

Bild © Patrick Klampfer

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 Vorlesung Kritische Informationsinfrastrukturen

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

2.1.5 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.

2.1.6 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 2016 sehr gut. Dies wurde über Aufträge im ETSI Standardisierungsmandat zu elektronischen Signaturen ergänzt.