Trent Jaeger

Office Address:
346A IST Building
Computer Science and Engineering Dept.
The Pennsylvania State University
Phone: +1 (814) 865-1042; Fax: +1 (814) 865-3176
Email: tjaeger@cse.psu.edu

Home Address:
153 Brothers Court
Port Matilda, PA 16870
Phone: +1 (814) 234-2075

Birth Date: June 14, 1962
Family Status: Married with two sons
Citizenship: USA

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, access control systems, trusted computing, source code analysis for security, and operating systems design and implementation

---

Awards and Honors

- Joel and Ruth Spira Excellence in Teaching Award, 2017
- Elected ACM SIGSAC Chair, July 2013-June 2017 term
- Outstanding Teaching Award, Penn State Computer Science and Engineering Department, 2012
- Hewlett-Packard Innovation Research Program Award, 2011-12 (renewed for 2012-13)
- Cisco University Research Program Award, 2007 (with La Porta and McDaniel)
- IBM Faculty Partnership Award, 2006
- Second Patent Plateau, IBM, 2005
- Papers invited for ACM TISSEC journal publication, 2000, 2001, 2002, and 2007
- Best Student Paper, USENIX Security Symposium, 1996
- USYSA "D" certificate (soccer coach), 2005

Professional Experience

The Pennsylvania State University, University Park, PA

2013-current *Professor, Computer Science and Engineering Department*
Co-director of the System Infrastructure and Internet Security (SIIS) Lab leading projects in systems security research projects for improving program, operating system, virtualization, and cloud security

2005-2013 *Associate Professor, Computer Science and Engineering Department (Tenured, 2008)*
Led research projects in computer security research on Linux operating systems, mobile phone systems, cloud computing systems, trusted computing and virtualization infrastructure, and retrofitting code

Trent Jaeger

IBM Thomas J. Watson Research Center, Hawthorne, NY
2001-2005 *Research Staff Member, Research Division, Security Department*
Research Liaison to the IBM Linux Technology Center leading group of researchers to improve Linux security through contributions to the Linux Security Modules framework, SELinux, and Labeled IPsec

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

Bell Communications Research (Bellcore), Morristown, NJ
1995 *Student Intern, Research Division, Network Security Department*
Research cryptographic protocols for verifying downloaded code

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

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

Electronic Data Systems, Troy, MI
1986-1991 *Advanced (1989) Knowledge Engineer, AI Services Department*
Built knowledge-based systems for gear set design, process planning, and manufacturing processes

Courses Taught

The Pennsylvania State University, University Park, PA (2005-present)

CMPSC 443	Introduction to Computer and Network Security (co-developed)
CMPSC 473	Introduction to Operating Systems
CSE 543	Computer and Network Security
CSE 544	Advanced Systems Security (developed)
CSE 597	Systems Security Seminar
CSE 598	Verification Methods for Security (developed)

Student Advising

Ph.D. Advisor for

- David H. King, *Retrofitting Programs for Complete Security Mediation*, August 2009 (co-advised with John Hannan) (Software Engineering Manager at Lyft)
- Sandra Rueda Rodriguez, *Methods for Specifying, Evaluating, and Resolving Security Policy Compliance Problems*, July 2011 (Assistant Professor at Universidad de los Andes, Bogota, Colombia)
- Joshua Seratelli Schiffman, *Practical System Integrity in Cloud Computing Environments*, July 2012 (Research Scientist at HP Labs)
- Divya Muthukumaran, *Automating the Placement of Authorization Hooks in Programs*, August 2013 (Postdoc at Imperial College, London)
- Hayawardh Vijayakumar, *Protecting Programs during Resource Access*, February 2014 (R&D Engineer at Samsung Research, USA)
- Xinyang Ge, *Enforcing Execution Integrity for Software Systems,* August 2016 (Senior Research Software Developer Engineer at Microsoft Research)

- Yuqiong Sun, *Protecting IAAS Clouds through Control of Cloud Services*, October 2016 (Principal Research Engineer at Symantec Research Labs)

Current Ph.D. Advisees

- Giuseppe Petracca, CSE Ph.D., expected graduation Spring 2018
- Frank Capobianco, CSE Ph.D., expected graduation Spring 2019
- Aditya Basu, CSE Ph.D., expected graduation Spring 2021
- Ben Heidorn, CSE Ph.D., expected graduation Spring 2021

Expert Witness Activities

- *Finjan, Inc. v. Blue Coat Systems, Inc. for the Northern District of California,* Civil Action No.: 5:15-cv-03295-BLF-PSG, 2016-present (client: Finjan)
- *Finjan, Inc. v. Sophos, Inc. for the Northern District of California,* Civil Action No. 3:2014-cv-01197, 2015-2016 (client: Finjan)
- *Finjan, Inc. v. Proofpoint, Inc. for the Northern District of California,* Civil Action No. 3:2013-cv-05808, 2015-2016 (client: Finjan)
- *Rembrandt Patent Innovations, LLC et al. vs. Apple Inc. for the Northern District of California,* Civil Action No. CAND-3-14-cv-05093, 2015-2016 (client: Apple)
- *Finjan, Inc. v. Websense, Inc. for the Northern District of California,* Civil Action No. 13-cv-04398-BLF, 2014 (client: Finjan)
- *Finjan, Inc. v. Blue Coat Systems, Inc. for the Northern District of California,* Civil Action No.: 13-cv-03999-BLF, 2014 (client: Finjan)
- *The Trustees of Columbia University in the City of New York v. Symantec Corporation for the Eastern District of Virginia,* Civil Action No. 3:13-cv-808-JRS, 2014-2015 (client: Symantec)
- *Inter Partes Review on behalf of Finjan, Inc. regarding patents of FireEye, Inc., 2013-14*
- *TQP Development LLC v. The Hertz Corporation, United States District Court for the Eastern District of Texas,* Civil Action No. 12-cv-702-WCB-RSP, 2013-14 (client: TQP)
- *TQP Development LLC v. Intuit, Inc., United States District Court for the Eastern District of Texas,* Civil Action No. 12-cv-180-WCB-RSP, 2013-14 (client: TQP)
- *TQP Development LLC v. Google, Inc., United States District Court for the Eastern District of Texas,* Civil Action No. 2:12-CV-061-JRG-RSP, 2013-14 (client: TQP)
- *TQP Development LLC v. 1-800-Flowers.com, Inc., et al.,* United States District Court for the Eastern District of Texas, Civil Action No. 2:11-cv-00248, 2013 (client: TQP)
- *TQP Development LLC v. Wells Fargo & Company, United States District Court for the Eastern District of Texas,* Civil Action No. 2:12-CV-00061-MHS-RSP, 2013 (client: TQP)
- *TQP Development LLC v. Alaska Air Group, et al., United States District Court for the Eastern District of Texas,* Civil Action No. 2:11-cv-00398**,** 2013 (client: TQP)
- *TQP Development LLC v. Merrill Lynch & Co., Inc., et al.,* United States District Court for the Eastern District of Texas, Civil Action No. 2:08-cv-00471, 2011-12 (client: TQP)
- *Motorola Mobility, Inc. v. Apple, Inc.,* United States District Court for the Southern District of Florida, Civil Action No. 10-cv-23580, 2011-14 (client: Apple)
- *Motorola Mobility, Inc. v. Apple, Inc.,* United States District Court for the Western District of Wisconsin, Civil Action No. 10-cv-662, 2011-12 (client: Apple)
- *The PacID Group LLC v. Apple, Inc., et al.,* United States District Court for the Eastern District of Texas, Civil Action No. 6:09-cv-143-LED-JDL, 2010 (client: The PacID Group)

- *Information Protection and Authentication of Texas, LLC v. Symantec, Corp. et al.,* United States District Court for the Eastern District of Texas, Civil Action No. 2:08-cv-00484-DF-CE, 2009 (client: Novell, a defendant)
- *Finjan Software Ltd. v. Secure Computing Corp.,* United States District Court for the District of Delaware, Civil Action No.: 06-369-GMS, 2007-8 (client: Finjan Software, as defendant in countersuit)

Other Consulting

- *Magic Pins, Inc.,* Product security evaluation, April 2006-December 2006*,* New York

---

Grants Awarded

- **Co-PI,** *Office of Naval Research*, Data-driven Vulnerability Repair in Programs with a Cloud Analytics Architecture for Practical Deployment, July 2017-June 2020, $1,200,000
- **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/ Vinod Ganapathy of Rutgers, Christian Skalka of Vermont, and Gang Tan of Lehigh, September 2014-August 2018, $1,200,000
- **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 2023, $48,200,000
- **Co-PI**, *Defense Advanced Research Projects Agency, VET Program*, Vetting Whole COTS Systems for Safety Against Malicious Functionality (w/ David Brumley and Virgil Gligor of CMU), October 2013-September 2017, $4,000,000
- **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
- **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/ Vinod Ganapathy of Rutgers and Somesh Jha of Wisconsin), April 2012-March 2015, $729,466
- **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/ Adam Smith), September 2010-June 2012, $254,019

- **Co-PI,** *Lockheed Martin Corporation*, Smart Grid Cyber Security Research (w/ Patrick McDaniel), January 2010-December 2010, $250,000
- **PI,** *National Science Foundation (TC:Medium),* CNS-0905343, Techniques to Retrofit Legacy Code with Security (w/ Michael Hicks of Maryland, Somesh Jha of Wisconsin, and Ninghui Li of Purdue), September 2009-September 2013, $1.2 million
- **Co-PI,** *National Science Foundation (CPS:Small),* CPS-0931914, Establishing Integrity in Dynamic Networks of Cyber Physical Devices (w/ Vinod Ganapathy and Uli Kremer, both of Rutgers), September 2009-August 2013, $540,000
- **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, 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/ Patrick McDaniel and Thomas La Porta), September 2007-September 2010, $658,200
- **PI**, *Disruptive Technology Office* (now IARPA)*,* System-Wide Information Flow Enforcement (w/ Patrick 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/ Thomas La Porta and Patrick 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/ Patrick McDaniel), September 2006-August 2010, $400,000
- **Co-PI**, *Raytheon Corporation,* Symbian Cellphone Attacks (w/ Yener and La Porta), 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

Penn State University

• OpenStack Pileus*	Extended OpenStack cloud that protects the execution of cloud users' commands by spawning cloud services for commands dynamically, scheduling them to cloud nodes to minimize interaction with other users, and governing services using decentralized information flow control
• Intel PT Linux*	Linux kernel that uses the Intel Processor Trace (PT) feature to record control

Trent Jaeger

(Griffin)	flow system-wide and enforce security policies, such as control-flow integrity
• CFI Kernels*	Automated method to retrofit kernel software (VMMs, microkernel systems, conventional kernels) to enforce fine-grained control flow integrity efficiently (currently supports MINIX and FreeBSD)
• 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
• AuDroid*	Android security mechanism to prevent unauthorized use of audio side channels, including eavesdropping and command replay
• Process Firewall*	Protect processes from vulnerabilities during retrieval of system resources by automatically inferring programmer intent
• Authorization Hook Placement	Automated placement of authorization hooks for legacy programs to mediate "choices" made by client requests where necessary to enforce access policies
• STING Testing*	Dynamic testing for name resolution vulnerabilities by detecting unsafe pathnames and replacing with malicious pathnames as a adversary might
• Mediation Placement	Automatically place runtime information flow mediation (declassification and endorsement) into legacy Java and C code
• Hippocrates*	Tool for compliance analysis of multiple network and host security policies with system-wide security requirements (e.g., firewall and SELinux policies)
• Integrity Verification Proxy*	Bind secure communication channels to integrity requirements of one or more of the host endpoints
• 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
• Shamon	Shared Reference Monitor System built using Xen, SELinux, Labeled IPsec, Linux IMA, to create a verifiable, distributed access control system
• 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)

* - check for availability (some are available via open-source)

IBM Research

• Labeled IPsec	Authorize network access via SELinux using IPsec SAs (in mainline Linux since Linux 2.6.18)
• Xen sHype	Reference monitor for Xen (in Xen 3.0)
• PRIMA/IMA	Integrity measurement using secure hardware for Linux
• Gokyo	Graph-based access control policy analysis tool (applied to SELinux)
• Vali	Tools for static and dynamic analysis of Linux security hooks www.research.ibm.com/vali
• SawMill multiserver	Linux multiserver on L4 including servers for ext2 file system, TCP networking, and various drivers www.research.ibm.com/sawmill
• 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)

Publications

Books, Books Edited, and Book Chapters

1. Shiho Moriai, Trent Jaeger, Kouichi Sakurai, editors. *Proceedings of the 9th ACM Symposium on Information, Computer and Communications Security*, ASIACCS '14, ACM, June 2014.
2. Trent Jaeger. Reference Monitor. In *Encyclopedia of Cryptography and Security,* H. van Tilborg (Ed.), Springer, 2011.
3. Trent Jaeger. *Operating Systems Security*. Morgan & Claypool Publishers Series: Synthesis Lectures on Information Security, Privacy and Trust, Morgan & Claypool, 2008 (218 pages).
4. Trent Jaeger and Jon Solworth, editors. *Proceedings of the 2nd ACM Computer Security Architectures Workshop*, ACM, October 2008.
5. Trent Jaeger, editor. *Proceedings of the 2nd USENIX Workshop on Hot Topics in Security*, USENIX, July 2007.
6. Trent Jaeger and Elena Ferrari, editors. *Proceedings of the 9th ACM Symposium on Access Control Models and Technologies*, ACM, June 2004.
7. Sushil Jajodia, Vijayalakshmi Atluri, and Trent Jaeger, editors. *Proceedings of the 10th ACM Conference on Computer and Communications Security*, ACM, October 2003.
8. Ravi Sandhu and Trent Jaeger, editors. *Proceedings of the 6th ACM Symposium on Access Control Models and Technologies*, ACM, June 2001.
9. 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. 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, accepted for publication.
2. 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), accepted for publication.
3. Steve Lipner, Trent Jaeger, Mary Ellen Zurko. Lessons from VAX/SVS for High Assurance VM Systems. *IEEE Security & Privacy* 10(5), September/October 2012.
4. Thomas Moyer, Kevin Butler, Joshua Schiffman, Patrick McDaniel, Trent Jaeger. Scalable Web Content Attestation. *IEEE Transactions on Computers* 61(5), April 2012.
5. 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.

6. 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.
7. 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.
8. 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.
9. 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.
10. 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.
11. Trent Jaeger, Antony Edwards, Xiaolan Zhang. Policy Management Using Access Control Spaces. *ACM Transactions on Information Systems Security* (ACM TISSEC) 6(3), August 2003.
12. Trent Jaeger and Jonathon Tidswell. Practical Safety in Flexible Access Control Models. *ACM Transactions on Information Systems Security* (ACM TISSEC) 4(3), August 2001.
13. 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.
14. 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. 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%)
2. 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%)
3. 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)
4. 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.
5. 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* (ACM MobiSys), June 2017. (acceptance rate: 18%)
6. 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. (awarded "Best Student Paper", acceptance rate: 23%)
7. 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%)
8. 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%)

Trent Jaeger

9. 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%)
10. 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%)
11. 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.
12. 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%)
13. 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%)
14. 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%)
15. 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.
16. 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.
17. 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%)
18. 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%)
19. 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.
20. 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%)
21. 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%)
22. 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%)
23. 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%)
24. 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%)

Trent Jaeger

25. 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%)
26. 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.
27. 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%)
28. 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%)
29. 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%)
30. 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.
31. 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%)
32. 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.
33. 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%)
34. 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.
35. 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%)
36. 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%)
37. 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.
38. 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.
39. 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%)
40. 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%)
41. 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%)

Trent Jaeger

42. 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%)
43. 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%)
44. 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 International Symposium on Reliable Distributed Systems* (SRDS), September 2009.
45. 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%*)*
46. 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%)
47. 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.
48. 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%)
49. 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%)
50. 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%)
51. 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.
52. 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%).
53. 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%)
54. 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%)
55. 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%)
56. 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%)
57. 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%)
58. 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%)

Trent Jaeger

59. 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%)
60. 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.
61. 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%)
62. 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.
63. 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%)
64. 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%)
65. 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%)
66. 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%)
67. Vinod Ganapathy, Trent Jaeger, Somesh Jha. Retrofitting Legacy Code for Authorization Policy Enforcement. In *Proceedings of the 2006 IEEE Symposium on Security and Privacy* (IEEE S&P), May 2006. (acceptance rate: 13%)
68. Vinod Ganapathy, Trent Jaeger, Somesh Jha. Towards Automated Authorization Policy Enforcement. In *Proceedings of the 2nd SELinux Symposium,* March 2006.
69. Trent Jaeger. SELinux Protected Paths Revisited. In *Proceedings of the 2nd SELinux Symposium,* March 2006.
70. Umesh Shankar, Trent Jaeger, Reiner Sailer. Towards Automated Information-flow Integrity Verification for Security-critical Applications. In *Proceedings of the 2006 Annual Network and Distributed Systems Symposium* (NDSS), February 2006. (acceptance rate: 13%)
71. 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%)
72. 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 Compute and Communications Security* (ACM CCS), October 2005. (acceptance rate: 15%)
73. 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.
74. Reiner Sailer, Trent Jaeger, Xiaolan Zhang, Leendert van Doorn. Attestation-based Policy Enforcement for Remote Access. In *Proceedings of the 11th ACM Conference on Compute and Communications Security* (ACM CCS), October 2004. (acceptance rate: 14%)
75. Xiaolan Zhang, Trent Jaeger, Larry Koved. Applying Static Analysis to Verifying Security Properties. In *Proceedings of the 2004 Grace Hopper Conference,* October 2004.
76. 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%)

Trent Jaeger

77. 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%)
78. 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%)
79. 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%)
80. Trent Jaeger, Antony Edwards, Xiaolan Zhang. Gaining and Maintaining Confidence in Operating Systems Security. In *Proceedings of the ACM SIGOPS European Workshop,* September 2002.
81. 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.
82. 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%)
83. 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.
84. 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.
85. 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.
86. 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%)
87. 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.
88. 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.
89. Jonathon Tidswell and Trent Jaeger. Integrated Constraints and Inheritance in DTAC. In *Proceedings of the 5th ACM Workshop on Role-based Access Control*, July 2000.
90. Trent Jaeger. On the Increasing Importance of Constraints. In *Proceedings of the 4th ACM Workshop on Role-based Access Control*, November 1999.
91. 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.
92. 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.
93. 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.
94. 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.
95. 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.

Trent Jaeger

96. 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.
97. 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.
98. Trent Jaeger, Jochen Liedtke, Nayeem Islam. Fine-grained Protection in Operating Systems. In *Proceedings of the 6th USENIX Security Symposium*, January 1998.
99. 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.
100.Rangachari Anand, Nayeem Islam, Trent Jaeger, Josyula R. Rao. A Flexible Security Model for Using Internet Content. In *Proceedings of the 1997 Symposium on Reliable Distributed Systems* (SRDS), September 1997.
101.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.
102. 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.
103. 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.
104. 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.
105. Trent Jaeger, Avi Rubin, Atul Prakash. Building Systems That Flexibly Control Downloaded Executable Content. In *Proceedings of the 6th USENIX Security Symposium,* July 1996 (awarded "Best Student Paper").
106. Trent Jaeger and Avi Rubin. Preserving Integrity in Remote File Location and Retrieval. In *Proceedings of the Internet Society 1996 Symposium on Network and Distributed System Security* (NDSS), February 1996.
107. 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.
108. 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.
109. 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.
110. Trent Jaeger and Atul Prakash. Representation and Adaptation of Organization Coordination Knowledge for Autonomous Agent Systems. In *Proceedings of the 9th Int'l Conference on Software Engineering and Knowledge Engineering*, June 1995.
111. 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.
112. 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.
113. Trent Jaeger and Atul Prakash. BizSpec: A Business-oriented Model for Specification and Analysis of Office Information Systems. In *Proceedings of the 7th Int'l Conference on Software Engineering and Knowledge Engineering*, June 1993.
114. Trent Jaeger. Using AI Paradigms in Solving Manufacturing Problems as Demonstrated by the CPC Stacking/Destacking Advisor. In *Proceedings of the 3rd Int'l Conference on CAD/CAM, Robotics, and Factories of the Future*, Volume 2, August 1988.

Trent Jaeger

Other Publications

1. 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.*
2. 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.*
3. 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.*
4. 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.*
5. 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.*
6. 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.*
7. 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.*
8. Robert F. Erbacher, Trent Jaeger, Nirupama Talele, Jason Teutsch. Directed Multicut with Linearly Ordered Terminals. *CoRR abs/1407.7498*, August 2014.
9. Thomas Moyer, Trent Jaeger, Patrick McDaniel. Scalable Integrity-guaranteed AJAX. In *Proceedings of the 14th Asia-Pacific Web Conference (APWeb)*, April 2012. *Invited Paper.*
10. 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.*
11. 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*, Penn State Univ., April 2009.
12. Kevin Butler, Stephen McLaughlin, Thomas Moyer, Patrick McDaniel, and Trent Jaeger. SwitchBlade: Policy-driven Disk Segmentation. *Technical Report NAS-TR-0098-2008*, Penn State Univ., 2008.
13. 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, Department of Computer Science and Engineering, Penn State Univ., 2006.
14. 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.
15. Trent Jaeger, David Safford, Hubertus Franke. Linux Security for the Enterprise: Executive Summary. *IBM Research Whitepaper*, 2002.
16. Trent Jaeger, David Safford, Hubertus Franke. Security Requirements for the Deployment of the Linux Kernel in Enterprise Systems. *IBM Research Whitepaper*, 2002.
17. 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.
18. 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.*

19. 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.
20. 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.
21. 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)

- **General Chair**, ISOC Network and Distributed Systems Security Symposium (NDSS), selected from 2019-2020, and as Shadow General Chair in 2018
- **Steering Committee Member**, ISOC Network and Distributed Systems Security Symposium (NDSS), selected to start in 2018
- **Steering Committee Member**, ACM Conference on Computer and Communications Security (ACM CCS), 2013-present
- **Academic Advisory Board**, The Cyber Security Body Of Knowledge Project, funded by the National Cyber Security Programme, UK, 2017-present
- **Special Interest Group Executive Committee Member,** ACM Special Interest Group on Security, Audit, and Control (ACM SIGSAC), 2013-present (as Chair and past Chair)
- **Special Interest Group Chair,** ACM Special Interest Group on Security, Audit, and Control (ACM SIGSAC), 2013-2017
- **Co-Director**, Systems and Internet Infrastructure Security Lab, Penn State, 2005-present
- **Institute Member**, Institute for Network and Security Research (formerly Network and Security Research Center), Penn State, 2005-present
- **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 (ASIACCS), 2014
- **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
- **Associate Editor,** ACM Transactions on Internet Technology, 2007-2013
- **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
- **Guest Editor**, ACM Transactions on Information Systems Security, November 2002 issue
- **Panels Chair**, ACM Symposium on Access Control Models and Technologies, 2002-2003
- **Program Chair**, ACM Conference on Computer and Communications Security, Industry Track, 2003
- **Program Chair**, ACM Symposium on Access Control Models and Technologies, 2001
- **Program Chair**, ACM Workshop on Role-based Access Control, 1998

Trent Jaeger

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
- **PC Member**, ACM Conference on Computer and Communication Security (ACM CCS), Research Track: 2000-2003, 2006, 2009-2010, 2013-2015, 2017; Industry Track: 2004-2005
- **PC Member**, USENIX Security Symposium (USENIX Security), 1999-2001, 2005-2006, 2008-2009
- **PC Member**, ISOC Network and Distributed System Security Symposium (NDSS), 2007
- **PC Member**, ACM International Conference on Architecture Support for Programming Languages and Operating Systems (ACM ASPLOS), 2018
- **PC Member**, ACM European Conference on Computer Systems (EuroSys), 2011
- **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**, 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
- **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**, for several workshops on various security topics
- **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, Computers & Security, Journal of Computer Security, IBM Systems Journal, IEEE Transactions on Parallel and Distributed Systems, IEEE Transactions on Computers, IEEE Transactions on Knowledge and Data Engineering, Journal of Digital Libraries, International Journal of Information and Computer Security, Transactions on Cloud Computing
- **External reviewer** for conferences: USENIX Symposium on Operating System Design and Implementation, ACM Symposium on Operating Systems Principles, IEEE Hot Topics in Operating Systems, USENIX Annual Technical Conference, IEEE Workshop on Policies for Distributed Systems and Networks, ACM Computer-Supported Collaborative Work, Principles of Distributed Computing. IEEE INFOCOM, International Conference on Distributed Systems and Networks

---

External Presentations (Since 2002)

- ***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

Trent Jaeger

- ***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 at Florida International University*, Miami, FL, October 2015
- ***Invited 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 Speaker***, 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*, 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*, Irvine and Los Angeles, CA, 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

Trent Jaeger

- ***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
- Configuring Cloud Computations for Integrity, *Computer and Electronics Security Applications Rendezvous*, Rennes, France, November 2012
- Automating 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
- Virtualization Security, Invited Lecture, *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
- A Case for Integrity-Verified Channels, Invited talk for the *Trusted Infrastructure Workshop (at CMU)*, Pittsburgh, PA, June 2009
- Building Integrity-Verified Channels, Invited talk for *ICT-FORWARD Workshop*. Beaulieu sur Mar, France, May 2009
- 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, *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,* panel presentation, 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, *et al*., "*Method, System, and Program Product for Remotely Attesting to a State of a Computer System,"* filed August 2006.
- 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.*, "*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

- 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

Trent Jaeger

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.
- Dongpeng Xu, Pennsylvania State University – IST Dept. In progress.
- Shaui Wang, Pennsylvania State University – IST Dept. In progress.
- Jun Xu, Pennsylvania State University – IST Dept. In progress.
- Stefan Achleitner, Pennsylvania State University. In progress.

Committees

Penn State, College of Engineering service

- Undergraduate Advising, College of Engineering, Fall 2006
- Sabbatical Leave Committee, 2007-2008, 2008-2009
- College of Engineering Representative to the Graduate Studies and Research Committee, 2009-2013
- EECS School Transition Committee, 2015

Penn State, Computer Science and Engineering Department committees

- Strategic Committee, 2014-2015, 2017-2018
- Department Head Search Committee, 2016-2017
- Faculty Recruiting, 2007-2009, 2014-2017
- Chair, Faculty Recruiting, 2008-2009
- Chair, IT Committee, 2011-2012
- Promotion and Tenure, 2008-2011, 2016-2019
- Graduate Admissions, 2006-2008, 2010-2012

Trent Jaeger

- Curriculum, 2016-2017
- Lab Space, 2005-2010
- ACM Advisor, 2013-2017
- Web/Newsletter, 2015-2017