stiftung secure information and communication

Jahresbericht 2018

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 2018 dargestellt.

Inhaltsverzeichnis

Inhaltsverzeichnis 1
Executive Summary 2
1 Einleitung 3
1.1 Stiftungszweck 3
1.2 Forschungsschwerpunkte 3
1.3 Zur Lage der Stiftung 4
1.4 Hilfsbetrieb JCE Toolkit 4
1.5 Stiftungsorgane und Organisationsstruktur 5
2 Leistungen im Sinne des Stiftungszwecks 7
2.1 Förderung von Forschung und Lehre, Wissenstransfer 7
2.1.1 Stiftungsprofessur Kryptographie 7
2.1.2 Stiftungsprofessur Cloud Computing Security 8
2.1.3 Stiftungsprofessur Cybersecurity 9
2.1.4 Research Excellence Awards 10
2.1.5 CREDENTIAL 11
2.1.6 E-Government 11
2.1.7 Eigene Forschungsleistungen 11
2.2 Organisatorisches und Sonstiges 11
2.2.3 Technische Infrastruktur 11
2.2.4 Entwicklungsaktivitäten JCE Toolkit 11

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 23. Mai 2019

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 2018 stellt die Leistungen der Stiftung nach dem Stiftungszweck im Zeitraum 1.1. - 31.12.2018 dar. Der Bericht behält die Struktur der bisherigen Berichte.

2018 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 eine Assistentinnenstelle zu zwei Drittel finanziert.
- Über eine Anstoßfinanzierung wurde die Laufbahnprofessur „*Cybersecurity*" von Ass.-Prof Daniel Gruß gestartet.
- Acht 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 2018 dargestellt. Es stellt dies auch den Bericht über die im Sinne des Stiftungszwecks erbrachten Leistungen gemäß StSFG § 14 (3) dar (Abschnitt 2 „“). In den Anhängen sind die weiteren nach StSFG § 14 (3) definierten Berichte an die Aufsichtsbehörde angefügt.

Entsprechend einem Beschluss des Kuratoriums vom 4. Juni 2019 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 https://jce.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 2018 über die Stiftungsprofessur Cloud Computing, die Stiftungsprofessur Kryptographie, den Anschub der Laufbahnprofessur Cybersecurity, sowie Research Excellence Awards vor allem Studierenden der Technischen Universität Graz zugute und stärken damit Ausbildung im Wirkungsbereich der Stiftung.

Über die Stiftungsprofessuren „*Kryptographie*“ und „*Cloud Computing Security*“ werden exzellente, international beachtete Forschungsleistungen in der Steiermark unterstützt. Mit Anstoßfinanzierung der Laufbahnprofessur „*Cybersecurity*“ wurde dies 2018 erweitert.

Die Stiftung war im EU Projekt „CREDENTIAL“ engagiert, womit sie auch in internationalen Forschungsaktivitäten verankert ist. Dieses Projekt ist 2018 ausgelaufen.

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

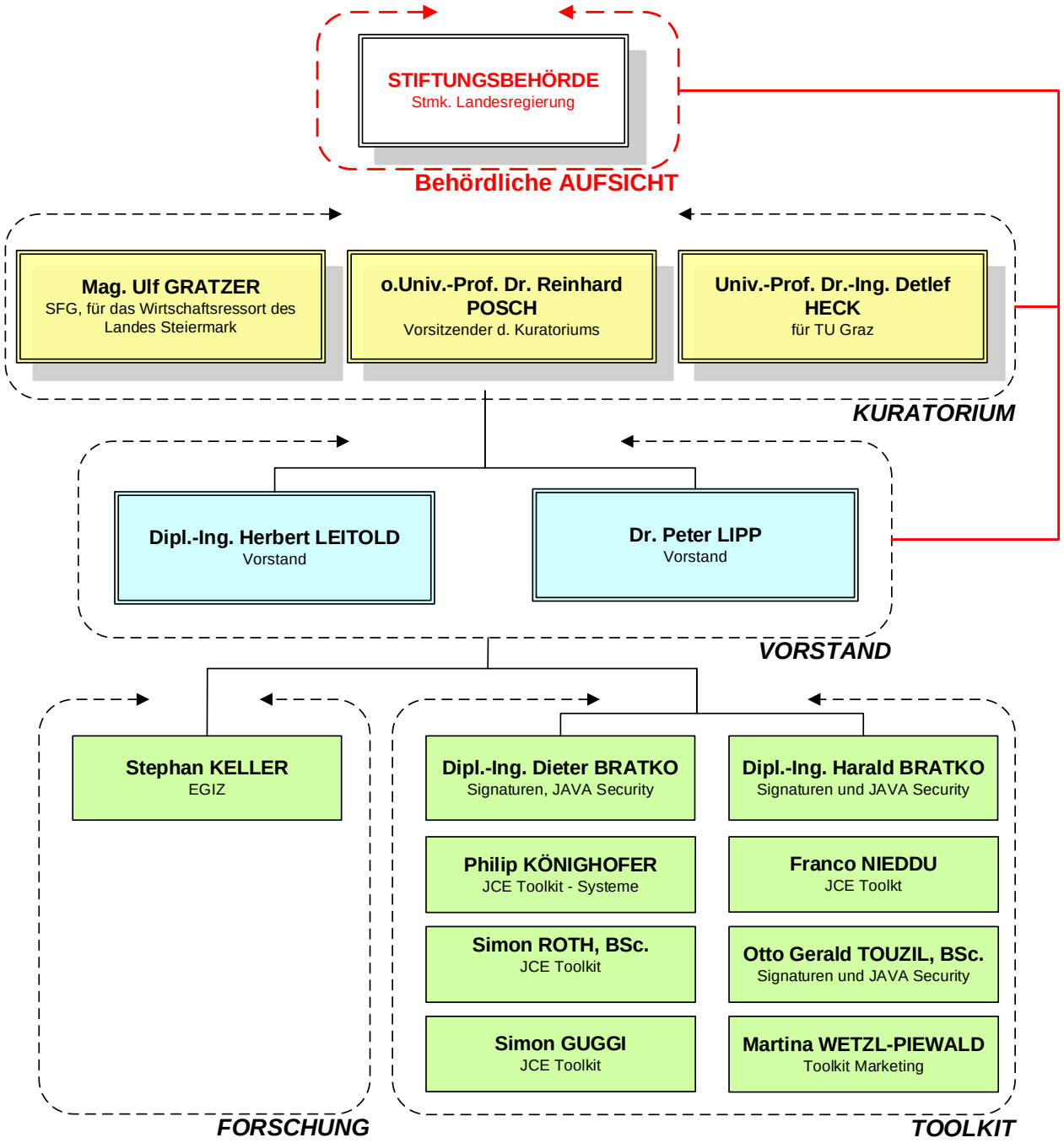
Die Abgrenzung zwischen gemeinnützigem und gewerblichem Bereich erfolgt über getrennte Kostenrechnung der Bereiche „Forschung“ (gemeinnützige Aktivitäten), „Toolkit“ (gewerblicher Hilfsbetrieb) und „Overheads“ (Gemeinkosten, die anteilig den Bereichen Toolkit und Forschung zugeordnet werden).

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 2018 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 31.12.2018 dargestellt. Administration und technische Infrastruktur wird gegen Kostenersatz vom IAIK der TU Graz gestellt.



Organigramm und Personalstand per 31.12.2018

2 Leistungen im Sinne des Stiftungszwecks

Über die Leistungen der Stiftung wird nach dem in der Satzung der Stiftung definierten Zweck „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 2017 ist die Professur mit Prof. Christian Rechberger besetzt. Die Stiftung hat eine vorgezogene Bestellung 2017 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 2018 ihre Ergebnisse an namhaften und auch erstklassigen wissenschaftlichen Tagungen und Journalen veröffentlichen:

1. Differential Cryptanalysis of Symmetric Primitives, Eichlseder, M; Dissertation.

2. Revisting Proxy Re-Encryption: Forward Secrecy, Improved Security and Applications; Derler, D., Krenn, S., Lorünser, T., Ramacher, S. & Slamanig, D., Strieck, S.; PKC 2018

3. Short Double- and N-Times-Authentication-Preventing Signatures from ECDSA and More; Derler, D., Ramacher, S. & Slamanig, D.; EuroS&P 2018.

4. Bloom Filter Encryption and Applications to Efficient Forward-Secret 0-RTT Key Exchange; Derler, D., Jager, T., Slamanig, D. & Striecks, C.; Advances in Cryptology - EUROCRYPT 2018

5. Clustering Related-Tweak Characteristics: Application to MANTIS-6; Eichlseder, M. & Kales, D.; IACR Transactions on Symmetric Cryptology. 2018

6. Cryptanalysis of MORUS; Ashur, T., Eichlseder, M., Lauridsen, M., Leurent, G., Minaud, B., Rotella, Y. & Viguier, B.; Advances in Cryptology – ASIACRYPT 2018

7. Differential Fault Attacks on Deterministic Lattice Signatures; Peßl, P. & Groot Bruinderink, L.; IACR Transactions on Cryptographic Hardware and Embedded Systems. 2018

8. Generic Double-Authentication Preventing Signatures and a Post-quantum Instantiation; Derler, D., Ramacher, S. & Slamanig, D.; Provable Security - 12th International Conference, ProvSec 2018

9. Highly-Efficient Fully-Anonymous Dynamic Group Signatures; Derler, D. & Slamanig, D.; AsiaCCS 2018

10. Key-homomorphic signatures: definitions and applications to multiparty signatures and non-interactive zero-knowledge; Derler, D. & Slamanig, D.; Designs, Codes, and Cryptography, 2018

11. Post-Quantum Zero-Knowledge Proofs for Accumulators with Applications to Ring Signatures from Symmetric-Key Primitives; Derler, D., Ramacher, S. & Slamanig, D.; Post-Quantum Cryptography - 9th International Conference, PQCrypto 2018

12. Practical Witness Encryption for Algebraic Languages Or How to Encrypt Under Groth-Sahai Proofs; Derler, D. & Slamanig, D.; Designs, codes and cryptography, 2018

13. Rasta: A Cipher with Low ANDdepth and Few ANDs per Bit; Dobraunig, C. E., Eichlseder, M., Grassi, L., Lallemend, V., Leander, G., List, E., Mendel, F. & Rechberger, C.; Advances in Cryptology – CRYPTO 2018

14. Short Double- and N-Times-Authentication-Preventing Signatures from ECDSA and More; Derler, D., Ramacher, S. & Slamanig, D.; IEEE European Symposium on Security and Privacy, EuroS&P 2018

15. Zero-Sum Partitions of PHOTON Permutations; Wang, Q., Grassi, L. & Rechberger, C.; Topics in Cryptology - CT-RSA 2018

In der Lehre wurden von der Gruppe unter anderem die Vorlesungen „*IT Sicherheit*“, „*Cryptography*“, „*Applied Cryptography*“ und „*Applied Cryptography 2*“ 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 2017 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 2018 wieder an teils erstklassigen Konferenzen und Journalen veröffentlichen:

1. A unified masking approach; Gross, H. & Mangard, S.; Journal of cryptographic engineering, 2018

2. Domain-Oriented Masking: Generically Masked Hardware Implementations; Groß, H.; Dissertation.

3. High Speed ASIC Implementations of Leakage-Resilient Cryptography; Schilling, R., Unterluggauer, T., Mangard, S., Gürkaynak, F. K., Mühlberghuber, M. & Benini, L.; Design, Automation & Test in Europe Conference - DATE 2018

4. KeyDrown: Eliminating Software-Based Keystroke Timing Side-Channel Attacks; Schwarz, M., Lipp, M., Gruss, D., Weiser, S., Maurice, C. L. N., Spreitzer, R. & Mangard, S.; Network and Distributed System Security Symposium 2018

5. MEAS: memory encryption and authentication secure against side-channel attacks; Unterluggauer, T., Werner, M. & Mangard, S.; Journal of cryptographic engineering, 2018

6. Pointing in the Right Direction - Securing Memory Accesses in a Faulty World; Schilling, R., Werner, M., Nasahl, P. & Mangard, S.; Annual Computer Security Applications Conference, 2018

7. ProcHarvester: Fully Automated Analysis of Procfs Side-Channel Leaks on Android; Spreitzer, R., Kirchengast, F., Gruss, D. & Mangard, S.; ASIACCS '18

8. SCAnDroid: Automated Side-Channel Analysis of Android APIs; Spreitzer, R., Palfinger, G. & Mangard, S.; WISEC '18, ndroid; Spreitzer, R., Kirchengast, F., Gruss, D. & Mangard, S.; ASIACCS '18

9. Securing Conditional Branches in the Presence of Fault Attacks; Schilling, R., Werner, M. & Mangard, S.; Design, Automation & Test in Europe Conference - DATE 2018:

10. Sharing Independence Relabeling: Efficient Formal Verification of Higher-Order Masking; Bloem, R., Groß, H., Iusupov, R., Krenn, M. & Mangard, S.; Cryptology ePrint Archive, 2018

11. SIFA: Exploiting Ineffective Fault Inductions on Symmetric Cryptography; Dobraunig, C. E., Eichlseder, M., Korak, T., Mangard, S., Mendel, F. & Primas, R.; IACR Transactions on Cryptographic Hardware and Embedded Systems. 2018

12. Single Trace Attack Against RSA Key Generation in Intel SGX SSL; Weiser, S., Spreitzer, R. & Bodner, L.; ASIACCS '18

13. Sponge-Based Control-Flow Protection for IoT Devices; Werner, M., Unterluggauer, T., Schaffenrath, D. & Mangard, S., IEEE European Symposium on Security and Privacy, 2018

14. Statistical Ineffective Fault Attacks on Masked AES with Fault Countermeasures; Dobraunig, C. E., Eichlseder, M., Groß, H., Mangard, S., Mendel, F. & Primas, R., Advances in Cryptology – ASIACRYPT 2018

15. Systematic Classification of Side-Channel Attacks: A Case Study for Mobile Devices; Spreitzer, R., Moonsamy, V., Korak, T. & Mangard, S.; IEEE Communications Surveys & Tutorials.

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

2.1.3 Stiftungsprofessur Cybersecurity

Die Stiftung hat eine Anstoßfinanzierung zu einer Laufbahnprofessur Cybersecurity für 2018 geleistet. Diese wurde im August mit Daniel Gruß (zuvor in Gruppe Prof. Mangard) besetzt.

Auch die Gruppe von Daniel Gruß konnte eine Reihe von Veröffentlichungen in namhaften Konferenzen landen. Eine Auswahl ist:

1. Another Flip in the Wall of Rowhammer Defenses; Gruss, D., Lipp, M., Schwarz, M., Genkin, D., Juffinger, J., O'Connell, S., Schoechl, W. & Yarom, Y.; 39th IEEE Symposium on Security and Privacy 2018

2. A Systematic Evaluation of Transient Execution Attacks and Defenses; Canella, C., Bulck, J. V., Schwarz, M., Lipp, M., Berg, B. V., Ortner, P., Piessens, F., Evtyushkin, D. & Gruss, D.; arXiv.org e-Print archive, 2018

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.; AsiaCCS' 18

4. JavaScript Zero: Real JavaScript and Zero Side-Channel Attacks; Schwarz, M., Lipp, M. & Gruss, D.; Network and Distributed System Security Symposium 2018

5. Kernel Isolation: From an Academic Idea to an Efficient Patch for Every Computer; Gruss, D., Hansen, D. & Gregg, B.; In: ;login: the USENIX Magazine, 2018

6. Meltdown; Lipp, M., Schwarz, M., Gruss, D., Prescher, T., Haas, W., Mangard, S., Kocher, P., Genkin, D., Yarom, Y. & Hamburg, M.; In: arXiv.org e-Print archive, 2018

7. Meltdown: Reading Kernel Memory from User Space; Lipp, M., Schwarz, M., Gruss, D., Prescher, T., Haas, W., Fogh, A., Horn, J., Mangard, S., Kocher, P., Genkin, D., Yarom, Y. & Hamburg, M.; 27th USENIX Security Symposium, 2018

8. Nethammer: Inducing Rowhammer Faults through Network Requests; Lipp, M., Aga, M. T., Schwarz, M., Gruss, D., Maurice, C., Raab, L. & Lamster, L.; In: arXiv.org e-Print, 2018

9. NetSpectre: Read Arbitrary Memory over Network; Schwarz, M., Schwarzl, M., Lipp, M. & Gruss, D.; In: arXiv.org e-Print archive, 2018

In der Lehre wurden von der Gruppe unter anderem die Vorlesungen „*Systemnahe Programmierung*“ und „*Betriebssysteme*“ betreut bzw. mitbetreut.

Die von der Stiftung mit-finanzierten Professuren 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.

2.1.4 Research Excellence Awards

Die Prämierung ausgezeichneter studentischer Leistungen wurde 2008 begonnen und seither jährlich fortgeführt. 2018 wurden Preise an acht Studierende der TU Graz vergeben, die bereits im Zuge ihrer studentischen Tätigkeiten Ergebnisse wissenschaftlich veröffentlichen konnten. Es waren dies:

- Lukas Bodner für “Single Trace Attack Against RSA Key Generation in Intel SGX SSL”
- Simon Guggi für “Use-After-FreeMail: Generalizing the Use-After-Free Problem and Applying it to Email Services”
- Vedad Hadzic für “Expansion-Based QBF Solving Without Recursion”
- Jonas Juffinger und Wolfgang Schoechl für “Another Flip in the Wall of Rowhammer Defenses”
- Emanuel Kirchengast für “Qualified eID Derivation into a Distributed Ledger based IdM System”
- Felix Kirchengast für “ProcHarvester: Fully Automated Analysis of Procfs Side-Channel Leaks on Android”

- Pascal Nasahl für “Pointing in the Right Direction-Securing Memory Accesses in a Faulty World”
- Thomas Schuster für “Automated Detection, Exploitation, and Elimination of Double-Fetch Bugs using Modern CPU Features”

Die prämierten Studierenden erhielten jeweils Bluetooth-Lautsprecher.

2.1.5 CREDENTIAL

Als EU Forschungsprojekt mit Beteiligung der Stiftung ist im Oktober 2015 das Projekt Secure Cloud Identity Wallet „CREDENTAL“ gestartet. Das Projekt wurde 2018 erfolgreich abgeschlossen. Ziel dieses ambitionierten Projekts mit zwölf Partnern in sieben Ländern war es, Lösungen zu sicherer Identität in Cloud-Umgebungen über fortgeschrittene kryptographische Protokolle zu erforschen.

2.1.6 E-Government

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

2.1.7 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.

2.2.3 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.

2.2.4 Entwicklungsaktivitäten JCE Toolkit

Die Umsatzerlöse aus dem Verkauf des JCE Toolkits im Hilfsbetrieb waren 2018 sehr gut. Dies wurde über Aufträge im ETSI Standardisierungsmandat zu elektronischen Signaturen sowie Lizenzierung von Software für Vertrauensdienstanbieter ergänzt.