ACADEMIC CURRICULUM VITAE

Prof. Dr. Michael Backes
CISPA Helmholtz Center i.G.
January 5, 2018

EMPLOYMENT HISTORY & SCHOLARSHIP

CISPA Helmholtz Center i.G. 2017 – present
Founding Director and Chairman (CEO) *Saarbrücken, Germany*

Saarland University 2005 – present
Professor *Saarbrücken, Germany*

CISPA, Saarland University 2011 – 2018
Scientific Director *Saarbrücken, Germany*

Max Planck Institute for Software Systems 2007 – 2017
Max Planck Fellow *Saarbrücken, Germany*

IBM Zurich Research Laboratory 2002 – 2005
Permanent research staff member *Zurich, Switzerland*

Saarland University 2001 – 2002
Scholarship of DFG graduate studies program *Saarbrücken, Germany*

School for Deaf Children 1997 - 1998
Community Service *Lebach, Germany*

EDUCATION

Ph.D Student, Saarland University *April 2001 – May 2002*
Ph.D in Computer Science *May 2002*
Thesis: "Cryptographically Sound Analysis of Security Protocols"
Advisor: Birgit Pfitzmann, Harald Ganzinger

Diploma Student (CS and Mathematics), Saarland University *October 1998 – August 2002*
Diploma in Computer Science *March 2001*
Diploma in Mathematics *August 2002*

RESEARCH INTERESTS

Information security and privacy, especially foundations of information security & privacy; design, analysis and verification for security-critical systems and services; methods and tools for assessing and enhancing end-user privacy; research on new attack vectors; and universal solutions in software and network security.

RESEARCH PROJECTS LED (SELECTION)

CISPA: Center for IT-Security, Privacy, and Accountability (21.6M Euro) 2011 – 2018
BMBF Competence Center IT-Security; Director; see `https://uds.cispa.saarland`, *and* `https://cispa.saarland` *for its successor - the CISPA Helmholtz Center i.G.*

CISPA-Stanford Center for Cybersecurity Research (≈20M Euro) 2017 – present
Director; see `https://cispa-stanford.org`

Methods and Tools for Understanding and Controlling Privacy (8.4M Euro) 2016 – 2020
DFG Collaborative Research Center (SFB); Speaker; see https://privacy-sfb.cispa.saarland

imPACT: Privacy, Accountability, Compliance, and Trust in Tomorrow's Internet (9.3M Euro) 2014 – 2020
ERC Synergy Grant; Speaker; see https://www.impact-erc.eu/

Multimodal Computing and Interaction (77.2M Euro) 2007 – 2019
DFG Excellence Cluster; Vice-coordinator; see https://www.mmci.uni-saarland.de

Methods and Tools for End-to-End Security (1.2M Euro) 2009 – 2013
ERC Starting Grant; Speaker

Federated Identity Management 2004 – 2005
IBM Research; Lead

Security of IBM's mainframe architecture 2004 – 2005
IBM Research; co-Lead

Security of Web Services Protocols 2002 – 2005
IBM Research, in cooperation with ETH Zürich; co-Lead

Enterprise Privacy Management 2002 – 2005
IBM Research; co-Lead

Relating Formal Methods and Cryptography 2002 – 2011
IBM Research (until 2005), DFG (from 2006); Lead

RECENT PROFESSIONAL ACTIVITIES (SELECTION)

Technical Program (PC) Chair:

ACM Computer and Communication Security Conference (CCS)	2018
IEEE European Symposium on Security and Privacy (EuroS&P)	2016
IEEE Symposium on Security and Privacy (S&P)	2014
IEEE Symposium on Security and Privacy (S&P)	2013
IEEE Computer Security Foundations Symposium (CSF)	2011
IEEE Computer Security Foundations Symposium (CSF)	2010
European Symposium on Research in Computer Security (ESORICS)	2009
Information Security Conference (ISC)	2006

Steering Committee Member:

IEEE European Symposium on Security and Privacy (EuroS&P, chair)	2015 – present
IEEE Symposium on Security and Privacy (S&P)	2013 – present
IEEE Computer Security Foundations Symposium (CSF)	2010 – present
European Symposium on Research in Computer Security (ESORICS)	2009 – present
ACM Workshop on Formal Methods in Systems Engineering (FMSE)	2003 – 2008

Editorial Responsibilities:

CACM's Research Highlights	2016 – present
Foundations and Trends in Security and Privacy, Editorial Board	2014 – present
Journal of Computer Security, Editor	2012 – 2013
International Journal of Information Security, Editorial Board	2007 – 2012

Program Committee Member:

Program Committee Member of more than 100 international conferences in the last ten years, with some of the most important ones being:
IEEE S&P (2005, 2006, 2009-2014, 2017, 2018); IEEE CSF (2004, 2006-2011, 2014); ACM CCS (2006, 2011, 2012, 2015, 2016); ESORICS (2005-2017); NDSS (2010, 2011); Usenix Security (2016); PETS

(2006, 2008-2011, 2016); Crypto (2011); Eurocrypt (2005); Asiacrypt (2004); TCC (2010); ICALP (2007).

Collaborative Research Center 1223 – Methods and Tools for Understanding and Controlling Privacy 2016 – present
Speaker

Cluster of Excellence MMCI: Multimodal Computing and Interaction 2007 – 2019
Vice-Coordinator

Bachelor Studies Program "Cybersecurity" 2014 – present
Program Coordinator

AWARDS AND HONORS

Scientific Awards:

NSA Cybersecurity Research Award	2017
IEEE Golden Core Award	2017
CNIL-INRIA Privacy Award	2017
ERC Synergy Grant	2014
IEEE Outstanding Community Service Award	2014
IEEE Outstanding Community Service Award	2011
ERC Starting Grant	2009
IBM Faculty Award	2008
Fellow of the German Max Planck Society	2007
IBM Outstanding Achievement Award for Linking Formal Verification and Cryptography	2005
IBM Research Division Award for contributions to Web Services Security	2005
Microsoft Award for outstanding research in privacy enhancing technologies	2004
IBM Outstanding Achievement Award for contributions to Enterprise Privacy Architectures	2004
VDI Diploma Thesis Award	2002
Scholarship of the DFG graduate studies program "Quality Guarantees for Computer Systems"	2001

Honors beyond the Scientific Community:

Member, Deutsche Akademie der Technikwissenschaften (acatech)	2015
Teaching Award of the State of Saarland	2015
Named one of Germany's Digital Minds by BM Wanka	2014
CS Teaching Award of Saarland University	2014
MIT TR35 (35 most outstanding researchers / innovators under the age of 35 worldwide)	2009
Top-40 of German IT people, ranking of Computerwoche	2010/11
Top-40-under-40 of German researchers, ranking of Capital	2010-14
CS Teaching Award of Saarland University	2009
CS Teaching Award of Saarland University	2007

INVITED PRESENTATIONS (SELECTION)

European Parliament, invited ERC grant holder	2017
Royal Society London	2016
11th ACM Symposium on Information, Computer and Communications Security (AsiaCCS)	2016
Leopoldina: Wissenschaftsfreiheit und Wissenschaftsverantwortung	2014
Max Planck Forum, Saarbrücken	2014
Distinguished CS Lecture Series at SnT, Luxembourg	2014
European Parliament, Invited Scientific Expert on Privacy in the Digital Society	2012
Distinguished CS Lecture Series at ETH, Zurich	2012
13th European Joint Conferences on Theory and Practice of Software (ETAPS)	2011

1st Grande Region Security Research Day (GRSRD)	2009
Distinguished CS Lecture Series at Harvard University	2009
15th Int. Conf. on Logic for Programming, Artificial Intelligence, Reasoning (LPAR)	2008
Interplay of Programming Languages and Cryptography Workshop	2007
2nd ECRYPT Workshop on Models for Cryptographic Protocols	2006
Guest professor at Tartu University, Estonia	2006
21st Annual Conference on Mathematical Foundations of Programming Semantics (MFPS)	2005
Automated Reasoning for Security Protocol Analysis (ARSPA)	2005
Toulouse Information Security Workshop	2005
16th IEEE Computer Security Foundations Symposium (CSF) (panelist)	2004
SAFE-NL Privacy workshop at Twente University	2004
4th International School on Foundations of Security Analysis and Design (FOSAD)	2004
6th Information Security Conference (ISC) (panelist)	2003
ZISC Fall School on Formal Security Engineering	2003

TEACHING

A total of 32 lectures and 43 seminars taught since April 2006. We refer to `https://infsec.cs.uni-saarland.de` for a comprehensive overview.

SUPERVISED STUDENTS AND POSTDOCS

Alumni of the IS&C group:
Rizwan Ashgar (*current position: Senior Lecturer, Auckland, New Zealand*)
Matthias Berg (*current position: Bundesamt für Sicherheit in der Informationstechnik, BSI*)
Sven Bugiel (*current position: Tenure-track Faculty, CISPA Helmholtz Center i.G.*)
Oana Ciobotaru (*current position: Postdoc, U Trier*)
Markus Dürmuth (*current position: W2 Professor, Bochum)*
Sascha Fahl (*current position: W2 Professor, Hannover*)
Dario Fiore (*current position: Assistant Professor, IMDEA, Spain*)
Martin Gagne (*current position: Assistant Professor, Wheaton, USA*)
Sebastian Gerling (*current position: Head of Scientific Strategy, CISPA Helmholtz Center i.G.*)
Catalin Hritcu (*current position: Tenured Scientist, INRIA, France*)
Mathias Humbert (*current position: Researcher, Swiss Data Center, Switzerland*)
Aniket Kate (*current position: Assistant Professor, Purdue University*)
Boris Köpf (*current position: Assistant Professor, IMDEA, Spain*)
Matteo Maffei (*current position: W2 Professor, Saarbrücken*)
Sebastian Meiser (*current position: PostDoc, UCL*)
Esfandiar Mohammadi (*current position: PostDoc, ETH Zurich*)
Stefan Nuernberger (*current position: Tenure-track Faculty, CISPA Helmholtz Center i.G.*)
Raphael Reischuk (*current position: PostDoc, ETH Zurich*)
Malte Skoruppa (*current position: Researcher, PHPSec*)
Ben Stock (*current position: Tenure-track Faculty, CISPA Helmholtz Center i.G.*)

Currently Supervised Ph.D Students and Postdocs:
Pascal Berrang, Erik Derr, Sanam Ghorbani Lyastani, Kathrin Grosse, Inken Hagestedt, Jie Huang, Robert Kuennemann, Praveen Manoharan, Duc Cuong Nguyen, Marten Oltrogge, David Pfaff, Ivan Pryvalov, Tahleen Rahman, Ahmed Salem, Jonas Schneider, Oliver Schranz, Milivoj Simeonovski, Patrick Speicher, Christian Stransky, Bartlomiej Surma, Marie-Therese Walter, and Yang Zhang. Please see `http://infsec.cs.uni-saarland.de` for more information.

Supervised Bachelor, Master and Diploma Students:

A total of 56 Bachelor students and 30 Master students supervised thus far. We refer to `https://infsec.cs.uni-saarland.de` for a comprehensive overview.

PUBLICATIONS

I published about 200 papers at international conferences and 80 papers in international journals and technical reports.[1] In particular, I have thus far published 37 publications at the IEEE flagship conferences – 14x IEEE Symposium on Security & Privacy (IEEE S&P), 17x IEEE Computer Security Foundations Symposium (IEEE CSF) and 6x IEEE European Symposium on Security & Privacy (IEEE EuroS&P) – 19 publications at the ACM Conference on Computer and Communications Security (ACM CCS), 19 publications at the European Symposium on Research in Security (ESORICS), 8 publications at the Usenix Security Symposium, and 7 publications at the Network and Distribution System Security Symposium (NDSS). I moreover edited 13 proceedings and filed 6 patents.

BIBLIOGRAPHY

Refereed Journal Papers

1. Yasemin Acar, Michael Backes, Sascha Fahl, Doowon Kim, Michelle L. Mazurek, Christian Stransky. *How Internet Resources Might Be Helping You Develop Faster but Less Securely.* IEEE Security & Privacy 15(2): 50-60, 2017.
2. Michael Backes, Sebastian Meiser, and Marcin Slowik. *Your Choice MATor(s).* In PoPETs 2016(2): 40-60, 2016.
3. Michael Backes, Sven Bugiel ,Oliver Schranz, and Philipp von Styp-Rekowsky. *Boxify: Bringing Full-Fledged App Sandboxing to Stock Android.* USENIX ;login:, 41 (2), pp. 1621, 2016.
4. Yasemin Acar, Michael Backes, Sascha Fahl, and Christian Stransky. *Leading By (Insecure) Example: How Internet Resources Might be Helping You Develop Faster But Less Securely.* In IEEE Security & Privacy, 2016.
5. Michael Backes, Niklas Grimm, and Aniket Kate. *Data Lineage in Malicious Environments.* In IEEE Transactions on Dependable and Secure Computing, 13(2): 178-191, 2016.
6. Michael Backes and Boris Köpf. *Quantifying Information Flow in Crypto Systems.* In Special issue of Mathematical Structures in Computer Science, 25(2): 457-479, 2015.
7. Michael Backes, Catalin Hritcu, and Matteo Maffei. *Union, intersection and refinement types and reasoning about type disjointness for secure protocol implementations.* Journal of Computer Security 22(2): 301 – 353, 2014.
8. Michael Backes, Iliano Cervesato, Aaron D. Jaggard, Andre Scedrov, and Joe-Kai Tsay. *Cryptographically Sound Security Proofs for Basic and Public-Key Kerberos.* In International Journal of Information Security (IJIS), Springer, 2011.
9. Michael Backes and Dominique Unruh. *Computational soundness of symbolic zero-knowledge proofs.* In Journal of Computer Security (JCS), 18(6), 1077 – 1155, 2010.
10. Michael Backes, Markus Dürmuth, Dennis Hofheinz, and Ralf Küsters. *Conditional Reactive Simulatability.* In International Journal of Information Security (IJIS), Springer, 2008.

[1] The IT security community considers publications in top-notch conferences (IEEE S&P, ACM CCS, NDSS, Usenix, IEEE EuroS&P, IEEE CSF, ESORICS) the premium way of disseminating novel results; publications in journals are considered less important.

11. Michael Backes, Birgit Pfitzmann, and Andre Scedrov. *Key-dependent Message Security under Active Attacks – BRSIM/UC-Soundness of Symbolic Encryption with Key Cycles.* In Journal of Computer Security (JCS), 2008.

12. Michael Backes and Birgit Pfitzmann. *Limits of the Cryptographic Realization of Dolev-Yao Style XOR.* In International Journal of Information Security (IJIS), 7(1), pages 33 - 54, Springer, 2008.

13. Michael Backes, Birgit Pfitzmann, and Michael Waidner. *The Reactive Simulatability Framework for Asynchronous Systems.* In Information & Computation, 205(12): pages 1685 - 1720, Elsevier, 2007.

14. Michael Backes, Anupam Datta, Ante Derek, John C. Mitchell, and Mathieu Turuani. *Compositional Analysis of Contract Signing Protocols.* In Theoretical Computer Science (TCS) 367(1,2), pages 33 - 56, Elsevier, 2006.

15. Michael Backes. *Real-or-random Key Secrecy of the Otway-Rees Protocol via a Symbolic Security Proof.* In Electronic Notes in Theoretical Computer Science (ENTCS) 155(12), pages 111 - 145, Elsevier, 2006.

16. Michael Backes and Birgit Pfitzmann. *Relating Symbolic and Cryptographic Secrecy.* In IEEE Transactions on Dependable and Secure Computing (TDSC) 2(2), pages 109 - 123, 2005.

17. Michael Backes, Birgit Pfitzmann, and Michael Waidner. *Reactively Secure Signature Schemes.* In International Journal of Information Security (IJIS) 4(4), pages 242 - 252, Springer, 2005.

18. Michael Backes. *Unifying Simulatability Definitions in Cryptographic Systems under Different Timing Assumptions.* In Journal of Logic and Algebraic Programming (JLAP) 64(2), pages 157 - 188, Elsevier, 2005.

19. Michael Backes, Birgit Pfitzmann, and Michael Waidner. *Symmetric Authentication within a Simulatable Cryptographic Library.* In International Journal of Information Security (IJIS) 4(3), 135 - 154, Springer, 2004.

20. Michael Backes and Birgit Pfitzmann. *A Cryptographically Sound Security Proof of the Needham-Schroeder-Lowe Public-Key protocol.* In IEEE Journal on Selected Areas of Computing (JSAC) 22(10), Special Issue on Design, Implementation and Analysis of Communication Protocols, pages 2075 - 2086, 2004.

21. Michael Backes and Birgit Pfitzmann. *Computational Probabilistic Non-Interference.* In International Journal of Information Security (IJIS) 3(1), pages 42 - 60, Springer, 2004.

22. Michael Backes, Birgit Pfitzmann, Michael Steiner, and Michael Waidner. *Polynomial Liveness.* In Journal of Computer Security (JCS) 12(3-4), pages 589 - 617, 2004.

Refereed Conference and Workshop Papers

23. Jie Huang, Oliver Schranz, Sven Bugiel, Michael Backes. *The ART of App Compartmentalization: Compiler-based Library Privilege Separation on Stock Android.* In Proceedings of 24th ACM Conference on Computer and Communications Security (CCS), 2017.

24. Duc-Cuong Nguyen, Dominik Wermke, Yasemin Acar, Michael Backes, Charles Weir, Sascha Fahl. *A Stitch in Time: Supporting Android Developers in Writing Secure Code.* In Proceedings of 24th ACM Conference on Computer and Communications Security (CCS), 2017.

25. Giancarlo Pellegrino, Martin Johns, Simon Koch, Michael Backes, Christian Rossow. *Deemon: Detecting CSRF with Dynamic Analysis and Property Graphs.* In Proceedings of 24th ACM Conference on Computer and Communications Security (CCS), 2017.

26. Michael Backes, Mathias Humbert, Jun Pang, Yang Zhang. *walk2friends: Inferring Social Links from Mobility Profiles.* In Proceedings of 24th ACM Conference on Computer and Communications Security (CCS), 2017.

27. Erik Derr, Sven Bugiel, Sascha Fahl, Yasemin Acar, Michael Backes. *Keep me Updated: An Empirical Study of Third-Party Library Updatability on Android.* In Proceedings of 24th ACM Conference on Computer and Communications Security (CCS), 2017.

28. Michael Backes, Manuel Gomez-Rodriguez, Praveen Manoharan, Bartlomiej Surma. *Reconciling Privacy and Utility in Continuous-Time Diffusion Networks.* In Proceedings of IEEE Computer Security Foundations Symposium (CSF), 2017.

29. Kathrin Grosse, Nicolas Papernot, Praveen Manoharan, Michael Backes, Patrick D. McDaniel. *Adversarial Examples for Malware Detection.* In Proceedings of 22nd European Symposium on Research in Computer Security (ESORICS), 2017.

30. Johannes Krupp, Mohammad Karami, Christian Rossow, Damon McCoy, Michael Backes. *Linking Amplification DDoS Attacks to Booter Services.* In Proceedings of RAID, 2017.

31. Felix Fischer, Konstantin Bttinger, Huang Xiao, Christian Stransky, Yasemin Acar, Michael Backes, Sascha Fahl. *Stack Overflow Considered Harmful? The Impact of Copy & Paste on Android Application Security.* In Proceedings of IEEE Symposium on Security and Privacy, 2017.

32. Yasemin Acar, Michael Backes, Sascha Fahl, Simson L. Garfinkel, Doowon Kim, Michelle L. Mazurek, Christian Stransky. *Comparing the Usability of Cryptographic APIs.* In Proceedings of IEEE Symposium on Security and Privacy, 2017.

33. Michael Backes, Sven Bugiel, Philipp von Styp-Rekowsky, Marvin Wissfeld. *Seamless In-App Ad Blocking on Stock Android.* In Proceedings of IEEE Symposium on Security and Privacy Workshops, 2017.

34. Michael Backes, Pascal Berrang, Matthias Bieg, Roland Eils, Carl Herrmann, Mathias Humbert, Irina Lehmann. *Identifying Personal DNA Methylation Profiles by Genotype Inference.* In Proceedings of IEEE Symposium on Security and Privacy, 2017.

35. Ben Stock, Martin Johns, Marius Steffens, Michael Backes. *How the Web Tangled Itself: Uncovering the History of Client-Side Web (In)Security.* In Proceedings of Usenix Security Symposium, 2017.

36. Christian Stransky, Yasemin Acar, Duc-Cuong Nguyen, Dominik Wermke, Doowon Kim, Elissa M. Redmiles, Michael Backes, Simson L. Garfinkel, Michelle L. Mazurek, Sascha Fahl. *Lessons Learned from Using an Online Platform to Conduct Large-Scale, Online Controlled Security Experiments with Software Developers.* In Proceedings of CSET Usenix Security Symposium, 2017.

37. Milivoj Simeonovski, Giancarlo Pellegrino, Christian Rossow, Michael Backes. *Who Controls the Internet?: Analyzing Global Threats using Property Graph Traversals.* In Proceedings of WWW, 2017.

38. Giorgi Maisuradze, Michael Backes, and Christian Rossow. *Dachshund: Digging for and Securing (Non-)Blinded Constants in JIT Code.* In Proceedings of 24th Annual Symposium on Network and Distributed System Security (NDSS), 2017.

39. Kangjie Lu, Marie-Therese Walter, David Pfaff, Stefan Nürnberger, Wenke Lee, and Michael Backes. *Unleashing Use-Before-Initialization Vulnerabilities in the Linux Kernel Using Targeted Stack Spraying.* In Proceedings of 24th Annual Symposium on Network and Distributed System Security (NDSS), 2017.

40. Michael Backes and Mohammad Nauman. *LUNA: Quantifying and Leveraging Uncertainty in Android Malware Analysis through Bayesian Machine Learning.* In Proceedings of 2nd IEEE

European Symposium on Security and Privacy (Euro S&P), 2017.

41. Michael Backes, Sven Bugiel, Oliver Schranz, Philipp von Styp-Rekowski and Sebastian Weisgerber. *ARTist: The Android Runtime Instrumentation and Security Toolkit.* In Proceedings of 2nd IEEE European Symposium on Security and Privacy (Euro S&P), 2017.

42. Michael Backes, Konrad Rieck, Malte Skoruppa, Bem Stock, and Fabian Yamaguchi. *Efficient and Flexible Discovery of PHP Application Vulnerabilities.* In Proceedings of 2nd IEEE European Symposium on Security and Privacy (Euro S&P), 2017.

43. M. Backes, annik. Dreier, Steve Kremer, and Robert Künnemann. *A Novel Approach for Reasoning about Liveness in Cryptographic Protocols and its Application to Fair Exchange.* In Proceedings of 2nd IEEE European Symposium on Security and Privacy (Euro S&P), 2017.

44. Michael Backes, Robert Kuennemann, and Esfandiar Mohammadi. *Computational Soundness of Dalvik Bytecode.* In Proceedings of 23rd ACM Conference on Computer and Communications Security (CCS), 2016.

45. Michael Backes, Sven Bugiel, and Erik Derr. *Reliable Third-Party Library Detection in Android and its Security Applications.* In Proceedings of 23rd ACM Conference on Computer and Communications Security (CCS), 2016.

46. Jonas Schneider, Nils Fleischhacker, Dominique Schroeder, and Michael Backes. *Efficient Cryptographic Password Hardening Services From Partially Oblivious Commitments.* In Proceedings of 23rd ACM Conference on Computer and Communications Security (CCS), 2016.

47. Johannes Krupp, Michael Backes, and Christian Rossow. *Identifying the Scanners and Attack Infrastructure behind Amplification DDoS attacks.* In Proceedings of 23rd ACM Conference on Computer and Communications Security (CCS), 2016r.

48. Michael Backes, Pascal Berrang, Mathias Huembert, and Praveen Manoharan. *Membership Privacy in MicroRNA-based Studies.* In Proceedings of 23rd ACM Conference on Computer and Communications Security (CCS), 2016.

49. Michael Backes, Pascal Berrang, Matthias Humbert, Xie Shen, Verene Wolf. *Simulating the Large-Scale Erosion of Genomic Privacy Over Time.* In Proceedings of 3rd International Workshop on Genome Privacy and Security (GenoPri'16) , 2016.

50. Michael Backes, Pascal Berrang, Oana Goga, Krishna P. Gummadi, Praveen Manoharan. *Profile Linkability despite Anonymity in Social Media Systems.* In Proceedings of the 2016 ACM Workshop on Privacy in the Electronic Society (WPES) , 2016.

51. Michael Backes, Amir Herzberg, Aniket Kate, and Ivan Pryvalov. *Anonymous RAM.* In Proceedings of 21st European Symposium on Research in Computer Security (ESORICS), 2016.

52. Michael Backes, Thorsten Holz, Christian Rossow, Teemu Rytilahti, Milivoj Simeonovski, and Ben Stock. *On the Feasibility of TTL-based Filtering for DRDoS Mitigation.* In Proceedings of19th International Symposium on Research in Attacks, Intrusions and Defenses (RAID), 2016.

53. Akira Yokoyama, Kou Ishii, Rui Tanabe, Yinmin Papa, Katsunari Yoshioka, Tsutomu Matsumoto, Takahiro Kasama, Daisuke Inou, Michael Brengel, Michael Backes, and Christian Rossow. *SANDPRINT: Fingerprinting Malware Sandboxes to Provide Intelligence for Sandbox Evasion.* In Proceedings of 19th International Symposium on Research in Attacks, Intrusions and Defenses (RAID), 2016.

54. Ben Stock, Giancarlo Pellegrino, Christian Rossow, Martin Johns, and Michael Backes. *Hey, You Have a Problem: On the Feasibility of Large-Scale Web Vulnerability Notification.* In Proceedings of Usenix Security Symposium, 2016.

55. Giorgi Maisuradze, Michael Backes, and Christian Rossow. *What Cannot be Read, Cannot be Leveraged? Revisiting Assumptions of JIT-ROP Defenses.* In Proceedings of Usenix Security Symposium, 2016.

56. Michael Backes, Sven Bugiel, Erik Derr, Patrick McDaniel, Damien Octeau, and Sebastian Weisgerber. *On Demystifying the Android Application Framework: Re-Visiting Android Permission Specification Analysis.* In Proceedings of Usenix Security Symposium, 2016.

57. Michael Backes, Pascal Berrang, Anna Hecksteden, Mathias Humbert, Andreas Keller, and Tim Meyer. *Privacy in Epigenetics: Temporal Linkability of MicroRNA Expression Profiles.* In Proceedings of Usenix Security Symposium, 2016.

58. Yasemin Acar, Michael Backes, Sven Bugiel, Sascha Fahl, Patrick McDaniel, and Matthew Smith. *SoK: Lessons Learned From Android Security Research For Appified Software Platforms.* In Proceedings of IEEE Symposium on Security and Privacy, 2016.

59. Yasemin Acar, Michael Backes, Sascha Fahl, Doowon Kim, Michelle L. Mazurek, and Christian Stransky. *You Get Where You're Looking For: The Impact Of Information Sources On Code Security.* In Proceedings of IEEE Symposium on Security and Privacy, 2016.

60. Michael Brengel, Michael Backes and Christian Rossow. *Detecting Hardware-Assisted Virtualized Systems.* In Proceedings of 13th Conference on Detection of Intrusions and Malware & Vulnerability Assessment (DIMVA), 2016.

61. Michael Backes, Christian Hammer, David Pfaff, and Malte Skoruppa. *Implementation-level analysis of the JavaScript helios voting client.* In Proceedings of SAC, 2071-2078, 2016.

62. Michael Backes, Pascal Berrang, and Praveen Manoharan, *From Zoos to Safaris – From Closed-World Enforcement to Open-World Assessment of Privacy.* In Proceedings of FOSAD 2016, 87-138, 2016.

63. Kangjie Lu, Wenke Lee, Stefan Nrnberger, and Michael Backes. *How to Make ASLR Win the Clone Wars: Runtime Re-Randomization.* In Proceedings of NDSS 2016.

64. Michael Backes, Sebastian Meiser, and Dominique Schröder. *Delegatable Functional Signatures.* In Proceedings of IACR International Conference on Practice and Theory of Public-Key Cryptography (PKC), 2016.

65. Michael Backes, Martin Gagn, and Sri Aravinda Krishnan Thyagarajan. *Fully Secure Inner-Product Proxy Re-Encryption with Constant Size Ciphertext.* In Proceedings of SCC@ASIACCS, 31-40, 2015.

66. Michael Backes, Simon Koch, Sebastian Meiser, Esfandiar Mohammadi, and Christian Rossow. *In the Net of the Spider: Measuring the Anonymity-Impact of Network-level Adversaries Against Tor (Poster).* In Proceedings of ACM Conference on Computer and Communications Security (CCS), 1626-1628, 2015.

67. Michael Backes, Oliver Schranz, and Philipp von Styp-Rekowsky. *Towards Compiler-Assisted Taint Tracking on the Android Runtime (Poster).* In Proceedings of ACM Conference on Computer and Communications Security, 1629-1631, 2015

68. Michael Backes, Fabian Bendun, Matteo Maffei, Esfandiar Mohammadi, and Kim Pecina. *Symbolic Malleable Zero-Knowledge Proofs.* In Proceedings of IEEE Computer Security Foundations Symposium (CSF), 412-426, 2015.

69. Michael Backes, Esfandiar Mohammadi, and Tim Ruffing. *Computational Soundness for Interactive Primitives.* In Proceedings of European Symposium on Research on Security and Privacy (ESORICS), 125-145, 2015.

70. Michael Backes, Manuel Barbosa, Dario Fiore, and Raphael M. Reischuk. *ADSNARK: Nearly Practical and Privacy-Preserving Proofs on Authenticated Data.* In Proceedings of IEEE Symposium on Security and Privacy, 271-286, 2015.

71. Michael Backes, Sven Bugiel, Christian Hammer, Oliver Schranz, and Philipp von Styp-Rekowsky. *Boxify: Full-fledged App Sandboxing for Stock Android.* In Proceedings of Usenix Security, 691-706, 2015.

72. Michael Backes, Fabian Bendun, Jörg Hoffmann, and Ninja Marnau. *PriCL: Creating a Precedent – A Framework for Privacy Law Cases.* In Proceedings of POST, 344-363, 2015.

73. Michael Backes, Aniket Kate, Sebastian Meiser, and Esfandiar Mohammadi. *(Nothing else) MATor(s): Monitoring the Anonymity of Tor's Path Selection.* In Proceedings of ACM Conference on Computer and Communications Security (CCS), 513-524, 2014

74. Michael Backes, Thorsten Holz, Benjamin Kollenda, Philipp Koppe, Stefan Nürnberger, and Jannik Pewny. *You Can Run but You Can't Read: Preventing Disclosure Exploits in Executable Code.* In Proceedings of ACM Conference on Computer and Communications Security (CCS), 1342-1353, 2014.

75. Michael Backes and Stefan Nürnberger. *Oxymoron: Making Fine-Grained Memory Randomization Practical by Allowing Code Sharing.* In Proceedings of USENIX Security, 433-447, 2014.

76. Michael Backes, Sven Bugiel, and Sebastian Gerling. *Scippa: system-centric IPC provenance on Android.* In Proceedings of ACSAC, 36-45, 2014.

77. Michael Backes, Sven Bugiel, Sebastian Gerling, and Philipp von Styp-Rekowsky. *Android Security Framework: extensible multi-layered access control on Android.* In Proceedings of ACSAC, 46-55, 2014.

78. Michael Backes, Praveen Manoharan, and Esfandiar Mohammadi. *TUC: Time-Sensitive and Modular Analysis of Anonymous Communication.* In Proceedings of IEEE CSF, 383–397, 2014.

79. Michael Backes, Fabian Bendun, Ashish Choudhury, and Aniket Kate. *Asynchronous MPC with a strict honest majority using non-equivocation.* In Proceedings of PODC, 10–19, 2014.

80. Michael Backes, Esfandiar Mohammadi, and Tim Ruffing. *Computational Soundness Results for ProVerif - Bridging the Gap from Trace Properties to Uniformity.* In Prroceedings of POST, 42–62, 2014.

81. Michael Backes, Niklas Grimm, and Aniket Kate. *Lime: Data Lineage in the Malicious Environment.* In Proceedings of STM, 183–187, 2014.

82. Michael Backes, Jeremy Clark, Aniket Kate, Milivoj Simeonovski, and Peter Druschel. *Practical Repudiation (or Traceability) for Anonymous Communication Networks.* In Proceedings of ACNS, 380–400, 2014.

83. Michael Backes, Rainer Gerling, Sebastian Gerling, Stefan Nürnberger, Dominique Schröder, and Mark Simkin. *WebTrust - A Comprehensive Authenticity and Integrity Framework for HTTP.* In Proceedings of ACNS, 401–418, 2014.

84. Michael Backes, Sebastian Gerling, Stefan Lorenz, and Stephan Lukas. *X-pire 2.0 - A User-Controlled Expiration Date and Copy Protection Mechanism.* In Proceedings of ACM Symposium on Applied Computing (SAC), 1633–1640, 2014.

85. Michael Backes, Dario Fiore, and Raphael M. Reischuk. *Verifiable delegation of computation on outsourced data.* In Proceedings of ACM Conference on Computer and Communications Security (CCS), 863 – 874, 2013.

86. Michael Backes, Aniket Kate, Praveen Manoharan, Sebastian Meiser, and Esfandiar Mohammadi. *AnoA: A Framework for Analyzing Anonymous Communication Protocols.* In Proceedings of CSF, 163–178, 2013.

87. Michael Backes, Amit Datta, and Aniket Kate. *Asynchronous Computational VSS with Reduced Communication Complexity.* In Proceedings of CT-RSA 2013: 259-276.

88. Michael Backes, Dario Fiore, and Esfandiar Mohammadi. *Privacy-Preserving Accountable Computation.* In Proceedings of ESORICS 2013: 38-56.

89. Michael Backes and Sebastian Meiser. *Differentially Private Smart Metering with Battery Recharging.* In Proceedings of DPM/SETOP 2013: 194-212.

90. Michael Backes, Sebastian Gerling, Christian Hammer, Matteo Maffei, and Philipp von Styp-Rekowsky. *AppGuard - Fine-Grained Policy Enforcement for Untrusted Android Applications.* In Proceedings of DPM/SETOP 2013: 213-231.

91. Philipp von Styp-Rekowsky, Sebastian Gerling, Michael Backes, and Christian Hammer. *Callee-Site Rewriting of Sealed System Libraries.* In Proceedings of ESSoS 2013: 33-41.

92. Michael Backes, Goran Doychev, and Boris Köpf. *Preventing Side-Channel Leaks in Web Traffic: A Formal Approach.* In Proceedings of NDSS 2013

93. Michael Backes, Fabian Bendun, and Dominique Unruh. *Computational Soundness of Symbolic Zero-Knowledge Proofs: Weaker Assumptions and Mechanized Verification.* In Proceedings of POST 2013: 206-225

94. Michael Backes, Sebastian Gerling, Christian Hammer, Matteo Maffei, and Philipp von Styp-Rekowsky. *AppGuard - Enforcing User Requirements on Android Apps.* In Proceedings of TACAS 2013: 543-548

95. Michael Backes, Martin Gagn, and Malte Skoruppa. *Using mobile device communication to strengthen e-Voting protocols.* In Proceedings of WPES 2013: 237-242.

96. Michael Backes, Ian Goldberg, Aniket Kate, and Tomas Toft. *Adding query privacy to robust DHTs.* In Proceedings of ASIACCS 2012: 30-31.

97. Michael Backes, Ankit Malik, and Dominique Unruh. *Computational soundness without protocol restrictions.* In Proceedigs of ACM Conference on Computer and Communications Security (CCS), 699-711, 2012.

98. Michael Backes, Gilles Barthe, Matthias Berg, Benjamin Grgoire, Csar Kunz, Malte Skoruppa, and Santiago Zanella Bguelin. *Verified Security of Merkle-Damgrd.* In Proceedings of CSF 2012: 354-368

99. Michael Backes, Ian Goldberg, Aniket Kate, and Esfandiar Mohammadi. *Provably Secure and Practical Onion Routing.* In Proceedings of CSF 2012: 369-385

100. Markus Mainberger, Christian Schmaltz, Matthias Berg, Joachim Weickert, and Michael Backes. *Diffusion-Based Image Compression in Steganography.* ISVC (2) 2012: 219-228

101. Michael Backes, Matteo Maffei, and Kim Pecina. *Automated Synthesis of Secure Distributed Applications.* In Proceedings of NDSS 2012

102. Michael Backes, Alex Busenius, and Catalin Hritcu. *On the Development and Formalization of an Extensible Code Generator for Real Life Security Protocols.* In Proceedings of NASA Formal Methods 2012: 371-387

103. Michael Backes, Fabian Bendun, and Aniket Kate. *Brief announcement: distributed cryptography using trinc.* In Proceedings of PODC 2012: 91-92

104. Michael Backes, Aniket Kate, Matteo Maffei, and Kim Pecina. *ObliviAd: Provably Secure and Practical Online Behavioral Advertising.* In Proceedings of IEEE Symposium on Security and Privacy 2012: 257-271

105. Michael Backes, Aniket Kate, and Esfandiar Mohammadi. *Ace: an efficient key-exchange protocol for onion routing.* In Proceedings of WPES 2012: 55-64

106. Raphael M. Reischuk, Michael Backes, and Johannes Gehrke. *SAFE extensibility of data-driven web applications.* In Proceedings of WWW, 799 – 808, 2012.

107. Michael Backes, Aniket Kate, and Arpita Patra. *Computational Verifiable Secret Sharing Revisited.* In Proceedings of ASIACRYPT, 590–609, 2011.

108. Michael Backes, Catalin Hritcu, and Thorsten Tarrach. *Automatically Verifying Typing Constraints for a Data Processing Language.* In Proceedings of CPP, 296 – 313, 2011.

109. Michael Backes, Matteo Maffei, and Kim Pecina. *A Security API for Distributed Social Networks.* In Proceedings of 18th Network and Distributed System Security Symposium (NDSS), 35 – 51, San Diego, California, 2011.

110. Michael Backes, Matteo Maffei, and Kim Pecina. *Securing Social Networks.* In Proceedings of 30th ACM Symposium on Principles of Distributed Computing (PODC), 2011.

111. Michael Backes, Matthias Berg, and Boris Köpf. *Non-uniform Distributions in Quantitative Information-flow.* In Proceeedings of 6th ACM Symposium on Information, Computer and Communications Security (AsiaCCS), 367-375, 2011.

112. Michael Backes, Matteo Maffei, Kim Pecina, and Raphael Reischuk. *G2C: Cryptographic Protocols from Goal-Driven Specifications.* In Proceedings of 1st Conference on Theory of Security and Applications (TOSCA '11, formerly ARSPA-WITS), Saarbrücken, Germany, 2011.

113. Michael Backes, Catalin Hritcu, and Matteo Maffei. *Union and Intersection Types for Secure Protocol Implementations.* In Proceedings of 1st Conference on Theory of Security and Applications (TOSCA '11, formerly ARSPA-WITS), Saarbrücken, Germany, 2011.

114. Michael Backes, Matteo Maffei, and Esfandiar Mohammadi. *Computationally Sound Abstraction and Verification of Secure Multi-Party Computations.* In Proceedings of 30th Annual Conference on Foundations of Software Technology and Theoretical Computer Science, (FSTTCS), 352 – 363, Chennai, India, 2010.

115. Michael Backes, Matteo Maffei, and Dominique Unruh. *Computationally sound verification of source code.* In Proceedings of 17th ACM Conference on Computer and Communications Security (CCS), 387 – 398, Chicago, Illinois, 2010.

116. Michael Backes, Oana Ciobotaru, and Anton Krohmer. *RatFish: A File Sharing Protocol Provably Secure against Rational Users.* In Proceedings of 15th European Symposium on Research in Computer Security (ESORICS), 607 – 625, Athens, Greece, 2010.

117. Michael Backes, Goran Doychev, Markus Dürmuth, and Boris Köpf. *Speaker Recognition in Encrypted Voice Streams.* In Proceedings of 15th European Symposium on Research in Computer Security (ESORICS), 508 – 523, Athens, Greece, 2010.

118. Michael Backes, Markus Dürmuth, Sebastian Gerling, Manfred Pinkal, and Caroline Sporleder. *Acoustic Side-Channel Attacks on Printers.* In Proceedings of 19th USENIX Security Symposium, 307 – 322, Washington, DC, USA, 2010.

119. Michael Backes, Stefan Lorenz, Matteo Maffei, and Kim Pecina. *Anonymity and Trust in Distributed Systems.* In Proceedings of 29th ACM Symposium on Principles of Distributed Computing (PODC), 237 – 238, Zurich, Switzerland, 2010.

120. Michael Backes, Stefan Lorenz, Matteo Maffei, and Kim Pecina. *Anonymous Webs of Trust.* In Proceedings of 10th International Symposim on Enhancing Technologies (PETS), 130 – 148, Berlin, Germany, 2010.

121. Michael Backes, Dennis Hofheinz, and Dominique Unruh. *CoSP: A General Framework for Computational Soundness Proofs.* In Proceedings of 16th ACM Conference on Computer and Communications Security (CCS), Chicago, IL, 2009.

122. Michael Backes, Martin Grochulla, Catalin Hritcu, and Matteo Maffei. *Achieving Security Despite Compromise Using Zero-Knowledge.* In 22nd IEEE Symposium on Computer Security Foundations (CSF), Port Jefferson, NY, 2009.

123. Michael Backes, Boris Köpf, and Andrey Rybalchenko. *Automatic Discovery and Quantification of Information Leaks.* In Proceedings of 30th IEEE Symposium on Security and Privacy, Oakland, CA, 2009.

124. Michael Backes, Tongbo Chen, Markus Dürmuth, Hendrik P. A. Lensch, and Martin Welk. *Tempest in a Teapot: Compromising Reflections Revisited.* In Proceedings of 30th IEEE Symposium on Security and Privacy, Oakland, CA, 2009.

125. Michael Backes and Matteo Maffei. *Design and Verification of Anonymous Trust Protocols.* In Proceedings of 17th International Workshop on Security Protocols, Cambridge, UK, 143-148, 2009.

126. Michael Backes. *Unifying Anonymity and Trust in Security Protocols* . In Proceedings of 17th International Workshop on Security Protocols, Cambridge, UK, 149-156, 2009.

127. Michael Backes, Peter Druschel, Andreas Haeberlen, and Dominique Unruh. *CSAR: A Practical and Provable Technique to Make Randomized Systems Accountable.* In Proceedings of 2009 Network and Distributed System Security Symposium (NDSS), San Diego, CA, 2009.

128. Michael Backes, Marek Hamerlik, Alessandro Linari, Matteo Maffei, Christos Tryfonopoulos, and Gerhard Weikum. *Anonymity and Censorship Resistance in Unstructured Overlay Networks.* In Proceedings of Confederated International Conferences (OTM), 147 – 164, Vilamoura, Portugal, 2009.

129. Michael Backes, Catalin Hritcu, and Matteo Maffei. *Type-checking zero-knowledge.* In Proceedings of 15th ACM Conference on Computer and Communications Security (CCS), Alexandria, VA, 2008.

130. Michael Backes and Dominique Unruh. *Limits of Constructive Security Proofs.* In Proceedings of Advances in Cryptology – ASIACRYPT, Melbourne, Australia, 2008.

131. Michael Backes, Markus Dürmuth, and Dominique Unruh. *OAEP Is Secure under Key-Dependent Messages.* In Proceedings of Advances in Cryptology – ASIACRYPT, Melbourne, Australia, 2008.

132. Michael Backes, Stefan Lorenz, Matteo Maffei, and Kim Pecina. *The CASPA Tool: Causality-Based Abstraction for Security Protocol Analysis.* In Proceedings of 20th International Conference on Computer Aided Verification (CAV), Princeton, NJ, 2008.

133. Michael Backes, Matthias Berg, and Dominique Unruh. *A Formal Language for Cryptographic Pseudocode.* In Proceedings of International Conference on Logic for Programming Artificial Intelligence and Reasoning (LPAR), Doha, Qatar, 2008.

134. Michael Backes and Boris Köpf. *Formally Bounding the Side-Channel Leakage in Unknown-Message Attacks.* In Proceedings of 13th European Symposium on Research in Computer Security (ESORICS), Malaga, Spain, 2008.

135. Michael Backes, Marek Hamerlik, Alessandro Linari, Matteo Maffei, Christos Tryfonopoulos, and Gerhard Weikum. *Anonymous and censorship resistant content sharing in unstructured over-*

lays. In Proceedings of 27th ACM Symposium on Principles of Distributed Computing (PODC), Toronto, Canada, 2008.

136. Michael Backes, Catalin Hritcu, and Matteo Maffei. *Automated Verification of Electronic Voting Protocols in the Applied Pi Calculus*. In Proceedings of 21st IEEE Computer Security Foundations Symposium (CSF), Pittsburgh, PA, 2008.

137. Michael Backes and Dominique Unruh. *Computational Soundness of Symbolic Zero-knowledge Proofs against Active Attackers*. In Proceedings of 21st IEEE Computer Security Foundations Symposium (CSF), Pittsburgh, PA, 2008.

138. Michael Backes, Matteo Maffei, and Dominique Unruh. *Zero-Knowledge in the Applied Pi-calculus and Automated Verification of the Direct Anonymous Attestation Protocol*. In Proceedings of 29th IEEE Symposium on Security and Privacy, Oakland, CA, 2008.

139. Michael Backes, Markus Dürmuth, and Dominique Unruh. *Compromising Reflections – or – How to Read LCD Monitors Around the Corner*. In Proceedings of 29th IEEE Symposium on Security and Privacy, Oakland, CA, 2008.

140. Michael Backes, Markus Dürmuth, and Ralf Küsters. *On Simulatability Soundness and Mapping Soundness of Symbolic Cryptography*. In Proceedings of 27th International Conference on Foundations of Software Technology and Theoretical Computer Science (FSTTCS), December 2007.

141. Michael Backes, Agostino Cortesi, Riccardo Focardi, and Matteo Maffei. *A Calculus of Challenges and Responses*. In Proceedings of 5th ACM Workshop on Formal Methods in Security Engineering (FMSE), November 2007.

142. Michael Backes, Birgit Pfitzmann, and Andre Scedrov. *Key-dependent Message Security under Active Attacks – BRSIM/UC-Soundness of Symbolic Encryption with Key Cycles*. In Proceedings of 20th IEEE Computer Security Foundation Symposium, CSF '07, Venice, Italy, July 2007.

143. Michael Backes, Agostino Cortesi, and Matteo Maffei. *Causality-based Abstraction of Multiplicity in Security Protocols*. In Proceedings of 20th IEEE Computer Security Foundation Symposium, CSF '07, Venice, Italy, July 2007.

144. Michael Backes, Matteo Maffei, and Dominique Unruh. *Zero-Knowledge in the Applied Pi-calculus and Automated Verification of the Direct Anonymous Attestation Protocol*. In Proceedings of Formal Protocol Verification Applied, 2007.

145. Michael Backes, Markus Dürmuth, and Dominique Unruh. *Information Flow in the Peer-Reviewing Process (Extended Abstract)*. In Proceedings of 28th IEEE Symposium on Security and Privacy, Oakland, CA, 2007.

146. Michael Backes, Jörn Müller-Quade, and Dominique Unruh. *On the Necessity of Rewinding in Secure Multiparty Computation*. In Proceedings of 4th Theory of Cryptography Conference (TCC), Amsterdam, The Netherlands, Springer, February 2007.

147. Michael Backes and Peeter Laud. *Computational Sound Secrecy Proofs by Mechanized Flow Analysis*. In Proceedings of 13th ACM Conference on Computer and Communications Security (CCS), Alexandria, VA, November 2006.

148. Michael Backes, Christian Cachin, and Alina Oprea. *Secure Key-Updating for Lazy Revocation*. In Proceedings of 11th European Symposium on Research in Computer Security, ESORICS'06, Hamburg, Germany, September 2006.

149. Michael Backes, Birgit Pfitzmann, and Michael Waidner. *Limits of the Reactive Simulatability/UC of Dolev-Yao Models with Hashes*. In Proceedings of 11th European Symposium on Research in Computer Security, ESORICS'06, Hamburg, Germany, September 2006.

150. Michael Backes, Markus Dürmuth, Dennis Hofheinz, and Ralf Küsters. *Conditional Reactive Simulatability.* In Proceedings of 11th European Symposium on Research in Computer Security, ESORICS'06, Hamburg, Germany, September 2006.

151. Michael Backes, Iliano Cervesato, Aaron D. Jaggard, Andre Scedrov, and Joe-Kai Tsay. *Cryptographically Sound Security Proofs for Basic and Public-key Kerberos.* In Proceedings of 11th European Symposium on Research in Computer Security, ESORICS'06, Hamburg, Germany, September 2006.

152. Michael Backes, Birgit Pfitzmann, and Michael Waidner. *Formal Methods and Cryptography.* In Proceedings of Formal Methods 2006, Hamilton, Ontario, Canada, August 2006.

153. Christoph Sprenger, Michael Backes, David Basin, Birgit Pfitzmann, and Michael Waidner. *Cryptographically Sound Theorem Proving.* In Proceedings of 19th IEEE Computer Security Foundations Workshop, CSFW '06, Venice, Italy, July 2006.

154. Michael Backes, Sebastian Mödersheim, Birgit Pfitzmann, and Luca Viganò. *Symbolic and Cryptographic Analysis of the Secure WS-ReliableMessaging Scenario.* In Proceedings of Foundations of Software Science and Computational Structures (FOSSACS), Vienna, Austria, pages 428 - 445, March 2006.

155. Michael Backes and Birgit Pfitzmann. *On the Cryptographic Key Secrecy of the Strengthened Yahalom Protocol.* In Proceedings of 21st IFIP International Information Security Conference (SEC), Karlstad, Sweden, May 2006.

156. Michael Backes, Christian Cachin, and Alina Oprea. *Lazy Revocation in Cryptographic File Systems.* In Proceedings of 3rd International IEEE Security in Storage Workshop (SISW), San Francisco, CA, USA, December 2005.

157. Michael Backes, Jan Camenisch, and Dieter Sommer. *Cryptographically Secure Anonymous Access Control with Accountability.* In Proceedings of 4th ACM Workshop on Privacy in the Electronic Society (WPES), Alexandria, VA, USA, pages 40 - 46, November 2005.

158. Michael Backes, Dennis Hofheinz, Jörn Müller-Quade, and Dominique Unruh. *On Fairness in Simulatability-based Cryptographic Systems.* In Proceedings of 3rd ACM Workshop on Formal Methods in Security Engineering (FMSE), Alexandria, VA, USA, pages 13 - 22, November 2005.

159. Michael Backes and Thomas Gross. *Tailoring the Dolev-Yao Abstraction to Web Services Realities – A Comprehensive Wish List.* In Proceedings of the 2005 ACM Secure Web Services Workshop (SWS), Alexandria, VA, USA, November 2005.

160. Michael Backes and Birgit Pfitzmann. *Limits of Cryptographic Soundness of Dolev-Yao-Style XOR.* In Proceedings of 10th European Symposium on Research in Computer Security, ESORICS '05, Milan, Italy, pages 178 - 196, volume 3679 of LNCS, September 2005.

161. Michael Backes. *Quantifying Probabilistic Information Flow in Reactive Systems.* In Proceedings of 10th European Symposium on Research in Computer Security, ESORICS '05, Milan, Italy, pages 336 - 354, volume 3679 of LNCS, September 2005.

162. Michael Backes, Anupam Datta, Ante Derek, John C. Mitchell, and Mathieu Turuani. *Compositional Analysis of Contract Signing Protocols.* In Proceedings of 18th IEEE Computer Security Foundations Workshop, CSFW '05, Aix-en-Provence, France, pages, 94 - 110, June 2005.

163. Michael Backes and Markus Dürmuth. *A Cryptographically Sound Dolev-Yao Style Security Proof of an Electronic Payment System.* In Proceedings of 18th IEEE Computer Security Foundations Workshop, CSFW '05, Aix-en-Provence, France, pages 78 - 93, June 2005.

164. Michael Backes and Birgit Pfitzmann. *Relating Symbolic and Cryptographic Secrecy.* In Proceedings of 26th IEEE Symposium on Security and Privacy, Oakland, CA, pages 171 - 182, May

2005.

165. Michael Backes and Christian Cachin. *Public-Key Steganography with Active Attacks.* In Proceedings of 2nd Theory of Cryptography Conference (TCC), Cambridge, MA, pages 210 - 226, volume of 2951 of LNCS, February 2005.

166. Michael Backes. *A Computationally Sound Dolev-Yao Style Security Proof of the Otway-Rees Protocol.* In Proceedings of 9th European Symposium on Research in Computer Security (ESORICS), Sophia-Antipolis, France, pages 89 - 108, volume 3193 of LNCS, September 2004.

167. Michael Backes, Markus Dürmuth, and Rainer Steinwandt. *An Algebra for Composing Enterprise Privacy Policies.* In Proceedings of 9th European Symposium on Research in Computer Security (ESORICS), Sophia-Antipolis, France, pages 33 - 52, volume 3193 of LNCS, September 2004.

168. Michael Backes, Birgit Pfitzmann, and Michael Waidner. *Low-level Ideal Signatures and General Integrity Idealization.* In Proceedings of 7th Information Security Conference (ISC), Palo Alto, CA, pages 39 - 51, volume 3225 of LNCS, September 2004.

169. Michael Backes and Dennis Hofheinz. *How to Break and Repair a Universally Composable Signature Functionality.* In Proceedings of 7th Information Security Conference (ISC), Palo Alto, CA, pages 61 - 72, volume 3225 of LNCS, September 2004.

170. Michael Backes and Birgit Pfitzmann. *Symmetric Encryption in A Simulatable Dolev-Yao Style Cryptographic Library.* In Proceedings of the 17th Computer Security Foundations Workshop (CSFW), Asilomar, CA, pages 204 - 218, June 2004.

171. Michael Backes, Markus Dürmuth, and Günter Karjoth. *Unification in Privacy Policy Evaluation – Translating EPAL into Prolog.* In Proceedings of 5th IEEE International Workshop on Policies for Distributed Systems and Networks (POLICY), New York, USA, pages 185 - 188, June 2004.

172. Michael Backes, Walid Bagga, Günter Karjoth, and Matthias Schunter. *Efficient Comparison of Privacy Policies.* In Proceedings of 19th ACM Symposium on Applied Computing (SAC), Nicosia, Cyprus, pages 375 - 382, March 2004.

173. Michael Backes, Birgit Pfitzmann, and Michael Waidner. *A General Composition Theorem for Secure Reactive Systems.* In Proceedings of 1st Theory of Cryptography Conference (TCC), Cambridge, MA, pages 336 - 354, volume 2951 of LNCS, February 2004.

174. Michael Backes and Birgit Pfitzmann. *A Cryptographically Sound Security Proof of the Needham-Schroeder-Lowe Public-key Protocol.* In Proceedings of the 23rd Conference on Foundations of Software Technology and Theoretical Computer Science (FSTTCS), Mumbai, India, pages 1 - 12, volume 2914 of LNCS, December 2003.

175. Michael Backes, Birgit Pfitzmann, and Michael Waidner. *A Composable Cryptographic Library with Nested Operations (Extended Abstract).* In Proceedings of 10th ACM Conference of Computer and Communications Security (CCS), Washington D.C., pages 220 - 230, October 2003.

176. Michael Backes, Birgit Pfitzmann, and Matthias Schunter. *A Toolkit for Managing Enterprise Privacy Policies.* In Proceedings of 8th European Symposium on Research in Computer Security (ESORICS), Gjøvik, Norway, pages 162 - 180, volume 2808 of LNCS, October 2003.

177. Michael Backes, Birgit Pfitzmann, and Michael Waidner. *Symmetric Authentication within a Simulatable Cryptographic Library.* In Proceedings of 8th European Symposium on Research in Computer Security (ESORICS), Gjøvik, Norway, pages 271 - 290, volume 2808 of LNCS, October 2003.

178. Michael Backes, Birgit Pfitzmann, and Michael Waidner. *Reactively Secure Signature Schemes.* In Proceedings of 6th Information Security Conference (ISC), Bristol, UK, pages 84-95, volume 2851 of LNCS, October 2003.

179. Michael Backes. *Unifying Simulatability Definitions in Cryptographic Systems under Different Timing Assumptions.* In Proceedings of 14th International Conference on Concurrency Theory (CONCUR), Marseille, France, pages 350-365, volume 2761 of LNCS, September 2003.

180. Michael Backes and Matthias Schunter. *From Absence of Certain Vulnerabilities towards Security Proofs – Pushing the Limits of Formal Verification.* In Proceedings of the 10th ACM Workshop on New Security Paradigms (NSPW), Ascona, Switzerland, pages 67 - 74, August 2003.

181. Michael Backes, Christian Cachin, and Reto Strobl. *Proactive Secure Message Transmission in Asynchronous Networks.* In Proceedings of 22nd ACM Symposium on Principles of Distributed Computing (PODC), Boston, MA, pages 223 - 232, July 2003.

182. Michael Backes, Catherine Meadows, and John C. Mitchell. *Relating cryptography and formal methods: a panel.* In Proceedings of ACM Workshop on Formal Methods in Security Engineering (FMSE), 61-66, 2003.

183. Michael Backes, Birgit Pfitzmann, and Michael Waidner. *Security in Business Process Engineering.* In Proceedings of the International Conference on Business Process Management (BPM), Eindhoven, The Netherlands, pages 168 - 183, volume 2678 of LNCS, June 2003.

184. Michael Backes and Christian Cachin. *Reliable broadcast in a computational hybrid model with Byzantine faults, crashes, and recoveries.* In Proceedings of the IEEE International Conference on Dependable Systems and Networks (DSN), San Francisco, CA, pages 37 - 46, June 2003.

185. Michael Backes and Birgit Pfitzmann. *Intransitive Non-Interference for Cryptographic Purposes.* In Proceedings of 24th IEEE Symposium on Security and Privacy, Oakland, CA, pages 140 - 152, May 2003.

186. Michael Backes and Christian Jacobi. *Cryptographically Sound and Machine-Assisted Verification of Security Protocols.* In Proceedings of 20th International Symposium on Theoretical Aspects of Computer Science (STACS), Berlin, Germany, pages 675 - 686, volume 2607 of LNCS, February 2003.

187. Michael Backes and Birgit Pfitzmann. *Computational Probabilistic Non-Interference.* In Proceedings of 7th European Symposium on Research in Computer Security (ESORICS), Zurich, Switzerland, pages 1 - 23, volume 2502 of LNCS, October 2002.

188. Michael Backes, Christian Jacobi, and Birgit Pfitzmann. *Deriving Cryptographically Sound Implementations Using Composition and Formally Verified Bisimulation.* In Proceedings of FME 2002: Getting it Right, 11th International Symposium on Formal Methods Europe '02, Copenhagen, Denmark, pages 310 - 329, volume 2391 of LNCS, July 2002.

189. Michael Backes, Birgit Pfitzmann, Michael Steiner, and Michael Waidner. *Polynomial Fairness and Liveness.* In Proceedings of 15th IEEE Computer Security Foundations Workshop (CSFW), Cape Breton, Nova Scotia, Canada, pages 160 - 174, June 2002.

Ph.D Thesis

190. Michael Backes. *Cryptographically Sound Analysis of Security Protocols.* Ph.D thesis, Department of Computer Science, Saarland University, Germany, 2002.

Master Theses

191. Michael Backes. *New Number-theoretic Assumptions in Cryptography (in german).* Master thesis, Department of Computer Science, Saarland University, Germany, 2001.

192. Michael Backes. *Factorization of Univariate Polynomials.* Master thesis, Department of Mathematics, Saarland University, Germany, 2002.

Edited

193. Michael Backes. *Proceedings of the 1st IEEE European Symposium on Security & Privacy (EuroS&P)*, March 2016.

194. Michael Backes, Adrian Perrig, and Helen Wang. *Proceedings of the 35th IEEE Symposium on Security & Privacy (S&P)*, May 2014.

195. Wenke Lee, Michael Backes, and Adrian Perrig. *Proceedings of the 34th IEEE Symposium on Security & Privacy (S&P)*, May 2013.

196. Michael Backes and Steve Zdancewic. *Special Issue of Journal of Computer Security (Best Papers of IEEE CSF'11)*, 2013.

197. Andrew Myers and Michael Backes. *Special Issue of Journal of Computer Security (Best Papers of IEEE CSF'10)*, 2012.

198. Michael Backes and Steve Zdancewic. *Proceedings of the 24rd IEEE Computer Security Foundations Symposium (CSF)*, June 2011.

199. Andrew Myers and Michael Backes. *Proceedings of the 23rd IEEE Computer Security Foundations Symposium (CSF)*, July 2010.

200. Michael Backes and Peng Ning. *Proceedings of 14th European Symposium on Research in Computer Security (ESORICS)*, September 2009.

201. Michael Backes, Stefanos Gritzalis, Bart Preneel, Sokratis Katsikas, and Javier Lopez. *Proceedings of 9th International Conference on Information Security (ISC)*, August 2006.

202. Michael Backes and Andre Scedrov. *Proceedings of 3rd International Workshop on Security Issues in Concurrency (SecCo)*, affiliated with CONCUR'05, San Francisco, October 2005. In Electronic Notes in Theoretical Computer Science, 180(1), 2007.

203. Michael Backes, David Basin, and Michael Waidner. *Special Issue of Journal of Computer Security (Best Papers of FMSE'04)*, 2005.

204. Michael Backes, David Basin, and Michael Waidner. *Proceedings of 2nd ACM Workshop on Formal Methods in Security Engineering (FMSE)*, affiliated with ACM CCS'04, Washington D.C., October 2004.

205. Michael Backes, David Basin, and Michael Waidner. *Proceedings of 1st ACM Workshop on Formal Methods in Security Engineering (FMSE)*, affiliated with ACM CCS'03, Washington D.C., October 2003.

Book Chapters

206. Michael Backes and Markus Dürmuth. *Enterprise Privacy Policies and Languages.* In Digital Privacy: Theory, Technologies and Practices.

207. Michael Backes, Birgit Pfitzmann, and Michael Waidner. *Justifying a Dolev-Yao Model under Active Attacks.* In Special Issue of International School of Foundations of Security Analysis and Design (FOSAD), LNCS.

Position Papers

208. Michael Waidner, Michael Backes, and Jörn Müller-Quade. *Runder Tisch der Bundesregierung - Sicherheitstechnik im IT-Bereich*, Positionspaper CISPA, EC-SPRIDE, KASTEL und Fraunhofer SIT, September 2013. `https://www.sit.fraunhofer.de/fileadmin/dokumente/studien_und_technical_reports/Positionspapier_IT-Sicherheit_Forschung.pdf`

209. Michael Waidner, Michael Backes, and Jörn Müller-Quade. *Entwicklung sicherer Software durch Security by Design*, Trend- und Strategieberich, Fraunhofer SIT Technical Reports SIT-TR-2013-01, September 2013. `http://www.kastel.kit.edu/downloads/Entwicklung_sicherer_Software_durch_Security_by_Design.pdf`

210. Peter Druschel, Michael Backes, and Rodica Tirtea. *The right to be forgotten - between expectations and practice*. Report of the European Agency for Network and Information Security (ENISA), November 20th, 2012. `https://www.enisa.europa.eu/activities/identity-and-trust/library/deliverables/the-right-to-be-forgotten`

211. Michael Backes, Jürgen Beyerer, Claudia Eckert, Hannes Federrath, Peter Martini, Günter Müller, Jörn Müller-Quade, Christof Paar, Kai Rannenberg, Ahmad-Reza Sadeghi, and Michael Waidner. *IT-Sicherheitsforschung im EU-Forschungsprogramm Horizon 2020*, Positionspaper Bitkom, Juni 2012. `http://www.bitkom.org/files/documents/Gemeinsames_Positionspapier_zur_IT-Sicherheitsforschung_im_Programm_Horizon_2020.pdf`

Peer-reviewed Works without Proceedings (selection)

212. Michael Backes, Pascal Berrang, Anne Hecksteden, Mathias Humbert, Andreas Keller and Tim Meyer. *Tracking Personal MicroRNA Expression Profiles over Time*. Grande Region Security and Reliability Day (GRSRD) 2016.

213. Michael Backes, Pascal Berrang, Anne Hecksteden, Mathias Humbert, Andreas Keller and Tim Meyer. *On Epigenomic Privacy: Tracking Personal MicroRNA Expression Profiles over Time*. Workshop on Understanding and Enhancing Online Privacy (UEOP), affiliated with NDSS'16, 2016.

214. Michael Backes, Praveen Manoharan and Pascal Berrang. *How well do you blend into the crowd? d-convergence: A novel paradigm for quantifying privacy in the age of Big-Data*. Grande Region Security and Reliability Day (GRSRD) 2015.

215. Michael Backes, Pascal Berrang and Praveen Manoharan. *Assessing the Effectiveness of Countermeasures Against Authorship Recognition*. Grande Region Security and Reliability Day (GRSRD) 2015.

216. Michael Backes, Aniket Kate, Praveen Manoharan, Sebastian Meiser and Esfandiar Mohammadi. *MATor: Towards Measuring the Degree of Anonymity in Tor*. Grande Region Security and Reliability Day (GRSRD) 2015.

217. Michael Backes, Esfandiar Mohammadi and Tim Ruffing. *Bridging the Gap from Trace Properties to Uniformity*. Grande Region Security and Reliability Day (GRSRD) 2014.

218. Michael Backes, Aniket Kate, Sebastian Meiser and Tim Ruffing. *Differential Indistinguishability for Cryptography with (Bounded) Weak Sources*. Grande Region Security and Reliability Day (GRSRD) 2014.

219. Michael Backes, Fabian Bendun, Peter Druschel and Milivoj Simeonovski. *Mitigating privacy leaks by controlling the discoverability of online information*. Grande Region Security and Reliability Day (GRSRD) 2014.

220. Michael Backes, Aniket Kate, Praveen Manoharan, Sebastian Meiser, and Esfandiar Mohammadi. *AnoA: A Framework for Analyzing Anonymous Communication Protocols.* 6th Workshop on Hot Topics in Privacy Enhancing Technologies (HotPETs 2013), Bloomington, USA.

221. Michael Backes, Fabian Bendun, Matteo Maffei and Esfandiar Mohammadi. *A Computationally Sound, Symbolic Abstraction for Malleable Zero-knowledge Proofs.* Grande Region Security and Reliability Day (GRSRD) 2013.

222. Michael Backes, Aniket Kate, Praveen Manoharan, Sebastian Meiser and Esfandiar Mohammadi. *AnoA: A Framework For Analyzing Anonymous Communication Protocols.* Grande Region Security and Reliability Day (GRSRD) 2013.

223. Michael Backes, Dario Fiore and Esfandiar Mohammadi. *Privacy-Preserving Accountable Computation.* Grande Region Security and Reliability Day (GRSRD) 2013.

224. Michael Backes, Jeremy Clark, Peter Druschel, Aniket Kate and Milivoj Simeonovski. *Introducing Accountability to Onion Routing.* Grande Region Security and Reliability Day (GRSRD) 2013.

225. Michael Backes, Fabian Bendun and Esfandiar Mohammadi. *Towards Composable Computational Soundness for Signatures and Zero-Knowledge Proofs.* 7th Workshop on Formal and Computational Cryptography (FCC), Cambridge, MA, 2012.

226. Michael Backes, Fabian Bendun and Dominique Unruh. *Computational Soundness of Symbolic Zero-knowledge Proofs: Weaker Assumptions and Mechanized Verification.* 7th Workshop on Formal and Computational Cryptography (FCC), Cambridge, MA, 2012.

227. Michael Backes, Gilles Barthe, Matthias Berg, Benjamin Grgoire, Csar Kunz, Malte Skoruppa and Santiago Zanella Bguelin. *Verifiable Security of Merkle-Damgard: towards the Formal Verification of SHA-3 Finalists.* Grande Region Security and Reliability Day (GRSRD) 2012.

228. Michael Backes, Matteo Maffei and Kim Pecina. *Automated Synthesis of Privacy-Preserving Distributed Applications.* Grande Region Security and Reliability Day (GRSRD) 2012.

229. Michael Backes, Aniket Kate, Matteo Maffei and Kim Pecina. *ObliviAd: Provably Secure and Practical Online Behavioral Advertising.* Grande Region Security and Reliability Day (GRSRD) 2012.

230. Michael Backes and Sebastian Meiser. *Differentially Private Smart Metering with Battery Recharging.* Grande Region Security and Reliability Day (GRSRD) 2012.

231. Michael Backes, Ian Goldberg, Aniket Kate and Esfandiar Mohammadi. *Provably Secure and Practical Onion Routing.* Grande Region Security and Reliability Day (GRSRD) 2012.

232. Michael Backes and Esfandiar Mohammadi. *Computational Soundness of Malleable Zero-Knowledge Proofs.* 6th Workshop on Formal and Computational Cryptography (FCC), Tartu, Estonia, 2011.

233. Michael Backes, Matteo Maffei, and Esfandiar Mohammadi. *Computationally Sound Abstraction and Verification of Secure Multi-Party Computations.* 6th Workshop on Formal and Computational Cryptography (FCC), Tartu, Estonia, 2011.

234. Michael Backes, Matthias Berg, Markus Mainberger, Christian Schmaltz and Joachim Weickert *SDI: Steganography with Diffusion Inpainting.* Grande Region Security and Reliability Day (GRSRD) 2011.

235. Michael Backes, Matteo Maffei and Esfandiar Mohammadi. *Computationally Sound Abstraction and Verification of Secure Multi-Party Computations.* Grande Region Security and Reliability Day (GRSRD) 2011.

236. Michael Backes, Stefan Lorenz, Matteo Maffei and Kim Pecina. *Anonymous Webs of Trust.* Grande Region Security and Reliability Day (GRSRD) 2010.

237. Michael Backes, Goran Doychev, Markus Dürmuth, and Boris Köpf. *Speaker Recognition in Encrypted Voice Streams.* Grande Region Security and Reliability Day (GRSRD) 2010.

238. Michael Backes. *On Machine-assisted Verification of Cryptography, and on Novel Eavesdropping Techniques.* Invited Talk Grande Region Security and Reliability Day (GRSRD) 2009.

239. Michael Backes, Martin Peter Grochulla, Catalin Hritcu and Matteo Maffei. *Achieving Security Despite Compromise Using Zero-Knowledge.* In Joint Workshop on Automated Reasoning for Security Protocol Analysis and Issues in the Theory of Security (ARSPA-WITS), York, UK, 2009.

240. Michael Backes, Catalin Hritcu, Matteo Maffei, and Thorsten Tarrach. *Type-checking Implementations of Protocols Based on Zero-knowledge Proofs.* 11th International Workshop on Foundations of Computer Security (FCS), 2009.

241. Michael Backes, Martin Grochulla, Catalin Hritcu, and Matteo Maffei. *Achieving Security Despite Compromise Using Zero-Knowledge.* 9th International Workshop on Issues in the Theory of Security (WITS), 2009.

242. Michael Backes, Matteo Maffei, and Dominique Unruh. *Computational Soundness of RCF Implementations.* 4th Workshop on Formal and Computational Cryptography (FCC), 2009.

243. Michael Backes, Dennis Hofheinz, and Dominique Unruh. *CoSP: A General Framework for Computational Soundness Proofs.* 4th Workshop on Formal and Computational Cryptography (FCC), 2009.

244. Michael Backes, Catalin Hritcu, and Matteo Maffei. *Type-checking Zero-knowledge.* 8th International Workshop on Issues in the Theory of Security (WITS), 2008.

245. Michael Backes, Matthias Berg, and Dominique Unruh. *A Formal Language for Cryptographic Pseudocode.* 3rd Workshop on Formal and Computational Cryptography (FCC), 2008.

246. Michael Backes, Markus Dürmuth, and Dominique Unruh. Datenspionage / Wie Brillenglser Geheimnisse verraten. In iX Magazin fr Professionelle Informationstechnik, Heise Verlag, Hannover, May 2008. In German.

247. Michael Backes, Markus Dürmuth, and Dominique Unruh. Bse Textdokumente Postscript gone wild. In iX Magazin fr Professionelle Informationstechnik, Heise Verlag, Hannover, August 2007. In German.

248. Michael Backes, Agostino Cortesi, Matteo Maffei, and Riccardo Focardi. *Causality-based Abstraction of Multiplicity in Security Protocol Analysis.* 7th International Workshop on Issues in the Theory of Security (WITS), Braga, Portugal, 2007.

249. Michael Backes, Agostino Cortesi, Matteo Maffei, and Riccardo Focardi. *A Calculus of Challenges and Reponses.* 7th International Workshop on Issues in the Theory of Security (WITS), Braga, Portugal, 2007.

250. Michael Backes, Anupam Datta, Ante Derek, John Mitchell, Ajith Ramanathan and Andre Scedrov. *Games and the Impossibility of Realizable Ideal Functionality.* 2nd Workshop on Formal and Computational Cryptography (FCC), 2006.

251. Michael Backes and Birgit Pfitzmann. *Soundness Limits of Dolev-Yao Models.* 2nd Workshop on Formal and Computational Cryptography (FCC), 2006.

252. Michael Backes and Peeter Laud. *Computationally Sound Secrecy Proofs by Mechanized Flow Analysis.* 2nd Workshop on Formal and Computational Cryptography (FCC), 2006.

253. Michael Backes, Birgit Pfitzmann, and Michael Waidner. *Limits of the Cryptographic Realization of Dolev-Yao-style XOR and Dolev-Yao-Style Hash Functions.* Abstract presented at 26th IEEE Symposium on Security and Privacy, Oakland, CA, 2005.

254. Michael Backes. *Justifying a Dolev-Yao Model under Active Attacks.* Abstract presented at 25th IEEE Symposium on Security and Privacy, Oakland, CA, 2004.

255. Michael Backes and Birgit Pfitzmann. *A Cryptographically Sound Security Proof of the Needham-Schroeder-Lowe Public-Key Protocol (Extended Abstract).* Workshop on Security Protocol Verification (SPV), affiliated with CONCUR'03, Marseille, France, 2003.

256. Michael Backes, Birgit Pfitzmann, and Michael Waidner. *Security and Privacy in the Modelling Process.* IBM Academy of Technology Workshop on Model Driven Technologies and Solutions, 2003.

Technical Reports

257. Kathrin Grosse, Praveen Manoharan, Nicolas Papernot, Michael Backes, Patrick D. McDaniel. *On the (Statistical) Detection of Adversarial Examples.* CoRR abs/1702.06280 (2017)

258. Michael Backes, Jrg Hoffmann, Robert Knnemann, Patrick Speicher, Marcel Steinmetz. *Simulated Penetration Testing and Mitigation Analysis.* CoRR abs/1705.05088 (2017)

259. Michael Backes, Mathias Humbert, Jun Pang, Yang Zhang. *walk2friends: Inferring Social Links from Mobility Profiles.* CoRR abs/1708.08221 (2017)

260. Giancarlo Pellegrino, Martin Johns, Simon Koch, Michael Backes, Christian Rossow. *Deemon: Detecting CSRF with Dynamic Analysis and Property Graphs.* CoRR abs/1708.08786 (2017)

261. Felix Fischer, Konstantin Bttinger, Huang Xiao, Christian Stransky, Yasemin Acar, Michael Backes, Sascha Fahl. *Stack Overflow Considered Harmful? The Impact of Copy & Paste on Android Application Security.* CoRR abs/1710.03135 (2017)

262. Yang Zhang, Mathias Humbert, Bartlomiej Surma, Praveen Manoharan, Jilles Vreeken, Michael Backes. *CTRL+Z: Recovering Anonymized Social Graphs.* CoRR abs/1711.05441 (2017)

263. Kathrin Grosse, David Pfaff, Michael Thomas Smith, Michael Backes. *How Wrong Am I? - Studying Adversarial Examples and their Impact on Uncertainty in Gaussian Process Machine Learning Models.* CoRR abs/1711.06598 (2017)

264. Sanam Ghorbani Lyastani, Michael Schilling, Sascha Fahl, Sven Bugiel, Michael Backes. *Studying the Impact of Managers on Password Strength and Reuse.* CoRR abs/1712.08940 (2017)

265. Kathrin Grosse, Nicolas Papernot, Praveen Manoharan, Michael Backes, Patrick D. McDaniel. *Adversarial Perturbations Against Deep Neural Networks for Malware Classification.* CoRR abs/1606.04435 (2016)

266. Michael Backes, Sven Bugiel, Oliver Schranz, Philipp von Styp-Rekowsky, Sebastian Weisgerber. *ARTist: The Android Runtime Instrumentation and Security Toolkit.* CoRR abs/1607.06619 (2016)

267. Michael Backes, Robert Knnemann, Esfandiar Mohammadi. *Computational Soundness for Dalvik Bytecode.* CoRR abs/1608.04362 (2016)

268. Fatemeh Shirazi, Milivoj Simeonovski, Muhammad Rizwan Asghar, Michael Backes, Claudia Diaz. *A Survey on Routing in Anonymous Communication Protocols.* CoRR abs/1608.05538 (2016)

269. Muhammad Rizwan Asghar, Michael Backes, Milivoj Simeonovski. *PRIMA: Privacy-Preserving Identity and Access Management at Internet-Scale.* CoRR abs/1612.01787 (2016)

270. Michael Backes, Amir Herzberg, Aniket Kate, Ivan Pryvalov. *Anonymous RAM.* IACR Cryptology ePrint Archive 2016: 678 (2016)

271. Michael Backes, Fabian Bendun, Jrg Hoffmann, and Ninja Marnau. *PriCL: Creating a Precedent A Framework for Reasoning about Privacy Case Law.* CoRR abs/1501.03353 (2015)

272. Michael Backes, Pascal Berrang, and Praveen Manoharan. *How well do you blend into the crowd? – d-convergence: A novel paradigm for quantifying privacy in the age of Big-Data.* CoRR abs/1502.03346 (2015)

273. Milivoj Simeonovski, Fabian Bendun, Muhammad Rizwan Asghar, Michael Backes, Ninja Marnau, and Peter Druschel. *Oblivion: Mitigating Privacy Leaks by Controlling the Discoverability of Online Information.* CoRR abs/1506.06033 (2015)

274. Michael Backes, Sven Bugiel, Sebastian Gerling, and Philipp von Styp-Rekowsky. *Android Security Framework: Enabling Generic and Extensible Access Control on Android.* CoRR abs/1404.1395 (2014)

275. Michael Backes, Niklas Grimm, and Aniket Kate: *Lime: Data Lineage in the Malicious Environment.* CoRR abs/1408.1076 (2014)

276. Michael Backes, Aniket Kate, Praveen Manoharan, Sebastian Meiser, and Esfandiar Mohammadi. *AnoA: A Framework For Analyzing Anonymous Communication Protocols.* IACR Cryptology ePrint Archive 2014: 87 (2014)

277. Michael Backes, Sven Bugiel, Sebastian Gerling, and Philipp von Styp-Rekowsky. *Android Security Framework: Enabling Generic and Extensible Access Control on Android*, Technical Report, Saarland University, 2014, A/01/2014.

278. Michael Backes, Dario Fiore, and Raphael M. Reischuk. *Nearly Practical and Privacy-Preserving Proofs on Authenticated Data.* IACR Cryptology ePrint Archive 2014: 617 (2014)

279. Michael Backes, Aniket Kate, Sebastian Meiser, and Esfandiar Mohammadi. *(Nothing else) MATor(s): Monitoring the Anonymity of Tor's Path Selection.* IACR Cryptology ePrint Archive 2014: 621 (2014)

280. Michael Backes, Özgür Dagdelen, Marc Fischlin, Sebastian Gajek, Sebastian Meiser, and Dominique Schröder: *Operational Signature Schemes.* IACR Cryptology ePrint Archive 2014: 820 (2014)

281. Michael Backes, Jeremy Clark, Peter Druschel, Aniket Kate, and Milivoj Simeonovski. *Introducing Accountability to Anonymity Networks.* CoRR abs/1311.3151 (2013)

282. Michael Backes, Sebastian Meiser, and Dominique Schröder. *Highly Controlled, Fine-grained Delegation of Signing Capabilities.* IACR Cryptology ePrint Archive 2013: 408 (2013)

283. Michael Backes, Dario Fiore, and Raphael M. Reischuk. *Verifiable Delegation of Computation on Outsourced Data.* IACR Cryptology ePrint Archive 2013: 469 (2013)

284. Michael Backes, Praveen Manoharan, and Esfandiar Mohammadi. *TUC: Time-sensitive and Modular Analysis of Anonymous Communication.* IACR Cryptology ePrint Archive 2013: 664 (2013)

285. Michael Backes, Sebastian Gerling, Christian Hammer, Matteo Maffei, and Philipp von Styp-Rekowsky. *AppGuard - Fine-grained Policy Enforcement for Untrusted Android Applications*, Technical Report, Saarland University, 2013, A/02/2013.

286. Michael Backes, Fabian Bendun, Ashish Choudhury, and Aniket Kate. *Asynchronous MPC with* $t < n/2$ *Using Non-equivocation.* IACR Cryptology ePrint Archive 2013: 745 (2013)

287. Michael Backes, Aniket Kate, Sebastian Meiser, and Tim Ruffing. *Differential Indistinguishability for Cryptographic Primitives with Imperfect Randomness.* IACR Cryptology ePrint Archive 2013: 808 (2013)

288. Michael Backes, Fabian Bendun, and Dominique Unruh. *2Computational Soundness of Symbolic Zero-knowledge Proofs: Weaker Assumptions and Mechanized Verification.* IACR Cryptology ePrint Archive 2012: 81 (2012)

289. Michael Backes, and Sebastian Meiser. *Differentially Private Smart Metering with Battery Recharging.* IACR Cryptology ePrint Archive 2012: 183 (2012)

290. Michael Backes, Ankit Malik, and Dominique Unruh. *Computational Soundness without Protocol Restrictions.* IACR Cryptology ePrint Archive 2012: 486 (2012)

291. Michael Backes, Amit Datta, and Aniket Kate. *Asynchronous Computational VSS with Reduced Communication Complexity.* IACR Cryptology ePrint Archive 2012: 619 (2012)

292. Michael Backes, Sebastian Gerling, Christian Hammer, Matteo Maffei, and Philipp von Styp-Rekowsky. *AppGuard - Real-time policy enforcement for third-party applications*, Technical Report, Saarland University, 2012, A/02/2012.

293. Michael Backes, Sebastian Gerling, and Philipp von Styp-Rekowsky. *A Novel Attack against Android Phones.* CoRR abs/1106.4184 (2011)

294. Michael Backes, Ian Goldberg, Aniket Kate, and Tomas Toft. *Adding Query Privacy to Robust DHTs.* CoRR abs/1107.1072 (2011)

295. Julian Backes, Michael Backes, Markus Dürmuth, Sebastian Gerling, and Stefan Lorenz. *X-pire! - A digital expiration date for images in social networks.* CoRR abs/1112.2649 (2011)

296. Michael Backes, Aniket Kate, and Arpita Patra. *Computational Verifiable Secret Sharing Revisited.* IACR Cryptology ePrint Archive 2011: 281 (2011)

297. Michael Backes, Ian Goldberg, Aniket Kate, and Esfandiar Mohammadi. *Provably Secure and Practical Onion Routing.* IACR Cryptology ePrint Archive 2011: 308 (2011)

298. Michael Backes, Matteo Maffei, and Dominique Unruh. *Computationally Sound Verification of Source Code.* IACR Cryptology ePrint Archive 2010: 416 (2010)

299. Michael Backes, Dennis Hofheinz, and Dominique Unruh. *CoSP: A General Framework For Computational Soundness Proofs.* IACR Cryptology ePrint Archive 2009: 80 (2009)

300. Michael Backes, and Dominique Unruh. *Computational soundness of symbolic zero-knowledge proofs.* IACR Cryptology ePrint Archive 2008: 152 (2008)

301. Michael Backes, and Boris Köpf. *Formally Bounding the Side-Channel Leakage in Unknown-Message Attacks.* IACR Cryptology ePrint Archive 2008: 162 (2008)

302. Michael Backes, and Dominique Unruh. *On the Security of Protocols with Logarithmic Communication Complexity.* IACR Cryptology ePrint Archive 2007: 169 (2007)

303. Michael Backes, Markus Dürmuth, and Ralf Küsters. *On Simulatability Soundness and Mapping Soundness of Symbolic Cryptography.* IACR Cryptology ePrint Archive 2007: 233 (2007)

304. Michael Backes, Matteo Maffei, and Dominique Unruh. *Zero-Knowledge in the Applied Pi-calculus and Automated Verification of the Direct Anonymous Attestation Protocol.* IACR Cryptology ePrint Archive 2007: 289 (2007)

305. Christoph Sprenger, Michael Backes, David A. Basin, Birgit Pfitzmann, and Michael Waidner. *Cryptographically Sound Theorem Proving.* IACR Cryptology ePrint Archive 2006: 47 (2006)

306. Michael Backes, Sebastian Mödersheim, Birgit Pfitzmann, and Luca Vigan. *Symbolic and Cryptographic Analysis of the Secure WS-ReliableMessaging Scenario.* IACR Cryptology ePrint Archive 2006: 58 (2006)

307. Michael Backes, Birgit Pfitzmann, and Michael Waidner. *Limits of the Reactive Simulatability/UC of Dolev-Yao Models with Hashes.* IACR Cryptology ePrint Archive 2006: 68 (2006)

308. Michael Backes, Markus Dürmuth, Dennis Hofheinz, and Ralf Küsters. *Conditional Reactive Simulatability.* IACR Cryptology ePrint Archive 2006: 132 (2006)

309. Michael Backes, Iliano Cervesato, Aaron D. Jaggard, Andre Scedrov, and Joe-Kai Tsay. *Cryptographically Sound Security Proofs for Basic and Public-Key Kerberos.* IACR Cryptology ePrint Archive 2006: 219 (2006)

310. Michael Backes, and Peeter Laud. *Computationally Sound Secrecy Proofs by Mechanized Flow Analysis.* IACR Cryptology ePrint Archive 2006: 266 (2006)

311. Michael Backes, Jörn Müller-Quade, and Dominique Unruh. *On the Necessity of Rewinding in Secure Multiparty Computation.* IACR Cryptology ePrint Archive 2006: 315 (2006)

312. Michael Backes, and Birgit Pfitzmann. *Limits of the Cryptographic Realization of Dolev-Yao-style XOR.* IACR Cryptology ePrint Archive 2005: 220 (2005)

313. Michael Backes, Dennis Hofheinz, Jörn Müller-Quade, and Dominique Unruh. *On Fairness in Simulatability-based Cryptographic Systems.* IACR Cryptology ePrint Archive 2005: 294 (2005)

314. Michael Backes, Christian Cachin, and Alina Oprea. *Secure Key-Updating for Lazy Revocation.* IACR Cryptology ePrint Archive 2005: 334 (2005)

315. Michael Backes, Birgit Pfitzmann, and Andre Scedrov. *Key-dependent Message Security under Active Attacks - BRSIM/UC-Soundness of Symbolic Encryption with Key Cycles.* IACR Cryptology ePrint Archive 2005: 421 (2005)

316. Michael Backes, and Birgit Pfitzmann. *Relating Symbolic and Cryptographic Secrecy.* IACR Cryptology ePrint Archive 2004: 300 (2004)

317. Michael Backes, Birgit Pfitzmann, and Michael Waidner. *The Reactive Simulatability (RSIM) Framework for Asynchronous Systems.* IACR Cryptology ePrint Archive 2004: 82 (2004)

318. Michael Backes, and Birgit Pfitzmann. *Symmetric Encryption in a Simulatable Dolev-Yao Style Cryptographic Library.* IACR Cryptology ePrint Archive 2004: 59 (2004)

319. Michael Backes, and Dennis Hofheinz. *How to Break and Repair a Universally Composable Signature Functionality.* IACR Cryptology ePrint Archive 2003: 240 (2003)

320. Michael Backes, and Christian Cachin. *Public-Key Steganography with Active Attacks.* IACR Cryptology ePrint Archive 2003: 231

321. Michael Backes, Birgit Pfitzmann, and Michael Waidner. *Symmetric Authentication Within a Simulatable Cryptographic Library.* IACR Cryptology ePrint Archive 2003: 145 (2003)

322. Michael Backes, and Birgit Pfitzmann. *A Cryptographically Sound Security Proof of the Needham-Schroeder-Lowe Public-Key Protocol.* IACR Cryptology ePrint Archive 2003: 121 (2003)

323. Michael Backes. *Unifying Simulatability Definitions in Cryptographic Systems under Different Timing Assumptions.* IACR Cryptology ePrint Archive 2003: 114 (2003)

324. Michael Backes, Birgit Pfitzmann, and Michael Waidner. *A Universally Composable Cryptographic Library.* IACR Cryptology ePrint Archive 2003: 15 (2003)

Patents filed

325. Michael Backes, Günter Karjoth, Birgit Pfitzmann, Matthias Schunter, and Michael Waidner. *Creating a privacy policy from a process model and verifying the compliance*, US20080294480 A1.

326. Michael Backes, Shmuel Ben-Yehuda, Jan Leonhard Camenisch, Ton Engbersen, Zorik Machulsky, Julian Satran, Leah Shalev, Ilan Shimony, Thomas Basil Smith, and Michael Waidner. *Memory protection and security using credentials*, US7757280 B2, US8161287 B2, and US8650406 B2.

327. Michael Backes, Thomas R. Gross, and Günter Karjoth. *Tag identification system*, US8009016 B2.

328. Michael Backes, Christian Cachin, Sastry Duri, Günter Karjoth, and Luke O'Connor, *Method and device for detecting an invalid RFID tag and method for manufactoring an RFID tag.* US20070194879 A1.

329. Michael Backes, Thomas R. Gross, Günter Karjoth, Luke J. O'Connor. *Verification Method and System for Tags*, US20080136586 A1.

330. Michael Backes, Günter Karjoth, and Luke O'Connor. *Detecting a blocker RFID tag*, US7847696 B2.