Trent Jaeger

Office Address:
Winston Chung Hall 442
Computer Science and Engineering Department
University of California, Riverside
Riverside, CA 92521
Email: trentj@ucr.edu and trentjaeger@gmail.com

Home Address:
2560 King Way
Claremont, CA 91711

Education

- Ph.D., Computer Science and Engineering, University of Michigan, Ann Arbor, 1997
  Thesis: *Flexible Control of Downloaded Executable Content*
  Advisor: Dr. Atul Prakash
- M.S.E., Computer Science and Engineering, University of Michigan, Ann Arbor, 1993
- B.S., Chemical Engineering, California State Polytechnic University, Pomona, 1985

Research Interests

Operating system security, trusted computing, software security, security policy analysis, program analysis for security, distributed systems (e.g., cloud, IoT, etc.) security, and operating systems design and implementation

Professional Experience

University of California, Riverside, CA
January 2024-Present *Computer Science and Engineering Professor*
Lead promotion of UCR Center for Research and Education in Cyber Security and Privacy (CRESP); research software and systems security; and teach security and operating systems courses

The Pennsylvania State University, University Park, PA
July 2005-December 2023 *Computer Science and Engineering Professor*
Co-director of the System Infrastructure and Internet Security (SIIS) Lab; research software and systems security; and teach security and operating systems courses

2013-2023 *Professor, Computer Science and Engineering Department*
2008-2013 *Associate Professor, Computer Science and Engineering Department*
2005-2008 *Untenured Associate Professor, Computer Science and Engineering Department*

Microsoft Research, Redmond, WA
August 2020-December 2020 *Visiting Researcher*
Research in systems and software security (sabbatical)

Hewlett-Packard Labs, Bristol, UK
February 2014-May 2014 *Visiting Scientist*
Research in binary analysis techniques and malware detection (sabbatical)

IBM Thomas J. Watson Research Center, Hawthorne, NY
2001-2005 *Research Staff Member, Security Department*
Research Liaison to the IBM Linux Technology Center to improve Linux security through contributions to the Linux Integrity Measurement Architecture (IMA), Linux Security Modules (LSM), and SELinux

1996-2001 *Research Staff Member, Systems Department*
Research in systems and security for microkernel-based and Linux operating systems

University of Michigan, Ann Arbor, MI
1992-1996 *Graduate Student Research Assistant, EECS Department*
Research security for mobile code and software engineering support for workflow systems

Bell Communications Research (Bellcore), Morristown, NJ
May 1995-September 1995 *Student Intern, Research Division, Network Security Department*
Research methods for securing the use of mobile code

General Motors, Warren, MI
May 1994-September 1994 *Student Intern, Manufacturing Information Systems*
Research mechanisms for adaptive, multi-agent systems

Electronic Data Systems, Troy, MI
1986-1991 *Advanced Knowledge Engineer, AI Services Department*
Built knowledge-based systems for gear set design, process planning, and manufacturing processes

Awards and Honors

- *ACM Fellow*, ACM, 2023
- *Outstanding Research Award*, Penn State Engineering Alumni Society, 2022
- *Outstanding Contributions Award*, ACM Special Interest Group in Security (SIGSAC), 2020
- *Associate Editor-in-Chief*, IEEE Security & Privacy, 2020-*present* (AE from 2018)
- *Android Security and PrIvacy REsearch* (ASPIRE) *Award*, Google, 2020
- *Editorial Board Member*, Communications of the ACM, 2020-*present*
- *Steering Committee Chair*, Network and Distributed Systems Security Symposium, 2019-2021
- *Chair of ACM Special Interest Group in Security* (SIGSAC), Elected July 2013-June 2017 term
- *Joel and Ruth Spira Excellence in Teaching Award*, 2017
- *Outstanding Teaching Award*, Penn State Engineering Alumni Society, CSE Nominee, 2014 and 2015
- *Steering Committee Chair*, ACM Conference on Computer and Communications Security, 2013-2014
- *Outstanding Teaching Award*, Penn State Computer Science and Engineering Department, 2012
- *Innovation Research Program Award*, Hewlett-Packard, 2011-12 (renewed for 2012-13)
- *University Research Program Award*, Cisco, 2007 (with La Porta and McDaniel)
- *Faculty Partnership Award*, IBM, 2006
- *Invited to present 18 Distinguished and Keynote Lectures*
- *Best Paper Awards*: ACM VEE 2020, SecureComm 2018
- *Best Student Paper Awards*: ACM SOSR 2017, USENIX Security 1996
- *Papers invited for journal publication*: ACM TISSEC/TOPS: 2000, 2001, 2002, and 2007
- *Steering Committee Membership* for NDSS (2018-2013), IEEE SecDev (2017-2020), ACM CCS (2013-present), ACM SACMAT (2001-2007)
- *Organizing Committee Chair* for IEEE Symposium on Security and Privacy 2024
- *Second Patent Plateau*, IBM, 2005
- *USYSA "D" certificate* (soccer coach), 2005

Trent Jaeger

Teaching Experience

University of California, Riverside (2024-present)

Courses Taught

CS 165	Computer Security (Undergraduate)

The Pennsylvania State University (2005-2023)
My teaching at Penn State has been recognized with two teaching awards:

- Joel and Ruth Spira Excellence in Teaching Award, 2017
- Outstanding Teaching Award, Penn State Computer Science and Engineering Department, 2012

Courses Taught
My SRTE scores for "overall quality of the instructor" have exceeded 5.25 out of 7.0 for all courses taught since at least Fall 2008

CMPSC 443	Introduction to Computer and Network Security **(co-developed, 2006)**
CMPSC 447	Software Security **(developed, 2018)**
CMPSC 473	Introduction to Operating Systems
CSE 543	Computer and Network Security
CSE 544	Advanced Systems Security **(developed, 2010)**
CSE 597	Systems Security Seminar
CSE 598	Verification Methods for Security **(developed, 2011)**

Programs Developed
Cybersecurity Computational Foundations Minor – Minor Degree Program now offered at Penn State

Student Advising

Ph.D. Advisor for

- Yu-Tsung Lee, *Tackling Filesystem Vulnerabilities in Android*, June 2024 (First Job: R&D Engineer at Samsung Research, USA)
- Giuseppe Petracca, *Regulating Programs' Access to Privacy-Sensitive Sensors*, July 2018 (First Job: Senior Security Engineer at Lyft, now at Rippling)
- Yuqiong Sun, *Protecting IAAS Clouds through Control of Cloud Services*, October 2016 (First Job: Principal Research Engineer at Symantec Research Labs, now at Meta)
- Xinyang Ge, *Enforcing Execution Integrity for Software Systems,* August 2016 (First Job: Researcher at Microsoft Research, now at Databricks)
- Hayawardh Vijayakumar, *Protecting Programs During Resource Access*, February 2014 (First Job: R&D Engineer at Samsung Research, USA)
- Divya Muthukumaran, *Automating the Placement of Authorization Hooks in Programs*, August 2013 (First Job: Postdoc at Imperial College, UK, now at Simply Business, UK)
- Joshua Seratelli Schiffman, *Practical System Integrity in Cloud Computing Environments*, July 2012 (First Job: Member of Technical Staff at AMD, now at HP Labs)
- Sandra Rueda Rodriguez, *Methods for Specifying, Evaluating, and Resolving Security Policy Compliance Problems*, July 2011 (First Job: Assistant Professor at Universidad de los Andes, Bogota, Colombia and she is now a tenured Associate Professor at Universidad de los Andes)

- David H. King, *Retrofitting Programs for Complete Security Mediation*, August 2009 (co-advised with John Hannan) (First Job: Security Engineer at Rackspace, now at Atlassian)

Current Ph.D. Advisees

- Aditya Basu, CSE Ph.D., expected graduation Summer 2024 (co-advised with Jack Sampson)
- Kaiming Huang, CSE Ph.D., expected graduation Fall 2024 (co-advised with Jack Sampson)
- Mingming Chen, CSE Ph.D., expected graduation Fall 2024 (co-advised with Thomas La Porta)
- Rahul George, CSE Ph.D., expected graduation Fall 2025

Grants Awarded

Total funding awarded of over $65M. The Penn State share of total funding awarded is approximately $22M. All co-PIs listed are from Penn State unless otherwise noted.

- **PI**, *Google Android Security and PrIvacy REsearch (ASPIRE) Award*, November 2020, $130,000
- **Co-PI**, *Defense Advanced Research Projects Agency, GAPS Program,* Secure Handling of Isolated Executables without Leaking Data (SHIELD) (w/ Gang Tan), September 2019-February 2024, $650,000 (subcontract to Perspecta Labs)
- **PI**, *Department of Defense, Small Business Innovation Research*, Program: Information Flow Control for Microkernels, AF191-063, Security Information Flow Control Study, July 2019-March 2020, $50,000 (sub-award from Trusted Science and Technology Inc.)
- **PI**, *Army Research Lab, Cyber Security Collaborative Research Alliance*, MACRO: Models for Enabling Continuous Reconfigurability of Secure Missions, renewal for second five-year phase (w/ 16 other PIs from Penn State, CMU, UC Davis, UC Riverside, Northeastern, IBM, and Perspecta Labs), October 2018-December 2023, $24,100,000 (PSU ~$6M)
- **Co-PI**, *National Science Foundation (SaTC:CORE:Medium:Collaborative Research)*, CNS-1801534, Threat-Aware Defenses: Evaluating Threats for Continuous Improvement (w/ Purdue, PI Mathias Payer and Gang Tan), August 2018-July 2022, $1,200,000 (PSU: $800,000)
- **PI**, *National Science Foundation (SaTC:CORE:Small)*, CNS-1816282, Information Flow Control Infrastructure for Single-Use Service Platforms (w/ Danfeng Zhang), August 2018-July 2021, $500,000
- **Co-PI**, *Office of Naval Research*, Data-driven Vulnerability Repair in Programs with a Cloud Analytics Architecture for Practical Deployment (w/ Virginia Tech, PI Daphne Yao), July 2017-June 2020, $1,200,000 (PSU: ~$333,000)
- **PI**, *Symantec Research Labs*, Intrusion Detection Systems for Cloud Computing*,* December 2014, $70,000
- **PI**, *National Science Foundation (TWC:Medium:Collaborative Research)*, CNS-1408880, Retrofitting Software for Defense-in-Depth (w/ Rutgers, Vermont, and Lehigh), September 2014-August 2018, $1,200,000 (PSU: $300,000)
- **Co-PI**, *Army Research Lab, Cyber Security Collaborative Research Alliance*, MACRO: Models for Enabling Continuous Reconfigurability of Secure Missions (w/ 16 other PIs from Penn State, CMU, Indiana, UC Davis, UC Riverside), October 2013-September 2018, $24,100,000 (PSU:~$6M)
- **Co-PI**, *Defense Advanced Research Projects Agency, VET Program*, Vetting Whole COTS Systems for Safety Against Malicious Functionality (w/ CMU, PI David Brumley), October 2013-September 2017, $4,000,000 (PSU: $1,000,000)
- **PI**, *Applied Communication Sciences, Cisco, Google, Hewlett-Packard, Microsoft, and Wave Systems,* Trusted Infrastructure Workshop 2013 Sponsorship*,* June 2013, $30,000
- **PI**, *US Department of Defense,* Trusted Infrastructure Workshop 2013 Sponsorship*,* June 2013-September 2013, $40,000

Trent Jaeger

- **PI**, *National Science Foundation,* Trusted Infrastructure Workshop 2013 Sponsorship, June 2013-August 2013, $15,000
- **PI**, Army *CERDEC subcontract via Telcordia*, Security Mobile Communications Program, October 2012-April 2014, $150,000
- **PI**, *Air Force Office of Scientific Research*, Information Flow Integrity for Systems of Independently-Developed Components (w/ Rutgers and Wisconsin), April 2012-March 2015, $729,466 (PSU: ~$300,000)
- **PI**, *Army Research Laboratory*, Automating Intrusion Monitor Placement for Defensive Mediation in Attack Graphs, October 2011-September 2013, $334,000
- **PI**, *National Science Foundation (TC:Small)*, CNS-1117692, Towards Customer-Centric Utility Computing, September 2011-August 2014, $488,024
- **PI**, *Hewlett-Packard Corporation*, Innovation Research Program Award, Towards Mostly-Automatic, System-Wide Integrity Policy Generation, August 2011-July 2012, $75,000, *renewed for 2012-13 for an additional $75,000*
- **Co-PI**, *National Science Foundation (TC),* CNS-1057312, Workshop on Trustworthy Computing Program (w/ PI Adam Smith), September 2010-June 2012, $254,019
- **Co-PI**, *Lockheed Martin Corporation*, Smart Grid Cyber Security Research (w/ PI Patrick McDaniel), January 2010-December 2010, $250,000
- **PI**, *National Science Foundation (TC:Medium),* CNS-0905343, Techniques to Retrofit Legacy Code with Security (w/ Maryland, Wisconsin, and Purdue), September 2009-September 2013, $1,200,000 (PSU: $300,000)
- **Co-PI**, *National Science Foundation (CPS:Small),* CPS-0931914, Establishing Integrity in Dynamic Networks of Cyber Physical Devices (w/ Rutgers), September 2009-August 2013, $540,000 (PSU: $180,000)
- **Co-PI**, *Defense University Research Instrumentation Program (DURIP), Army Research Office (ARO),* Characterizing and Mitigating Wireless Systems Vulnerabilities, May 2009-May 2010, $150,000
- **PI**, *Telcordia Corporation*, Verifiable Configuration Synthesis and Debugging for High Assurance Platform, May 2009-August 2009, $8,661
- **PI**, *Air Force Research Lab (AFRL),* Policy Analysis Tools for XSM/Flask, January 2009-January 2010, $193,000
- **Co-PI**, *Ben Franklin Technology Partners*, Center of Excellence (Penn State NSRC), 2008-2009, $75,000
- **Sr. Personnel**, *National Science Foundation (MRI),* Acquisition of a Scalable Instrument for Discovery through Computing (w/ Raghavan (PI), Chen, Hudson, Kandemir, Smith), July 2008-June 2012, $1,255,500
- **PI**, *Air Force Research Lab (AFRL),* Policy Design and Analysis for XSM/Flask, June 2008-June 2009, $200,000
- **Co-PI**, *National Science Foundation (NETS)*, CNS-0721579, Protecting Services for Emerging Wireless Telecommunications Infrastructure (w/ La Porta (PI) and McDaniel), September 2007-September 2010, $658,200
- **PI**, *Disruptive Technology Office* (now IARPA)*,* System-Wide Information Flow Enforcement (w/ McDaniel), February 2007-August 2008, $500,000
- **Co-PI**, *Ben Franklin Technology Partners*, Center of Excellence (Penn State NSRC), 2007-2008, $75,000
- **Co-PI**, *Cisco Corporation*, University Research Program, Security Testbed for IMS/Internet Convergence (w/ La Porta (PI) and McDaniel), 2007, $100,000
- **PI**, *Samsung Electronics Corporation,* Integrity Protection for Linux Cellphones, January 2007-December 2007, $92,717
- **Co-PI**, *Raytheon via the Penn State Network Security Research Center,* Symbian Cellphone Attacks, January-December 2007, $50,000
- **PI**, *IBM Faculty Partnership Award,* Distributed Access Control and Attestation Mechanisms, 2006, $30,000

- **PI**, *National Science Foundation (CT:Small)*, CNS-0627551, Shamon: Systems Approaches to Composing Distributed Trust (w/ McDaniel), September 2006-August 2010, $400,000
- **Co-PI**, *Raytheon Corporation,* Symbian Cellphone Attacks (w/ La Porta (PI) and Yener), May-August 2006, $50,000
- **PI**, *Technology Collaborative via the Penn State Cyber Security Research*, An End-Host Security Analysis and Training Environment, January-May 2006, $5,000

Major Software Systems

University of California, Riverside

- Memory Safety Defense (*OptiSan**) — Analysis tool for optimizing the memory safety defense against stack spatial errors with a prescribed cost budget by selecting among multiple defenses

Penn State University

- Heap Memory Defense (*Uriah**) — Analysis tool for validating which heap objects satisfy spatial and type memory safety using temporal type safe allocation for comprehensive safety
- Stack Memory Defense (*DataGuard**) — A static and concolic analysis tool for validating which stack objects have only safe memory accesses to isolate those objects on an isolated Safe Stack
- Driver Isolation System (*LVD*/*KSplit**) — Automated methods to enable the secure isolation of modules in the Linux kernel applied to a variety of device drivers
- Access Control Analysis (*PolyScope**) — Multiple policy analysis that computes the specific attack operations to which adversaries are authorized by the combination of policies (for Android)
- Automated Exploit Analysis (*BOPC*+) — Block Oriented Programming for detecting whether software defenses, such as Control-Flow Integrity are sufficient to prevent vulnerability exploitation
- Linux Security Namespaces* — Linux namespace for specifying security configurations for visibility resources, including access control and integrity measurement
- Automated Privilege Separation (*PtrSplit/PrograMander*)* — Method for automating privilege separation of programs into separate processes to protect sensitive data from unauthorized access that addresses the challenge of marshaling pointer data between processes correctly
- Android Sensor Authorization (*EnTrust/Aware*+) — Android authorization mechanism extension to control when apps may use their authorized permissions to access mobile device sensors by requiring common user input events
- Cloud Computing Info Flow Control (*OpenStack Pileus*) — Extended OpenStack cloud that protects the execution of cloud users' commands by spawning cloud services for commands dynamically and governing services using decentralized information flow control
- Intel PT Linux (*Griffin**) — Linux kernel that uses the Intel Processor Trace (PT) feature to record control flow system-wide and enforce security policies, such as control-flow integrity
- CFI Policy Generation and Enforcement (*Kernel-CFI*+) — Automated method to retrofit kernel software (VMMs, microkernel systems, conventional kernels) to generate enforce the finest, stateless control flow integrity policies (as of 2019) (currently supports MINIX and FreeBSD)
- Android Sound Control (*AuDroid*) — Android authorization extension to control untrusted apps use of sensors to generate audio commands and/or snoop on users on their mobile device
- Cloud Platform (*CloudArmor*) — Hardened OpenStack cloud platform that leverages trusted computing to validate cloud nodes, mandatory enforcement over the execution of cloud commands, and user-configurable monitoring of compute instances
- TOCTTOU Defense (*Process Firewall**) — Protect processes from vulnerabilities during retrieval of system resources by automatically inferring programmer intent
- Authorization Hook — Automated placement of authorization hooks for legacy programs to mediate

Placement	"choices" made by client requests where necessary to enforce access policies
• TOCTTOU Testing (*STING+*)	Dynamic testing for name resolution vulnerabilities by detecting unsafe pathnames and replacing with malicious pathnames
• Mediation Placement	Automatically place runtime information flow mediation (declassification and endorsement) into legacy Java and C code
• Policy Compliance (*Hippocrates*)	Tool for compliance analysis of multiple network and host security policies with system-wide security requirements (e.g., firewall and SELinux)
• Integrity Verification Proxy	Bind secure communication channels to integrity requirements of one or more of the host endpoint VMs or cloud instances
• Async Attestation	Bind all web content (static and dynamic) with current system attestations
• *PALMS*	Information flow compliance checking tool for SELinux policies
• Root of Trust Installer	Bind integrity of a system to its installer to attest code and site-specific data
• Integrity-Verified Sys (*Shamon*)	Shared Reference Monitor System built using Xen, SELinux, Labeled IPsec, Linux IMA, to create a verifiable, distributed access control system
• Info Flow Browser (*FlowwolF)*	Information flow-aware web browser client built using Java and Jif and mechanisms (VM and SELinux) to ensure compliance with system policy
• High-Integrity Phones	Build Linux phones systems capable of protecting high-integrity processes from downloaded code (also supports integrity measurement via PRIMA)
• *Labeled IPsec+*	Authorize network access via SELinux using IPsec SAs (*in Linux mainline*)

IBM Research

• *Xen sHype+*	Reference monitor for Xen (in Xen 3.0)
• *PRIMA/IMA/LIM+*	Integrity measurement using secure hardware for Linux (*in Linux mainline*)
• *Gokyo+*	Graph-based access control policy analysis tool (applied to SELinux)
• *Vali+*	Tools for static and dynamic analysis of Linux security hooks
• *SawMill multiserver*	Linux multiserver on L4 including servers for ext2 file system, TCP networking, and various drivers
• *L4 microkernel*	Kernel security extensions, including policy server architecture, IPC redirection, and synchronous IPC over redirection
• *Lava Hit Server*	Maximum possible Ethernet throughput software stack
• *FlexxGuard*	Java authorization mechanism and policy model

University of Michigan

• Mobile Monitor	Reference monitors for downloaded mobile code runtimes
• *UARC*	Access control mechanisms and policy models for collaboration
• File Distribution	Download and authenticate files over untrusted network – Bellcore
• *BizSpec*	Business process reengineering system

EDS

• *GMGear*	Knowledge-based gear set design tool (LISP)
• *Shaft Planner*	Knowledge-based system to develop manufacturing plans automatically for transmission shafts (LISP)
• *Stacker*	Knowledge-based configuration of manufacturing equipment (C/OPS83)

* - maintaining as open source
+ - released as open source

Trent Jaeger

Publications

Books, Books Edited, and Book Chapters

1. Trent Jaeger and Zhiyun Qian, editors. *Proceedings of the 8th ACM Workshop on Moving Target Defense*, MTD '21, ACM, November 2021.
2. Vinod Ganapathy, Trent Jaeger, R.K. Shyamasundar, editors. *Proceedings of the 14th International Conference on Information Systems Security*, ICISS '18, Springer, December 2018.
3. Summer Craze Fowler and Trent Jaeger, editors. *Proceedings of the 2017 IEEE Cybersecurity Development* Conference, IEEE SecDev '17, IEEE, September 2017.
4. Shiho Moriai, Trent Jaeger, Kouichi Sakurai, editors. *Proceedings of the 9th ACM Symposium on Information, Computer and Communications Security*, ASIACCS '14, ACM, June 2014.
5. Trent Jaeger. Reference Monitor. In *Encyclopedia of Cryptography and Security,* H. van Tilborg (Ed.), Springer, 2011.
6. Trent Jaeger. *Operating Systems Security*. Synthesis Lectures on Information Security, Privacy and Trust, Morgan & Claypool Publishers, 2008 (218 pages).
7. Trent Jaeger and Jon Solworth, editors. *Proceedings of the 2nd ACM Computer Security Architectures Workshop*, ACM, October 2008.
8. Trent Jaeger, editor. *Proceedings of the 2nd USENIX Workshop on Hot Topics in Security*, USENIX, July 2007.
9. Trent Jaeger and Elena Ferrari, editors. *Proceedings of the 9th ACM Symposium on Access Control Models and Technologies*, ACM, June 2004.
10. Sushil Jajodia, Vijayalakshmi Atluri, and Trent Jaeger, editors. *Proceedings of the 10th ACM Conference on Computer and Communications Security*, ACM, October 2003.
11. Ravi Sandhu and Trent Jaeger, editors. *Proceedings of the 6th ACM Symposium on Access Control Models and Technologies*, ACM, June 2001.
12. Trent Jaeger. Access Control in Configurable Operating Systems. In *Secure Internet Programming: Security Issues for Mobile and Distributed Objects*, J. Vitek and C. Jensen (Eds.), Springer, 1999.

Refereed Journal Publications

1. Kaiming Huang, Mathias Payer, Zhiyun Qian, John Sampson, Gang Tan, Trent Jaeger. Comprehensive Memory Safety Validation: An Alternative Approach to Memory Safety. *IEEE Security & Privacy*, accepted for publication March 2024.
2. Zheng Fang, Hao Fu, Tainbo Gu, Pengfei Hu, Jinyue Song, Trent Jaeger, Prasant Mohapatra. Towards System-Level Security Analysis of IoT Using Attack Graphs. *IEEE Transactions on Mobile Computing* (IEEE TMC), 23(2), February 2024.
3. Yu-Tsung Lee, Haining Chen, William Enck, Hayawardh Vijayakumar, Ninghui Li, Zhiyun Qian, Giuseppe Petracca, Trent Jaeger. PolyScope: Multi-Policy Access Control Analysis to Triage Android Scoped Storage. *IEEE Transactions on Dependable and Secure Computing* (IEEE TDSC), IEEE Early Access, September 2023.
4. Quinn Burke, Fidan Mehmeti, Rahul George, Kyle Ostrowski, Trent Jaeger, Thomas La Porta, Patrick McDaniel. Enforcing Multilevel Security Policies in Unstable Networks. *IEEE Transactions on Network and Service Management* (IEEE TNSM), 19(3), September 2022.
5. Yu-Tsung Lee, Haining Chen, Trent Jaeger. Demystifying Android's Scoped Storage Defense. *IEEE Security & Privacy*, 19(5), September/October 2021. *Cover article*.
6. Long Cheng, Salman Ahmed, Hans Liljestrand, Thomas Nyman, Haipeng Cai, Trent Jaeger, N. Asokan, Danfeng Yao. Exploitation Techniques for Data-Oriented Attacks with Existing and Potential Defense

Approaches. *ACM Transactions on Privacy and Security* (ACM TOPS), formerly ACM Transactions on Information Systems Security, 24(4), September 2021.

7. Zheng Fang, Hao Fu, Tainbo Gu, Zhiyun Qian, Trent Jaeger, Pengfei Hu, Prasant Mohapatra. A Model Checking-Based Security Analysis Framework for IoT Systems. *Elsevier High-Confidence Computing*, 1(1), June 2021.
8. Amit Kumar Sikder, Giuseppe Petracca, Hidayet Aksu, Trent Jaeger, and A. Selcuk Uluagac. A Survey on Sensor-based Threats and Attacks to Smart Devices and Applications. *IEEE Communications Surveys and Tutorials*, 23(2), May 2021.
9. Stefan Achleitner, Quinn Burke, Patrick McDaniel, Trent Jaeger, Thomas La Porta, Srikanth Krishnamurthy. MLSNet: A Policy Complying Multilevel Security Framework for Software Defined Networking. *IEEE Transactions on Network and Service Management* (IEEE TNSM), 18(1), March 2021.
10. Zhen Huang, David Lie, Gang Tan, Trent Jaeger. Using Safety Properties to Generate Vulnerability Patches. USENIX *;login*, 45(4), Winter 2020.
11. Asmit De, Aditya Basu, Swaroop Ghosh, Trent Jaeger. Hardware Assisted Buffer Protection Mechanisms for Embedded RISC-V. *IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems* (IEEE TCAD), 39(12), December 2020.
12. Le Guan, Peng Liu, Xinyu Xing, Xinyang Ge, Shengzhi Zhang, Meng Yu, Trent Jaeger. Building a Trustworthy Execution Environment to Defeat Exploits from both Cyber Space and Physical Space for ARM. *IEEE Transactions on Dependable and Secure Computing* (IEEE TDSC), 16(3), May/June 2019.
13. Xiaokui Shu, Naren Ramakrishnan, Danfeng (Daphne) Yao, Trent Jaeger. Long-Span Program Behavior Modeling and Attack Detection. *ACM Transactions on Privacy and Security* (ACM TOPS), formerly ACM Transactions on Information Systems Security, 20(4), October 2017.
14. Adam Bates, Dave (Jing) Tian, Grant Hernandez, Kevin Butler, Trent Jaeger, Thomas Moyer. Taming the Costs of Trustworthy Provenance through Policy Reduction. *ACM Transactions on Internet Technology* (ACM TOIT), 17(4), September 2017.
15. Steve Lipner, Trent Jaeger, Mary Ellen Zurko. Lessons from VAX/SVS for High Assurance VM Systems. *IEEE Security & Privacy*, 10(5), September/October 2012.
16. Thomas Moyer, Kevin Butler, Joshua Schiffman, Patrick McDaniel, Trent Jaeger. Scalable Web Content Attestation. *IEEE Transactions on Computers* (IEEE ToC), 61(5), April 2012.
17. Trent Jaeger, Paul van Oorschot, Glenn Wurster. Countering Unauthorized Code Execution on Commodity Kernels: A Survey of Common Interfaces Allowing Kernel Code Modification. *Computers & Security*, 30(8), November 2011.
18. Divya Muthukumaran, Joshua Schiffman, Mohamed Hassan, Anuj Sawani, Vikhyath Rao, Trent Jaeger. Protecting the Integrity of Trusted Applications on Mobile Phone Systems. *Security and Communication Networks*, 4(6), June 2011.
19. Patrick Traynor, Vikhyath Rao, Trent Jaeger, Thomas La Porta, Patrick McDaniel. From Mobile Phones to Responsible Devices. *Security and Communication* Networks, 4(6), June 2011.
20. Joshua Schiffman, Trent Jaeger, Patrick McDaniel. Network-based Root of Trust for Installation. *IEEE Security & Privacy*, 9(1), Special Issue on Systems Security for January/February 2011.
21. Boniface Hicks, Sandra Rueda, Luke St. Clair, Trent Jaeger, and Patrick McDaniel. A Logical Specification and Analysis for SELinux MLS policy. *ACM Transactions on Information Systems Security* (ACM TISSEC), 13(3), July 2010.
22. Trent Jaeger, Antony Edwards, Xiaolan Zhang. Consistency Analysis of Authorization Hook Placement in the Linux Security Modules Framework. *ACM Transactions on Information Systems Security* (ACM TISSEC), 7(2), May 2004.
23. Trent Jaeger, Antony Edwards, Xiaolan Zhang. Policy Management Using Access Control Spaces. *ACM Transactions on Information Systems Security* (ACM TISSEC), 6(3), August 2003.
24. Trent Jaeger and Jonathon Tidswell. Practical Safety in Flexible Access Control Models. *ACM Transactions on Information Systems Security* (ACM TISSEC), 4(3), August 2001.
25. Trent Jaeger, Atul Prakash, Jochen Liedtke, Nayeem Islam. Flexible Control of Downloaded Executable Content. *ACM Transactions on Information Systems Security* (ACM TISSEC), 2(2), May 1999.

26. Nayeem Islam, Rangachari Anand, Trent Jaeger, Josyula R. Rao. A Flexible Security System for Using Internet Content. *IEEE Software*, 14(5), September/October 1997.

Refereed Conference and Workshop Publications

1. Rahul George, Mingming Chen, Kaiming Huang, Zhiyun Qian, Thomas La Porta, Trent Jaeger. OptiSan: Using Multiple Spatial Error Defenses to Optimize Stack Memory Protection within a Budget. In *Proceedings of the 33rd USENIX Security Symposium*, August 2024.
2. Yizhuo Zhai, Zhiyun Qian, Chengyu Song, Manu Sridharan, Trent Jaeger, Paul Yu, Srikanth Krishnamurthy. Don't Waste My Efforts: Pruning Redundant Sanitizer Checks of Developer-Implemented Type Checks. In *Proceedings of the 33rd USENIX Security Symposium*, August 2024.
3. Abdulrahman Fahim, Shitong Zhu, Zhiyun Qian, Chengyu Song, Vagelis Papalexakis, Supriyo Chakraborty, Kevin Chan, Paul Yu, Trent Jaeger, Srikanth Krishnamurthy. DNS Exfiltration Guided by Generative Adversarial Networks. In *Proceedings of the IEEE European Symposium on Security and Privacy* (Euro S&P), July 2024.
4. Mingming Chen, Tom La Porta, Trent Jaeger and Srikanth Krishnamurthy. Lightweight Coordinated Sampling for Dynamic Flows under Budget Constraints. In *Proceedings of the 33rd International Conference on Computer Communications and Networks* (ICCCN), July 2024.
5. Kaushal Kafle, Kirti Jagtap, Mansoor Ahmed-Rengers, Trent Jaeger, Adwait Nadkarni. Practical Integrity Validation in the Smart Home with HomeEndorser. In *Proceedings of the 17th Conference on Security and Privacy in Wireless and Mobile Networks* (WiSec), May 2024.
6. Xingyu Li, Zheng Zhang, Zhiyun Qian, Trent Jaeger, Chengyu Song. An Investigation of Patch Porting Practices of the Linux Kernel Ecosystem. In *Proceedings of the IEEE/ACM 21st International Conference on Mining Software Repositories* (MSR), April 2024.
7. Frank Capobianco, Quan Zhou, Aditya Basu, Trent Jaeger, Danfeng Zhang. Talisman: Tamper Analysis for Reference Monitors. In *Proceedings of the 2024 Network and Distributed Systems Security Symposium* (NDSS), February 2024. (acceptance rate: 15%)
8. Kaiming Huang, Jack Sampson, Trent Jaeger. Assessing the Impact of Efficiently Protecting Ten Million Stack Objects from Memory Errors Comprehensively. In *Proceedings of the 2023 IEEE Secure Development Conference* (IEEE SecDev), October 2023. (acceptance rate: 32%)
9. Yu-Tsung Lee, Rahul George, Haining Chen, Kevin Chan, Tina Eliassi-Rad, Trent Jaeger. Triaging Android Systems Using Bayesian Attack Graphs. In *Proceedings of the 2023 IEEE Secure Development Conference* (IEEE SecDev), October 2023. (acceptance rate: 32%)
10. Jiyong Yu, Aishani Datta, Trent Jaeger, David Kohlbrenner, Christopher Fletcher. Synchronization Storage Channels (S2C): Timer-less Cache Side-Channel Attacks on the Apple M1 via Hardware Synchronization Instructions. In *Proceedings of the 32nd USENIX Security Symposium*, August 2023. (acceptance rate: 29%)
11. Sebastian Angel, Aditya Basu, Weidong Cui, Trent Jaeger, Stella Lau, Srinath Setty, Sudheesh Singanamalla. Nimble: Rollback Protection for Confidential Cloud Services. In *Proceedings of the 17th USENIX Symposium on Operating Systems Design and Implementation* (OSDI), July 2023. *Artifact Available, Functional, and Reproduced Badges.* (acceptance rate: 20%)
12. Anton Burtsev, Vikram Narayanan, Yongzhe Huang, Kaiming Huang, Gang Tan, Trent Jaeger. Evolving Operating System Kernels Towards Secure Kernel-Driver Interfaces. In *Proceedings of the 19th Workshop on Hot Topics in Operating Systems* (HotOS), June 2023. (acceptance rate: 26%)
13. Naiqian Zhang, Daroc Alden, Dongpeng Xu, Shuai Wang, Trent Jaeger, Wheeler Ruml. No Free Lunch: On the Increased Code Reuse Attack Surface of Obfuscated Programs. In *Proceedings of the 53rd Annual IEEE/IFIP International Conference on Dependable Systems and Networks* (DSN), June 2023. (acceptance rate: 20%)
14. Jiyong Yu, Trent Jaeger, Christopher Fletcher. All your PC are belong to us: Exploiting Non-control-transfer Instruction BTB Updates for Dynamic PC Extraction. In *Proceedings of the 2023 International Symposium on Computer Architecture* (ISCA), June 2023. (acceptance rate: 21%)

15. Aditya Basu, Jack Sampson, Zhiyun Qian, Trent Jaeger. Unsafe at Any Copy: Name Collisions from Mixing Case Sensitivities. In *Proceedings of the 21st USENIX Conference on File and Storage Technologies* (FAST), February 2023. (acceptance rate: 23%)
16. Jiyong Yu, Xinyang Ge, Christopher Fletcher, Trent Jaeger, Weidong Cui. Pagoda: Towards Binary Code Privacy Protection with SGX-based Execute-Only Memory. In *Proceedings of the 2022 IEEE International Symposium on Secure and Private Execution Environment Design* (SEED), September 2022.
17. Yongzhe Huang, Vikram Narayanan, David Detweiler, Kaiming Huang, Gang Tan, Trent Jaeger, Anton Burtsev. KSplit: Automating Device Driver Isolation. In *Proceedings of the 16th USENIX Symposium on Operating Systems Design and Implementation* (OSDI), July 2022. *Artifact Available, Functional, and Reproduced Badges.* (acceptance rate: 19%)
18. Zheng Fang, Hao Fu, Tainbo Gu, Pengfei Hu, Jinyue Song, Trent Jaeger, Prasant Mohapatra. Iota: A Framework for Analyzing System-Level Security of IoTs. In *Proceedings of the ACM/IEEE International Conference on Internet of Things Design and Implementation* (IoTDI), May 2022. (acceptance rate: 30%)
19. Yizhuo Zhai, Yu Hao, Zheng Zhang, Weiteng Chen, Guoren Li, Zhiyun Qian, Chengyu Song, Manu Sridharan, Srikanth Krishnamurthy, Trent Jaeger, Paul Yu. Progressive Scrutiny: Incremental Detection of UBI bugs in the Linux Kernel. In *Proceedings of the 2022 Network and Distributed System Security Symposium* (NDSS), April 2022. (acceptance rate: 16%)
20. Kaiming Huang, Yongzhe Huang, Mathias Payer, Zhiyun Qian, Jack Sampson, Gang Tan, Trent Jaeger. The Taming of the Stack: Isolating Stack Data from Memory Errors. In *Proceedings of the 2022 Network and Distributed System Security Symposium* (NDSS), April 2022. (acceptance rate: 16%)
21. Yu-Tsung Lee, William Enck, Haining Chen, Hayawardh Vijayakumar, Ninghui Li, Zhiyun Qian, Daimeng Wang, Giuseppe Petracca, Trent Jaeger. PolyScope: Multi-Policy Access Control Analysis to Compute Authorized Attack Operations in Android Systems. In *Proceedings of the 30th USENIX Security Symposium*, August 2021. (acceptance rate: 19%)
22. Wenhui Zhang, Peng Liu, Trent Jaeger. Analyzing the Overhead of File Protection by Linux Security Modules. In *Proceedings of the 16th ACM Asia Conference on Computer and Communications Security* (ACM AsiaCCS), June 2021. (acceptance rate: 19%)
23. Zhen Huang, Trent Jaeger, Gang Tan. Fine-grained Program Partitioning for Security. In *Proceedings of the 14th European Workshop on Systems Security* (EuroSec), April 2021.
24. Christian Skalka, David Darais, Trent Jaeger, Frank Capobianco. Types and Abstract Interpretation for Authorization Hook Advice. In *Proceedings of the 2020 IEEE Computer Security Foundations Symposium* (CSF), June 2020. (acceptance rate: 24%)
25. Vikram Narayanan, Yongzhe Huang, Gang Tan, Trent Jaeger, Anton Burtsev. Lightweight Kernel Isolation with Virtualization and VM Functions. In *Proceedings of the 16th ACM SIGPLAN/SIGOPS International Conference on Virtual Execution Environments* (VEE), March 2020. **Best Paper Award**. (acceptance rate: 41%)
26. Shen Liu, Dongrui Zeng, Yongzhe Zhang, Frank Capobianco, Stephen McCammant, Trent Jaeger, Gang Tan. Program-mandering: Quantitative Privilege Separation. In *Proceedings of the 26th ACM Conference on Computer and Communications Security* (ACM CCS), November 2019. (acceptance rate: 16%)
27. Zheng Fang, Hao Fu, Tainbo Gu, Zhiyun Qian, Trent Jaeger, Prasant Mohapatra. FORESEE: A Cross-Layer Vulnerability Detection Framework for the Internet of Things. In *Proceedings of the 16th IEEE International Conference on Mobile Ad-Hoc and Smart Systems* (IEEE MASS), November 2019.
28. Frank Capobianco, Rahul George, Kaiming Huang, Trent Jaeger, Mathias Payer, Srikanth Krishnamurthy, Zhiyun Qian, Paul Yu. Employing Attack Graphs for Intrusion Detection. In *Proceedings of the 2019 New Security Paradigms Workshop* (NSPW), September 2019.
29. Long Cheng, Hans Liljestrand, Thomas Nyman, Danfeng Yao, Trent Jaeger, N. Asokan. Exploitation Techniques and Defenses for Data-Oriented Attacks. In *Proceedings of the 2019 IEEE Secure Development Conference* (IEEE SecDev), September 2019. (acceptance rate: 36%)
30. Giuseppe Petracca, Yuqiong Sun, Ahmad-Atamli Reineh, Jens Grossklags, Patrick McDaniel, Trent Jaeger.

EnTrust: Regulating Sensor Access by Cooperating Programs via Delegation Graphs. In *Proceedings of the 28th USENIX Security Symposium*, August 2019. (acceptance rate: 16%)

31. Zhen Huang, David Lie, Gang Tan, Trent Jaeger. Using Safety Properties to Generate Vulnerability Patches. In *Proceedings of the 40th IEEE Symposium on Security & Privacy* (IEEE S&P), May 2019. (acceptance rate: 12%)
32. Asmit De, Aditya Basu, Trent Jaeger, Swaroop Ghosh. FIXER: Flow Integrity Extensions for Embedded RISC-V. In *Proceedings of the 2019 Design, Automation, and Test in Europe Conference & Exhibition* (DATE), March 2019. (acceptance rate: 23%)
33. Kyriakos Ispoglou, Bader Al Bassam, Trent Jaeger, Mathias Payer. Block Oriented Programming: Automating Data-Only Attacks. In *Proceedings of the 25th ACM Conference on Computer and Communications Security* (ACM CCS), October 2018. (acceptance rate: 17%)
34. Yuqiong Sun, David Safford, Mimi Zohar, Dimitrios Pendarakis, Zhongshu Gu, Trent Jaeger. Security Namespace: Making Linux Security Frameworks Available to Containers. In *Proceedings of the 27th USENIX Security Symposium*, August 2018. (acceptance rate: 19%)
35. Sayed M. Saghaian, Thomas La Porta, Trent Jaeger, Z. Berkay Celik, Patrick McDaniel. Mission-oriented Security Model, Incorporating Security Risk, Cost and Payout. In *Proceedings of the 2018 International Conference on Security and Privacy in Communication Networks* (SecureComm), August 2018. **Best Paper Award.** (acceptance rate: 30%)
36. Azeem Aqil, Karim Khalil, Ahmed O.F. Atya, Evangelos E. Papalexakis, Srikanth V. Krishnamurthy, Trent Jaeger, K.K. Ramakrishnan, Paul Yu, Ananthram Swami. Towards Network Intrusion Detection at ISP Scale. In *Proceedings of the 13th International Conference on Emerging Networking EXperiments and Technologies* (CoNEXT), December 2017. (acceptance rate: 18%)
37. Shen Liu, Gang Tan, Trent Jaeger. PtrSplit: Supporting General Pointers in Automatic Program Partitioning. In *Proceedings of the 24th ACM Conference on Computer and Communications Security* (ACM CCS), October 2017. (acceptance rate: 18%)
38. Gang Tan and Trent Jaeger. CFG Construction Soundness in Control-Flow Integrity. In *Proceedings of the 2017 ACM SIGSAC Workshop on Programming Languages and Analysis for Security* (ACM PLAS), October 2017.
39. Giuseppe Petracca, Ahmad-Atamli Reineh, Yuqiong Sun, Jens Grossklags, Trent Jaeger. AWare: Preventing Abuse of Privacy-Sensitive Sensors via Operation Bindings. In *Proceedings of the 26th USENIX Security Symposium*, August 2017. (acceptance rate: 16%)
40. Giuseppe Petracca, Frank Capobianco, Christian Skalka, Trent Jaeger. On Risk in Access Control Enforcement. In *Proceedings of the 22nd ACM Symposium on Access Control Models and Technologies* (ACM SACMAT), June 2017. (acceptance rate: 30% for full papers)
41. Frank Capobianco, Christian Skalka, Trent Jaeger. AccessProv: Tracking the Provenance of Access Control Decisions. In *Proceedings of the 9th International Workshop on Theory and Practice of Provenance* (TaPP), June 2017.
42. Le Guan, Peng Liu, Xinyu Xing, Xinyang Ge, Shengzhi Zhang, Meng Yu, Trent Jaeger. TrustShadow: Secure Execution of Unmodified Applications with ARM TrustZone. In *Proceedings of the 15th ACM International Conference on Mobile Systems, Applications, and Services* (MobiSys), June 2017. (acceptance rate: 18%)
43. Stefan Achleitner, Thomas La Porta, Trent Jaeger, Patrick McDaniel. Adversarial Network Forensics in Software Defined Networking. In *Proceedings of the 2017 ACM Symposium on SDN Research* (ACM SOSR), April 2017. **Best Student Paper Award**. (acceptance rate: 23%)
44. Xinyang Ge, Weidong Cui, Trent Jaeger. GRIFFIN: Guarding Control Flows Using Intel Processor Trace. In *Proceedings of the 22nd ACM International Conference on Architectural Support for Programming Languages and Operating Systems* (ASPLOS), April 2017. (acceptance rate: 17%)
45. Xinyang Ge, Mathias Payer, Trent Jaeger. An Evil Copy: How the Loader Betrays You. In *Proceedings of the 2017 Network and Distributed System Security Symposium* (NDSS), February-March 2017. (acceptance rate: 16%)

46. Yuqiong Sun, Giuseppe Petracca, Xinyang Ge, Trent Jaeger. Pileus: Protecting User Resources from Vulnerable Cloud Services. In *Proceedings of the 32nd Annual Computer Security Applications Conference* (ACSAC), December 2016. (acceptance rate: 21%)
47. Thomas Moyer, Patrick Cable, Karishma Chadha, Robert Cunningham, Nabil Schear, Warren Smith, Adam Bates, Kevin Butler, Frank Capobianco, Trent Jaeger. Leveraging Data Provenance to Enhance Cyber Resilience. In *Proceedings of the 1st IEEE Cybersecurity Development Conference* (IEEE SecDev), November 2016. (acceptance rate 38%)
48. Giuseppe Petracca, Trent Jaeger, Lisa Marvel, Ananthram Swami. Agility Maneuvers to Mitigate Inference Attacks on Sensed Location Data. In *Proceedings of the International Conference for Military Communications* (MILCOM), November 2016.
49. Xinyang Ge, Nirupama Talele, Mathias Payer, Trent Jaeger. Fine-Grained Control-Flow Integrity for Kernel Software. In *Proceedings of the 1st European Symposium on Security and Privacy* (IEEE EuroS&P), March 2016. (acceptance rate: 17%)
50. Giuseppe Petracca, Yuqiong Sun, Trent Jaeger, Ahmad Atamli. AuDroid: Preventing Attacks on Audio Channels in Mobile Devices. In *Proceedings of the 31st Annual Computer Security Applications Conference* (ACSAC), December 2015. (acceptance rate: 24%)
51. Yuqiong Sun, Susanta Nanda, Trent Jaeger. Security-as-a-Service for Microservices-Based Cloud Applications. In *Proceedings of the 7th International Conference on Cloud Computing Technology and Science* (IEEE CloudCom), November 2015. (acceptance rate: 24%)
52. Connor Jackson, Trent Jaeger, Karl Levitt, Jeff Rowe, Srikanth V. Krishnamurthy, Ananthram Swami. A Diagnosis Based Intrusion Detection Approach. In *Proceedings of the International Conference for Military Communications* (MILCOM), October 2015.
53. Azeem Aqil, Ahmed Fathy Atya, Trent Jaeger, Srikanth V. Krishnamurthy, Karl Levitt, Patrick McDaniel, Jeff Rowe, Ananthram Swami. Detection of Stealthy TCP-based DoS Attacks. In *Proceedings of the International Conference for Military Communications* (MILCOM), October 2015.
54. Yuqiong Sun, Giuseppe Petracca, Trent Jaeger, Hayawardh Vijayakumar, Joshua Schiffman. CloudArmor: Protecting Cloud Commands from Compromised Cloud Services. In *Proceedings of the 8th IEEE International Conference on Cloud Computing* (IEEE CLOUD), June 2015. (acceptance rate: 17%)
55. Divya Muthukumaran, Nirupama Talele, Trent Jaeger, Gang Tan. Producing Hook Placements to Enforce Expected Access Control Policies. In *Proceedings of the 2015 International Symposium on Engineering Secure Software and Systems* (ESSoS), March 2015. (acceptance rate: 27%)
56. Vinod Ganapathy, Trent Jaeger, Christian Skalka, Gang Tan. Assurance for Defense in Depth via Retrofitting. In *Proceedings of the 2014 Layered Assurance Workshop* (LAW), in conjunction with the *Annual Computer Security Applications Conference*, December 2014.
57. Yuqiong Sun, Giuseppe Petracca, Trent Jaeger. Inevitable Failure: The Flawed Trust Assumption in the Cloud. In Proceedings of the *ACM Cloud Computing Security Workshop* (ACM CCSW), in conjunction with the ACM Conference on Computer and Communications Security, November 2014. (acceptance rate: 33%)
58. Hayawardh Vijayakumar, Xinyang Ge, Mathias Payer, Trent Jaeger. Jigsaw: Protecting Resource Access by Inferring Programmer Expectations. In *Proceedings of the 23rd USENIX Security Symposium,* August 2014. (acceptance rate: 19%)
59. Hayawardh Vijayakumar, Xinyang Ge, Trent Jaeger. Policy Models to Protect Resource Retrieval. In *Proceedings of the 19th ACM Symposium on Access Control Models and Technologies* (ACM SACMAT), June 2014. (acceptance rate: 29%)
60. Nirupama Talele, Jason Teutsch, Robert Erbacher, Trent Jaeger. Monitor Placement for Large-Scale Systems. In *Proceedings of the 19th ACM Symposium on Access Control Models and Technologies* (ACM SACMAT), June 2014. (acceptance rate: 29%)
61. Xinyang Ge, Hayawardh Vijayakumar, Trent Jaeger. SPROBES: Enforcing Kernel Code Integrity on the TrustZone Architecture. In Proceedings of the *Mobile Security Technologies 2014 Workshop* (IEEE MoST'14), in conjunction with the IEEE Symposium on Security and Privacy, May 2014. (acceptance rate: 35%)

62. David Schmidt and Trent Jaeger. Pitfalls in the Automated Strengthening of Passwords. In *Proceedings of the 29th Annual Computer Security Applications Conference* (ACSAC), December 2013. (acceptance rate: 19%)
63. Joshua Schiffman, Yuqiong Sun, Hayawardh Vijayakumar, Trent Jaeger. Cloud Verifier: Verifiable Auditing Service for IaaS Clouds. In *Proceedings of the IEEE 2013 First International Workshop on Cloud Security Auditing*, June 2013.
64. Hayawardh Vijayakumar, Joshua Schiffman, Trent Jaeger. Process Firewalls: Protecting Processes During Resource Access. In *Proceedings of the 2013 ACM European Conference on Computer Systems* (ACM EuroSys), April 2013. (acceptance rate: 18%)
65. Nirupama Talele, Jason Teutsch, Trent Jaeger, Robert F. Erbacher. Using Available Security Policies to Automate Placement of Network Intrusion Detection. In *Proceedings of the 2013 International Symposium on Engineering Secure Software and Systems* (ESSoS), February 2013. (acceptance rate: 25%)
66. Divya Muthukumaran, Sandra Rueda, Nirupama Talele, Hayawardh Vijayakumar, Jason Teutsch, Trent Jaeger, Nigel Edwards. Transforming Commodity Security Policies to Enforce Clark-Wilson Integrity. In *Proceedings of the 28th Annual Computer Security Applications Conference* (ACSAC), December 2012. (acceptance rate: 19%)
67. Trent Jaeger, Divya Muthukumaran, Joshua Schiffman, Yuqiong Sun, Nirupama Talele, Hayawardh Vijayakumar. Configuring Cloud Deployments for Integrity. In *Proceedings of the Computer & Security Applications Rendez-vous: Cloud and Security*, November 2012.
68. Divya Muthukumaran, Trent Jaeger, Vinod Ganapathy. Leveraging “Choice” to Automate Authorization Hook Placement. In *Proceedings of the 19th ACM Conference on Computer and Communications Security* (ACM CCS), October 2012. (acceptance rate: 19%)
69. Hayawardh Vijayakumar and Trent Jaeger. The Right Files at the Right Time. In *Proceedings of the 5th Symposium on Configuration Analytics and Automation* (SafeConfig), October 2012.
70. Hayawardh Vijayakumar, Joshua Schiffman, Trent Jaeger. STING: Finding Name Resolution Vulnerabilities in Programs. In *Proceedings of the 21st USENIX Security Symposium,* August 2012. (acceptance rate: 19%)
71. Joshua Schiffman, Hayawardh Vijayakumar, Trent Jaeger. Verifying System Integrity by Proxy. In *Proceedings of the 5th International Conference on Trust and Trustworthy Computing* (TRUST), June 2012.
72. Hayawardh Vijayakumar, Guruprasad Jakka, Sandra Rueda, Joshua Schiffman, Trent Jaeger. Integrity Walls: Finding Attack Surfaces from Mandatory Access Control Policies. In *Proceedings of the 7th ACM Symposium on Information, Computer, and Communications Security* (ACM ASIACCS), May 2012. (acceptance rate: 22%)
73. Hayawardh Vijayakumar, Joshua Schiffman, Trent Jaeger. A Rose by Any Other Name or an Insane Root? Adventures in Namespace Resolution. In *Proceedings of the 7th European Conference on Computer Network Defense* (EC2ND), September 2011. (acceptance rate: 32%)
74. Joshua Schiffman, Thomas Moyer, Hayawardh Vijayakumar, Trent Jaeger, Patrick McDaniel. Seeding Clouds with Trust Anchors. In *Proceedings of the ACM Cloud Computing Security Workshop* (ACM CCSW), in conjunction with the ACM Conference on Computer and Communications Security, October 2010.
75. Divya Muthukumaran, Sandra Rueda, Hayawardh Vijayakumar, Trent Jaeger. Cut Me Some Security! In *Proceedings of the 3rd ACM Workshop on Configurable and Usable Security* (SafeConfig), October 2010.
76. Boniface Hicks, Sandra Rueda, David H. King, Thomas Moyer, Joshua Schiffman, Yogesh Sreenivasan, Patrick McDaniel, Trent Jaeger. An Architecture for Enforcing End-to-End Access Control over Web Applications. In *Proceedings of the 15th ACM Symposium on Access Control Models and Technologies* (ACM SACMAT), June 2010. (acceptance rate: 25%)
77. David H. King, Susmit Jha, Divya Muthukumaran, Trent Jaeger, Somesh Jha, Sanjit A. Seshia. Automating Security Mediation Placement. In *Proceedings of the 19th European Symposium on Programming* (ESOP), March 2010. (acceptance rate: 25%)

78. Joshua Schiffman, Thomas Moyer, Christopher Shal, Trent Jaeger, Patrick McDaniel. Justifying Integrity Using a Virtual Machine Verifier. In *Proceedings of the 25th Annual Computer Security Applications Conference* (ACSAC), December 2009. (acceptance rate: 19%)
79. Thomas Moyer, Kevin Butler, Joshua Schiffman, Patrick McDaniel, Trent Jaeger. Scalable Asynchronous Web Content Attestation. In *Proceedings of the 25th Annual Computer Security Applications Conference* (ACSAC), December 2009. (acceptance rate: 19%)
80. Patrick Traynor, Michael Lin, Machigar Ongtang, Vikhyath Rao, Trent Jaeger, Thomas La Porta, Patrick McDaniel. On Cellular Botnets: Measuring the Impact of Malicious Devices on the Cellular Network Core. In *Proceedings of the 16th ACM Conference on Computer and Communications Security* (ACM CCS), November 2009. (acceptance rate: 18%)
81. Liang Xie, Xinwen Zhang, Ashwin Chaugule, Trent Jaeger, and Sencun Zhu. Designing System-level Defenses against Cellphone Malware (short paper). In *Proceedings of the 28th IEEE International Symposium on Reliable Distributed Systems* (SRDS), September 2009.
82. Sandra Rueda, Hayawardh Vijayakumar, and Trent Jaeger. Analysis of Virtual Machine System Policies. In *Proceedings of the 14th ACM Symposium on Access Control Models and Technologies* (ACM SACMAT), June 2009. (acceptance rate: 31%)
83. Vikhyath Rao and Trent Jaeger. Dynamic Access Control for Multiple Stakeholders. In *Proceedings of the 14th ACM Symposium on Access Control Models and Technologies* (ACM SACMAT), June 2009. (acceptance rate: 31%)
84. David H. King, Boniface Hicks, Michael Hicks, and Trent Jaeger. Implicit Flows: Can't Live with 'em, Can't Live without 'em. In *Proceedings of the Fourth International Conference on Information Systems Security* (ICISS), December 2008.
85. William Enck, Patrick McDaniel, and Trent Jaeger. PinUP: Pinning User Files to Known Applications. In *Proceedings of the 24th Annual Computer Security Applications Conference* (ACSAC), December 2008. (acceptance rate: 24%)
86. Albert Tannous, Jonathan Trostle, Mohamed Hassan, Stephen E. McLaughin, and Trent Jaeger. New Side Channel Attacks Targeting Passwords. In *Proceedings of the 24th Annual Computer Security Applications Conference* (ACSAC), December 2008. (acceptance rate: 24%)
87. David H. King, Trent Jaeger, Somesh Jha, and Sanjit Seshia. Effective Blame for Information-flow Violations. In *Proceedings of the Sixteenth ACM SIGSOFT International Symposium on Foundations of Software Engineering* (ACM FSE), November 2008. (acceptance rate: 20%)
88. Sandra Rueda, Yogesh Sreenivasan, and Trent Jaeger. Flexible Security Configuration for Virtual Machines. In *Proceedings of the 2nd ACM Computer Security Architecture Workshop*, October 2008.
89. Sandra Rueda, David H. King, and Trent Jaeger. Verifying Compliance of Trusted Programs. In *Proceedings of the 17th USENIX Security Symposium,* August 2008. (acceptance rate: 16%).
90. Divya Muthukumaran, Anuj Sawani, Joshua Schiffman, Brian M. Jung, and Trent Jaeger. Measuring Integrity on Mobile Phone Systems. In *Proceedings of the 13th ACM Symposium on Access Control Models and Technologies* (ACM SACMAT), June 2008. (acceptance rate: 22%)
91. Luke St. Clair, Joshua Schiffman, Trent Jaeger, and Patrick McDaniel. Establishing and Sustaining System Integrity via Root of Trust Installation. In *Proceedings of the 23rd Annual Computer Security Applications Conference* (ACSAC), December 2007. (acceptance rate: 23%)
92. William Enck, Sandra Rueda, Yogesh Sreenivasan, Joshua Schiffman, Luke St. Clair, Trent Jaeger and Patrick McDaniel. Protecting Users from "Themselves." In *Proceedings of the First ACM Computer Security Architectures Workshop,* November 2007. (acceptance rate: 30%)
93. Boniface Hicks, Sandra Rueda, Trent Jaeger, Patrick McDaniel. From Trusted to Secure: Building and Executing Applications That Enforce System Security. In *Proceedings of the 2007 USENIX Annual Technical Conference*, June 2007. (acceptance rate: 19%)
94. Boniface Hicks, Sandra Rueda, Luke St. Clair, Trent Jaeger, Patrick McDaniel. A Logical Specification and Analysis for SELinux MLS. In *Proceedings of the 12th ACM Symposium on Access Control Models and Technologies* (ACM SACMAT), invited for ACM TISSEC publication, June 2007. (acceptance rate: 35%)

95. Trent Jaeger, Reiner Sailer, Yogesh Sreenivasan. Managing the Risk of Covert Information Flows in Virtual Machine Systems. In *Proceedings of the 12th ACM Symposium on Access Control Models and Technologies* (ACM SACMAT), June 2007. (acceptance rate: 35%)
96. Vinod Ganapathy, David H. King, Trent Jaeger, Somesh Jha. Mining Security-sensitive Operations in Legacy Code Using Concept Analysis. In *Proceedings of the 2007 IEEE International Conference on Software Engineering* (IEEE ICSE), May 2007. (acceptance rate: 15%)
97. Boniface Hicks, Sandra Rueda, Trent Jaeger, Patrick McDaniel. Integration of SELinux and Security-typed Languages. In *Proceedings of the 2007 Security-Enhanced Linux Workshop*, March 2007.
98. Jonathan McCune, Stefan Berger, Ramon Caceres, Trent Jaeger, Reiner Sailer. Shamon: A System for Distributed Mandatory Access Control. In *Proceedings of the 2006 Annual Computer Security Applications Conference* (ACSAC), December 2006. (acceptance rate: 30%)
99. Luke St. Clair, Lisa Johansen, William Enck, Matthew Pirretti, Patrick Traynor, Patrick McDaniel, Trent Jaeger. Password Exhaustion: Predicting the End of Password Usefulness. *Proceedings of the 2nd International Conference on Information Systems Security* (ICISS), December 2006.
100. Trent Jaeger, Kevin Butler, David H. King, Serge Hallyn, Joy Latten, Xiaolan Zhang. Leveraging IPsec for Mandatory Access Control across Systems. In *Proceedings of the Second International Conference on Security and Privacy in Communication Networks* (SecureComm), August 2006. (acceptance rate: 25%)
101. Trent Jaeger, Patrick McDaniel, Luke St. Clair, Ramon Caceres, Reiner Sailer. Shame on Trust in Distributed Systems. In *Proceeedings of the 2006 Workshop on Hot Topics in Security* (HotSec), August 2006. (acceptance rate: 19%)
102. Xiaolan Zhang, Larry Koved, Marco Pistoia, Sam Weber, Trent Jaeger, Guillaume Marceau, Liangzhao Zheng. The Case for Analysis Preserving Language Transformation. In *Proceedings of the 2006 International Symposium on Software Testing and Analysis* (ISSTA), July 2006. (acceptance rate: 26%)
103. Trent Jaeger, Reiner Sailer, Umesh Shankar. PRIMA: Policy-reduced Integrity Measurement Architecture. In *Proceedings of the 11th ACM Symposium on Access Control Models and Technologies* (ACM SACMAT), June 2006. (acceptance rate: 29%)
104. Vinod Ganapathy, Trent Jaeger, Somesh Jha. Retrofitting Legacy Code for Authorization Policy Enforcement. In *Proceedings of the 2006 IEEE Symposium on Security & Privacy* (IEEE S&P), May 2006. (acceptance rate: 13%)
105. Vinod Ganapathy, Trent Jaeger, Somesh Jha. Towards Automated Authorization Policy Enforcement. In *Proceedings of the 2nd SELinux Symposium,* March 2006.
106. Trent Jaeger. SELinux Protected Paths Revisited. In *Proceedings of the 2nd SELinux Symposium,* March 2006.
107. Umesh Shankar, Trent Jaeger, Reiner Sailer. Towards Automated Information-flow Integrity Verification for Security-critical Applications. In *Proceedings of the 2006 Network and Distributed System Security Symposium* (NDSS), February 2006. (acceptance rate: 13%)
108. Reiner Sailer, Enriquillo Valdez, Trent Jaeger, Ronald Perez, Leendert van Doorn, John L. Griffin, Stefan Berger. Building a MAC-based Security Architecture for the Xen Opensource Hypervisor. In *Proceedings of the 2005 Annual Computer Security Applications Conference* (ACSAC), December 2005. (acceptance rate: 23%)
109. Vinod Ganapathy, Trent Jaeger, Somesh Jha. Automatic Placement of Authorization Hooks in the Linux Security Modules Framework. In *Proceedings of the 12th ACM Conference on Computer and Communications Security* (ACM CCS), October 2005. (acceptance rate: 15%)
110. John L. Griffin, Trent Jaeger, Ronald Perez, Reiner Sailer, Leendert van Doorn, Ramon Caceres. Trusted Virtual Domains: Towards Secure, Virtual Services. In *Proceedings of the First Workshop on Hot Topics in Systems Dependability* (HotDep), May 2005.
111. Reiner Sailer, Trent Jaeger, Xiaolan Zhang, Leendert van Doorn. Attestation-based Policy Enforcement for Remote Access. In *Proceedings of the 11th ACM Conference on Computer and Communications Security* (ACM CCS), October 2004. (acceptance rate: 14%)
112. Xiaolan Zhang, Trent Jaeger, Larry Koved. Applying Static Analysis to Verifying Security Properties. In *Proceedings of the 2004 Grace Hopper Conference,* October 2004.

113. Reiner Sailer, Xiaolan Zhang, Trent Jaeger, Leendert van Doorn. Design and Implementation of a TCG-based Integrity Measurement Architecture. In *Proceedings of the 13th USENIX Security Symposium,* August 2004. (acceptance rate: 12%)
114. Trent Jaeger, Reiner Sailer, Xiaolan Zhang. Resolving Constraint Conflicts. In *Proceedings of the 9th ACM Symposium on Access Control Models and Technologies* (ACM SACMAT), June 2004. (acceptance rate: 28%)
115. Trent Jaeger, Reiner Sailer, Xiaolan Zhang. Analyzing Integrity Protection in the SELinux Example Policy. In *Proceedings of the 12th USENIX Security Symposium,* August 2003. (acceptance rate: 16%)
116. Antony Edwards, Trent Jaeger, Xiaolan Zhang. Runtime Verification of the Linux Security Modules Framework. In *Proceedings of the 9th. ACM Conference on Computer and Communications Security* (ACM CCS), invited for ACM TISSEC publication*,* November 2002. (acceptance rate: 18%)
117. Trent Jaeger, Antony Edwards, Xiaolan Zhang. Gaining and Maintaining Confidence in Operating Systems Security. In *Proceedings of the ACM SIGOPS European Workshop,* September 2002.
118. Xiaolan Zhang, Leendert van Doorn, Trent Jaeger, Ron Perez, Reiner Sailer. Secure Coprocessor-based Intrusion Detection. In *Proceedings of the ACM SIGOPS European Workshop,* September 2002.
119. Xiaolan Zhang, Antony Edwards, Trent Jaeger. Using CQUAL for Static Analysis of Authorization Hook Placement. In *Proceedings of the 11th USENIX Security Symposium,* August 2002. (acceptance rate: 17%)
120. Trent Jaeger, Antony Edwards, Xiaolan Zhang. Managing Access Control Policies Using Access Control Spaces. In *Proceedings of the 7th ACM Symposium on Access Control Models and Technologies* (ACM SACMAT), invited for ACM TISSEC special issue, June 2002.
121. Trent Jaeger. Managing Access Control Complexity Using Metrics. In *Proceedings of the 6th ACM Symposium on Access Control Models and Technologies* (ACM SACMAT), May 2001.
122. Mohit Aron, Yoonho Park, Trent Jaeger, Kevin Elphinstone, Jochen Liedtke, Luke Deller. The SawMill Framework for Virtual Memory Diversity. In *Proceedings of the 2001 Australian Computer Science Conference*, January 2001.
123. Jonathon Tidswell and Trent Jaeger. An Access Control Model for Simplifying Constraint Expression. In *Proceedings of the 7th ACM Conference on Computer and Communication Security Technologies* (ACM CCS), invited for ACM TISSEC special issue, November 2000. (acceptance rate: 21%)
124. Alain Gefflaut, Trent Jaeger, Yoonho Park, Jochen Liedtke, Kevin Elphinstone, Volkmar Uhlig, Jonathon Tidswell, Luke Deller, Lars Reuther. The SawMill Multiserver Approach. In *Proceedings of the 8th ACM SIGOPS European Workshop*, September 2000.
125. Trent Jaeger, Jonathon Tidswell, Alain Gefflaut, Yoonho Park, Jochen Liedtke, Kevin Elphinstone. Synchronous IPC over Transparent Monitors. In *Proceedings of the 8th ACM SIGOPS European Workshop*, September 2000.
126. Jonathon Tidswell and Trent Jaeger. Integrated Constraints and Inheritance in DTAC. In *Proceedings of the 5thACM Workshop on Role-based Access Control*, July 2000.
127. Trent Jaeger. On the Increasing Importance of Constraints. In *Proceedings of the 4th ACM Workshop on Role-based Access Control*, November 1999.
128. Trent Jaeger, Tony Michailidis, Roy Rada. Access Control in a Virtual University. In *Proceedings of the 8th IEEE International Workshop on Enabling Technologies*, June 1999.
129. Jochen Liedtke, Volkmar Uhlig, Kevin Elphinstone, Trent Jaeger, Yoonho Park. How to Schedule Unlimited Memory Pinning of Untrusted Processes or Provisional Ideas about Service-neutrality. In *Proceedings of the 6th Workshop on Hot Topics in Operating Systems* (HotOS), March 1999.
130. Trent Jaeger, Kevin Elphinstone, Jochen Liedtke, Vsevolod Panteleenko, Yoonho Park. Flexible Access Control Using IPC Redirection. In *Proceedings of the 6th Workshop on Hot Topics in Operating Systems* (HotOS), March 1999.
131. Trent Jaeger, Jochen Liedtke, Vsevolod Panteleenko, Yoonho Park, Nayeem Islam. Security Architecture for Component-based Operating Systems. In *Proceedings of the 7th ACM SIGOPS European Workshop*, September 1998.

132. Jochen Liedtke, Nayeem Islam, Trent Jaeger, Vsevolod Panteleenko, Yoonho Park. An Unconventional Proposal: Using the x86 Architecture as the Ubiquitous Virtual Standard Architecture. In *Proceedings of the 7th ACM SIGOPS European Workshop*, September 1998.
133. Jochen Liedtke, Nayeem Islam, Trent Jaeger, Vsevolod Panteleenko, Yoonho Park. Irreproducible Benchmarks Might Be Sometimes Helpful. In *Proceedings of the 7th ACM SIGOPS European Workshop*, September 1998.
134. Jochen Liedtke, Vsevolod Panteleenko, Trent Jaeger, Nayeem Islam. High-performance Caching with the Lava Hit-server. In *Proceedings of the 1998 USENIX Annual Technical Conference*, June 1998.
135. Trent Jaeger, Jochen Liedtke, Nayeem Islam. Fine-grained Protection in Operating Systems. In *Proceedings of the 6th USENIX Security Symposium*, January 1998.
136. Trent Jaeger, Frederique Giraud, Nayeem Islam, Jochen Liedtke. A Role-based Access Control Model for Protection Domain Derivation and Management. In *Proceedings of the 2nd ACM Workshop on Role-based Access Control*, November 1997.
137. Rangachari Anand, Nayeem Islam, Trent Jaeger, Josyula R. Rao. A Flexible Security Model for Using Internet Content. In *Proceedings of the 1997 IEEE International Symposium on Reliable Distributed Systems* (SRDS), September 1997.
138. Jochen Liedtke, Kevin Elphinstone, Sebastian Schönberg, Hermann Härtig, Gernot Heiser, Nayeem Islam, Trent Jaeger. Achieved IPC Performance. In *Proceedings of the IEEE Workshop on Hot Topics in Operating Systems* (HotOS), May 1997.
139. Jochen Liedtke, Nayeem Islam, Trent Jaeger. Preventing Denial of Service Attacks on a μ-kernel for WebOSes. In *Proceedings of the IEEE Workshop on Hot Topics in Operating Systems* (HotOS), May 1997.
140. Jang Ho Lee, Atul Prakash, Trent Jaeger, Gwobaw Wu. Supporting Multi-user, Multi-applet Workspaces in CBE. In *Proceedings of ACM Computer Supported Cooperative Work '96 Conference* (CSCW), November 1996.
141. Trent Jaeger, Atul Prakash, Avi Rubin. A System Architecture for Flexible Control of Downloaded Executable Content. In *Proceedings of the IEEE International Workshop on Object-oriented Operating Systems*, October 1996.
142. Trent Jaeger, Avi Rubin, Atul Prakash. Building Systems That Flexibly Control Downloaded Executable Content. In *Proceedings of the 6th USENIX Security Symposium,* July 1996. **Best Student Paper**.
143. Trent Jaeger and Avi Rubin. Preserving Integrity in Remote File Location and Retrieval. In *Proceedings of the 1996 Symposium on Network and Distributed System Security* (NDSS), February 1996.
144. Trent Jaeger and Atul Prakash. Requirements of Role-based Access Control for Collaborative Systems. In *Proceedings of the 1st ACM Workshop on Role-based Access Control*, November 1995.
145. Trent Jaeger and Atul Prakash. Management and Utilization of Knowledge for the Automatic Improvement of Workflow Performance. In *Proceedings of the 1995 Conference on Organizational Computing Systems*, August 1995.
146. Trent Jaeger and Atul Prakash. Implementation of a Discretionary Access Control Model for Script-based Systems. In *Proceedings of the 8th IEEE Computer Security Foundations Workshop* (IEEE CSFW), June 1995.
147. Trent Jaeger and Atul Prakash. Representation and Adaptation of Organization Coordination Knowledge for Autonomous Agent Systems. In *Proceedings of the 9th International Conference on Software Engineering and Knowledge Engineering*, June 1995.
148. Trent Jaeger and Atul Prakash. Support for the File System Security Requirements for Computational E-Mail Systems. In *Proceedings of the 2nd ACM Conference on Computer and Communications* Security (ACM CCS), November 1994.
149. Trent Jaeger, Atul Prakash, Masayoki Ishikawa. A Framework for the Automatic Improvement of Workflows to Meet Performance Goals. In *Proceedings of the 6th IEEE Conference on Tools with Artificial Intelligence*, November 1994.
150. Trent Jaeger, Atul Prakash, Masayoki Ishikawa. Automatic Reengineering of Business Processes. In *Proceedings of the 4th Reengineering Forum*, Section 53, September 1994.

151. Trent Jaeger and Atul Prakash. BizSpec: A Business-oriented Model for Specification and Analysis of Office Information Systems. In *Proceedings of the 7th International Conference on Software Engineering and Knowledge Engineering*, June 1993.
152. Trent Jaeger. Using AI Paradigms in Solving Manufacturing Problems as Demonstrated by the CPC Stacking/Destacking Advisor. In *Proceedings of the 3rd International Conference on CAD/CAM, Robotics, and Factories of the Future*, Volume 2, August 1988.

Other Publications

1. Fred Araujo, Teryl Taylor, Aditya Basu, Rahul George, Yu-Tsung Lee, Trent Jaeger. Provenance-Aware Integrity Monitoring with Linux Security Identifiers. Presentation at the *Linux Security Summit North America 2024*, April 2024.
2. Kaiming Huang, Mathias Payer, Zhiyun Qian, Jack Sampson, Gang Tan, Trent Jaeger. Top of the Heap: Efficient Memory Error Protection for Many Heap Objects. In *arXiv*, 2310.06397, October 2023.
3. Sebastian Angel, Aditya Basu, Weidong Cui, Trent Jaeger, Stella Lau, Srinath Setty, Sudheesh Singanamalla. Nimble: Rollback Protection for Confidential Cloud Services (extended version). In *Cryptology ePrint Archive*, Paper 2023/761, May 2023. *Extended version of the OSDI 2023 paper.*
4. Naiqian Zhang, Daroc Alden, Dongpeng Xu, Shuai Wang, Trent Jaeger, Wheeler Ruml. Using Planning to Construct Code-Reuse Attacks in Obfuscated Programs. In *Proceedings of the 16th Scheduling and Planning Applications Workshop* (SPARK), in conjunction with 33rd International Conference on Automated Planning and Scheduling (ICAPS), July 2023. *Related to the DSN 2023 paper.*
5. Trent Jaeger. On Bridges and Software. In *IEEE Security & Privacy*, 21(3), May/June 2023. *Column.*
6. Trent Jaeger, Brent ByungHoon Kang, Nele Mentens, Cynthia Sturton. Impact of Emerging Hardware on Security and Privacy. In *IEEE Security & Privacy*, 21(3), May/June 2023. *Guest Editors' Introduction.*
7. Carl Landwehr, Michael Reiter, Laurie Williams, Gene Tsudik, Trent Jaeger, Yoshi Kohno, Apu Kapadia. Looking Backwards (and Forwards): NSF Secure and Trustworthy Computing 20-Year Retrospective Panel Transcription. In *IEEE Security & Privacy*, 21(2), March/April 2023. *Panel summary*.
8. Valentin Vie, Ryan Sheatsley, Sophia Beyda, Sushrut Shringarputale, Kevin Chan, Trent Jaeger, Patrick McDaniel. Adversarial Planning. *arXiv, CoRR abs/2205.00566*, May 2022.
9. Trent Jaeger. Towards Fail Safety for Security Decisions. In *IEEE Security & Privacy,* 19(6), November/December 2021. *Column.*
10. Fabio Massacci and Trent Jaeger. SolarWinds and the Challenges of Patching: Can We Ever Stop Dancing with the Devil? In *IEEE Security & Privacy*, 19(2), March/April 2021. *Column.*
11. Trent Jaeger. Static Analysis Opportunities for Improving Agile and Moving Target Defenses. In *Proceedings of the 7th Moving Target Defense Workshop* (ACM MTD). November 2020. *Keynote abstract*.
12. Aditya Basu and Trent Jaeger. Flexible Process Monitoring with the Process Firewall. In the *Office of Naval Research* (ONR) *Total Platform Cyber Protection* (TPCP) *Software Security Summer School* (SSSS'20), August 2020. *Software Demonstration.*
13. Asmit De, Aditya Basu, Swaroop Ghosh, Trent Jaeger. Buffer Protection using PUF-based Randomized Canaries. In *2019 Design Automation Conference Work-in-Progress Session*, June 2019.
14. Asmit De, Aditya Basu, Swaroop Ghosh, Trent Jaeger. Reconfigurable Security Extensions in Hardware for RISC-V Architecture. In *Proceedings of the IEEE International Symposium on Hardware Oriented Security and Trust* (HOST)*,* May 2018. *Hardware Demonstration.*
15. Amit Kumar Sikder, Giuseppe Petracca, Hidayet Aksu, Trent Jaeger, A. Selcuk Uluagac. A Survey on Sensor-based Threats to Internet-of-Things (IoT) Devices and Applications. arXiv:1802.02041, February 2018.
16. Archer Batcheller, Summer Craze Fowler, Robert Cunningham, Dinara Doyle, Trent Jaeger, Ulf Lindqvist. Building on the Success of Building Security In. In *IEEE Security & Privacy*, 15(4), July/August 2017. *Column.*

17. Anirudh Iyengar, Swaroop Ghosh, Trent Jaeger. A Processor + FPGA based Platform for Control Flow Integrity Enforcement. In *Proceedings of the IEEE International Symposium on Hardware Oriented Security and Trust* (HOST), May 2017. *Hardware Demonstration.*
18. Nirupama Talele, Divya Muthukumaran, Frank Capobianco, Trent Jaeger, Gang Tan. Maintaining Authorization Hook Placements Across Program Versions. In *Proceedings of the 1st IEEE Cybersecurity Development Conference* (SecDev), November 2016. *Abstract.*
19. Trent Jaeger. Configuring Software and Systems for Defense-in-Depth. In *Proceedings of the 2016 ACM Workshop on Automated Decision Making for Active Cyber Defense* (SafeConfig), October 2016. *Keynote Abstract.*
20. Trent Jaeger, Xinyang Ge, Divya Muthukumaran, Sandra Rueda, Joshua Schiffman, Hayawardh Vijayakumar. Designing for Attack Surfaces: Keep Your Friends Close, but Your Enemies Closer. In *Proceedings of the Fifth International Conference on Security, Privacy, and Applied Cryptography Engineering* (SPACE), October 2015. *Invited Paper.*
21. Trent Jaeger. Challenges in Making Access Control Sensitive to the "Right" Contexts. In *Proceedings of the 19th ACM Symposium on Access Control Models and Technologies* (SACMAT), June 2015. *Keynote Abstract.*
22. Patrick McDaniel, Trent Jaeger, Thomas F. La Porta, Nicolas Papernot, Robert J. Walls, Alexander Kott, Lisa Marvel, Ananthram Swami, Prasant Mohapatra, Srikanth V. Krishnamurthy, Iulian Neamtiu. Security and Science of Agility. In *Proceedings of the ACM Moving Target Defense Workshop*, in conjunction with the ACM Conference on Computer and Communications Security, November 2014. *Invited Paper.*
23. Robert F. Erbacher, Trent Jaeger, Nirupama Talele, Jason Teutsch. Directed Multicut with Linearly Ordered Terminals. *CoRR abs/1407.7498*, August 2014.
24. Thomas Moyer, Trent Jaeger, Patrick McDaniel. Scalable Integrity-guaranteed AJAX. In *Proceedings of the 14th Asia-Pacific Web Conference (APWeb)*, April 2012. *Invited Paper.*
25. Trent Jaeger and Joshua Schiffman. Outlook: Cloudy with a Chance of Security Challenges and Improvements. In *IEEE Security & Privacy*, 8(1), January/February 2010. *Column.*
26. Kevin Butler, Stephen McLaughlin, Thomas Moyer, Joshua Schiffman, Patrick McDaniel, and Trent Jaeger. Firma: Disk-based Foundations for Trusted Operating Systems. *Technical Report NAS-TR-0114-2009*, Network and Security Research Center, Penn State University, April 2009.
27. Kevin Butler, Stephen McLaughlin, Thomas Moyer, Patrick McDaniel, and Trent Jaeger. SwitchBlade: Policy-driven Disk Segmentation. *Technical Report NAS-TR-0098-2008*, Network and Security Research Center, Penn State University, 2008.
28. Luke St. Clair, Joshua Schiffman, Trent Jaeger, and Patrick McDaniel, Sum of the Parts: Composing Trust from Validation Primitives. *Technical Report NAS-TR-0056-2006*, Network and Security Research Center, Penn State University, November 2006.
29. Boniface Hicks, Sandra Rueda, Trent Jaeger, Patrick McDaniel. Breaking Down the Walls of Mutual Distrust: Security-typed Email Using Labeled IPsec. *Technical Report NAS-TR-0049-2006*, Network and Security Research Center, Penn State University, 2006.
30. Trent Jaeger, Serge Hallyn, Joy Latten. Leveraging IPsec for Mandatory Access Control of Linux Network Communications. In *Proceedings of the 21st Annual Computer Security Applications Conference*, 2005. *Case Study Session.*
31. Ron Perez, Reiner Sailer, Ray Valdez, Trent Jaeger, Leendert van Doorn, John Linwood Griffin, Stefan Berger. sHype – Hypervisor Security Architecture. In *Deutscher IT-Sicherheitskongress*, 2005.
32. Trent Jaeger, David Safford, Hubertus Franke. Linux Security for the Enterprise: Executive Summary. *IBM Research Whitepaper*, 2002.
33. Trent Jaeger, David Safford, Hubertus Franke. Security Requirements for the Deployment of the Linux Kernel in Enterprise Systems. *IBM Research Whitepaper*, 2002.
34. Trent Jaeger, Antony Edwards, Xiaolan Zhang. Maintaining the Correctness of the Linux Security Modules Framework. In *Proceedings of the 2002 Ottawa Linux Symposium,* June 2002.

35. Elisa Bertino, Trent Jaeger, Jonathan D. Moffett, Sylvia Osborn, Ravi Sandhu. Making Access Control More Usable. In *Proceedings of the 7th Symposium on Access Control Models and Technologies*, June 2002. *Panel statement.*
36. Trent Jaeger and Jonathon Tidswell. Rebuttal to the NIST RBAC Model Proposal. In *Proceedings of the 5th ACM Workshop on Role-based Access Control*, July 2000. *Invited Paper*.
37. Trent Jaeger and Atul Prakash. Using Simulation and Performance Improvement Knowledge for Redesigning Business Processes. *University of Michigan Tech Report, CSE-TR-278-96*, January 1996.
38. Trent Jaeger and Aviel Rubin. Protocols for Authenticated Download to Mobile Information Appliances. *University of Michigan Tech Report, CSE-TR-275-95,* December 1995.

Professional Service

Leadership Positions (chronological order by end date)

- **Co-Director,** Center for Research and Education in Cyber Security and Privacy (CRESP), UC Riverside, 2024-present
- **Associate Editor-in-Chief**, IEEE Security & Privacy, 2020-present
- **Associate Editor**, Communications of the ACM, for Contributions, 2020-present
- **Academic Advisory Board**, The Cyber Security Body of Knowledge Project, funded by the National Cyber Security Programme, UK, 2017-present
- **Steering Committee Member**, ACM Conference on Computer and Communications Security (ACM CCS), 2013-present
- **General Chair**, IEEE Symposium on Security and Privacy, 2024, Vice Chair in 2023
- **Consortium Program Manager**, Army Research Lab Cybersecurity Collaborative Research Alliance (CSec CRA), 2018-2023
- **Co-Director**, Systems and Internet Infrastructure Security Lab, Penn State, 2005-2023
- **Steering Committee Member**, Network and Distributed Systems Security Symposium (NDSS), 2018-2023
- **Guest Editor**, IEEE Security & Privacy, May/June 2023 issue
- **Committee Chair**, ACM SIGSAC Awards Committee, 2022
- **Executive Committee Member**, ACM Special Interest Group on Security, Audit, and Control (ACM SIGSAC), 2013-2021 (as Chair and past Chair)
- **Steering Committee Chair**, ISOC Network and Distributed Systems Security Symposium (NDSS), 2018-2021
- **General Chair**, Network and Distributed Systems Security Symposium (NDSS), 2019-2021, and as Shadow General Chair in 2018
- **Program Co-Chair**, ACM Moving Target Defense Workshop (co-located with ACM CCS), 2021
- **Organizer**, Corona-Def Workshop: Call for Innovative Secure IT Technologies against COVID-19, co-located with NDSS, 2021
- **Steering Committee Member**, IEEE Secure Development Conference (IEEE SecDev), 2017-2020
- **Associate Editor**, IEEE Security & Privacy, 2018-2020
- **Program Co-Chair**, 14th International Conference on Information Systems Security, 2018
- **Special Interest Group Chair,** ACM Special Interest Group on Security, Audit, and Control (ACM SIGSAC), 2013-2017
- **Program Chair,** 2nd IEEE Secure Development Conference (SecDev), 2017
- **Steering Committee Chair**, ACM Conference on Computer and Communications Security (ACM CCS), 2013-2014
- **Program Co-Chair,** 9th ACM Symposium on Information, Computer and Communications Security (ACM ASIACCS), 2014

- **Associate Editor,** ACM Transactions on Internet Technology, 2007-2013
- **Organizer**, Trusted Infrastructure Workshop, at Penn State, June 2013
- **Co-Organizer**, Summer School on Principles of Software Security, at Penn State, June 2012
- **Co-Organizer,** 2010 NSF Workshop on the Future of Trustworthy Computing, Arlington, VA, 2010
- **Program Chair**, ACM Second Computer Security Architectures Workshop, 2008
- **Program Vice Chair**, Reliable Software Systems Track, IEEE International Conference on Sensor Networks, Ubiquitous and Trustworthy Computing, 2008
- **Organizing Committee**, First Computer Security Architecture Workshop, 2007
- **Program Chair**, USENIX Workshop on Hot Topics in Security, 2007
- **Steering Committee Member**, ACM Symposium on Access Control Models and Technologies, 2001-2007
- **General Chair**, ACM Symposium on Access Control Models and Technologies, 2004
- **Panels Chair**, ACM Symposium on Access Control Models and Technologies, 2002-2003
- **Program Chair**, ACM Conference on Computer and Communications Security, Industry Track, 2003
- **Guest Editor**, ACM Transactions on Information Systems Security, November 2002 issue
- **Program Chair**, ACM Symposium on Access Control Models and Technologies, 2001
- **Program Chair**, ACM Workshop on Role-based Access Control, 1998

Program Committees and Other Reviewing (grouped by conference)

- **PC Member**, IEEE Symposium on Security and Privacy (IEEE S&P, “Oakland”), 2003-2004, 2007-2008, 2011, 2015, 2018-2019, 2023, 2025 (ten times)
- **PC Member**, ACM Conference on Computer and Communication Security (ACM CCS), Research Track: 2000-2003, 2006, 2009-2010, 2013-2015, 2017, 2019, 2023; Industry Track: 2004-2005 (15 times)
- **PC Member**, USENIX Security Symposium (USENIX Security), 1999-2001, 2005-2006, 2008-2009, 2018-2020 (ten times)
- **PC Member**, Network and Distributed System Security Symposium (NDSS), 2007, 2020-2024 (six times)
- **PC Member**, ACM European Conference on Computer Systems (EuroSys), 2011, 2023
- **PC Member**, USENIX Annual Technical Conference (USENIX ATC), 2020
- **PC Member**, 23rd International Conference on Architectural Support for Programming Languages and Operating Systems (ASPLOS), 2018
- **PC Member**, European Symposium on Research in Computer Security (ESORICS), 2002-2003
- **PC Member**, Annual Computer Security Applications Conference (ACSAC), 2005, 2010-2014
- **PC Member**, ACM Asia Conference on Computer and Communications Security (ACM AsiaCCS) formerly ACM Symposium on Information, Computer and Communications Security (ACM ASIACCS), 2013, 2017
- **PC Member**, IEEE European Symposium on Security and Privacy (IEEE EuroS&P), 2016
- **PC Member**, AAAI Conference on Artificial Intelligence (AAAI), 2021
- **PC Member**, International Symposium on Engineering Secure Software and Systems (ESSoS), 2017
- **PC Member**, International Conference on Trust and Trustworthy Computing (TRUST), 2012-2013
- **PC Member**, ACM Symposium on Access Control Models and Technologies (SACMAT), 2002-2017, 2022
- **PC Member**, International Conference on Distributed Computing Systems (ICDCS), Security & Privacy Track, 2008
- **PC Member**, International World Wide Web Conference (WWW), Security and Privacy Track, 2003-2005
- **PC Member**, Financial Cryptography and Data Security, 2016
- **PC Member**, IEEE International Conference on Cloud Computing Technology and Science (IEEE

CloudCom), 2016
- **PC Member**, International Conference on Information System Security (ICISS), 2009
- **PC Member**, Information Security Conference (ISC), 2007
- **PC Member**, New Security Paradigms Workshop (NSPW), 2020
- **PC Member**, for several workshops
- **Reviewer** for funding agencies including the National Science Foundation, Air Force Research Lab, Canada Foundation for Innovation, Canada National Research Council, Luxembourg National Research Fund,
- **External reviewer for journals**: ACM Transactions on Information Systems Security, ACM Transactions on Privacy and Security, ACM Transactions on Computer Systems, IEEE Transactions on Dependable and Secure Computing, IEEE Transactions on Parallel and Distributed Systems, IEEE Transactions on Computers, IEEE Transactions on Knowledge and Data Engineering, IEEE Transactions on Cloud Computing, Communications of the ACM, Computers & Security, Journal of Computer Security, IBM Systems Journal of Digital Libraries, International Journal of Information and Computer Security
- **External reviewer for other conferences**: ACM Symposium on Operating Systems Principles (SOSP), ACM/USENIX Symposium on Operating System Design and Implementation (OSDI), IEEE Hot Topics in Operating Systems (HotOS), ACM Computer-Supported Collaborative Work (CSCW), Principles of Distributed Computing (PODC), IEEE International Conference on Computer Communications (IEEE INFOCOM), International Conference on Distributed Systems and Networks (ICDCN)

Other Service Roles

- **Committee Member,** ACM SIGSAC Outstanding Early-Career Researcher Award, 2024
- **Committee Member,** CACM Research Highlights Committee for ACM SIGSAC, 2022-present
- **Institute Member,** Institute for Network and Security Research (formerly Network and Security Research Center), Penn State, 2005-2023
- **Test-of-Time Award Committee Member,** ISOC Network and Distributed Systems Security Symposium (NDSS), 2022

External Presentations (Since 2002)

- *The Benefits of Performing Comprehensive Memory Safety Validation*, University of Alabama Birmingham, Birmingham, AL and Trusted Computing Center of Excellence Summit 2024, Annapolis, MD, May 2024
- ***Panel**, Technology Advances and Modern Software Development,* Trusted Computing Center of Excellence Summit, Annapolis, MD, May 2024
- *KSplit: Automating Device Driver Isolation,* UC Riverside, Riverside, CA, January 2023
- ***Panel**, SaTC Retrospective,* 2022 Secure and Trustworthy Cyberspace Principal Investigators' Meeting (SaTC PI Meeting '22), 10 Years of National Science Foundation Support for SaTC Research, Arlington, VA, June 2022
- *Using Memory Safety Validation to Improve Security and Performance,* UC Riverside, Riverside, CA, April 2022
- ***Keynote Talk**, Can Security Risk Management Become Practical?,* 8th International Conference on Networking, Systems and Security, Cox's Bazar, Bangladesh (Hybrid), December 2021
- *Utilizing Safety Validation in Systems and Programs*, Worchester Polytechnic University, Virtual, September 2021
- ***Keynote Talk**, Static Analysis Opportunities for Improving Agile and Moving Target Defenses*, Moving

Target Defenses Workshop (with the 2020 ACM Conference on Computer and Communications Security), Virtual, November 2020

- ***Keynote Talk***, *Adventures with Hardware-Based Control-Flow Tracing*, Security of Software/Hardware Interfaces 2020 Workshop (with the 2020 IEEE European Symposium on Security and Privacy), Virtual, September 2020
- *Scalable Hypothesis-Based Intrusion Detection for Mission Resilience,* Army Research Lab, Adelphi, MD, March 2020 and May 2020
- *Preventing Abuse of Privacy-Sensitive Sensors via Operation Bindings,* UC Riverside, Riverside, CA, February 2020
- *Building Systems That Protect Code and Data Integrity,* UC Riverside, Riverside, CA, January 2020
- *Principled Unearthing of TCP Side Channel Vulnerabilities,* ACM Conference on Computer and Communications Security, London, UK, November 2019
- *Current Research Summaries*, Hewlett-Packard Enterprise and Hewlett-Packard, Inc., Bristol, UK, November 2019
- ***Keynote Talk***, *Challenges in Leveraging Available Defenses to Improve Detection*, Cyber Security at-Scale: Challenges for Research, Education and Training, Bristol, UK, October 2019
- ***Keynote Talk***, *Developing Software to Leverage seL4's Formal Correctness for Achieving Security Guarantees*, The Second Annual seL4 Summit, Herndon, VA, September 2019
- ***Keynote Talk***, *The Science of Attack Surfaces and Its Applications*, 2019 Hot Topics in the Science of Security (HoTSoS), Nashville, TN, April 2019
- *Block Oriented Programming* and *Why Paying Attention to Attack Surfaces Is Important – A Case Study for Opening Files*, Dixie State University, St. George, UT, March 2019
- ***Panel**, seL4 Center of Excellence Panel Discussion*, The First Annual seL4 Summit, Herndon, VA, November 2018
- ***Keynote Talk***, *The Evolution of Secure Operating Systems*, The First Annual seL4 Summit, Herndon, VA, November 2018
- ***Distinguished Lecture***, *Designing System Platforms for Cloud and Edge Computing*, The Ohio State University, Columbus, OH, October 2018
- ***Distinguished Lecture***, *Enforcing Control-Flow Integrity System-Wide*, University of Florida, Gainesville, FL, February 2018
- *Enforcing Control-Flow Integrity System-Wide,* University of North Carolina, Charlotte, Charlotte, NC, November 2017
- *AWare: Preventing Abuse of Privacy-Sensitive Sensors via Operation Bindings*, Northeastern University, Boston, MA, September 2017
- ***Keynote Talk***, *Fixing Security Problems for and with Programmers*, ACM SIGSAC China Symposium, Shanghai, China, May 2017
- *Kernel Enforcement of Control-Flow Integrity*, University of Texas at Austin, Austin, TX, May 2017
- ***Panel***, *Hardware and Software Security: Gaps and Synergies*, IEEE Custom Integrated Circuits Conference, Austin, TX, May 2017
- *Kernel Enforcement of Control-Flow Integrity*, Clemson University, Clemson, SC, March 2017
- *Fine-Grained Control-Flow Integrity for Kernel Software*, Binghamton University, Binghamton, NY, November 2016
- ***Keynote Talk***, *Configuring Software and Systems for Defense-in-Depth*, ACM SafeConfig Workshop (affiliated with the ACM Conference on Computer and Communications Security), Vienna, Austria, October 2016
- ***Keynote Talk***, *Software and Systems Security in the Cyber-Physical Systems*, IEEE CPS-SEC-International Workshop on Cyber-Physical Systems Security (affiliated with the IEEE Conference on Communications and Network Security), Philadelphia, PA, October 2016
- *Retrofitting Software for Defense-in-Depth*, DARPA Transparent Computing PI Meeting, Cambridge, MA, July 2016

- *Fine-Grained Control-Flow Integrity for Kernel Software*, Stonybrook University*,* Stony Brook, NY, April 2016
- ***Keynote Talk***, *Software and Systems Security in the Internet of Things*, Trends in Cybersecurity Workshop, Miami, FL, October 2015
- ***Keynote Talk***, *Inferring Programmer Expectations to Protect Program Execution***,** Fifth International Conference on Security, Privacy, and Applied Cryptography Engineering, Jaipur, India, October 2015
- *Process Firewalls: Protecting Programs During Resource Access*, University of Buffalo, Buffalo, NY, September 2015
- ***Invited Lectures***, (1) *Designing system mechanisms to detect and block program vulnerabilities*; (2) *Developing automated mechanisms to compute and leverage "adversary accessibility" to improve system security*; and (3) *Retrofitting programs mostly-automatically for security*, International Summer School on Information Security (InfoSec 2015), Bilbao, Spain, July 2015
- *JIGSAW: Protecting Resource Access by Inferring Programmer Expectations*, Universidad Carlos III de Madrid (UC3M), Madrid, Spain, July 2015
- ***Keynote Talk***, *Challenges in Making Access Control Sensitive to the "Right" Contexts*, ACM Symposium on Access Control Models and Technologies, Vienna, Austria, June 2015
- *Research on Restricting Attack Vectors on Clouds and Kernels*, Samsung Research America, San Jose, CA and Rambus Computer Research Associates, San Francisco, CA, May 2015
- ***Distinguished Lecture***, *Process Firewalls: Protecting Programs During Resource Access*, Florida International University, Miami, FL, March 2015
- *Process Firewalls: Protecting Programs During Resource Access*, University of Illinois, Chicago, Chicago, IL, October 2014
- *Process Firewalls: Protecting Programs During Resource Access*, Symantec Research Labs, Los Angeles, CA, July 2014 and *IBM Research Watson*, Yorktown Heights, NY, September 2014
- ***Panel***, *What are the Most Important Challenges for Access Control in New Computing Domains, such as Mobile, Cloud and Cyber-physical Systems?* ACM Symposium on Access Control Models and Technologies, London, Ontario, Canada, June 2014
- *Policy Models to Protect Resource Retrieval*, ACM Symposium on Access Control Models and Technologies, London, Ontario, Canada, June 2014
- *Protecting Programs During Resource Access*, Microsoft Research Cambridge and Cambridge University, Cambridge, UK, April 2014
- *Producing Minimal Hook Placements to Enforce Authorization Policies*, UC Irvine and UCLA, January and February 2014
- *Detecting and Preventing Vulnerabilities During Resource Access*, Virginia Tech University*,* Blacksburg, VA, October 2013
- *Cloud Computing Security (Parts 1 and 2) and Cloud Verifier (Hands-On) Lab*, Howard University, Washington, DC, September and October 2013
- ***Keynote Talk***, *How Much Control Should Customers Demand over Cloud-based Applications?* Trusted Clouds Workshop 2013 (TClouds) (affiliated with the European Symposium on Computer and Information Security (ESORICS)), Egham, UK*,* September 2013
- *Cloud Verifier (Hands-On) Lab*, Trusted Infrastructure Workshop, State College, PA, June 2013
- *System-wide Vulnerability Testing by Emulating Authorized Adversary Actions*, Microsoft Corporation, Redmond, WA, May 2013
- ***Distinguished Lecture***, *Detecting and Preventing Vulnerabilities During Resource Access*, Kansas State University, Manhattan, KS, April 2013
- *Adversary Accessibility: The Key to Finding and Fixing Vulnerabilities*, Intelligent Automation, Rockville, MD, November 2012, Lehigh University, Bethlehem, PA, January 2013, Purdue University, West Lafayette, IN, and University of Vermont, Burlington, VT, March 2013
- *Transforming Commodity Security Policies to Enforce Clark-Wilson Integrity*, Annual Computer Security Applications Conference, Orlando, FL, December 2012

Trent Jaeger

- *Configuring Cloud Computations for Integrity*, Computer and Electronics Security Applications Rendezvous, Rennes, France, November 2012
- *Leveraging Choice to Automate Authorization Hook Placement*, ACM Conference on Computer and Communications Security, Raleigh, NC, October 2012
- *Automating Authorization Hook Placement*, Microsoft Research, Redmond, WA, August 2012
- *Practical Verification of Integrity for Cloud Computing Environments*, University of Oxford*,* Oxford, UK, June 2012
- *STING: Finding Program Vulnerabilities to Name Resolution Attacks*, Imperial College, London and HP Labs, Bristol, UK, June 2012
- *Towards System-Wide, Deployment-Specific MAC Policy Generation for Proactive Integrity*, ETISS (at TU Darmstadt), HP Labs, Bristol UK, and Royal Holloway University of London, September 2011
- *Tackling System-Wide Integrity*, Purdue University, West Lafayette, IN, November 2010
- *High Integrity Computing for Embedded Systems*, Trusted Computing for Embedded Systems, Carnegie-Mellon University, Pittsburgh, PA, November 2010
- *Cloud Security: Challenges and Opportunities*, USENIX HotCloud (Panel), Boston, MA, June 2010
- ***Invited Lecture***, *Virtualization Security*, Trusted Infrastructure Workshop, Carnegie-Mellon University, Pittsburgh, PA, June 2010
- *Designing Systems to Manage Attack Surfaces*, Georgia Institute of Technology, Atlanta, GA and Carleton University, Ottawa, ON, April 2010
- *Building Systems to Enforce Measurable Security Goals*, University of Michigan, Ann Arbor, MI, and Telcordia Technologies, Piscataway, NJ, October 2009
- *Analysis of Virtual Machine Policies*, SELinux Summit, Portland, OR, September 2009
- *Building Systems to Enforce Measurable Security Goals*, Microsoft Research, Redmond, WA, and Galois, Inc., Portland, OR, September 2009
- *Towards Automatic Retrofitting of Programs for Security*, IBM Research*,* Hawthorne, NY, August 2009
- ***Invited Talk****, A Case for Integrity-Verified Channels*, Trusted Infrastructure Workshop (at CMU), Pittsburgh, PA, June 2009
- ***Invited Talk****, Building Integrity-Verified Channels*, ICT-FORWARD Workshop, Beaulieu sur Mar, France, May 2009
- ***Invited Talk****, Building Systems to Enforce Measurable Security Goals*, Invited talk for the Zurich Information Security Center (ZISC) Workshop on Advanced Concepts in Access and Usage Control, Zurich, Switzerland, September 2008
- *Verifying Compliance for Trusted Programs*, IBM Research*,* Hawthorne, NY, June 2008
- *Building High-Integrity Phone Systems*, Samsung Digital Corporation, Suwon, South Korea, June 2008
- *Verifying Compliance for Trusted Programs*, Cornell University*,* Ithaca, NY, April 2008
- *Building High-Integrity Phone Systems*, NSF Wireless Security Workshop*,* Atlanta, GA, April 2008
- *Building Shared Reference Monitors*, Johns Hopkins University*,* Baltimore, MD, October 2007
- *A Logical Specification and Analysis for SELinux MLS* and *Managing the Risk of Covert Information Flows in Virtual Machine Systems*, 12th ACM Symposium on Access Control Models and Technologies, Sophia Antipolis, France, June 2007
- *Building Shared Reference Monitors*, Dartmouth College, Hanover, NH, April 2007
- *Cell Phone System Integrity*, Penn State Applied Research Lab*,* University Park, PA, April 2007
- *From Trusted to Secure*, Georgia Institute of Technology*,* Atlanta, GA, January 2007
- *Leveraging IPsec for Mandatory Access Control across Systems*, Second International Conference on Security and Privacy in Communication Networks, Baltimore, MD, August 2006
- *Shame on Trust in Distributed Systems*. 2006 Workshop on Hot Topics in Security, August 2006
- *Towards a Shared Reference Monitor System*, Air Force Research Lab, Rome, NY, July 2006
- *PRIMA: Policy-reduced Integrity Measurement Architecture*, 11th Symposium on Access Control Models and Technologies. Lake Tahoe, CA, June 2006

- *SELinux Protected Paths Revisited*, 2nd SELinux Symposium, Baltimore, MD, March 2006
- *Computer Security Heresies Revisited*, University of Wisconsin, Madison, Madison, WI, January 2006
- *Leveraging IPsec for Network Access Control in Linux*, 2005 Annual Computer Security Applications Conference, Tucson, AZ, December 2005
- *Leveraging IPsec for Network Access Control in Linux*, 2005 SELinux Symposium, Silver Spring, MD, March 2005
- *Clark-Wilson Integrity as a Security Goal for SELinux Policies*, 2005 SELinux Symposium, Silver Spring, MD, March 2005
- *Analytic Integrity*, Carnegie-Mellon University and University of Pittsburgh, Pittsburgh, PA, December 2004
- *Fun and Progress in Using Static Analysis for Security*, University of Michigan, Ann Arbor, MI, September 2003
- *Analyzing Integrity Protection in the SELinux Example Policy*, 12th USENIX Security Symposium, Washington, DC, August 2003
- *Verification of the Linux Security Modules Framework*, UC Berkeley, Berkeley, CA and Stanford University, Stanford, CA, May 2003
- *Verification of the Linux Security Modules Framework*, SUNY Stony Brook, Stony Brook, NY, April 2003
- *Runtime Verification of the Linux Security Modules Framework*, 9th Conference on Computer and Communications Security, Washington, DC, November 2002
- *Managing Access Control Policies Using Access Control Spaces*, 7th Symposium on Access Control Models and Technologies, Monterey, CA, June 2002
- ***Panels***, *Making Access Control More Usable* and *Analysis Approaches for Verification of the Linux Security Modules Framework*, 7th Symposium on Access Control Models and Technologies, Monterey, CA, June 2002

Patents

IBM Research

- Stefan Berger, Kenneth Goldman, Trent Jaeger, Ronald Perez, Reiner Sailer, Enriquillo Valdez, "*Method, System, and Program Product for Remotely Attesting to a State of a Computer System,"* US Patent Number 10,242,192 (March 26, 2019)
- Stefan Berger, Kenneth Goldman, Trent Jaeger, Ronald Perez, Reiner Sailer, Enriquillo Valdez, "*Method, System, and Program Product for Remotely Attesting to a State of a Computer System,"* US Patent Number 9,836,607 (December 5, 2017)
- Stefan Berger, Kenneth Goldman, Trent Jaeger, Ronald Perez, Reiner Sailer, Enriquillo Valdez, "*Method, System, and Program Product for Remotely Attesting to a State of a Computer System,"* US Patent Number 9,536,092 (January 3, 2017)
- Stefan Berger, Kenneth Goldman, Trenton R. Jaeger, Ronald Perez, Reiner Sailer, Enriquillo Valdez, "*Method, System, and Program Product for Remotely Attesting to a State of a Computer System,"* US Patent Number 9,298,922 (March 29, 2016)
- Trent Jaeger, Lawrence Koved, Liangzhao Zeng, Xiaolan Zhang, *"Methods and Arrangements for Unified Program Analysis,"* US Patent Number 8,640,107 (January 28, 2014)
- Trent Jaeger, Reiner Sailer, Leendert van Doorn, "*Method, System and Program Product for Remotely Verifying Integrity of a System,"* US Patent Number 8,434,147 (April 30, 2013)
- Trent Jaeger, Lawrence Koved, Liangzhao Zeng, Xiaolan Zhang, *"Methods and Arrangements for Unified Program Analysis,"* US Patent Number 8,370,813 (February 5, 2013)

- Kay Anderson *et al.*, “*System and Method for Security Planning with Soft Security Constraints,”* US Patent Number 8,132,259 (March 6, 2012)
- Kay Anderson *et al.*, “*Method of Managing and Mitigating Security Risks Through Planning,”* US Patent Number 8,099,781 (January 17, 2012)
- Pau-Chen Cheng *et al.*, “*Fuzzy Multi-level Security*,” US Patent Number 8,087,090 (December 27, 2011)
- Stefan Berger, Trent Jaeger, Ronald Perez, Reiner Sailer, Enriquillo Valdez*, “Method and Apparatus to Protect Policy State Information During the Life-Time of Virtual Machines,”* US Patent Number 7,856,653 (December 21, 2010)
- Kay Anderson *et al.*, “*Method of Managing and Mitigating Security Risks Through Planning,”* US Patent Number 7,832,007 (November 9, 2010)
- Pau-Chen Cheng *et al.*, “*System and Method for Fuzzy Multi-level Security*”, US Patent Number 7,530,110 (May 5, 2009)
- Trent Jaeger, Lawrence Koved, Liangzhao Zeng, Xiaolan Zhang, *“Methods and Arrangements for Unified Program Analysis,”* US Patent Number 7,493,602 (February 17, 2009)
- Trent Jaeger, John Earnshaw Tidswell, *“Mechanism for Synchronous Interprocess Communication over Transparent External Monitors,”* US Patent Number 6,862,734 (March 1, 2005)
- Kevin Elphinstone, Trent Jaeger, *“Flexible Interprocess Communication via Redirection,”* US Patent Number 6,748,452 (June 8, 2004)
- Nayeem Islam, Trent Jaeger, Jochen Liedtke, Vsevelod Pantelenko, *“Powerful and Flexible Server Architecture,”* US Patent Number 6,490,625 (December 2, 2002)
- Nayeem Islam, Trent Jaeger, Jochen Liedtke, Vsevelod Pantelenko, *“Flexible Cache-Coherency Mechanism,”* US Patent Number 6,202,132 (March 13, 2001)
- Rangachari Anand, Frederique Giraud, Nayeem Islam, Trent Jaeger, Jochen Liedtke, *“Flexible and Dynamic Derivation of Permissions,”* US Patent Number 6,044,466 (March 28, 2000)
- Nayeem Islam, Trent Jaeger, Jochen Liedtke, Vsevelod Pantelenko, *“Flexible Cache-Coherency Mechanism,”* US Patent Number 6,032,228 (February 29, 2000)

General Motors

- Kent Kienzle, Mark, Jeffery, Trent Jaeger, Karon Barber, *“Expert System for Automatically Generating Gear Designs,”* US Patent Number 5,297,054 (March 22, 1994)

University Service

Masters and Undergraduates Advised

- Curtis Walker, M.S.E., CSE, Summer 2006 (co-advised with Padma Raghavan, CSE)
- Craig Suchanec, B.S., CMPSC, Schreyer Honors College, Fall 2006
- Vikhyath Rao, M.S., EE, Fall 2007 (co-advised with Ken Jenkins, EE)
- Albert Tannous, M.S., CSE, Spring 2008
- Chandrika Gopalakrishna, M.S., CSE, Spring 2008 (co-advised with Jim Jansen, IST)
- Radhesh Kamath, M.S., CSE, Summer 2008
- Yogesh Sreenivasan, M.S., CSE, Summer 2008
- Mohamed Hassan, M.S., CSE, Summer 2008
- Anuj Sawani, M.S., EE, Summer 2008 (co-advised with George Kesidis, EE)
- Dhivarkar Mani, M.S., CSE, Spring 2009
- Christopher Shal, B.S. and M.S., CMPSC and CSE, Spring 2009
- Vikhyath Rao, M.S., CSE, Fall 2009
- Guruprasad Jakka, M.S., CSE, Summer 2010

- David Schmidt, M.S., CSE, Fall 2013
- Adam Bergstein, M.S., CSE, Summer 2014
- Caleb Severn, M.S.E., CSE, Winter 2015
- Taylor Loz, B.S., CMPSC, Spring 2017
- Nirupama Talele, M.S., CSE, Fall 2017
- Kushal Dayananda, M.S.E., CSE, Summer 2018
- Mihir Gorecha, M.S.E., CSE, Summer 2018
- Michael Steward, M.S., CSE, Spring 2020
- Kirti Jagtap, M.S., CSE, Summer 2020
- Kaiming Huang, M.S., CSE, Summer 2020
- Dovile Drozdovaite, B.S., CMPSC, Fall 2020
- John Dukewich, B.S., CMPSC, Spring 2021
- Rahul George, M.S., CSE, Summer 2021
- Ryan Pasculano, M.S., CSE, Summer 2021
- Gabriel Stewart, B.S., CMPSC, Spring 2022
- Sophia Beyda, M.S., CSE, Fall 2022
- David Reinoso, M.S., CSE, Spring 2023
- Frank Capobianco, M.S., CSE, Summer 2023

Ph.D. Thesis Committee Member for (all Computer Science and related unless indicated)

- Patrick McDaniel, University of Michigan, Ann Arbor. Completed in 2001.
- Paolo Perlasca, University of Milan (Italy). Completed in 2004.
- Vinod Ganapathy, University of Wisconsin, Madison. Completed in 2007.
- Boniface Hicks, Pennsylvania State University. Completed in 2007.
- Kameswari Kotapati, Pennsylvania State University. Completed in 2007.
- Patrick Traynor, Pennsylvania State University. Completed in 2008.
- Hung-Yuan Hsu, Pennsylvania State University. Completed in 2008.
- Yan Sun, Pennsylvania State University. Completed in 2009.
- Glenn Wurster, Carleton University (Canada). Completed in 2010.
- Christian Payne, Murdoch University (Australia). Completed in 2010.
- Yi Yang, Pennsylvania State University. Completed in 2010.
- Kevin Butler, Pennsylvania State University. Completed in 2010.
- Machigar Ongtang, Pennsylvania State University. Completed in 2010.
- William Enck, Pennsylvania State University. Completed in 2011.
- Sriram Govindan, Pennsylvania State University. Completed in 2011.
- Thomas Moyer, Pennsylvania State University. Completed in 2011.
- Byung Chul Tak, Pennsylvania State University. Completed in 2012.
- Xi Xiong, Pennsylvania State University – IST Dept. Completed in 2012.
- Stephen McLaughlin, Pennsylvania State University. Completed in 2014.
- Damien Octeau, Pennsylvania State University. Completed in 2014.
- David Cock, University of New South Wales (Australia). Completed in 2014.
- Ye Zhang, Pennsylvania State University. Completed in 2015.
- Peter Johnson, Dartmouth College. Completed in 2016.
- Xiaokui Shu, Virginia Tech University. Completed in 2016.
- Wai-Kit Sze, Stonybrook University. Completed in 2016.
- Wenhui Hu, Pennsylvania State University. Completed in 2016.
- Stefan Achleitner, Pennsylvania State University. Completed in 2017.
- Nicolas Papernot, Pennsylvania State University. Completed in 2018.
- Zhen (James) Huang, University of Toronto (Canada). Completed in 2018.

- Dongpeng Xu, Pennsylvania State University – IST Dept. Completed in 2018.
- Jun Xu, Pennsylvania State University – IST Dept. Completed in 2018.
- Shuai Wang, Pennsylvania State University – IST Dept. Completed in 2018.
- Anirudh S. Iyengar, Pennsylvania State University – EE Dept. Completed in 2018.
- Hai Nguyen, Rutgers University. Completed in 2018.
- Nasim Imtiaz Khan, Pennsylvania State University – EE Dept. Completed in 2019.
- Shen Liu, Pennsylvania State University. Completed in 2020.
- Asmit De, Pennsylvania State University – EE Dept. Completed in 2021.
- Peixuan Li, Pennsylvania State University. Completed in 2021.
- Dongrui Zeng, Pennsylvania State University. Completed in 2021.
- Guillaume Hiet, University of Rennes 1 (France) – Habilitation à Diriger des Recherche (HDR, accreditation to supervise research). Completed in 2021.
- Yueqi Chen, Pennsylvania State University – IST Dept. Completed in 2022.
- Jiyong Yu, University of Illinois. Completed in 2023.
- Wenhui Zhang, Pennsylvania State University – IST Dept. Completed in 2023.
- Vikram Narayan, University of Utah. Completed in 2023.
- Michael Norris, Pennsylvania State University, in progress.
- Yongzhe Huang, Pennsylvania State University, in progress.
- Guoren Li. UC Riverside, in progress.

University Service Committees

University of California, Riverside, University Committees

- Special Review Committee, 2024

University of California, Riverside, Computer Science and Engineering Department

- Graduate Admissions, 2023-2024

Penn State, College of Engineering

- Promotion and Tenure, 2022-2023
- AC14 Administrative Review Committee for the Department Head for Chemical Engineering, 2019
- EECS School Transition Committee, 2015
- College of Engineering Representative to the Graduate Studies and Research Committee, 2009-2013
- Sabbatical Leave Committee, 2007-2008, 2008-2009
- Undergraduate Advising, College of Engineering, 2006

Penn State, School of Electrical Engineering and Computer Science

- Promotion and Tenure (elected), 2016-2019, 2019-2021, 2021-2023
- EECS Strategic Committee, 2017-2020

Penn State, Computer Science and Engineering Department

- Promotion and Tenure (elected): 2008-2011, 2016-2019, 2019-2022
- Faculty Recruiting, 2007-2009, 2014-2017, 2019-2023
- Graduate Admissions, 2006-2008, 2010-2012, 2021-2023
- ABET Committee, 2018-2020
- Curriculum, 2016-2019
- ACM Advisor, 2013-2019
- Web/Newsletter, 2015-2019
- Department Head Search Committee, 2016-2017

- CSE Strategic Committee, 2014-2015
- Chair, IT Committee, 2011-2012
- Chair, Faculty Recruiting, 2008-2009
- Lab Space, 2005-2010

Organization Memberships

- ACM Fellow
- IEEE Senior Member
- USENIX