Patrick Drew McDaniel

Tsun-Ming Shih Professor of Computer Sciences
School of Computer, Data and Information Sciences ⋄ University of Wisconsin-Madison
Office : 7657 Morgridge Hall, 1205 University Ave ⋄ Madison, WI 53706 ⋄
email: mcdaniel@cs.wisc.edu ⋄ *Homepage*: `https://patrickmcdaniel.org/`
Phone (608) 263-1008 ⋄ *ORCID*: 0000-0003-2091-7484

ACADEMIC AND RESEARCH APPOINTMENTS

Tsun-Ming Shih Professor of Computer Sciences, 2022-Present
University of Wisconsin-Madison, Madison, WI

William L. Weiss Professor of Information and Communications Technology 2017-2022
Computer Science and Engineering, Pennsylvania State University, University Park, PA

Distinguished Professor 2016-2017
Computer Science and Engineering, Pennsylvania State University, University Park, PA

Professor 2011-2015
Computer Science and Engineering, Pennsylvania State University, University Park, PA

Associate Professor 2007-2011
Computer Science and Engineering, Pennsylvania State University, University Park, PA

Hartz Family Career Development Assistant Professor 2004-2007
Computer Science and Engineering, Pennsylvania State University, University Park, PA

Adjunct Professor 2003-2009
Stern School of Business, New York University, New York, NY

Senior Research Staff Member 2001-2004
AT&T Labs - Research, Florham Park, NJ

RESEARCH LEADERSHIP APPOINTMENTS

Director, National Science Foundation, Center for Trustworthy Machine Learning 2018-present
Participants: Penn State, Stanford, UC Berkeley, UC San Diego, Univ. of Wisconsin, Univ. of Virginia

Director, Institute for Networking and Security Research 2016-2022
College of Engineering, Pennsylvania State University, University Park, Pennsylvania

Program Manager, Cyber-Security Collaborative Research Alliance (CRA) 2013-2018
Army Research Laboratory/Pennsylvania State University, University Park, Pennsylvania

Co-Director, Systems and Internet Infrastructure Laboratory 2004-2022
College of Engineering, Pennsylvania State University, University Park, Pennsylvania

EDUCATION

Ph.D., Computer Science and Engineering, **University of Michigan**, Ann Arbor, MI 2001

M.S., Computer Science, **Ball State University**, Muncie, IN 1991

B.S., Computer Science **Ohio University**, Athens, OH 1989

AFFILIATIONS

Association for Computing Machinery (ACM), *Fellow*

The Institute of Electrical and Electronics Engineers (IEEE), *Fellow*

American Association for the Advancement of Science (AAAS), *Fellow*

USENIX Advanced Computing Systems Association (USENIX)

NON-PROFESSIONAL AFFILIATIONS

Aircraft Owners and Pilots Association

Porsche Club of America

Alumni Association of the University of Michigan, *Lifetime member*

Penn State Alumni Association, *Lifetime member*

STUDENTS

Past PhD Students

- *Eric Pauley*, Spring 2025, now **CEO/Assistant Professor**, DScope Security/Virginia Tech
- *Ryan Sheatsley*, Spring 2024, now **Post-doc**, University of Wisconsin-Madison
- *Z. Berkay Celik*, Spring 2019, now **Associate Professor**, Purdue University
- *Nicolas Papernot*, Spring 2018, now **Associate Professor**, University of Toronto
- *Wenhui Hu*, Fall 2016, now **Senior Member of Technical Staff**, Oracle
- *Devin Pohly*, Spring 2016, now **Senior Lecturer**, Wheaton College
- *Damien Octeau*, Summer 2014, now **Senior Staff Software Engineer**, Google
- *Steve McLaughlin*, Spring 2014, now **Senior Software Engineer**, Samsung Research America
- *Thomas Moyer*, Summer 2011, now **Assistant Professor**, University of North Carolina-Charlotte
- *William Enck*, Spring 2011, now **Goodnight Distinguished Professor in Security Sciences**, North Carolina State University
- *Kevin Butler*, Summer 2010, now **Professor**, University of Florida
- *Machigar Ongtang*, Summer 2010, now **Assistant Professor**, Dhurakij Pundit University
- *Patrick Traynor*, Spring 2008, now **John and Mary Lou Dasberg Preeminent Chair, Professor**, University of Florida, co-advisor
- *Fr. Boniface Hicks*, Fall 2007, now **Assistant Professor**, St. Vincent College

Current PhD Students

- *Jean-Charles Noirot Ferrand*, University of Wisconsin-Madison, Spring 2028
- *Kyle Domico*, University of Wisconsin-Madison, Spring 2028
- *Kunyang Li*, University of Wisconsin-Madison, Spring 2027
- *Yohan Beugin*, University of Wisconsin-Madison, Spring 2027
- *Blaine Hoak*, University of Wisconsin-Madison, Spring 2026
- *Quinn Burke*, University of Wisconsin-Madison, Spring 2026

Past Masters Students

- *Jean-Charles Noirot Ferrand*, University of Wisconsin-Madison, Spring 2025
- *Kyle Domico*, University of Wisconsin-Madison, Spring 2025
- *Ryan Guide*, Pennsylvania State University, Spring 2023
- *Rachel King*, Pennsylvania State University, Summer 2022
- *Alban Heon*, Pennsylvania State University, Spring 2023
- *Yohan Beugin*, Pennsylvania State University, Spring 2021
- *Ahmed Abdou*, Pennsylvania State University, Spring 2021
- *Adrien Cosson*, Pennsylvania State University, Summer 2020
- *Bolor Zolbayar*, Pennsylvania State University, Summer 2020
- *Alejandro Andrade*, Pennsylvania State University, Summer 2020
- *Quinn Burke*, Pennsylvania State University, Spring 2020
- *Eric Pauley*, Pennsylvania State University, Spring 2020
- *Sushrut Shringarputal*, Pennsylvania State University, Fall 2019

- *Raquel Alvarez*, Pennsylvania State University, Spring 2019
- *Valentin Vie*, Pennsylvania State University, Spring 2019
- *Ryan Sheatsley*, Pennsylvania State University, Fall 2018
- *Eric Kilmer*, Pennsylvania State University, Spring 2016
- *Nathan Lagerman*, Pennsylvania State University, Spring 2016
- *Matthew Dering*, Pennsylvania State University, Spring 2014
- *Phil Koshy*, M.S. Pennsylvania State University, Fall 2013
- *Diana Koshy*, M.S. Pennsylvania State University, Fall 2013
- *Steve McLaughlin*, M.S. Pennsylvania State University, Spring 2011
- *Sergei Miadzvezhanka*, M.S. Pennsylvania State University, Spring 2011
- *Adam Delozier*, M.S. Pennsylvania State University, Spring 2011
- *Juliet Uhlott*, M.Eng. Pennsylvania State University, Fall 2010
- *Damien Octeau*, M.S. Pennsylvania State University, Spring 2010
- *Thomas Moyer*, M.S. Pennsylvania State University, Spring 2009
- *Luke St. Clair*, M.S. Pennsylvania State University, Summer 2008
- *Lisa Johansen*, M.S. Pennsylvania State University, Spring 2008
- *Sunam Ryu*, M.S. Pennsylvania State University, Spring 2007
- *Dhananjay Bapat*, M.S. Pennsylvania State University (Electrical Engineering), Fall 2006
- *Jennifer Plasterr*, M.Eng. Pennsylvania State University, Summer 2006
- *Adam Kerr*, M.Eng. Pennsylvania State University, Fall 2006
- *William Enck*, M.S. Pennsylvania State University, Spring 2006
- *Wesam Lootah*, M.S. Pennsylvania State University, Spring 2006
- *Jon Hansford*, M.Eng. Pennsylvania State University, Fall 2005
- *John van Bremer*, M.Eng. Pennsylvania State University, Spring 2005

Past Post-Docs

- *Ryan Sheatsley*, graduated University of Wisconsin-Madison
- *Vaibhav Rastogi*, graduated Northwestern University
- *Robert Walls*, graduated University of Massachusetts, Amherst

TEACHING

University of Wisconsin-Madison, College of Letters and Science

- **CompSci 642 - Intro to Information Security** - Fall 2023, Fall 2024, Fall 2025
- **CompSci 839 - Emerging Trends in Systems Security and Privacy** - Spring 2025

Pennsylvania State University, College of Engineering

- **CMPSC311 - Introduction to Systems Programming** - Fall 2013, Fall 2014, Fall 2015, Fall 2016, Summer 2019, Spring 2020, Fall 2020, Fall 2021
- **CMPSC443 - Introduction to Computer and Network Security** - Spring 2006, Spring 2009, Fall 2017, Fall 2018
- **CSE543 - Computer and Network Security** - Fall 2004, Fall 2005, Fall 2008, Fall 2009, Fall 2011, Fall 2014
- **CSE544 - Advanced System Security** - Spring 2005, Spring 2007
- **CSE545 - Advanced Network Security** - Spring 2006, Spring 2008, Spring 2011
- **CSE597g - Principles, Analysis, and Applications of Computer Security** - Fall 2015
- **Security and Privacy of Machine Learning** - Fall 2016

- **Advanced Topics in the Security and Privacy of Machine Learning** - Spring 2017
- **CSE598 - Cell Phone Operating Systems** - Spring 2009
- **CSE598i - Web 2.0 Security** - Spring 2010
- **CSE598d - Topics in Applied Systems Security** - Fall 2010
- **CSE598e - Critical Infrastructure Security** - Fall 2011
- **CSE 597 – Emerging Trends in Computer Security** - Fall 2021
- **CMPSC297 – Introduction to C Programming in UNIX** - Fall 2021

New York University, Stern School of Business

- **B20.3157 Computer and Network Security** - Spring 2003, Summer 2004, Summer 2005
- **B20.3156 - Online Privacy** - Spring 2003, Summer 2004

HONORS, AWARDS, AND KEYNOTE ADDRESSES

Tsun-Ming Shih Professor of Computer Sciences, Endowed Professorship, University of Wisconsin-Madison, 2022

SIGSAC Outstanding Innovation Award, for innovative research in mobile device security, trustworthiness of machine learning, and systems security, ACM Special Interest Group on Security, Audit and Control (SIGSAC), 2021

AAAS Fellow, for distinguished contributions to the field of computational security and privacy, particularly for advancing algorithms for the formal analysis of mobile devices and applications, American Association for the Advancement of Science (AAAS), 2021

Penn State Engineering Society Premier Research Award, Given to one faculty member per year, the Penn State Engineering Alumni Society Premier Research Award recognizes and rewards an individual whose contributions to scientific knowledge through research are exemplary and internationally acclaimed, Penn State University, 2021

SIGOPS Hall of Fame Award, recognizing the paper "TaintDroid: an information-flow tracking system for realtime privacy monitoring on smartphones" (Will Enck first author), "which sparked an important research agenda on smartphone privacy that continues to this day", ACM Special interest Group in Operating Systems (SIGOPS), 2020

Penn State Engineering Society Outstanding Advising Award, award by the Penn State Engineering Society given to faculty in the College of Engineering who have made significant contributions as advisor, Penn State University, 2018

William L. Weiss Professor of Information and Communications Technology, Endowed Professorship, Pennsylvania State University, 2017

Outstanding Community Service Award, n recognition for leadership of the Technical Committee on Security and Privacy, IEEE Technical Committee on Security and Privacy, 2016

ACM Fellow, for contributions to computer and mobile systems security, Association for Computing Machinery (ACM), 2015

IEEE Fellow, for contributions to the security of mobile communication, Institute of Electrical and Electronics Engineers (IEEE), 2014

Faculty Marshal, College of Engineering, selected by student marshals for contributions to undergraduate education, leads procession into graduation ceremony, Penn State University, 2009

Penn State Engineering Society Outstanding Research Award, award by the Penn State Engineering Society given to faculty in the College of Engineering who have made significant contributions to knowledge in their field, Penn State University, 2009

Security and Product Safety Acknowledgement, in recognition of efforts in improving the security of Google Android cellular phone operating system, Google, 2008

Commendation for Exceptional Leadership and Achievement, in recognition of efforts as PI of the EVEREST study on election security in the state of Ohio, State of Ohio, 2008

IEEE Technical Committee on Security and Privacy Outstanding Community Service Award, in recognition for technical program management of the IEEE Security and Privacy symposia, Institute of Electrical and Electronics Engineers (IEEE), 2008

CAREER Award, highly competitive faculty early career research grant, National Science Foundation, 2007

Penn State Computer Science and Engineering Outstanding Teaching Award, given to best teacher in the department as selected by students, Department of Computer Science and Engineering, Penn State University, 2007

Certificate of Meritorious Service, acknowledging exemplary service as associate editor of ACM Transactions on Internet Technologies, Association for Computing Machinery (ACM), 2007

Hartz Family Career Development Professor, Devlopment Chair Professorship, Penn State University, 2004

Bang for the Buck Award, award for most feature-rich/useful software system in Dynamic Coalitions program, Defense Advanced Research Projects Agency (DARPA), 2002

Kennedy Space Center Fellowship, Graduate Research Fellowship, National Aeronautics and Space Administration (NASA), 1997

Electrical Engineering and Computer Science Summer Fellowship Award, summer research fellowship, University of Michigan, Ann Arbor, 1997

Dean's Citation for Perfect Academic Record, acknowledement of perfect academic record earned during master's degree, Ball State University, 1991

Paper Awards

1. **Most Influential Paper Award of ICSE 2015**, IccTA: Detecting Inter-Component Privacy Leaks in Android Apps, Proceedings of the 37th International Conference on Software Engineering (ICSE), 2025

2. **Andreas Pfitzmann Best Student Paper Award (runner-up)**, Interest-disclosing Mechanisms for Advertising are Privacy-Exposing (not Preserving), Proceedings on Privacy Enhancing Technologies (PETS), 2024

3. **Most Influential Paper of PLDI 2014**, FlowDroid: Precise Context, Flow, Field, Object-sensitive and Lifecycle-aware Taint Analysis for Android Apps, Proceedings of the 35th Conference on Programming Language Design and Implementation (PLDI), 2024

4. **Test of Time Award**, Semantically Rich Application-Centric Security in Android, Proceedings of the 25th Annual Computer Security Applications Conference (ACSAC), 2024

5. **Best paper (runner up)**, The CVE Wayback Machine: Measuring Coordinated Disclosure from Exploits Against Two Years of Zero-Days, Proceedings of the ACM 2023 Internet Measurement Conference (IMC), 2023

6. **CSAW ARC Finalist**, DScope: A Cloud-Native Internet Telescope, 32nd USENIX Security Symposium (USENIX Security 23), 2023

7. **Best paper**, Understanding the Ethical Frameworks of Internet Measurement Studies, The 2nd International Workshop on Ethics in Computer Security (EthiCS 2023), 2023

8. **J. D. Williams student paper award, Nuclear Security and Physical Protection division**, Development of Machine Learning Algorithms for Directional Gamma Ray Detection, Proceedings of the Institute of Nuclear Materials Management Annual Meeting (INMM), 2019

9. **Best paper**, Mission-oriented Security Model, Incorporating Security Risk, Cost and Payout, EAI International Conference on Security and Privacy in Communication Networks (SECURECOMM), 2018

10. **Best student paper**, Adversarial Network Forensics in Software Defined Networking, ACM Symposium on SDN Research (SOSR), 2017

11. **Science of Security Index of Significant Research in Cyber Security, Science of Security Virtual Organization (SOS-VO)**, Toward a Science of Secure Environments, IEEE Security &amp; Privacy Magazine, 2015
12. **Research Highlight**, TaintDroid: An Information-Flow Tracking System for Realtime Privacy Monitoring on Smartphones, Communications of the ACM, 2014
13. **Best artifact**, Retargeting Android Applications to Java Bytecode, 20th International Symposium on the Foundations of Software Engineering (FSE), 2012
14. **Best Paper**, Semantically Rich Application-Centric Security in Android, Proceedings of the 25th Annual Computer Security Applications Conference (ACSAC), 2009
15. **Best Student Paper**, Understanding Practical Application Development in Security-Typed Languages, 22st Annual Computer Security Applications Conference (ACSAC), 2006
16. **Best paper**, The Sleep Deprivation Attack in Sensor Networks: Analysis and Methods of Defense, Proceedings of the Innovations and Commercial Applications of Distributed Sensor Networks Symposi, 2005

Keynote Addresses

1. Keynote Adversarial Machine Learning: A 10-year Perspective, US-Taiwan Workshop on Cybersecurity, National Science Foundation, Arlington, VA, March, 2025.
2. Keynote Securitys Role in Achieving Sustainability, 29th ACM Conference on Computer and Communications Security (CCS), Los Angeles, CA, November, 2022.
3. Keynote Security, Game Theory, and Their Role in Achieving Sustainability, Conference on Decision and Game Theory for Security, Pittsburgh, PA, October, 2022.
4. Keynote Prognosticating the Future of IoT Security, 2022 IEEE SafeThings Workshop, San Francisco, CA, May, 2022.
5. Keynote The Challenges of Machine Learning in Adversarial Settings: A Systems Perspective, Robustness of AI Systems to Adversarial Attacks (RAISA3), Online, August, 2020.
6. Keynote The Challenges of Machine Learning in Adversarial Settings, Triangle Area Privacy and Security Day, Durham, NC, October, 2019.
7. Keynote The Challenges of Machine Learning in Adversarial Settings, 2019 Subversion and Assurance of AI Workshop, US National Reconnaissance Office, Washington, DC, March, 2019.
8. Keynote Attacks, Defenses, and Impacts of Machine Learning in Adversarial Settings, 2017 Conference on Security and Privacy in Communication Networks (SecureComm), Niagara Falls, Canada, October, 2017.
9. Keynote Tracing the Arc of Smartphone Application Security, 2017 ACM on International Workshop on Security And Privacy Analytics, Scottsdale, AZ, March, 2017.
10. Keynote Tracing the Arc of Smartphone Application Security, 12th International Conference on Information Systems Security , Jaipur, India, December, 2016.
11. Keynote The Limitations of Machine Learning in Adversarial Settings, 25th International Conference on Computer Communication and Networks (ICCCN 2016), Waikoloa, HI, August, 2016.
12. Keynote Learning from Ourselves: Where are we and where can we go in mobile systems security?, Mobile Security Technologies (MOST) 2016 Workshop, IEEE Computer Society Security and Privacy Workshops, San Jose, CA, May, 2016.
13. Keynote Eight Years of Mobile Smartphone Security, Center for Secure and Dependable Systems (CSDS) Cybersecurity Symposium, Coeur d'Alene, April, 2016.
14. Keynote The Importance of Measurement and Decision Making to a Science of Security, 2015 IEEE Conference on Communications and Network Security, Florence, Italy, September, 2015.

15. Keynote The Importance of Measurement and Decision Making to a Science of Security, 3rd International Symposium on Resilient Cyber Systems, Philadelphia, PA, August, 2015.
16. Keynote The Importance of Measurement and Decision Making to a Science of Security, 2015 Symposium and Bootcamp on the Science of Security (Hotsos), University of Illinois at Urbana-Champaign, April, 2015.
17. Keynote Security and Science of Agility, First ACM Workshop on Moving Target Defense (MTD 2014), Scottsdale, AZ, November, 2014.
18. Keynote A Secondary Internet Revolution: How the Smart Device has Changed the Information Security Landscape, IEEE New Technology Industry Seminar (NTIS '13), Everett, WA, August, 2013.
19. Keynote Permission-based Application Governance; A Step Forward or Backward?, 26th Annual WG 11.3 Conference on Data and Applications Security and Privacy (DBSec'12), Paris, France, July, 2012.
20. Keynote Scalable Integrity-Guaranteed AJAX, The 14th Asia-Pacific Web Conference (APWeb), Kunming, China, April, 2012.
21. Keynote Security Challenges and Solutions in Mobile Smartphone Applications, Computer Security Foundations Symposium, Domaine de l'Abbaye des Vaux de Cernay, France, June, 2011.
22. Keynote Password Exhaustion: Predicting the End of Password Usefulness, 2nd International Conference on Information Systems Security , Kolkata, India, December, 2006.
23. Keynote Physical and Digital Convergence: Where the Internet is the Enemy, Eighth International Conference on Information and Communications Security (ICICS '06), Raleigh, NC, December, 2006.

Distinguished Lectures

1. Distinguished Lecture Adversarial Machine Learning: A 10-year Perspective, Department of Electrical and Computer Engineering, Iowa State University, Ames, IA, January, 2025.
2. Distinguished Lecture Adversarial Machine Learning: A 10-year Perspective, NSF ACTION AI Institute Distinguished Lecture Series, Virtual, December, 2024.
3. Distinguished Lecture Adversarial Machine Learning: A 10-year Perspective, Department of Electrical and Computer Engineering, University of Illinois, Champaign-Urbana, Champaign, IL, November, 2024.
4. Distinguished Lecture The Challenges of Machine Learning in Adversarial Settings: A Systems Perspective, Department of Electrical and Computer Engineering, University of California, Los Angeles, Los Angeles, CA, December, 2023.
5. Distinguished Lecture The Challenges of Machine Learning in Adversarial Settings: A Systems Perspective, Computer Science Department, Michigan State University, Lansing, MI, November, 2023.
6. Distinguished Lecture The Challenges of Machine Learning in Adversarial Settings: A Systems Perspective, Temple University, Philadelphia, PA, March, 2022.
7. Distinguished Lecture The Challenges of Machine Learning in Adversarial Settings: A Systems Perspective, Computer Science Department, University of Wisconsin-Madison, Madison, WI, February, 2020.
8. Shutterstock Distinguished Lecture The Challenges of Machine Learning in Adversarial Settings, Computer Science Department, Stonybrook University, Stonybrook, NY, December, 2019.
9. Distinguished Blockchain Lecture The Challenges of Machine Learning in Adversarial Settings, Cylab Security and Privacy Institute, Carnegie Mellon University, Pittsburgh, PA, December, 2019.
10. Distinguished Speaker Series The Challenges of Machine Learning in Adversarial Settings, Department of Computer Science, University at Buffalo, Buffalo, NY, November, 2018.
11. Samuel D. Conte Distinguished Lecture Series The Challenges of Machine Learning in Adversarial Settings, Department of Computer Science, Purdue University, West Lafeyette, Indiana, November, 2018.

12. Distinguished Lecture The Challenges of Machine Learning in Adversarial Settings, Department of Software and Information Systems, University of North Carolina at Charlotte, Charlotte, NC, February, 2018.

13. Distinguished Lecture Attacks, Defenses, and Impacts of Machine Learning in Adversarial Settings, Celebrating 50 Years of Computer Science @ NC State, North Carolina State University, Raleigh, NC, October, 2017.

14. Distinguished Lecture Tracing the Arc of Smartphone Application Security, Computer Science Department and the Electrical and Computer Engineering Department Seminar Series, Colorado State University, Fort Collins, CO, October, 2017.

15. Distinguished Lecture Tracing the Arc of Smartphone Application Security, Rochester Institute of Technology, College of Computing and Information Sciences, Rochester, NY, September, 2017.

16. Distinguished Lecture Tracing the Arc of Smartphone Application Security, University of Texas-Dallas, Department of Computer Science, Dallas, TX, May, 2017.

17. Distinguished Lecture Tracing the Arc of Smartphone Application Security, The Ohio State University, Department of Computer Science and Engineering, Columbus, OH, March, 2017.

18. Distinguished Lecture Tracing the Arc of Smartphone Application Security, University of California-Irvine, Computer Science Department, Irvine, CA, March, 2017.

19. Distinguished Lecture Tracing the Arc of Smartphone Application Security, Virginia Technical University, Department of Computer Science, Blacksburg, VA, March, 2017.

20. Distinguished Lecture Six Years of Mobile Smartphone Security, CISPA Distinguished Lecture Series, Max Planck Institute/Saarland University, Saarbrucken Germany, July, 2015.

21. Distinguished Lecture Six Years of Mobile Smartphone Security, Technische Universtat Darmstadt, Darmstadt Germany, July, 2015.

22. Distinguished Lecture Security Challenges and Solutions in Mobile Smartphone Applications, Computer and Information Science Department, University of Oregon, Eugene, OR, April, 2011.

23. Distinguished Lecture Security Challenges and Solutions in Mobile Smartphone Applications, Department of Software Information SystemsCollege of Computing and Informatics, UNC Charlotte, Charlotte, NC, December, 2010.

24. Distinguished Lecture Exploiting Open Functionality in SMS-Capable Cellular Networks, Computer Science Department, University of Virginia, Charlottesville, VA, January, 2006.

RESEARCH SUPPORT

co-PI, *MURI: Cohesive and Robust Human-Bot Cybersecurity Teams*, Army Research Office, *$6,000,0000* (PSU award $739,527), 07/01/2021-06/30/2026, Collaborators: Many.

co-PI, *SaTC: CORE: Small: Adversarial Network Reconnaissance in Software Defined Networking*, NSF (CNS), *$500,000* (PSU award $500,000), 1/1/2020-12/31/2022, Collaborators: He (Penn State).

PI, *CNS Core: Medium: Automated IoT Safety and Security Analysis and Synthesis*, NSF (CNS), *$272,033* (PSU award $272,033), 6/25/2019-6/24/2022, Collaborators: Tan (Penn State).

PI, *Mapping Black-Box Attack Metrics and Parameter Spaces in Machine Learning*, US Army Aviation and Missile Research, Development and Engineering Center, *$436,677* (PSU award $436,677), 6/25/2019-6/24/2022, Collaborators: (single PI).

PI, *SaTC CORE: Frontier: Collaborative: End-to-End Trustworthiness of Machine-Learning Systems*, NSF (CNS), *$9,649,366* (PSU award $2,044,550), 8/15/2018-3/31/2023, Collaborators: Boneh (Stanford), Chaudhuri (UCSD), Evans (Virginia), Jha (Wisconsin), Liang (Stanford), Song (Berkeley).

PI, *2017 SaTC PI Meeting*, NSF (CNS), *$99,999* (PSU award $50,230), 8/15/2016-3/31/2017, Collaborators: Antonakakis (GaTech), Mason (UIUC).

PI, *TWC: Medium: Collaborative: Scaling and Prioritizing Market-Sized Application Analysis*, NSF (CNS), *$1,147,213* (PSU award $547,213), 7/01/2016-6/30/2020, Collaborators: Jha (Wisconsin).

PI, *Student Travel Support for Symposium on Security and Privacy 2014*, Army Research Office, *$10,000* (PSU award $10,000), 5/1/14-5/1/15.

PI, *Models for Enabling Continuous Reconfigurability of Secure Missions (MACRO) Cyber-Security Collaborative Research Alliance (CRA)*, Army Research Laboratory, *$24.1 million ($48.2 million with renewal at 12/17)*, 9/20/2013-9/19/2023 (renewed at 5 years), Collaborators: PSU, Carnegie Mellon, Indiana, UC Davis, UC Riverside, ARL, CERDEC.

PI, *Google Faculty Research Award, Plotting a Map of Android Inter-App Communication*, Google, *$50,000*, 3/1/2012-2/28/2013, Collaborators: PSU (McDaniel), TU Darmstadt (Bodden), University of Luxembourg (Traon), .

PI, *Battelle BGP Security Study (Phase 2)*, Battelle, *$102,815*, 10/1/2012-9/30/2013, Collaborators: PSU (McDaniel), Oregon (Butler).

PI, *TWC: Medium: Collaborative: Extending Smart-Phone Application Analysis*, NSF (CNS), *$1,386,518 (plus 16k REU supplement)* (PSU award $534,748), 8/1/2012-7/31/2016, Collaborators: PSU (McDaniel), Wisconsin (Jha).

PI, *Battelle BGP Security Study (Phase 1)*, Battelle, *$94,400*, 2/15/2012-9/30/2012, Collaborators: PSU (McDaniel).

co-PI, *TC: Medium: Collaborative Research: Building Trustworthy Applications for Mobile Devices*, NSF (CNS), *$1,386,518* (PSU award $350,000), 8/1/2011-7/31/2014, Collaborators: PSU (McDaniel), Wisconsin (Banerjee, Jha, Swift).

PI, *Closing the Loop on Security Testing and Security Requirements*, Security and Software Engineering Research Center, *$31,000*, 8/1/2011-7/31/2012.

co-PI, *Managing Security and Vulnerability Risks in the Smart Grid*, Institute for CyberScience and The Penn State Institutes of Energy and the Environment, *$31,000*, 08/1/09-12/16/09, Collaborators: PSU (Blumsack, McDaniel).

PI, *Smart Grid Cyber Security Research*, Lockheed Martin, *$250,000*, 1/1/10-12/16/10.

PI, *NSF HECURA: Collaborative Research: Secure Provenance in High-End Computing Systems*, NSF (CCF), *$1,000,000* (PSU award $307,073), 08/1/09-8/31/13, Collaborators: PSU (McDaniel), UIUC (Winslett), Stonybrook (Sion, Zadok).

PI, *TC: Medium: Collaborative Research: Security Services in Open Telecommunications Networks*, NSF (CNS), *$1,386,518* (PSU award $594,941), 08/01/09-08/01/12, Collaborators: PSU (McDaniel, La Porta), UPenn (Blaze), Columbia (Schulzrinne).

PI, *Characterizing and Mitigating Wireless Systems Vulnerabilities*, Defense University Research Instrumentation Program (DURIP), Army Research Office (ARO), *$150,000*, 05/22/09-02/28/11, Collaborators: PSU (La Porta, McDaniel).

co-PI, *Integrity Management for ICT Development*, Bell Labs Network Reliability and Security Office, Alcatel-Lucent , *$100,000*, 11/30/08-11/30/09, Collaborators: PSU (La Porta, McDaniel).

PI, *Utility Grid Automation and Risk Management*, Lockheed Martin, *$400,000*, 11/30/08-12/16/09.

PI, *EVEREST: Evaluation and Validation of Election-Related Equipment, Standards, and Testing*, The State of Ohio, *$716,336* (PSU award $332,066), 10/01/07-01/07/08, Collaborators: PSU (McDaniel), UPenn (Blaze), UCSB (Kemmerer, Vigna), Berkeley (Hall, Quilter).

Co-PI, *Protecting Services for Emerging Wireless Telecommunications Infrastructure*, NSF (CNS), *$658,032*, 09/01/07-08/31/11, Collaborators: PSU (La Porta, Jaeger, McDaniel).

Co-PI, *Security for Internet/IMS Convergence*, Cisco, *$100,000*, 9/1/07-8/31/08, Collaborators: PSU (La Porta, McDaniel).

Co-PI, *System-Wide Information Flow Enforcement*, BAA 06-11-IFKA, "National Intelligence Community Enterprise Cyber Assurance Program", *$496,000*, 2/1/07-8/1/08, Collaborators: PSU (Jaeger, McDaniel).

PI, *CAREER: Realizing Practical High Assurance through Security-Typed Information Flow Systems*, NSF (CNS), *$400,000*, 1/2/07-1/1/12.

Co-PI, *CT-IS: Shamon: Systems Approaches for Constructing Distributed Trust*, NSF (CNS), *$400,000*, 9/1/06-8/31/10, Collaborators: PSU (Jaeger, McDaniel).

Co-PI, *Center of Excellence*, Ben Franklin Technology Partners, *$75,000*, 01/01/07-07/01/07, Collaborators: PSU (Cao, Jaeger, La Porta, McDaniel, Smith).

Co-PI, *Exploiting Asymmetry in Performance and Security Requirements for I/O in High-end Computing*, NSF (CFF), *$699,690*, 9/1/06-8/31/10, Collaborators: PSU (McDaniel, Sivasubramaniam).

PI, *Automated Configuration with the PRESTO Network Management Platform*, AT&T, *$100,000*, 6/1/06-5/31/07.

PI, *Testbed for Network-Scale Countermeasure Evaluation*, Cisco, *$45,938*, 9/1/05-8/31/06.

PI, *Collaborative Research: CT-T: Flexible, Decentralized Information-flow Control for Dynamic Environments*, NSF (CFF), *$1,057,427* (PSU award $234,585), 8/1/05-7/31/08, Collaborators: PSU (McDaniel), UPenn (Zdancewic), Maryland (Hicks), GMU (Winsborough).

PI, *Extending Developer Tools for Security-typed Languages*, Software Engineering Research Center, Sponsor: Motorola, *$23,200*, 7/1/05-6/30/06.

PI, *Student Travel Support for ACM SIGCOMM 2005 Conference*, NSF, *$19,620*, 4/1/05-3/31/06.

Co-PI, *NSF CyberTrust: Collaborative Research: Testing and Benchmarking Methodologies for Future Network Security Mechanisms (EMIST)*, NSF/DHS, *$5,344,459* (PSU award $2,533,447), 8/1/04-8/31/06, Collaborators: PSU (Kesidis, Miller, Liu), Purdue (Fahmy, Rosenberg, Spafford, Shroff, Brodley), UCDavis (Wu, Levitt, Bishop, Rowe), ICSI/Berkeley (Paxson, Floyd, Weaver).

PROFESSIONAL ACTIVITIES

Editorial Positions, Panels, and Boards

ACM Transactions on AI Security and Privacy

- *Founding Editor in Chief*–May 2025-

IEEE Technical Committee on Security and Privacy

- *Chair*–January 2014-January 2016
- *Vice Chair*–January 2012-December 2014

ACM Transactions on Internet Technology (TOIT)

- *Editor in Chief*–September 2007-December 2012
- *Associate Editor*–April 2004-August 2007

IEEE Security and Privacy Magazine

- *Area Editor, Secure Systems*–January 2009-2015

IEEE Transactions on Computers (TC)

- *Associate Editor*–August 2008-2014

ACM Transactions on Information and System Security (TISSEC)

- *Associate Editor*–May 2007-May 2012

IEEE Transactions on Software Engineering (TSE)

- *Associate Editor*–January 2007-April 2012
- *Guest Editor, Special Issue on Topics in Security*–Fall 2006-April 2012

IEEE Transactions on Parallel and Distributed Systems (TPDS)

- *Guest Editor, Special Issue on Trust, Security and Privacy in Parallel and Distributed Systems*–Fall 2012

Elsevier Journal of Computer Networks

- *Guest Editor, Special Issue on Web Security*–Fall 2003-Spring 2005

Encyclopedia of Cryptography and Security

- *Editorial Board Member*–Fall 2002-Spring 2005

Journal of Defense Modeling and Simulation

- *Guest Editor, Special Issue on Cyber Risk and Vulnerability Estimation*–Winter 2018-

Other Professional Activities

IEEE Workshop on the Internet of Safe Things (SafeThings)

- *Steering Committee*–2022-present

Helmholtz Center for Information Security (CISPA), Scientific Advisory Board gGmbH

- *Member*–2019-present

Ohio University College of Engineering, Board of Vistors

- *Member*–2018-present

Penn State CISO Advisory Board

- *Member*–2016-2022

Member, Technical Guideline Development Committee, U.S. Election Assistance Commission

- *Member*–2010-2011

Natural Sciences and Engineering Research Council of Canada, Internetworked Systems Security Network

- *Scientific Advisory Board*–2008-2013

Technology for Cyber Physical System Security Forum, Cyber Security Research and Development, (Senators Joseph I. Lieberman and Susan Collins, Chairs)

- *Speaker and Participant*–September 2008

ACM Student Organization Advisor

- *Penn State Computer Science and Engineering Department*–2006-2012

The Technology Collaborative

- *Penn State Representative (Pennsylvania economic development consortium)*–2007-2008

President's National Security Telecommunications Advisory Panel

- *Member, Next Generation Networks Task Force*–2005-2006

Abusable Technologies Awareness Center (ATAC)

- *Panelist*–October 2003-2010

AT&T IP Services Security Council

- *Member*–June 2003-August 2004

AT&T Internet Intellectual Property Review Team

- *Member*–September 2001-May 2002

ACM SIGCOMM Student Travel Grant Committee

- *Member*–August 2005

National Science Foundation, Grant Review Panel

- *Member*–2003-2004, 2006-2007, 2009-2021

Department of Energy SciDAC Review Panel

- *Member*–2001

Conference and Workshop Participation

IEEE Symposium on Security and Privacy

- *Technical Program Co-Chair*–2007, 2008
- *Program Committee*–2011, 2012, 2013, 2022, 2023, 2024

USENIX Security Symposium

- *Program Chair*–2005
- *Invited Talks Chair*–2006, 2009
- *Program Committee*–2001, 2003, 2004, 2007, 2014, 2018, 2019, 2020, 2021, 2022, 2023, 2024

ACM Conference on Computer and Communications Security (CCS)

- *Program Committee*–2006, 2008, 2009, 2010, 2012, 2018, 2019, 2020, 2021, 2022, 2023
- *Industry and Government Track Chair*–2004, 2007
- *Program Committee-Industry and Government Track*–2003, 2005, 2006
- *Test of Time Committee*–2019, 2020

IEEE Conference on Secure and Trustworthy Machine Learning (SaTML)

- *Founding Program Co-Chair*–2023

IEEE European Symposium on Security and Privacy

- *Steering Committee*–2015-present
- *Program Committee*–2016, 2017

International Conference on Privacy, Security and Trust (PST)

- *Steering Committee*–2019-

International Conference on Learning Representations (ICLR)

- *Program Committee*–2024

ACM Conference on Security and Privacy in Wireless and Mobile Networks (WiSec)

- *Program Committee*–2017

Network and Distributed System Security Symposium (NDSS)

- *Program Committee*–2009, 2012, 2013, 2017

Annual Computer Security Applications Conference (ACSAC)

- *Program Committee*–2004, 2005, 2006, 2007, 2010, 2011, 2019
- *Test of Time Committee*–2019

Financial Cryptography

- *General Chair*–2006

- *Program Committee*–2007, 2008, 2012

Computer Security Foundations Symposium (CSF)

- *Program Committee*–2011, 2021

European Symposium on Research in Computer Security (ESORICS)

- *Program Committee*–2004, 2005, 2021

ACM Symposium of SDx Research 2021 (SOSR)

- *Program Committee*–2021

International Symposium on Engineering Secure Software and Systems (ICISSP)

- *Program Committee*–2015

IEEE Conference on Communications and Network Security (CNS)

- *Program Committee*–2015, 2017

ACM Annual International Conference on Mobile Computing and Networking (MobiCom)

- *Program Committee*–2010, 2011, 2012
- *Program Committee, Distinguished Member*–2021

ACM Annual International Conference on Mobile Systems, Applications, and Services (MobiSys)

- *Program Committee*–2012

ACM Symposium on Access Control Models and Technologies (SACMAT)

- *Program Committee*–2002, 2003, 2004, 2005, 2006, 2007, 2008, 2009, 2011

ACM Conference on ASIA Computer and Communications Security (ASIA CCS)

- *Program Committee*–2008

ACM Conference on Electronic Commerce (ACM EC)

- *Program Committee*–2005

EAI International Conf. on Security and Privacy in Communication Networks (SecureComm)

- *Program Committee*–2020

International Conference on Applied Cryptography and Network Security (ACNS)

- *Program Committee*–2006

ACM Annual Digital Forensics Conference

- *Program Committee*–2012

IEEE Workshop on the Internet of Safe Things

- *Program Committee*–2019, 2022

ACM Workshop on Moving Target Defense (MTD)

- *Program Committee*–2015, 2016

IEEE ICNP Workshop on Secure Network Protocols (NPSec)

- *Program Committee*–2005, 2006

Conference on Decision and Game Theory for Security (GameSec)

- *Program Committee*–2012, 2018

ACM Symposium on Applied Computing (SAC)

- *Program Committee, Information Security Research and Applications* –2010

USENIX Annual Technical Conference

- *Program Committee*–2002, 2003

World Wide Web Conference (WWW)

- *Security and Privacy Track Vice-Chair*–2005
- *Security and Privacy Track Deputy Vice-Chair*–2004
- *Program Committee*–2003, 2007, 2010, 2011

Intl. Conference on Emerging Trends in Information and Communication Security (ETRICS)

- *Program Committee*–2006

International Conference On Distributed Computing Systems (ICDCS)

- *Program Committee*–2011

IEEE INFOCOM

- *Program Committee*–2007

IEEE GLOBECOM

- *Program Committee*–2010

Military Communications Conference (MILCOM)

- *Program Committee*–2015, 2016, 2017, 2018, 2019, 2021, 2022

The Five Nines Workshop on Designing and Managing High Availability Internet Services (INM)

- *Program Committee*–2007

International Conference on Information Systems Security (ICISS)

- *Steering Committee*–2007
- *Program Co-Chair*–2007
- *Program Committee*–2005, 2006, 2009, 2011

International Conference on Parallel Processing

- *Program Committee-Network Security*–2003

USENIX Workshop on Large-Scale Exploits and Emergent Threats (LEET)

- *Program Committee*–2010

ACM Workshop on Networking, Systems, Applications on Mobile Handhelds (MobiHand)

- *Program Committee*–2009

ACM Workshop on Cloud Computing Security

- *Program Committee*–2009, 2010

ACM Workshop on Security and Privacy in Smartphones and Mobile Devices (SPSM)

- *Program Committee*–2011, 2012, 2013

International Workshop on Security in Software Engineering

- *Founding General Co-Chair*–2007

USENIX Workshop On Offensive Technology (WOOT)

- *Program Committee*–2007

ACM Storage Security and Survivability Workshop

- *Program Committee*–2006

ACM SIGCOMM Workshop on Internet Network Management

- *Program Committee*–2006, 2007

Annual IFIP WG 11.3 Working Conference on Data and Applications Security (DBSec)

- *Program Committee*–2006, 2007, 2008

Workshop on Workshop on Telecommunications Infrastructure Protection and Security (TIPS)

- *General Chair*–2009

USENIX Workshop on Hot Topics in Security (HotSec)

- *Program Chair*–2011
- *Program Committee*–2007, 2008, 2009, 2010, 2012

ACM Workshop TPC on Security and Privacy in Smartphones and Mobile Devices

- *Program Committee*–2011

International Workshop on Security (IWSEC)

- *Program Committee*–2006

International Workshop on Systems and Network Security (SNS)

- *Program Committee*–2005, 2006

COLLABORATORS (Last 48 Months)

Hidayet Aksu, Leonardo Babun, Paul Barford, Alexandre Bartel, Novella Bartolini, Yohan Beugin, Quinn Burke, Z. Berkay Celik, Muhao Chen, Kyle Domico, Matthew Durbin, Jean-Charles Noirot Ferrand, Jean-Charles Noirot Ferrand, Anshul Gandhi, Rahul George, Kanad Ghose, Kartik Gopalan, Ryan Guide, Josiah Hanna, Ting He, Alban Heon, Owen Hines, Blaine Hoak, Sabine Houy, Junjie Hu, Syed Rafiul Hussain, Trent Jaeger, Somesh Jha, Rachel King, Engin Kirda, Farinaz Koushanfar, Bruno Kreyssig, Srikanth V. Krishnamurthy, Thomas La Porta, Dongyoon Lee, Bo Li, Yiquan Li, Peiran Li, Guancheng Li, Kunyang Li, Jiazhao Li, Yixuan Li, Azaree Lintereur, Xiaogeng Liu, Yu David Liu, Zhenhua Liu, David Liu, David Yu Liu, Zhuoqing Mao, Patrick McDaniel, Patrick Mcdaniel, Fidan Mehmeti, Shuai Mu, Yujin Nam, Namitha Nambiar, Michael Norris, Kyle Ostrowski, Nicolas Papernot, Eric Pauley, Jingyuan Qi, Xiangyu Qi, Timothee Riom, Timothée Riom, Tajana Rosing, Ryan Sheatsley, Ryan, Ryan Sheatsley, Amit Kumar Sikder, Anand Sivasubramaniam, Wenjia Song, Edward Suh, Huan Sun, Michael Swift, Gang Tan, Sanchal Thakkar, Selcuk Uluagac, Anjo Vahldiek-Oberwagner, Prasanna Venkatesh, Gunjan Verma, Bimal Viswanath, Yevgeniy Vorobeychik, Jiongxiao Wang, Michael J. Weisman, Ya Xiao, Chaowei Xiao, Tian Xie, Danfeng Yao, Mingli Yu, Erez Zadok, Danfeng Zhang, Changyu Zhao, Shulin Zhao, Zhengyue Zhao, Minxuan Zhou, Sencun Zhu, Shitong Zhu, Bolor-Erdene Zolbayarn

CASES (Expert Witness, last 4 years)

Certain Mobile Phones, Components Thereof, and Products Containing Same, ITC Inv. No. 337-TA-1375, and In the Matter of Certain Electronic Devices, Including Mobile Phones, Tablets, Laptops, Components Thereof, and Products Containing the Same, Expert for Expert for the defense (Lenovo), International Trade Court, Case no. No. 337-TA-1375; No. 337-TA-1376; No. 5:23- cv-569; No. 5:23-cv-570.

DivX, LLC v. Hulu, LLC and Netflix, Inc., Expert for Expert for the defense, Central District of California, Case no. Case No. 2:19-cv-01602.

Inter Partes Review, Expert for Expert for Apple Inc., United States Patent and Trademark Office, Case no. Patent No 10,929,512.

Finjan Inc., vs. Rapid7 Inc and Rapid7 LLC, Expert for Expert for Rapid7, District of Delaware, Case no. C.A. No. 1:18-CV-01519-MN.

Finjan Inc., vs. Cisco Systems, Inc., Expert for Expert for CISCO, Northern District of California, San Jose Division, Case no. Case No. 5:17-cv-00072-BLF-SVK.

Rimini Street, Inc. v. Oracle International Corporation, Expert for Expert for Oracle, United States District Court, District of Nevada, Case no. Case No. 2:14-cv-01699.

Inter Partes Review, Expert for Expert for Samsung Electronics Co., Ltd., United States Patent and Trademark Office, Case no. Patent Nos 9,277,433 and 9,521,578.

Inter Partes Review, Expert for Expert for Dropbox Inc., United States Patent and Trademark Office, Case no. Patent Nos 8,484,260 and 8,296,338.

Finjan, LLC. v. SonicWall Inc., Expert for Expert for SonicWall, Northern District of California, Case no. Case No. 5:17-cv-04467-BLF-VKD.

WebRoot, INC. and OpenText, Inc. v Kaspersky Lab, Trent Micro, Sophos LTD., Crowdstrike Holdings, INC, and Forcepoint, LCC., Expert for Expert for the Plaintiff, Western District of Texas, Case no. 6:22-CV-00243-ADA-DTG, 6:22-CV-00239-ADA-DTG, 6:22-CV-00240-ADA-DTG, 6:22-CV-00241-ADA-DTG, FORCEPOINT, LLC, and 6:22-CV-00342-ADA-DTG.

INDUSTRIAL EXPERIENCE

Software Developer 1994-1995
Applied Innovation, Inc., Columbus, OH

Project Manager 1993-1994
Primary Access Corporation, San Diego, CA

Software Developer 1991-1993
Primary Access Corporation, San Diego, CA

Software Developer 1989
Integrated Technologies, Inc., Muncie, IN

PUBLICATIONS

Books and Book Chapters

Patrick Traynor and Patrick McDaniel and Thomas La Porta, *Security for Telecommunications Networks*, Springer, Advances in Information Security, July, 2008, ISBN: 978-0-387-72441-6.

Bolor-Erdene Zolbayar and Ryan Sheatsley and Patrick McDaniel, *Evading Machine Learning based Network Intrusion Detection Systems with GANs*, Game Theory and Machine Learning for Cyber Security, John Wiley & Sons, 2021. Eds. Charles A Kamhoua and Christopher D. Kiekintveld and Fei Fang and Quanyan Zhu. Hoboken, New Jersey.

Kevin Butler and William Enck and Patrick Traynor and Jennifer Plasterr and Patrick McDaniel, *Privacy Preserving Web-Based Email*, Algorithms, Architectures and Information Systems Security, Statistical Science and Interdisciplinary Research, World Scientific Computing, 349-371, November, 2008. Eds. Bhargab Bhattacharya, Susmita Sur-Kolay, Subhas Nandy and Aditya Bagchi.

Patrick McDaniel, *Authentication*, Handbook of Computer Networks, Volume II, Chapter 171, John Wiley and Sons, May, 2007. Eds. Hossein Bidgoli.

Patrick McDaniel, *Computer and Network Authentication*, Handbook of Information Security, John Wiley and Sons, September, 2004. Eds. Hossein Bidgoli.

Patrick McDaniel, *IPsec*, Encyclopedia of Information Security, Kluwer, 2003. Eds. Hossein Bidgoli.

Patrick McDaniel, *Policy*, Encyclopedia of Information Security, Kluwer, 2003. Eds. Hossein Bidgoli.

Patrick McDaniel, *Authentication*, The Internet Encyclopedia, John Wiley and Sons, 2002.

Journal Articles

Syed Rafiul Hussain and Patrick McDaniel and Anshul Gandhi and Kanad Ghose and Kartik Gopalan and Dongyoon Lee and Yu David Liu and Zhenhua Liu and Shuai Mu and Erez Zadok, *Verifiable Sustainability in Data Centers*, IEEE Security and Privacy Magazine, 22, November, 2024.

Quinn Burke and Yohan Beugin and Blaine Hoak and Rachel King and Eric Pauley and Ryan Sheatsley and Mingli Yu and Ting He and Thomas La Porta and Patrick McDaniel, *Securing Cloud File Systems with Trusted Execution*, IEEE Transactions on Dependable and Secure Computing (TDSC), September, 2024.

Mingli Yu and Quinn Burke and Thomas La Porta and Patrick McDaniel, *Stealthy Misreporting Attacks Against Load Balancing*, IEEE/ACM Transactions on Networking (TON), 2024.

Anshul Gandhi and Dongyoon Lee and Zhenhua Liu and Shuai Mu and Erez Zadok and Kanad Ghose and Kartik Gopalan and David Yu Liu and Syed Rafiul Hussain and Patrick McDaniel, *Metrics for Sustainability in Data Centers*, SIGENERGY Energy Inform. Rev., New York, NY, USA, ACM, 3, 3, 40-46, October, 2023.

Quinn Burke and Patrick McDaniel and Thomas La Porta and Mingli Yu and Ting He, *Misreporting Attacks Against Load Balancers in Software-Defined Networking*, Mobile Networks and Applications, Springer, 2023.

Tian Xie and Sanchal Thakkar and Ting He and Patrick McDaniel and Quinn Burke, *Joint Caching and Routing in Cache Networks with Arbitrary Topology*, IEEE Transactions on Parallel and Distributed Systems, May, 2023.

Ya Xiao and Wenjia Song and Jingyuan Qi and Bimal Viswanath and Patrick McDaniel and Danfeng Yao, *Specializing Neural Networks for Cryptographic Code Completion Applications*, IEEE Transactions on Software Engineering, IEEE, 2023.

Matthew Durbin and Ryan Sheatsley and Patrick McDaniel and Azaree Lintereur, *Experimental tests of Gamma-ray Localization Aided with Machine-learning (GLAM) capabilities*, Nuclear Instruments and Methods in Physics Research Section A: Accelerators, Spectrometers, Detectors and Associated Equipment, 1038, 2022.

Amit Kumar Sikder and Leonardo Babun and Z. Berkay Celik and Hidayet Aksu and Patrick McDaniel and Engin Kirda and Selcuk Uluagac, *Who's Controlling My Device? Multi-User Multi-Device-Aware Access Control System for Shared Smart Home Environment*, ACM Transactions on Internet of Things, Association for Computing Machinery, May, 2022.

Michael Norris and Z. Berkay Celik and Prasanna Venkatesh and Shulin Zhao and Patrick McDaniel and Anand Sivasubramaniam and Gang Tan, *IoTRepair: Flexible Fault Handling in Diverse IoT Deployments*, ACM Transactions on Internet of Things, ACM, 2022.

Tian Xie and Namitha Nambiar and Ting He and Patrick McDaniel, *Attack Resilience of Cache Replacement Policies: A Study Based on TTL Approximation*, IEEE/ACM Transactions on Networking, 2022.

Quinn Burke and Fidan Mehmeti and Rahul George and Kyle Ostrowski and Trent Jaeger and Thomas La Porta and Patrick Mcdaniel, *Enforcing Multilevel Security Policies in Unstable Networks*, IEEE Transactions on Network and Service Management, IEEE, June, 2022.

Ryan Sheatsley and Nicolas Papernot and Michael J. Weisman and Gunjan Verma and Patrick McDaniel, *Adversarial Examples for Network Intrusion Detection Systems*, Journal of Computer Security (JCS), IOS Press, January, 2022.

Quinn Burke and Patrick McDaniel and Thomas La Porta and Mingli Yu and Ting He, *Misreporting Attacks Against Load Balancers in Software-Defined Networking*, Mobile Networks and Applications, Springer, 2021.

Daniel E. Krych and Patrick McDaniel, *Exposing Android Social Applications: Linking Data Leakage to Privacy Policies*, Journal of Cyber Security Technology, Taylor & Francis, 5, 3-4, 2021.

Alejandro Andrade Salazar and Ryan Sheatsley and Jonathan Petit and Patrick McDaniel, *Physics-based Misbehavior Detection System for V2X Communications*, SAE International Journal of Connected and Automated Vehicles, SAE International, June, 2021.

Mingli Yu and Tian Xie and Ting He and Patrick McDaniel and Quinn Burke, *Flow Table Security in SDN: Adversarial Reconnaissance and Intelligent Attacks*, IEEE/ACM Transactions on Networking, 29, 6, 1063-6692, December, 2021.

Leonardo Babun and Kyle Denney and Z. Berkay Celik and Patrick McDaniel and Selcuk Uluagac, *A Survey on IoT Platforms: Communication, Security, and Privacy Perspectives*, Computer Networks, 192, 19, June, 2021.

Ryan Sheatsley and Matthew Durbin and Azaree Lintereur and Patrick McDaniel, *Improving Radioactive Material Localization by Leveraging Cyber-Security Model Optimizations*, IEEE Sensors, 21, 8, April, 2021.

Stefan Achleitner and Quinn Burke and Patrick McDaniel and Trent Jaeger and Thomas La Porta and Srikanth V. Krishnamurthy, *MLSNet: A Policy Complying Multilevel Security Framework for Software Defined Networking*, IEEE Transactions on Network and Service Management, 18, 1, March, 2021.

Dan Boneh and Andrew J. Grotto and Patrick McDaniel and Nicolas Papernot, *Preparing for the Age of Deepfakes and Disinformation*, Stanford HAI Policy Brief, 2020.

Dan Boneh and Andrew J. Grotto and Patrick McDaniel and Nicolas Papernot, *How Relevant Is the Turing Test in the Age of Sophisbots?*, IEEE Security & Privacy Magazine, 17, 64-71, Nov/Dec, 2019.

Z. Berkay Celik and Patrick McDaniel and Thomas Bowen, *Malware Modeling and Experimentation through Parameterized Behavior*, Journal of Defense Modeling and Simulation (JDMS), 15, 1, 31-48, 2017.

Z. Berkay Celik and Earlence Fernandes and Eric Pauley and Gang Tan and Patrick McDaniel, *Program Analysis of Commodity IoT Applications for Security and Privacy: Opportunities and Challenges*, ACM Computing Surveys (CSUR), ACM, 42, 4, 2019.

Z. Berkay Celik and Patrick McDaniel and Gang Tan and Leonardo Babun and Selcuk Uluagac, *Verifying IoT Safety and Security in Physical Spaces*, IEEE Security & Privacy Magazine, IEEE, 17, 5, 30-37, 2019.

Ahmed Atya and Zhiyun Qian and Srikanth V. Krishnamurthy and Thomas La Porta and Patrick McDaniel and Lisa Marvel, *Catch Me if You Can: Malicious Co-Residency on the Cloud*, IEEE/ACM Transactions on Networking, 27, 2, April, 2019.

Ian Goodfellow and Patrick McDaniel and Nicolas Papernot, *Making machine learning robust against adversarial inputs*, Communications of the ACM, ACM, 61, 7, 56-6, June/July, 2018.

Dave Tian and Kevin Butler and Joseph Choi and Patrick McDaniel and Padma Krishnaswamy, *Securing ARP/NDP From the Ground Up*, IEEE Transactions on Information Forensics and Security, 12, 9, 2131-2143, April, 2017.

Stefan Achleitner and Thomas La Porta and Patrick McDaniel and Shridatt Sugrim and Srikanth V. Krishnamurthy and Ritu Chada, *Deceiving Network Reconnaissance Unsing SDN-based Virtual Topologies*, IEEE Transactions on Network and Service Management, Special Issue on Advances in Management of Softwarized Networks, 14, 4, July, 2017.

Chaz Lever and Robert Walls and Yacin Nadji and David Dagon and Patrick McDaniel and Manos Antonakakis, *Dawn of the Dead Domain: Measuring the Exploitation of Residual Trust in Domains*, IEEE Security & Privacy Magazine (Secure Systems issue column), April, 2017.

Patrick McDaniel and Nicolas Papernot and Z. Berkay Celik, *Machine Learning in Adversarial Settings*, IEEE Security & Privacy Magazine, 14, 3, May/June, 2016.

Patrick McDaniel and Ananthram Swami, *The Cyber Security Collaborative Research Alliance:Unifying Detection, Agility, and Risk in Mission-Oriented Cyber Decision Making*, CSIAC Journal, Army Research Laboratory (ARL) Cyber Science and Technology, 5, 1, January, 2017.

Damien Octeau and Daniel Luchaup and Somesh Jha and Patrick McDaniel, *Composite Constant Propagation and its Application to Android Program Analysis*, IEEE Transactions on Software Engineering, 42, 11, 999-1014, 2016.

Steven Arzt and Siegfried Rasthofer and Christian Fritz and Eric Bodden and Alexandre Bartel and Jacques Klein and Yves Le Traon and Damien Octeau and Patrick McDaniel, *FlowDroid: Precise Context, Flow, Field, Object-sensitive and Lifecycle-aware Taint Analysis for Android Apps*, ACM SIGPLAN Notices, 49, 6, 259-269, June, 2014.

Alexander Kott and Ananthram Swami and Patrick McDaniel, *Security Outlook: Six Cyber Game Changers for the Next 15 Years*, IEEE Computer, 47, 12, 104-106, 2014.

Zhenfu Cao and Keqiu Li and Xu Li and Patrick McDaniel and Radha Poovendran and Guojun Wang and Yang Xiang, *Guest Editors' Introduction: Special Issue on Trust, Security, and Privacy in Parallel and Distributed Systems*, IEEE Transactions on Parallel and Distributed Systems, 25, 2, 279-28, 2014.

Patrick McDaniel and Brian Rivera and Ananthram Swami, *Toward a Science of Secure Environments*, IEEE Security & Privacy Magazine, 12, 4, July/August, 2014. Science of Security Index of Significant Research in Cyber Security, Science of Security Virtual Organization (SOS-VO) 2015

William Enck and Peter Gilbert and Seungyeop Han and Vasant Tendulkar and Byung-Gon Chun and Landon Cox and Jaeyeon Jung and Patrick McDaniel and Anmol Sheth, *TaintDroid: An Information-Flow Tracking*

System for Realtime Privacy Monitoring on Smartphones, ACM Transactions on Computer Systems (TOCS), 32, 2, June, 2014.

William Enck and Peter Gilbert and Byung-Gon Chun and Landon Cox and Jaeyeon Jung and Patrick McDaniel and Anmol Sheth, *TaintDroid: An Information-Flow Tracking System for Realtime Privacy Monitoring on Smartphones*, Communications of the ACM, 57, 3, March, 2014. Research Highlight

Machigar Ongtang and Stephen McLaughlin and William Enck and Patrick McDaniel, *Semantically Rich Application-Centric Security in Android*, Security and Communication Networks, 5, 6, 658-673, 2012.

Patrick McDaniel, *Bloatware Comes to the Smartphone*, IEEE Security & Privacy Magazine, 10, 4, July/August, 2011.

Thomas Moyer and Kevin Butler and Joshua Schiffman and Patrick McDaniel and Trent Jaeger, *Scalable Web Content Attestation*, IEEE Transactions on Computers, 61, 5, 686–699, April, 2011.

Patrick McDaniel, *Data Provenance and Security*, IEEE Security & Privacy Magazine, 9, 3, March/April, 2011.

Joshua Schiffman and Thomas Moyer and Trent Jaeger and Patrick McDaniel, *Network-based Root of Trust for Installation*, IEEE Security & Privacy Magazine, 40-48, Jan/Feb, 2011.

Kevin Butler and Stephen McLaughlin and Thomas Moyer and Patrick McDaniel, *New Security Architectures Based on Emerging Disk Functionality*, IEEE Security and Privacy Magazine, 8, 5, October, 2010.

Patrick McDaniel and William Enck, *Not So Great Expectations: Why Application Markets Haven't Failed Security*, IEEE Security & Privacy Magazine, 8, 5, 76–78, September/October, 2010.

Patrick Traynor and Chaitrali Amrutkar and Vikhyath Rao and Trent Jaeger and Patrick McDaniel and Thomas La Porta, *From Mobile Phones to Responsible Devices*, Journal of Security and Communication Networks (SCN), 4, 6, 719 – 726, June, 2011.

Patrick Traynor and Kevin Butler and William Enck and Kevin Borders and Patrick McDaniel, *malnets: Large-Scale Malicious Networks via Compromised Wireless Access Points*, Journal of Security and Communication Networks (SCN), 2, 3, 102-113, March, 2010.

Matthew Pirretti and Patrick Traynor and Patrick McDaniel and Brent Waters, *Secure Attribute-Based Systems*, Journal of Computer Security (JCS), 18, 5, 799–837, 2010.

Boniface Hicks and Sandra Rueda and Luke St. Clair and Trent Jaeger and Patrick McDaniel, *A Logical Specification and Analysis for SELinux MLS Policy*, ACM Transactions on Information and System Security (TISSEC), 13, 26, 2010.

Kevin Butler and Toni Farley and Patrick McDaniel and J. Rexford, *A Survey of BGP Security Issues and Solutions*, Proceedings of the IEEE, 2010, 1, 100-122, January, 2010.

Kevin Butler and Sunam Ryu and Patrick Traynor and Patrick McDaniel, *Leveraging Identity-based Cryptography for Node ID Assignment in Structured P2P Systems*, IEEE Transactions on Parallel and Distributed Systems (TPDS), 20, 12, 1803-1815, December, 2009.

Patrick McDaniel and Stephen McLaughlin, *Security and Privacy Challenges in the Smart Grid*, IEEE Security & Privacy Magazine (Secure Systems issue column), 7, 3, 75-77, May/June, 2009.

Patrick Traynor and William Enck and Patrick McDaniel and Thomas La Porta, *Mitigating Attacks on Open Functionality in SMS-Capable Cellular Networks*, IEEE/ACM Transactions on Networking (TON), 17, 1, 40-53, February, 2009.

William Enck and Machigar Ongtang and Patrick McDaniel, *Understanding Android Security*, IEEE Security & Privacy Magazine, 7, 1, 50–57, January/February, 2009.

William Enck and Thomas Moyer and Patrick McDaniel and Shubho Sen and Panagiotis Sebos and Sylke Spoerel and Albert Greenberg and Yu-Wei Sung and Sanjay Rao and William Aiello, *Configuration Management at Massive Scale: System Design and Experience*, IEEE Journal on Selected Areas in Communications (JSAC), 27, 3, 323-335, 2009.

Heesook Choi and William Enck and Jaesheung Shin and Patrick McDaniel and Thomas La Porta, *ASR: Anonymous and Secure Reporting of Traffic Forwarding Activity in Mobile Ad Hoc Networks*, Wireless Networks (WINET), ACM/Kluwer, 15, 4, 525-539, May, 2009.

Patrick Traynor and William Enck and Patrick McDaniel and Thomas La Porta, *Exploiting Open Functionality in SMS-Capable Cellular Networks*, Journal of Computer Security, 16, 6, 713-742, Febraury, 2009.

Patrick Traynor and Michael Chien and Scott Weaver and Boniface Hicks and Patrick McDaniel, *Non-Invasive Methods for Host Certification*, ACM Transactions on Information and System Security (TISSEC), 11, 3, 2008.

Patrick McDaniel and Bashar Nuseibeh, *Guest Editorial: Special Issue on Software Engineering for Secure Systems*, IEEE Transactions on Software Engineering, 34, 1, 3–4, 2008.

Wesam Lootah and William Enck and Patrick McDaniel, *TARP: Ticket-based Address Resolution Protocol*, Computer Networks, Elsevier, 51, 15, 4322–4337, October, 2007.

Patrick McDaniel and Avi Rubin, *Guest Editorial: Special Issue on Web Security*, Computer Networks, Elsevier, 22, 2, 2005.

Patrick McDaniel and Atul Prakash, *Enforcing Provisioning and Authorization Policy in the Antigone System*, Journal of Computer Security, 14, 6, 483–511, November, 2006.

Patrick McDaniel and Atul Prakash, *Methods and Limitations of Security Policy Reconciliation*, ACM Transactions on Information and System Security (TISSEC), Association for Computing Machinery, 9, 3, 259-291, August, 2006.

Patrick McDaniel and William Aiello and Kevin Butler and JohnIoannidis, *Origin Authentication in Interdomain Routing*, Journal of Communication Networks, Elsevier, 50, 16, 2953-2980, November, 2006.

Matthew Pirretti and Sencun Zhu and VijaykrishnanNarayanan and Patrick McDaniel and Mahmut Kandemir and Richard Brooks, *The Sleep Deprivation Attack in Sensor Networks: Analysisand Methods of Defense*, International Journal of Distributed Sensor Networks, 2, 3, 267-287, June, 2005.

Simon Byers and Lorrie Cranor and Eric Cronin and DaveKormann and Patrick McDaniel, *Analysis of Security Vulnerabilities in the Movie Productionand Distribution Process*, Telecommunications Policy, 28, 8, 619-644, August, 2004.

Conference Publications

Quinn Burke and Anjo Vahldiek-Oberwagner and Michael Swift and Patrick McDaniel, *It's a Feature, Not a Bug: Secure and Auditable State Rollback for Confidential Cloud Applications*, 2026 IEEE Symposium on Security and Privacy (S&P), May, 2026. San Francisco, CA.

Kyle Domico and Jean-Charles Noirot Ferrand and Ryan Sheatsley and Eric Pauley and Josiah Hanna and Patrick McDaniel, *Adversarial Agents: Black-Box Evasion Attacks with Reinforcement Learning*, Findings of the IEEE/CVF Conference on Computer Vision and Pattern Recognition (CVPR), June, 2026. Denver, CO.

Jean-Charles Noirot Ferrand and Yohan Beugin and Eric Pauley and Ryan Sheatsley and Patrick McDaniel, *Targeting Alignment: Extracting Safety Classifiers of Aligned LLMs*, IEEE Secure and Trustworthy Machine Learning Conference (SaTML), March, 2026.

Sabine Houy and Bruno Kreyssig and Timothée Riom and Alexandre Bartel and Patrick McDaniel, *SoK: A Practical Guideline and Taxonomy to LLVM's Control Flow Integrity*, 2025 IEEE Secure Development Conference (SecDev 2025), October, 2025.

Blaine Hoak and Patrick McDaniel, *On Synthetic Texture Datasets: Challenges, Creation, and Curation*, European Conference on Artificial Intelligence (ECAI), October, 2025.

Kunyang Li and Jean-Charles Noirot Ferrand and Ryan Sheatsley andBlaine Hoak and Yohan Beugin and Eric Pauley and Patrick McDaniel, *On the Robustness Tradeoff in Fine-Tuning*, IEEE/CVF International Conference on Computer Vision (ICCV), October, 2025.

Quinn Burke and Ryan Sheatsley and Yohan Beugin and Eric Pauley and Owen Hines and Michael Swift and Patrick McDaniel, *Efficient Storage Integrity in Adversarial Settings*, 2025 IEEE Symposium on Security and Privacy (IEEE S&P), May, 2025.

Zhengyue Zhao and Xiaogeng Liu and Somesh Jha and Patrick McDaniel and Bo Li and Chaowei Xiao, *Can Watermarks be Used to Detect LLM IP Infringement For Free?*, International Conference on Learning Representations (ICLR), April, 2025. Singapore.

Xiaogeng Liu and Peiran Li and Edward Suh and Yevgeniy Vorobeychik and Zhuoqing Mao and Somesh Jha and Patrick McDaniel and Huan Sun and Bo Li and Chaowei Xiao, *AutoDAN-Turbo: A Lifelong Agent for Strategy Self-Exploration to Jailbreak LLMs*, International Conference on Learning Representations (ICLR), April, 2025. Singapore.

Blaine Hoak and Ryan Sheatsley and Patrick McDaniel, *Err on the Side of Texture: Texture Bias on Real Data*, IEEE Secure and Trustworthy Machine Learning Conference (SaTML 2025), IEEE, April, 2025. Copenhagen, Denmark.

Eric Pauley and Kyle Domico and Blaine Hoak and Ryan Sheatsley, Ryan and Quinn Burke and Yohan Beugin and Engin Kirda and Patrick McDaniel, *Secure IP Address Allocation at Cloud Scale*, 2025 Network and Distributed Systems Security Symposium (NDSS), Internet Society, February, 2025. San Diego, CA.

Quinn Burke and Ryan Sheatsley and Rachel King and Owen Hines and Michael Swift and Patrick McDaniel, *On Scalable Integrity Checking For Secure Cloud Disks*, 23rd USENIX Conference on File and Storage Technologies (FAST '25), USENIX Association, February, 2025.

Jiongxiao Wang and Jiazhao Li and Yiquan Li and Xiangyu Qi and Junjie Hu and Yixuan Li and Patrick McDaniel andMuhao Chen and Bo Li and Chaowei Xiao, *Mitigating Fine-tuning based Jailbreak Attack with Backdoor Enhanced Safety Alignment*, Proceedings of Conference on Neural Information Processing Systems (NeurIPS), December, 2024.

Yohan Beugin and Patrick McDaniel, *Interest-disclosing Mechanisms for Advertising are Privacy-Exposing (not Preserving)*, Proceedings on Privacy Enhancing Technologies (PETS), July, 2024. Andreas Pfitzmann Best Student Paper Award (runner-up)

Blaine Hoak and Patrick McDaniel, *Explorations in Texture Learning*, 12th International Conference on Learning Representations, Tiny Papers Track (ICLR), May, 2024.

Tian Xie and Sanchal Thakkar and Ting He and Novella Bartolini and Patrick McDaniel, *Host-based Flow Table Size Inference in Multi-hop SDN*, Proceedings of the IEEE GLOBECOM, IEEE, December, 2023. Kuala Lumpur, Malaysia.

Eric Pauley and Paul Barford and Patrick McDaniel, *The CVE Wayback Machine: Measuring Coordinated Disclosure from Exploits Against Two Years of Zero-Days*, Proceedings of the ACM 2023 Internet Measurement Conference (IMC), October, 2023. Montreal, Canada. Best paper (runner up)

Mingli Yu and Quinn Burke and Thomas La Porta and Patrick McDaniel, *mMLSnet: Multilevel Security Network With Mobility*, Proceedings of the Military Communications Conference (MILCOM), IEEE, October, 2023. Boston, MA.

Ryan Guide and Eric Pauley and Yohan Beugin and Ryan Sheatsley and Patrick McDaniel, *Characterizing the Modification Space of Signature IDS Rules*, MILCOM 2023 - 2023 IEEE Military Communications Conference (MILCOM), IEEE, October, 2023. Boston, MA.

Eric Pauley and Paul Barford and Patrick McDaniel, *DScope: A Cloud-Native Internet Telescope*, 32nd USENIX Security Symposium (USENIX Security 23), USENIX Association, August, 2023. Anaheim, CA. CSAW ARC Finalist

Ryan Sheatsley and Blaine Hoak and Eric Pauley and Patrick McDaniel, *The Space of Adversarial Strategies*, 32nd USENIX Security Symposium (USENIX Security 23), USENIX Association, August, 2023.

Eric Pauley and Gang Tan and Danfeng Zhang and Patrick McDaniel, *Performant Binary Fuzzing without Source Code using Static Instrumentation*, Conference on Communications and Network Security (CNS), IEEE, October, 2022.

Patrick McDaniel, *Keynote Address: Sustainability is a Security Problem (extended abstract)*, Proceedings of the ACM Conference on Computer and Communications Security (CCS), ACM, November, 2022.

Kyle Domico and Ryan Sheatsley and Yohan Beugin and Quinn Burke and Patrick McDaniel, *A Machine Learning and Computer Vision Approach to Geomagnetic Storm Forecasting*, Machine Learning in Heliophysics (ML-Helio), AGU, November, 2022.

Tian Xie and Sanchal Thakkar and Ting He and Patrick Mcdaniel and Quinn Burke, *Joint Caching and Routing in Cache Networks with Arbitrary Topology*, Proceedings of the International Conference on Distributed Computing Systems (ICDCS), July, 2022.

Yohan Beugin and Quinn Burke and Blaine Hoak and Ryan Sheatsley and Eric Pauley and Gang Tan and Syed Rafiul Hussain and Patrick McDaniel, *Building a Privacy-Preserving Smart Camera System*, Proceedings on Privacy Enhancing Technologies (PETS), July, 2022.

Eric Pauley and Ryan Sheatsley and Blaine Hoak and Quinn Burke and Yohan Beugin and Patrick McDaniel, *Measuring and Mitigating the Risk of IP Reuse on Public Clouds*, 2022 IEEE Symposium on Security and Privacy (IEEE S&P), IEEE, May, 2022. San Francisco, CA.

Ahmed Abdou and Ryan Sheatsley and Yohan Beugin and Tyler Shipp and Patrick McDaniel, *HoneyModels: Machine Learning Honeypots*, Proceedings of the Military Communications Conference (MILCOM), IEE, November, 2021.

Ryan Sheatsley and Blaine Hoak and Eric Pauley and Yohan Beugin and Michael J. Weisman and Patrick McDaniel, *On the Robustness of Domain Constraints*, Proceedings of the ACM Conference on Computer and Communications Security (CCS), ACM, November, 2021.

Tian Xie and Ting He and Patrick McDaniel and Namitha Nambiar, *Attack Resilience of Cache Replacement Policies*, IEEE International Conference on Computer Communications (INFOCOM), IEEE, May, 2021.

Adrien Cosson and Amit Kumar Sikder and Leonardo Babun and Z. Berkay Celik and Patrick McDaniel and Selcuk Uluagac, *Sentinel: A Robust Intrusion Detection System for IoT Networks Using Kernel-Level System Information*, In 6th ACM/IEEE Conference on Internet of Things Design and Implementation (IoTDI), April, 2021.

Matthew Durbin and Ryan Sheatsley and Patrick McDaniel and Azaree Lintereur, *A Multi-Step Machine Learning Approach to Directional Gamma Ray Detection*, 2020 IEEE Nuclear Science Symposium and Medical Imaging Conference (NSS/MIC), October, 2020.

Sayed M. Saghaian and Thomas La Porta and Simone Silvestri and Patrick McDaniel, *Improving Robustness of a Popular Probabilistic Clustering Algorithm Against Insider Attacks*, International Conference on Security and Privacy in Communication Networks (SecureComm 2020), EAI, October, 2020.

Quinn Burke and Patrick McDaniel and Thomas La Porta and Mingli Yu and Ting He, *Misreporting Attacks in Software-Defined Networking*, International Conference on Security and Privacy in Communication Networks (SecureComm 2020), EAI, October, 2020.

Amit Kumar Sikder and Leonardo Babun and Z. Berkay Celik and Abbas Acar and Hidayet Aksu and Patrick McDaniel and Engin Kirda and Selcuk Uluagac, *KRATOS: Multi-User Multi-Device-Aware Access Control System for the Smart Home*, 13th ACM Conference on Security and Privacy in Wireless and Mobile Networks (WiSec '20), ACM, July, 2020.

Mingli Yu and Ting He and Patrick McDaniel and Quinn Burke, *Flow Table Security in SDN: Adversarial Reconnaissance and Intelligent Attacks*, IEEE INFOCOM, IEEE Conference on Computer Communications, June, 2020. Beijing, China.

Michael Norris and Z. Berkay Celik and Prasanna Venkatesh and Shulin Zhao and Patrick McDaniel and Anand Sivasubramaniam and Gang Tan, *IoTRepair: Systematically addressing device faults in commodity IoT*, In 5th ACM/IEEE Conference on Internet of Things Design and Implementation (IoTDI), April, 2020.

Raquel Alvarez and Jake Levenson and Ryan Sheatsley and Patrick McDaniel, *Application Transiency: Towards a Fair Trade of Personal Information for Application Services*, Proceedings of the EAI Conference on Security and Privacy in Communication Networks (SecureComm), October, 2019. Orlando, FL.

Giuseppe Petracca and Yuqiong Sun and Ahmad-Atamli Reineh and Jens Grossklags and Patrick McDaniel and Trent Jaeger, *EnTrust: Regulating Sensor Access by Cooperating Programs via Delegation Graphs*, Proceedings of the 28th USENIX Security Symposium, Augus, 2019. Santa Clara, CA.

Matthew Durbin and Ryan Sheatsley and Christopher Balbier and Tristan Grieve and Patrick McDaniel and Azaree Lintereur, *Development of Machine Learning Algorithms for Directional Gamma Ray Detection*, Proceedings of the Institute of Nuclear Materials Management Annual Meeting (INMM), July, 2019. Palm Desert, CA. J. D. Williams student paper award, Nuclear Security and Physical Protection division

Z. Berkay Celik and Abbas Acar and Hidayet Aksu and Abbas Acar and Ryan Sheatsley and Selcuk Uluagac and Patrick McDaniel, *Curie: Policy-based Secure Data Exchange*, ACM Conference on Data and Applications Security (CODASPY), March, 2019. Dallas, TX.

Z. Berkay Celik and Gang Tan and Patrick McDaniel, *IoTGuard: Dynamic Enforcement of Security and Safety Policy in Commodity IoT*, Network and Distributed System Security Symposium (NDSS), February, 2019. San Diego, CA.

Dang Tu Nguyen and Chengyu Song and Zhiyun Qian and Srikanth V. Krishnamurthy and Edward J. M. Colbert and Patrick McDaniel, *IoTSan: Fortifying the Safety of IoT Systems*, Proceedings of the 14th International Conference on emerging Networking EXperiments and Technologies (CoNEXT '18), December, 2018.

Z. Berkay Celik and Leonardo Babun and Amit Kumar Sikder and Hidayet Aksu and Gang Tan and Patrick McDaniel and Selcuk Uluagac, *Sensitive Information Tracking in Commodity IoT*, Proceedings of the 27th USENIX Security Symposium, August, 2018. Baltimore, MD.

Rauf Izmailov and Shridatt Sugrim and Ritu Chadha and Patrick McDaniel and Ananthram Swami, *Enablers Of Adversarial Attacks in Machine Learning*, Proceedings of the Military Communications Conference (MILCOM), IEEE, October, 2018.

Sayed M. Saghaian and Thomas La Porta and Trent Jaeger and Z. Berkay Celik and Patrick McDaniel, *Mission-oriented Security Model, Incorporating Security Risk, Cost and Payout*, EAI International Conference on Security and Privacy in Communication Networks (SECURECOMM), August, 2018. Best paper

Z. Berkay Celik and Patrick McDaniel and Gang Tan, *Soteria: Automated IoT Safety and Security Analysis*, USENIX Annual Technical Conference (USENIX ATC), July, 2018. Boston, MA.

Z. Berkay Celik and Patrick McDaniel and Rauf Izmailov and Nicolas Papernot and Ryan Sheatsley and Raquel Alvarez and Ananthram Swami, *Detection under Privileged Information*, ACM Asia Conference on Computer and Communications Security (ASIACCS), June, 2018.

Florian Tramer and Alexey Kurakin and Nicolas Papernot and Ian Goodfellow and Dan Boneh and Patrick McDaniel, *Ensemble Adversarial Training: Attacks and Defenses*, International Conference on Learning Representations (ICLR), 2018. Vancouver, Canada.

Nicolas Papernot and Patrick McDaniel and Arunesh Sinha and Michael Wellman, *SoK: Security and Privacy in Machine Learning*, Security and Privacy (EuroS&P), 2018 IEEE European Symposium on on Security and Privacy (EuroS&P), IEEE, April, 2018. London, UK.

Chun-Ming Lai and Xiaoyun Wang and Yunfeng Hong and Yu-Cheng Lin and Felix Wu and Patrick McDaniel and Hasan Cam, *Attacking Strategies and Temporal Analysis Involving Facebook Discussion Groups*, 13th IEEE International Conference on Network and Service Management, November, 2017. Tokyo, Japan.

Kathrin Grosse and Nicolas Papernot and Praveen Manoharan and Michael Backes and Patrick McDaniel, *Adversarial Examples for Malware Detection*, 22nd European Symposium on Research in Computer Security (ESORICS '17), September, 2017. Oslo, Norway.

Z. Berkay Celik and David Lopez-Paz and Patrick McDaniel, *Patient-Driven Privacy Control through Generalized Distillation*, Proceedings of the Privacy-Aware Computing (PAC), IEEE, 2017.

Abbas Acar and Z. Berkay Celik and Hidayet Aksu and Selcuk Uluagac and Patrick McDaniel, *Achieving Secure and Differentially Private Computations in Multiparty Settings*, Proceedings of the Privacy-Aware Computing (PAC), IEEE, 2017.

Vaibhav Rastogi and Drew Davidson and Lorenzo De Carli and Somesh Jha and Patrick McDaniel, *Cimplifier: Automatically Debloating Containers*, 11Th Joint Meeting of the European Software Engineering Conference and the Acm Sigsoft Symposium on the Foundations of Software Engineering, September, 2017. Paderborn, Germany.

Yunfeng Hong and Yongjian Hu and Chun-Ming Lai and Felix Wu and Iulian Neamtiu and Yu Paul and Patrick McDaniel and Hasan Cam and Gail-Joon Ahn, *Defining and Detecting Environment Discrimination in Android Apps*, The 13th EAI International Conference on Security and Privacy in Communication Networks (SecureComm 17), October, 2017.

Nicolas Papernot and Patrick McDaniel and Ian Goodfellow and Somesh Jha and Z. Berkay Celik and Ananthram Swami, *Practical Black-Box Attacks against Machine Learning*, ACM Asia Conference on Computer and Communications Security (ASIACCS) 2017, April, 2017.

Stefan Achleitner and Thomas La Porta and Trent Jaeger and Patrick McDaniel, *Adversarial Network Forensics in Software Defined Networking*, ACM Symposium on SDN Research (SOSR), ACM, April, 2017. Best student paper

Stefan Achleitner and Thomas La Porta and Patrick McDaniel and Srikanth V. Krishnamurthy and Alexander Poylisher and Constantin Serban, *Stealth Migration: Hiding Virtual Machines on the Network*, IEEE International Conference on Computer Communications (INFOCOM), IEEE, 2017.

Ahmed Atya and Zhiyun Qian and Srikanth V. Krishnamurthy and Thomas La Porta and Patrick McDaniel and Lisa Marvel, *Malicious Co-Residency on the Cloud: Attacks and Defense*, IEEE International Conference on Computer Communications (INFOCOM), IEEE, 2017.

Nathaniel Lageman and Eric Kilmer and Robert Walls and Patrick McDaniel, *BinDNN: Resilient Function Matching Using Deep Learning*, 2016 International Conference on Security and Privacy in Communication Networks (SECURECOMM), October, 2016.

Z. Berkay Celik and Nan Hu and Yun Li and Nicolas Papernot and Patrick McDaniel and Jeff Rowe and Robert Walls and Karl Levitt and Novella Bartolini and Thomas La Porta and Ritu Chadha, *Mapping Sample Scenarios to Operational Models*, Proceedings of the Military Communications Conference (MILCOM), IEEE, 2016.

Nicolas Papernot and Patrick McDaniel and Ananthram Swami and Richard Harang, *Crafting Adversarial Input Sequences for Recurrent Neural Networks*, Proceedings of the Military Communications Conference (MILCOM), IEEE, 2016.

Michael Backes and Sven Bugiel and Erik Derr and Patrick McDaniel and Damien Octeau and Sebastian Weisgerber, *On Demystifying the Android Application Framework: Re-Visiting Android Permission Specification Analysis*, Proceedings of the 25th USENIX Security Symposium, August, 2016.

Devin Pohly and Patrick McDaniel, *Modeling Privacy and Tradeoffs in Multichannel Secret Sharing Protocols*, 46th IEEE/IFIP International Conference on Dependable Systems and Networks (DSN), June, 2016.

Chaz Lever and Robert Walls and Yacin Nadji and David Dagon and Patrick McDaniel and Manos Antonakakis, *Domain-Z: 28 Registrations Later*, Proceedings of the 37th IEEE Symposium on Security and Privacy, May, 2016. San Francisco, CA.

Yasemin Acar and Michael Backes and Sven Bugiel and Sascha Fahl and Patrick McDaniel and Matthew Smith, *SoK: Lessons Learned From Android Security Research For Appified Software Platforms*, Proceedings of the 37th IEEE Symposium on Security and Privacy, May, 2016. San Francisco, CA.

Nicolas Papernot and Patrick McDaniel and Xi Wu and Somesh Jha and Ananthram Swami, *Distillation as a Defense to Adversarial Perturbations Against Deep Neural Networks*, Proceedings of the 37th IEEE Symposium on Security and Privacy, May, 2016. San Francisco, CA.

Charles Huber and Scott Brown and Patrick McDaniel and Lisa Marvel, *Cyber Fighter Associate: A Decision Support System for Cyber Agility*, Proceedings of the 50th Annual Conference on Information Sciences and Systems (CISS), March, 2016. Princeton, NJ.

Nicolas Papernot and Patrick McDaniel and Somesh Jha and Matthew Fredrikson and Z. Berkay Celik and Ananthram Swami, *The Limitations of Deep Learning in Adversarial Settings*, Proceedings of the 1st IEEE European Symposium on Security and Privacy, IEEE, 2016. Saarbrucken, Germany.

Damien Octeau and Somesh Jha and Matthew Dering and Patrick McDaniel and Alexandre Bartel and Li Li and Jacques Klein and Yves Le Traon, *Combining Static Analysis with Probabilistic Models to Enable Market-Scale Android Inter-Component Analysis*, Proceedings of the 43rd ACM SIGPLAN-SIGACT Symposium on Principles of Programming Languages (POPL), January, 2016. St. Petersburg, Florida, USA.

Devin Pohly and Patrick McDaniel, *MICSS: A Realistic Multichannel Secrecy Protocol*, IEEE Global Communications Conference (GLOBECOM), December, 2015. San Diego, CA.

Robert Walls and Eric Kilmer and Nathaniel Lageman and Patrick McDaniel, *Measuring the Impact and Perception of Acceptable Advertisements*, Proceedings of the ACM 2015 Internet Measurement Conference (IMC), October, 2015. Tokyo, Japan.

Nicolas Papernot and Patrick McDaniel and Robert Walls, *Enforcing Agile Access Control Policies in Relational Databases using Views*, Proceedings of the Military Communications Conference (MILCOM), October, 2015. Tampa, FL.

Alessandro Oltramari and Lorrie Cranor and Robert Walls and Patrick McDaniel, *Computational Ontology of Network Operations*, Proceedings of the Military Communications Conference (MILCOM), October, 2015. Tampa, FL.

Z. Berkay Celik and Robert Walls and Patrick McDaniel and Ananthram Swami, *Malware Traffic Detection using Tamper Resistant Features*, Proceedings of the Military Communications Conference (MILCOM), October, 2015. Tampa, FL.

Devin Pohly and Charles Sestito and Patrick McDaniel, *Adaptive Protocol Switching Using Dynamically Insertable Bumps in the Stack*, Proceedings of the Military Communications Conference (MILCOM), October, 2015. Tampa, FL.

Azeem Aqil and Ahmed Atya and Trent Jaeger and Srikanth V. Krishnamurthy and Karl Levitt and Patrick McDaniel and Jeff Rowe and Ananthram Swami, *Detection of Stealthy TCP-based DoS Attacks*, Proceedings of the Military Communications Conference (MILCOM), October, 2015. Tampa, FL.

Daniel E. Krych and Stephen Lange-Maney and Patrick McDaniel and William Glodek, *Investigating Weaknesses in Android Certificate Security*, SPIE 9478, Modeling and Simulation for Defense Systems and Applications X, May, 2015.

Damien Octeau and Daniel Luchaup and Matthew Dering and Somesh Jha and Patrick McDaniel, *Composite Constant Propagation: Application to Android Inter-Component Communication Analysis*, Proceedings of the 37th International Conference on Software Engineering (ICSE), May, 2015. Florence, Italy.

Li Li and Alexandre Bartel and Tegawende Bissyande and Jacques Klein and Yves Le Traon and Steven Arzt and Siegfried Rasthofer and Eric Bodden and Damien Octeau and Patrick McDaniel, *IccTA: Detecting Inter-Component Privacy Leaks in Android Apps*, Proceedings of the 37th International Conference on Software Engineering (ICSE), May, 2015. Florence, Italy. Most Influential Paper Award of ICSE 2015 2025

Jing Tian and Kevin Butler and Patrick McDaniel and Padma Krishnaswamy, *Securing ARP From the Ground Up*, CODASPY '15: Proceedings of the 5th ACM Conference on Data Application and Security and Privacy, March, 2015. San Antonio, TX, USA.

Alessandro Oltramari and Lorrie Cranor and Robert Walls and Patrick McDaniel, *Building an Ontology of Cyber Security*, Proc. Intl. Conference on Semantic Technologies for Intelligence, Defense, and Security (STIDS), November, 2014.

Matthew Dering and Patrick McDaniel, *Android Market Reconstruction and Analysis*, Proceedings of the Military Communications Conference (MILCOM), October, 2014. Baltimore, MD.

Wenhui Hu and Damien Octeau and Patrick McDaniel and Peng Liu, *Duet: Library Integrity Verification for Android Applications*, Proceedings of the ACM Conference on Security and Privacy in Wireless and Mobile Networks (WiSec), July, 2014. Oxford, United Kingdom.

Steven Arzt and Siegfried Rasthofer and Christian Fritz and Eric Bodden and Alexandre Bartel and Jacques Klein and Yves Le Traon and Damien Octeau and Patrick McDaniel, *FlowDroid: Precise Context, Flow, Field, Object-sensitive and Lifecycle-aware Taint Analysis for Android Apps*, Proceedings of the 35th Conference on Programming Language Design and Implementation (PLDI), June, 2014. Edinburgh, UK. Most Influential Paper of PLDI 2014 2024

Phillip Koshy and Diana Koshy and Patrick McDaniel, *An Analysis of Anonymity in Bitcoin Using P2P Network Traffic*, Proceedings of Financial Cryptography 2014, International Financial Cryptography Association (IFCA), February, 2014. Christ Church, Barbado.

Stephen McLaughlin and Devin Pohly and Patrick McDaniel and Saman Zonouz, *A Trusted Safety Verifier for Process Controller Code*, Proc. ISOC Network and Distributed Systems Security Symposium (NDSS), February, 2014. San Diego, CA.

Damien Octeau and Patrick McDaniel and Somesh Jha and Alexandre Bartel and Eric Bodden and Jacques Klein and Yves Le Traon, *Effective Inter-Component Communication Mapping in Android with Epicc: An Essential Step Towards Holistic Security Analysis*, Proceedings of the 22th USENIX Security Symposium, August, 2013. Washington, DC.

Devin J. Pohly and Stephen McLaughlin and Patrick McDaniel and Kevin Butler, *Hi-Fi: Collecting High-Fidelity Whole-System Provenance*, Proceedings of the 28th Annual Computer Security Applications Conference (ACSAC), December, 2012. Orlando, Florida.

Stephen McLaughlin and Patrick McDaniel, *SABOT: Specification-based Payload Generation for Programmable Logic Controllers*, 19th ACM Conference on Computer and Communications Security (CCS), October, 2012.

Weining Yang and Ninghui Li and Yuan Qi and Wahbeh Qardaji and Stephen McLaughlin and Patrick McDaniel, *Minimizing Private Data Disclosures in the Smart Grid*, 19th ACM Conference on Computer and Communications Security (CCS), October, 2012.

Eun Kyoung Kim and Patrick McDaniel and Thomas La Porta, *A Detection Mechanism for SMS Flooding Attacks in Cellular Networks*, Proceedings of the 8th International Conference on Security and Privacy in Communication Networks (SECURECOMM 2012), September, 2012. Padua, Italy.

Damien Octeau and Somesh Jha and Patrick McDaniel, *Retargeting Android Applications to Java Bytecode*, 20th International Symposium on the Foundations of Software Engineering (FSE), November, 2012. Research Triangle Park, NC. Best artifact

Thomas Moyer and Trent Jaeger and Patrick McDaniel, *Scalable Integrity-Guaranteed AJAX*, Proceedings of the 14th Asia-Pacific Web Conference (APWeb), April, 2012. Kunming, China. (*Invited Paper*)

Patrick McDaniel and Stephen McLaughlin, *Structured Security Testing in the Smartgrid*, Proceedings of 5th International Symposium on Communications, Control, and Signal Processing, May, 2012. Rome, Italy. (*Invited Paper*)

Stephen McLaughlin and Patrick McDaniel and William Aiello, *Protecting Consumer Privacy from Electric Load Monitoring*, The 18th ACM Conference on Computer and Communications Security (CCS), October, 2011. Chicago, IL.

William Enck and Damien Octeau and Patrick McDaniel and Swarat Chaudhuri, *A Study of Android Application Security*, Proceedings of the 20th USENIX Security Symposium, August, 2011. San Francisco, CA.

Kevin Butler and Stephen McLaughlin and Patrick McDaniel, *Kells: A Protection Framework for Portable Data*, Proceedings of the 26th Annual Computer Security Applications Conference (ACSAC), December, 2010. Austin, TX.

Stephen McLaughlin and Dmitry Podkuiko and Adam Delozier and Sergei Miadzvezhanka and Patrick McDaniel, *Multi-vendor Penetration Testing in the Advanced Metering Infrastructure*, Proceedings of the 26th Annual Computer Security Applications Conference (ACSAC), December, 2010. Austin, TX.

Machigar Ongtang and Kevin Butler and Patrick McDaniel, *Porscha: Policy Oriented Secure Content Handling in Android*, Proceedings of the 26th Annual Computer Security Applications Conference (ACSAC), December,

2010. Austin, TX.

Patrick Traynor and Joshua Schiffman and Thomas La Porta and Patrick McDaniel and Abhrajit Ghosh and Farooq Anjum, *Constructing Secure Localization Systems with Adjustable Granularity*, IEEE Global Communications Conference (GLOBECOM), December, 2010. Miami, FL.

William Enck and Peter Gilbert and Byung-Gon Chun and Landon Cox and Jaeyeon Jung and Patrick McDaniel and Anmol Sheth, *TaintDroid: An Information-Flow Tracking System for Realtime Privacy Monitoring on Smartphones*, Proceedings of the 9th USENIX Symposium on Operating Systems Design and Implementation (OSDI), October, 2010. Vancouver, BC.

Toby Ehrenkranz and Jun Li and Patrick McDaniel, *Realizing A Source Authentic Internet*, Proceedings of the 6th International ICST Conference on Security and Privacy in Communications Networks (Securecomm), September, 2010. Singapore.

Boniface Hicks and Sandra Rueda and David King and Thomas Moyer and Joshua Schiffman and Yogesh Sreenivasan and Patrick McDaniel and Trent Jaeger, *An Architecture for Enforcing End-to-End Access Control over Web Applications*, Proceedings of the Fifteenth ACM Symposium on Access Control Models and Technologies (SACMAT 2010), 163-172, June, 2010. Pittsburgh, PA.

Kevin Butler and Stephen McLaughlin and Patrick McDaniel, *Disk-Enabled Authenticated Encryption*, Proceedings of the 26th IEEE Symposium on Massive Storage Systems and Technologies (MSST), May, 2010.

Machigar Ongtang and Stephen McLaughlin and William Enck and Patrick McDaniel, *Semantically Rich Application-Centric Security in Android*, Proceedings of the 25th Annual Computer Security Applications Conference (ACSAC), 340-349, December, 2009. Honolulu, Hawaii. Best Paper, Test of Time Award 2024

Thomas Moyer and Kevin Butler and Joshua Schiffman and Patrick McDaniel and Trent Jaeger, *Scalable Asynchronous Web Content Attestation*, Proceedings of the 25th Annual Computer Security Applications Conference (ACSAC), 95-104, December, 2009. Honolulu, Hawaii.

Joshua Schiffman and Thomas Moyer and Christopher Shal and Trent Jaeger and Patrick McDaniel, *Justifying Integrity Using a Virtual Machine Verifier*, Proceedings of the 25th Annual Computer Security Applications Conference (ACSAC), 83-92, December, 2009. Honolulu, Hawai.

William Enck and Machigar Ongtang and Patrick McDaniel, *On Lightweight Mobile Phone App Certification*, Proceedings of the 16th ACM Conference on Computer and Communications Security (CCS), 235-245, November, 2009.

Patrick Traynor and Michael Lin and Machigar Ongtang and Vikhyath Rao and Trent Jaeger and Thomas La Porta and Patrick McDaniel, *On Cellular Botnets: Measuring the Impact of Malicious Devices on a Cellular Network Core*, Proceedings of the 16th ACM Conference on Computer and Communications Security (CCS), 223-234, November, 2009.

William Enck and Patrick McDaniel and Trent Jaeger, *PinUP: Pinning User Files to Known Applications*, Proceedings of the 24th Annual Computer Security Applications Conference (ACSAC), December, 2008.

William Enck and Kevin Butler and Thomas Richardson and Patrick McDaniel and Adam Smith, *Defending Against Attacks on Main Memory Persistence*, Proceedings of the 24th Annual Computer Security Applications Conference (ACSAC), December, 2008.

Kevin Butler and Stephen McLaughlin and Patrick McDaniel, *Rootkit-Resistant Disks*, Proceedings of the 15th ACM Conference on Computer and Communications Security (CCS), November, 2008. Alexandria, VA.

Patrick Traynor and Kevin Butler and William Enck and Patrick McDaniel, *Realizing Massive-Scale Conditional Access Systems Through Attribute-Based Cryptosystems*, ISOC Network & Distributed System Security Symposium (NDSS), February, 2008. San Diego, CA.

Luke St. Clair and Joshua Schiffman and Trent Jaeger and Patrick McDaniel, *Establishing and Sustaining System Integrity via Root of Trust Installation*, 23rd Annual Computer Security Applications Conference (ACSAC), 19-29, December, 2007. Miami, FL.

Boniface Hicks and Tim Misiak and Patrick McDaniel, *Channels: Runtime System Infrastructure for Security-typed Languages*, 23rd Annual Computer Security Applications Conference (ACSAC), 443-452, December, 2007. Miami, FL.

Dhananjay Bapat and Kevin Butler and Patrick McDaniel, *Towards Automated Privilege Separation*, Proceedings of 2nd International Conference onInformation Systems Security (short paper), December, 2007. Delhi, India.

Lisa Johansen and Kevin Butler and Michael Rowell and Patrick McDaniel, *Email Communities of Interest*, Fourth Conference on Email and Anti-Spam (CEAS 2007, August, 2007. Mountain View, California.

Patrick Traynor and Patrick McDaniel and Thomas La Porta, *On Attack Causality in Internet-Connected Cellular Networks*, Proceedings of the 16th USENIX Security Symposium, 1–16, August, 2007. Boston, MA.

Boniface Hicks and Sandra Rueda and Trent Jaeger and Patrick McDaniel, *From Trusted to Secure: Building and Executing Applications that Enforce System Security*, Proceedings of the USENIX Annual Technical Conference, June, 2007. Santa Clara, CA.

William Enck and Patrick McDaniel and Shubho Sen and Panagiotis Sebos and Sylke Spoerel and Albert Greenberg and Sanjay Rao and William Aiello, *Configuration Management at Massive Scale: System Design and Experience*, Proceedings of the USENIX Annual Technical Conference, June, 2007. Santa Clara, CA.

Boniface Hicks and Sandra Rueda and Luke St. Clair and Trent Jaeger and Patrick McDaniel, *A Logical Specification and Analysis for SELinux MLS*, 12th ACM Symposium on Access Control Models andTechnologies (SACMAT), ACM, June, 2007. Sophia Antipolis, France.

Anusha Sriraman and Kevin Butler and Patrick McDaniel and Padma Raghavan, *Analysis of IPv4 Address Space Delegation Structure*, 12th IEEE Symposium on Computers and Communications (ISCC), July, 2007. Aveiro, Portugal.

Heesook Choi and Thomas La Porta and Patrick McDaniel, *Privacy Preserving Communication in MANETs*, Proceedings of Fourth Annual IEEE CommunicationsSociety Conference on Sensor, Mesh, and Ad Hoc Communications andNetworks (SECON 07), June, 2007. San Diego, CA.

Sophie Qiu and Patrick McDaniel and Fabian Monrose, *Toward Valley-Free Inter-domain Routing*, Proceedings of 2007 IEEE International Conference onCommunications (ICC 2007), June, 2007. Glasgow, Scottlan.

Sunam Ryu and Kevin Butler and Patrick Traynor and Patrick McDaniel, *Leveraging Identity-based Cryptography for Node IDAssignment in Structured P2P Systems*, Proceedings of the 3rd IEEE International Symposium onSecurity in Networks and Distributed Systems (SSNDS-07), June, 2007. Niagra Falls, Canada.

Hosam Rowaihy and William Enck and Patrick McDaniel andThomas La Porta, *Limiting Sybil Attacks in Structured Peer-to-Peer Networks*, Proceedings of IEEE INFOCOM 2007 MiniSymposiu, May, 2007. Anchorage, AK.

Boniface Hicks and Kiyan Ahmadizadeh and Patrick McDaniel, *Understanding Practical Application Development in Security-Typed Languages*, 22st Annual Computer Security Applications Conference (ACSAC), 153–164, December, 2006. Miami, Fl. Best Student Paper

Luke St. Clair and Lisa Johansen and William Enck and Matthew Pirretti and Patrick Traynor and Patrick McDaniel and Trent Jaeger, *Password Exhaustion: Predicting the End of Password Usefulness*, Proceedings of

2nd International Conference on Information Systems Security (ICISS), 37–55, December, 2006. Kolkata, India.

Kevin Butler and William Enck and Jennifer Plasterr and Patrick Traynor and Patrick McDaniel, *Privacy-Preserving Web-Based Email*, Proceedings of 2nd International Conference on Information Systems Security (ICISS), 116–131, December, 2006. Kolkata, India.

Matthew Pirretti and Patrick Traynor and PatrickMcDaniel and Brent Waters, *Secure Attribute-Based Systems*, Proceedings of the 13th ACM Conference on Computer and Communications Security (CCS), 99-112, November, 2006. Alexandria, VA.

Kevin Butler and William Aiello and Patrick McDaniel, *Optimizing BGP Security by Exploiting Path Stability*, Proceedings of the 13th ACM Conference on Computer and Communications Security (CCS), 298-310, November, 2006. Alexandria, VA.

Patrick Traynor and William Enck and Patrick McDaniel andThomas La Porta, *Mitigating Attacks on Open Functionality in SMS-CapableCellular Networks*, Proceedings of the Twelfth Annual InternationalConference on Mobile Computing and Networking (MobiCom), 182-193, September, 2006. Los Angeles, CA.

Patrick Traynor and Michael Chien and Scott Weaver andBoniface Hicks and Patrick McDaniel, *Non-Invasive Methods for Host Certification*, Proceedings of the Second IEEE CommunicationsSociety/CreateNet International Conference on Security and Privacyin Communication Networks (SecureComm), August, 2006. Baltimore, MD.

Sophie Qiu and Patrick McDaniel and Fabian Monrose andAvi Rubin, *Characterizing Address Use Structure and Stabillity ofOrigin Advertisement in Interdomain Routing*, 11th IEEE Symposium on Computers and Communications, 489-496, June, 2006. Pula-Cagliari, Sardinia, Italy.

Patrick McDaniel and Shubho Sen and Oliver Spatscheck andJacobus Van der Merwe and William Aiello and Charles Kalmanek, *Enterprise Security: A Community of Interest Based Approach*, Proceedings of Network and Distributed Systems Security2006 (NDSS), February, 2006. San Diego, CA.

Kevin Butler and Patrick McDaniel, *Understanding Mutable Internet Pathogens, or How I Learnedto Stop Worrying and Love Parasitic Behavior*, Proceedings of 1st International Conference onInformation Systems Security (ICISS), Springer-Verlag Lecture Notes in Computer Science, volume 3803, 36-48, December, 2005. Kolkata, India. (*Invited Paper*)

Wesam Lootah and William Enck and Patrick McDaniel, *TARP: Ticket-Based Address Resolution Protocol*, 21st Annual Computer Security Applications Conference(ACSAC), 95-103, December, 2005. Tuscon, AZ.

William Enck and Patrick Traynor and Patrick McDaniel andThomas La Porta, *Exploiting Open Functionality in SMS-Capable Cellular Networks*, Proceedings of the 12th ACM Conference on Computer and CommunicationsSecurity (CCS), 393–404, May, 2005. Alexandria, VA.

Matthew Pirretti and Sencun Zhu and VijaykrishnanNarayanan and Patrick McDaniel and Mahmut Kandemir and Richard Brooks, *The Sleep Deprivation Attack in Sensor Networks: Analysis and Methods of Defense*, Proceedings of the Innovations and Commercial Applications of Distributed Sensor Networks Symposi, October, 2005. Bethesda, Maryland. Best paper

Louis Kruger and Somesh Jha and Patrick McDaniel, *Privacy Preserving Clustering*, 10th European Symposium on Research in ComputerSecurity (ESORICS '05), September, 2005. Milan, Italy.

Heesook Choi and William Enck and Jaesheung Shin andPatrick McDaniel and Thomas La Porta, *Secure Reporting of Traffic Forwarding Activity in Mobile AdHoc Networks*, MobiQuitous 2005, July, 2005. San Diego, CA.

Simon Byers and Lorrie Cranor and Eric Cronin and DaveKormann and Patrick McDanie, *Exposing Digital Content Piracy: Approaches, Issues and Experiences*, Thirty-Eighth Conference on Signals, Systems, and Computers, 45–50, Nov, 2004. Monterey, CA. (*Invited paper*)

William Aiello and John Ioannidis and Patrick McDaniel, *Origin Authentication in Interdomain Routing*, Proceedings of 10th ACM Conference on Computer andCommunications Security (CCS), ACM, 165-178, October, 2003. Washington, DC.

Eric Cronin and Sugih Jamin and Tal Malkin and PatrickMcDaniel, *On the Performance, Feasibility, and Use of Forward SecureSignatures*, Proceedings of 10th ACM Conference on Computer andCommunications Security (CCS), ACM, 131-144, October, 2003. Washington, DC.

Patrick McDaniel, *On Context in Authorization Policy*, 8th ACM Symposium on Access Control Models andTechnologies (SACMAT), ACM, 80-8, June, 2003. Como, Italy.

Geoff Goodell and William Aiello and Tim Griffin and John Ioannidis and Patrick McDaniel and Avi Rubin, *Working Around BGP: An Incremental Approach to ImprovingSecurity and Accuracy of Interdomain Routing*, Proceedings of Network and Distributed Systems Security2003 (NDSS), Internet Society, 75-8, February, 2003. San Diego, CA.

Patrick McDaniel and Atul Prakash, *Methods and Limitations of Security Policy Reconciliation*, 2002 IEEE Symposium on Security and Privacy, IEEE Computer Society Press, 73-87, May, 2002. Oakland, CA.

Patrick McDaniel and Atul Prakash and Jim Irrer and Sharad Mittal and Thai-Chuin Thuang, *Flexibly Constructing Secure Groups in Antigone 2.0*, Proceedings of DARPA Information SurvivabilityConference and Exposition II, IEEE Computer Society Press, 55-67, June, 2001. Los Angeles, CA.

Hugh Harney and Andrea Colegrove and Patrick McDaniel, *Principles of Policy in Secure Groups*, Proceedings of Network and Distributed Systems Security2001 (NDSS), Internet Society, 125-13, February, 2001. San Diego, CA.

Patrick McDaniel and Sugih Jamin, *Windowed Certificate Revocation*, Proceedings of IEEE INFOCOM 2000, IEEE, 1406-1414, March, 2000. Tel Aviv, Israel.

Patrick McDaniel and Avi Rubin, *A Response to 'Can We Eliminate Certificate RevocationLists?'*, Proceedings of Financial Cryptography 2000, International Financial Cryptography Association(IFCA), February, 2000. Anguilla, British West Indies.

Andrew Adamson and Charles J. Antonelli and Kevin Coffman andPatrick McDaniel and Jim Rees, *Secure Distributed Virtual Conferencing*, Proceedings of Communications and Multimedia Security(CMS '99), 176-190, September, 1999. Katholieke Universiteit, Leuven, Belgium.

Patrick McDaniel and Atul Prakash and Peter Honeyman, *Antigone: A Flexible Framework for Secure Group Communication*, Proceedings of the 8th USENIX Security Symposium, 99-114, August, 1999. Washington, DC.

Workshop Papers

Changyu Zhao and Yohan Beugin and Jean-Charles Noirot Ferrand and Quinn Burke and Guancheng Li and Patrick McDaniel, *LibIHT: A Hardware-Based Approach to Efficient and Evasion-Resistant Dynamic Binary Analysis*, Proceedings of the 1st Workshop on Software Understanding and Reverse Engineering (SURE 2025), ACM, October, 2025.

Blaine Hoak and Kunyang Li and Patrick McDaniel, *Alignment and Adversarial Robustness: Are More Human-Like Models More Secure?*, Proceedings of the 1st International Workshop on Security andPrivacy-Preserving AI/ML (SPAIML 2025), CEUR, October, 2025.

Yujin Nam and Rachel King and Quinn Burke and Minxuan Zhou and Patrick McDaniel and Tajana Rosing, *Efficient Host Intrusion Detection using Hyperdimensional Computing*, Proceedings of the 2024 IEEE International

Conference on Big Data workshop Cyber Threat Intelligence and Hunting, IEEE, December, 2024.

Rachel King and Quinn Burke and Yohan Beugin and Blaine Hoak and Kunyang Li and Eric Pauley and Ryan Sheatsley and Patrick McDaniel, *ParTEETor: A System for Partial Deployments of TEEs within Tor*, Proceedings of the 23rd Workshop on Privacy in the Electronic Society (WPES), ACM, October, 2024. Salt Lake City, UT, USA.

Yohan Beugin and Patrick McDaniel, *The Need for a (Research) Sandstorm through the Privacy Sandbox*, 17th Workshop on Hot Topics in Privacy Enhancing Technologies (HotPETs), July, 2024.

Yohan Beugin and Patrick McDaniel, *A Public and Reproducible Assessment of the Topics API on Real Data*, SecWeb 2024 Workshop, IEEE Security and Privacy Workshops (SPW), May, 2024.

Kunyang Li and Kyle Domico and Jean-Charles Noirot Ferrand and Patrick McDaniel, *The Efficacy of Transformer-Based Adversarial Attacks in Security Domains*, Workshop on Artificial Intelligence for Cyber (MILCOM 2023), October, 2023. Boston, MA.

Eric Pauley and Patrick McDaniel, *Understanding the Ethical Frameworks of Internet Measurement Studies*, The 2nd International Workshop on Ethics in Computer Security (EthiCS 2023), February, 2023. San Diego, CA. Best paper

Anshul Gandhi and Kanad Ghose and Kartik Gopalan and Syed Rafiul Hussain and Dongyoon Lee and David Liu and Zhenhua Liu and Patrick McDaniel and Shuai Mu and Erez Zadok, *Metrics for Sustainability in Data Centers*, Proceedings of the 1st Workshop on Sustainable Computer Systems Design and Implementation (HotCarbon'22), USENIX, July, 2022. San Diego, CA.

Leonardo Babun and Z. Berkay Celik and Patrick McDaniel and Selcuk Uluagac, *Real-time Analysis of Privacy-(un)aware IoT Applications*, Privacy Enhancing Technologies Symposium (PETS), 2021.

Sushrut Shringarputale and Patrick McDaniel and Kevin Butler and Thomas La Porta, *Co-residency Attacks on Containers are Real*, The ACM Cloud Computing Security Workshop (CCSW 2020), 2020.

Z. Berkay Celik and Patrick McDaniel, *Extending Detection with Privileged Information via Generalized Distillation*, IEEE Security & Privacy Workshop on Deep Learning and Security (IEEE S&P DLS), 2018.

Alexander Alexeev and Diane Henshel and Karl Levitt and Patrick McDaniel and Brian Rivera and Steve Templeton and Michael J. Weisma, *Constructing a Science of Cyber-Resilience for Military Systems*, Information Systems and Technology (IST) Panel, IST-153/RWS-21, CEUR Workshop Proceeding, 30-42, October, 2017.

Z. Berkay Celik and Patrick McDaniel and Rauf Izmailov, *Feature Cultivation in Privileged Information-augmented Detection*, Proceedings of the International Workshop on Security And Privacy Analytics (IWSPA 2017), 2017. (*Invited Paper*)

Stefan Achleitner and Thomas La Porta and Patrick McDaniel and Shridatt Sugrim and Srikanth V. Krishnamurthy and Ritu Chadha, *Cyber Deception: Virtual Networks to Defend Insider Reconnaissance*, Proceedings of the 8th ACM CCS International Workshop on Managing Insider Security Threats, ACM, 2016.

Patrick McDaniel and Robert Walls, *Estimating Attack Intent and Mission Impact from Detection Signals*, Proceedings of the NATO IST-128 Workshop: Assessing Mission Impact of Cyberattacks, Army Research Laboratory, July, 2015.

Patrick McDaniel and Trent Jaeger and Thomas La Porta and Nicolas Papernot and Robert Walls and Alexander Kott and Lisa Marvel and Ananthram Swami and Prasant Mohapatra and Srikanth V. Krishnamurthy and Iulian Neamtiu, *Security and Science of Agility*, First ACM Workshop on Moving Target Defense (MTD 2014), November, 2014. Scottsdale, AZ.

Joshua Schiffman and Thomas Moyer and Hayawardh Vijayakumar and Trent Jaeger and Patrick McDaniel, *Seeding Clouds with Trust Anchors*, Proccedings of CCSW 2010: The ACM Cloud Computing Security Workshop, October, 2010. Chicago, IL.

Stephen McLaughlin and Dmitry Podkuiko and Adam Delozier and Sergei Miadzvezhanka and Patrick McDaniel, *Embedded Firmware Diversity for Smart Electric Meters*, Proceedings of the 5th Workshop on Hot Topics inSecurity (HotSec '10), August, 2010. Washington, DC.

Patrick McDaniel and Kevin Butler and Stephen McLaughlin and Radu Sion and Erez Zadok and Marianne Winslett, *Towards a Secure and Efficient System for End-to-End Provenance*, the 2nd USENIX Workshop on the Theory and Practice of Provenance, February, 2010. San Jose, CA.

Thomas La Porta and Patrick McDaniel and Karl Rauscher and Jun Shu, *The Impact of Supply Chain on Information and Communications Technology Security*, In the 1st Workshop on Workshop on Telecommunications Infrastructure Protection and Security, December, 2009. Honolulu, Hawaii.

Stephen McLaughlin and Dmitry Podkuiko and Patrick McDaniel, *Energy Theft in the Advanced Metering Infrastructure*, In the 4th International Workshop on Critical Information Infrastructure Security, September, 2009. Bonn, Germany.

Matthew Blaze and Patrick McDaniel, *Below the Salt: The Dangers of Unfulfilled Physical Media Assumptions*, In Proceedings of Seventeenth International Workshop on Security Protocols, April, 2009. Cambridge, England.

Kevin Butler and William Enck and Harri Hursti and StephenMcLaughlin and Patrick Traynor and Patrick McDaniel, *Systemic Issues in the Hart InterCivic and Premier VotingSystems: Reflections Following Project EVEREST*, In Proceedings of the 3rd USENIX/ACCURATE ElectronicVoting Technology Workshop (EVT '08), July, 2008.

Kevin Butler and Stephen McLaughlin and Patrick McDaniel, *Non-Volatile Memory and Disks: Avenues for Policy Architectures*, Proceedings of the 1st ACM Computer Security Architectures Workshop, November, 2007. Alexandria, VA.

William Enck and Sandra Rueda and Yogesh Sreenivasan and JoshuaSchiffman and Luke St. Clair and Trent Jaeger and Patrick McDaniel, *Protecting Users from "Themselves"*, Proceedings of the 1st ACM Computer Security Architectures Workshop, November, 2007. Alexandria, VA.

Boniface Hicks and David King and Patrick McDaniel, *Jifclipse: Development Tools for Security-Typed Applications*, Proceedings of the 2nd ACM SIGPLAN Workshop on Programming Languages and Analysis for Security (PLAS '07), ACM Press, June, 2007. San Diego, CA.

Boniface Hicks and Sandra Rueda and Trent Jaeger andPatrick McDaniel, *Integration of SELinux and Security-typed Languages*, Proceedings of the 2007 Security-Enhanced Linux Workshop, March, 2007. Baltimore, MD.

Sophie Qiu and Fabian Monrose and Andreas Terzis and Patrick McDaniel, *Efficient Techniques for Detecting False Origin Advertisements in Inter-domain Routing*, Proceedings of The Second Workshop on Secure Network Protocols (NPSec), November, 2006. Santa Barbara.

Shiva Chaitanya and Kevin Butler and Patrick McDaniel andAnand Sivasubramaniam, *Design, Implementation and Evaluation of Security iniSCSI-based Network Storage Systems*, Proceedings of 2nd International Workshop on StorageSecurity and Survivability (StorageSS 2006), October, 2006. Alexandria, Virginia.

Trent Jaeger and Patrick McDaniel and Luke St. Clair and RamonCaceres and Reiner Sailer, *Shame on Trust in Distributed Systems*, Proceedings of the First Workshop on Hot Topics inSecurity (HotSec '06), July, 2006. Vancouver, B.C., Canada.

Kevin Butler and Patrick McDaniel and Sophie Qiu, *BGPRV: A Library for Fast and Efficient Routing Data Manipulation*, Proceedings of DETER Community Workshop, June, 2006. Arlington, VA.

Kevin Butler and Patrick McDaniel, *Testing Large Scale BGP Security in Replayable NetworkEnvironments*, Proceedings of DETER Community Workshop, June, 2006. Arlington, VA.

Boniface Hicks and David King and Patrick McDaniel andMichael Hicks, *Trusted Declassification: High-level Policy for aSecurity-Typed Language*, Proceedings of ACM SIGPLAN Workshop on ProgrammingLanguages and Analysis for Security, 65-74, June, 2006. Ottawa, Canada.

Ali Al-Lawati and Dongwon Lee and Patrick McDaniel, *Blocking in Private Information Matching*, Proceedings of Second International ACM SIGMOD Workshopon Information Quality in Information Systems, June, 2005. Baltimore, MD.

William Aiello and Charles Kalmanek and Patrick McDaniel andShubho Sen and Oliver Spatscheck and Jacobus Van der Merwe, *Analysis of Communities Of Interest in Data Networks*, Passive and Active Measurement Workshop 2005, March, 2005. Boston, M.

Simon Byers and Lorrie Cranor and David Kormann andPatrick McDaniel, *Searching for Privacy: Design and Implementation of aP3P-Enabled Search Engine*, Proceedings of 2004 Workshop on Privacy EnhancingTechnologies (PETS), May, 2004. Toronto, Canad.

Hao Wang and Somesh Jha and Patrick McDaniel and MironLivn, *Security Policy Reconciliation in Distributed ComputingEnvironments*, Proceedings of 5th International Workshop on Policiesfor Distributed Systems and Networks (Policy 2004), IEEE Computer Society Press, 137-146, June, 2004. Yorktown Heights, N.

Simon Byers and Lorrie Cranor and Eric Cronin and DaveKormann and Patrick McDaniel, *Analysis of Security Vulnerabilities in the Movie Productionand Distribution Process*, Proceedings of 2003 ACM Workshop on Digital RightsManagement, ACM, October, 2003. Washington, DC, also appeared in Telecommunications PolicyResearch Conference – September 2003.

Patents

U.S. Patent No. 7,873,350, Patrick McDaniel and Martin Strauss, *End-to-end secure wireless communication for requesting a more secure channel*, January, 2011.

U.S. Patent No. 7,975,044, Oliver Spatscheck and Subhabrata Sen and Jacobus Van der Merwe and Patrick McDaniel, *Automated disambiguation of fixed-serverport-based applications from ephemeral applications*, July, 2011.

U.S. Patent No. 8,175,580, Patrick McDaniel and Martin Strauss, *End-to-end secure wireless communication for requesting a more secure channel*, May, 2012.

U.S. Patent No. 8,453,227, William Aiello and Charles Kalmanek and William Leighton III and Patrick McDaniel and Subhabrata Sen and Oliver Spatscheck and Jacobus Van der Merwe, *Reverse firewall with self-provisioning*, May, 2013.

U.S. Patent No. 8,732,293, Patrick McDaniel and Subhabrata Sen and Oliver Spatscheck and Jacobus Van der Merwe, *System and method for tracking individuals on a data network using communities of interest*, May, 2014.

U.S. Patent No. 8,813,213, William Aiello and Charles Kalmanek and William Leighton III and Patrick McDaniel and Subhabrata Sen and Oliver Spatscheck and Jacobus Van der Merwe, *Reverse firewall with self-provisioning*, August, 2014.

Other Publications

Patrick McDaniel and Farinaz Koushanfar, *NSF Secure and Trustworthy Computing 2.0 Vision Statement*, Public Report, August, 2023.

Patrick McDaniel and Thorsten Holz and Indra Spiecker and Genannt Dohmann and Christopher Burchard and Ahmad-Reza Sadeghi and Konrad Rieck and Kamalika Chaudhuri and Somesh Jha and Andrea Matwyshyn and David Evans and Felix Freiling and Amy Hasan, *Cybersecurity and Machine Learning: Vision Document, Report on the joint NSF/DFG Cybersecurity and Machine Learning Research Workshop*, Public Report, National Science Foundation/Deutsche Forschungsgemeinschaf, December, 2021.

Patrick McDaniel and John Launchbury, *Artificial Intelligence and Cybersecurity: Opportunities and Challenges 2019 Technical Workshop Report*, Public Report, Networking and Information Technology Research and Development Subcommittee, Machine Learning and Artificial Intelligence Subcommittee, and the Special Cyber Operations Research and Engineering Subcommittee of the National Science and Technology Council, 2020.

Patrick McDaniel and Avi Rubin, *Conference Proceedings*, 2008 IEEE Symposium on Security and Privacy, IEEE, May, 2008. Oakland, CA.

Patrick McDaniel and Kevin Butler and William Enck and Harri Hursti and Stephen McLaughlin and Patrick Traynor and Matthew Blaze and Adam Aviv and Pavol Cerny and Sandy Clark and Eric Cronin and Gaurav Shah and Micah Sherr and Giovanni Vigna and Richard Kemmerer and David Balzarotti and Greg Banks and Marco Cova and Viktoria Felmetsger and William Robertson and Fredrik Valeur and Joseph Lorenzo Hall and Laura Quilter, *EVEREST: Evaluation and Validation of Election-Related Equipment, Standards and Testing*, Ohio Secretary of State, Public Report, 2007.

Patrick McDaniel and Shyam K. Gupta, *Conference Proceedings*, The Third International Conference Information Systems Security, Springer, December, 2007. Delhi, India.

Birgit Pfitzmann and Patrick McDaniel, *Conference Proceedings*, 2007 IEEE Symposium on Security and Privacy, IEEE, May, 2007. Oakland, CA.

Patrick McDaniel, *Conference Proceedings*, The 14th USENIX Security Symposium, USENIX, August, 2005. Baltimore, MD.

Patrick McDaniel, *Policy Evolution: Autonomic Environmental Security*, Software Engineering Research Center Showcase, USA, December, 2004.

Hugh Harney and Uri Meth and Andrea Colegrove and AngelaSchuett and Patrick McDaniel and Gavin Kenny and HaithamCruickshank and Sunil Iyengar, *GSAKMP*, Internet Research Task Force, August, 2003. (*Draft*).

Patrick McDaniel and Atul Prakash, *A Flexible Architecture for Security Policy Enforcement*, Proceedings of DARPA Information SurvivabilityConference and Exposition III, Research Summaries, 234-239, April, 2003.

Jim Irrer and Atul Prakash and Patrick McDaniel, *Antigone: Policy-Based Secure Group Communications Systems and AMirD: Antigone-Based Secure File Mirroring System*, Proceedings of DARPA Information SurvivabilityConference and Exposition III, Demo Summaries, 44-4, April, 2003.

Patrick McDaniel and Sugih Jamin, *Windowed Key Revocation in Public Key Infrastructures*, NASA Tech Briefs, 55, August, 2002.

Patrick McDaniel and Atul Prakash, *Antigone Secure Group Communication System*, NASA Tech Briefs, 2001.

Patrick McDaniel, *Policy Management in Secure Group Communication*, PhD Thesis, University of Michigan, Ann Arbor, MI, August, 2001.

Patrick McDaniel and Hugh Harney and Andrea Colegrove andAtul Prakash and Peter Dinsmore, *Multicast Security Policy Requirements and Building Blocks*, Internet Research Task Force, Secure MulticastResearch Group

(SMuG), November, 2000. (*Draft*).

Tom Hardjono and Hugh Harney and Patrick McDaniel and Andrea Colegroveand Peter Dinsmore, *Group Security Policy Token*, Internet Research Task Force, Secure MulticastResearch Group (SMuG), November, 2001. (*Draft*).

Patrick McDaniel and Hugh Harney and Peter Dinsmore and Atul Prakash, *Multicast Security Policy*, Internet Research Task Force, Secure MulticastResearch Group (SMuG), June, 2000. (*Draft*).

Patrick McDaniel, *8th USENIX Security Symposium Conference Summaries,Potpourri Session*, USENIX Login Magazine, 9-12, November, 1999.

Patrick McDaniel, *The Analysis of D_i, a Detailed Design Metric on LargeScale Software*, Masters Thesis, Ball State University, Muncie, IN, June, 1991.

Technical Reports

Yohan Beugin and Patrick McDaniel, *Technical Report: The Need for a (Research) Sandstorm through the Privacy Sandbox*, Technical Report 2512.03207, arXiv preprint, December, 2025.

Kyle Domico and Jean-Charles Noirot Ferrand and Ryan Sheatsley and Eric Pauley and Josiah Hanna and Patrick McDaniel, *Adversarial Agents: Black-Box Evasion Attacks with Reinforcement Learning*, Technical Report 2503.01734 cs.CV, arXiv preprint, March, 2025.

Blaine Hoak and Kunyang Li and Patrick McDaniel, *Alignment and Adversarial Robustness: Are More Human-Like Models More Secure?*, Technical Report 2502.12377 cs.CV, arXiv preprint, February, 2025.

Bruno Kreyssig and Timothee Riom and Sabine Houy and Alexandre Bartel and Patrick McDaniel, *Deserialization Gadget Chains are not a Pathological Problem in Android: an In-Depth Study of Java Gadget Chains in AOSP*, Technical Report 2502.0847 cs.CR, arXiv preprint, February, 2025.

Jean-Charles Noirot Ferrand and Yohan Beugin and Eric Pauley and Ryan Sheatsley and Patrick McDaniel, *Targeting Alignment: Extracting Safety Classifiers of Aligned LLMs*, Technical Report 2409.10297 cs.CV, arXiv preprint, January, 2025.

Blaine Hoak and Patrick McDaniel, *On Synthetic Texture Datasets: Challenges, Creation, and Curation*, Technical Report 2409.10297 cs.CV, arXiv preprint, 2024.

Rachel King and Quinn Burke and Yohan Beugin and Blaine Hoak and Kunyang Li and Eric Pauley and Ryan Sheatsley and Patrick McDaniel, *ParTEETor: A System for Partial Deployments of TEEs within Tor*, Technical Report 2408.14646, arXiv preprint, August, 2024.

Quinn Burke and Ryan Sheatsley and Rachel King and Michael Swift and Patrick McDaniel, *Cloud Storage Integrity at Scale: A Case for Dynamic Hash Trees*, Technical Report 2405.03830, arXiv preprint, May, 2024.

Alban Heon and Ryan Sheatsley and Quinn Burke and Blaine Hoak and Eric Pauley and Yohan Beugin and Patrick McDaniel, *Systematic Evaluation of Geolocation Privacy Mechanisms*, Technical Report 2309.06263, arXiv preprint, September, 2023.

Yohan Beugin and Patrick McDaniel, *Interest-disclosing Mechanisms for Advertising are Privacy-Exposing (Not Preserving)*, Technical Report 2306.03825, arXiv preprint, May, 2023.

Quinn Burke and Yohan Beugin and Blaine Hoak and Rachel King and Eric Pauley and Ryan Sheatsley and Mingli Yu and Ting He and Thomas La Porta and Patrick McDaniel, *Securing Cloud File Systems using Shielded Execution*, Technical Report 2305.18639, arXiv preprint, May, 2023.

Yohan Beugin and Quinn Burke and Blaine Hoak and Ryan Sheatsley and Eric Pauley and Gang Tan and Syed Rafiul Hussain and Patrick McDaniel, *Privacy-Preserving Protocols for Smart Cameras and Other IoT Devices*, Technical Report 2208.09776, arXiv preprint, August, 2022.

Eric Pauley and Kyle Domico and Blaine Hoak and Ryan Sheatsley and Quinn Burke and Yohan Beugin and Patrick McDaniel, *EIPSIM: Modeling Secure IP Address Allocation at Cloud Scale*, Technical Report arXiv:2210.14999, arXiv preprint, 2022.

Bolor-Erdene Zolbayarn and Ryan Sheatsley and Patrick McDaniel and Michael J. Weisman and Sencun Zhu and Shitong Zhu and Srikanth V. Krishnamurthy, *Generating Practical Adversarial Network Traffic Flows using NIDSGAN*, Technical Report arXiv:2203.06694, arXiv preprint, March, 2022.

Ryan Sheatsley and Blaine Hoak and Eric Pauley and Yohan Beugin and Michael J. Weisman and Patrick McDaniel, *On the Robustness of Domain Constraints*, Technical Report arXiv:2105.08619, arXiv preprint, 2021.

Ryan Sheatsley and Nicolas Papernot and Michael J. Weisman and Gunjan Verma and Patrick McDaniel, *Adversarial Examples in Constrained Domains*, Technical Report arXiv:2011.01183, arXiv preprint, 2020.

Stefan Achleitner and Quinn Burke and Patrick McDaniel and Trent Jaeger and Thomas La Porta and Srikanth V. Krishnamurthy, *MLSNet: A Policy Complying Multilevel Security Framework for Software Defined Networking*, Technical Report INSR-500-TR-0500-2019, Institute of Networking and Security Research, Department of Computer Science and Engineering, Pennsylvania State University, University Park, PA, USA, January, 2019.

Michael Norris and Z. Berkay Celik and Patrick McDaniel and Gang Tan and Prasanna Venkatesh and Shulin Zhao and Anand Sivasubramaniam, *IoTRepair: Systematically Addressing Device Faults in Commodity IoT (Extended Paper)*, Technical Report arXiv:2002.07641, arXiv preprint, 2020.

Amit Kumar Sikder and Leonardo Babun and Z. Berkay Celik and Abbas Acar and Hidayet Aksu and Patrick McDaniel and Engin Kirda and Selcuk Uluagac, *KRATOS: Multi-User Multi-Device-Aware Access Control System for the Smart Home*, Technical Report arXiv:1911.10186, arXiv preprint, 2020.

Leonardo Babun and Z. Berkay Celik and Patrick McDaniel and Selcuk Uluagac, *Real-time Analysis of Privacy-(un)aware IoT Applications*, Technical Report arXiv:1911.10461, arXiv preprint, 2019.

Dan Boneh and Andrew J. Grotto and Patrick McDaniel and Nicolas Papernot, *How Relevant is the Turing Test in the Age of Sophisbots?*, Technical Report arXiv:1909.00056, arXiv preprint, 2019.

Chun-Ming Lai and Xiaoyun Wang and Jon W. Chapman and Yu-Cheng Lin and Yu-Chang Ho and Felix Wu and Patrick McDaniel and Hasan Cam, *More or Less? Predict the Social Influence of Malicious URLs on Social Media*, Technical Report arXiv:1812.02978, arXiv preprint, 2018.

Dang Tu Nguyen and Chengyu Song and Zhiyun Qian and Srikanth V. Krishnamurthy and Edward J. M. Colbert and Patrick McDaniel, *IoTSan: Fortifying the Safety of IoT Systems*, Technical Report arXiv:1810.09551, arXiv preprint, 2018.

Z. Berkay Celik and Earlence Fernandes and Eric Pauley and Gang Tan and Patrick McDaniel, *Program Analysis of Commodity IoT Applications for Security and Privacy: Challenges and Opportunities*, Technical Report arXiv:1809.06962, arXiv preprint, 2018.

Giuseppe Petracca and Jens Grossklags and Patrick McDaniel and Trent Jaeger, *Regulating Access to System Sensors in Cooperating Programs*, Technical Report arXiv:1808.05579, arXiv preprint, 2018.

Z. Berkay Celik and Patrick McDaniel and Gang Tan, *Soteria: Automated IoT Safety and Security Analysis*, Technical Report arXiv:1805.08876, arXiv preprint, 2018.

Nicolas Papernot and Patrick McDaniel, *Deep k-Nearest Neighbors: Towards Confident, Interpretable and Robust Deep Learning*, Technical Report arXiv:1803.04765, arXiv preprint, 2018.

Z. Berkay Celik and Leonardo Babun and Amit Kumar Sikder and Hidayet Aksu and Gang Tan and Patrick McDaniel and Selcuk Uluagac, *Sensitive Information Tracking in Commodity IoT*, Technical Report arXiv:1802.08307, arXiv preprint, 2018.

Chun-Ming Lai and Xiaoyun Wang and Yunfeng Hong and Yu-Cheng Lin and Felix Wu and Patrick McDaniel and Hasan Cam, *Attacking Strategies and Temporal Analysis Involving Facebook Discussion Groups*, Technical Report arXiv:1802.04500, arXiv preprint, 2017.

Abbas Acar and Z. Berkay Celik and Hidayet Aksu and Selcuk Uluagac and Patrick McDaniel, *Achieving Secure and Differentially Private Computations in Multiparty Settings*, Technical Report arXiv:1707.01871, arXiv preprint, 2017.

Florian Tramer and Alexey Kurakin and Nicolas Papernot and Ian Goodfellow and Dan Boneh and Patrick McDaniel, *Ensemble Adversarial Training: Attacks and Defenses*, Technical Report arXiv:1705.07204, arXiv preprint, 2017.

Nicolas Papernot and Patrick McDaniel, *Extending Defensive Distillation*, Technical Report arXiv:1705.05264, arXiv preprint, 2017.

Florian Tramer and Nicolas Papernot and Ian Goodfellow and Dan Boneh and Patrick McDaniel, *The Space of Transferable Adversarial Examples*, Technical Report arXiv:1704.03453, arXiv preprint, 2017.

Z. Berkay Celik and Hidayet Aksu and Abbas Acar and Ryan Sheatsley and Selcuk Uluagac and Patrick McDaniel, *Curie: Policy-based Secure Data Exchange*, Technical Report arXiv:1702.08342, arXiv preprint, 2017.

Kathrin Grosse and Praveen Manoharan and Nicolas Papernot and Michael Backes and Patrick McDaniel, *On the (Statistical) Detection of Adversarial Examples*, Technical Report arXiv:1702.06280, arXiv preprint, 2017.

Z. Berkay Celik and David Lopez-Paz and Patrick McDaniel, *Patient-Driven Privacy Control through Generalized Distillation*, Technical Report arXiv:1611.08648, arXiv preprint, 2017.

Nicolas Papernot and Patrick McDaniel and Arunesh Sinha and Michael Wellman, *Towards the Science of Security and Privacy in Machine Learning*, Technical Report arXiv:1611.03814, arXiv preprint, 2016.

Nicolas Papernot and Ian Goodfellow and Ryan Sheatsley and Reuben Feinman and Patrick McDaniel, *cleverhans v1.0.0: an adversarial machine learning library*, Technical Report arXiv:1610.0076, arXiv preprint, 2016.

Nicolas Papernot and Patrick McDaniel, *On the Effectiveness of Defensive Distillation*, Technical Report arXiv:1607.05113, arXiv preprint, 2016.

Kathrin Grosse and Nicolas Papernot and Praveen Manoharan and Michael Backes and Patrick McDaniel, *Adversarial Perturbations Against Deep Neural Networks for Malware Classification*, Technical Report arXiv:1606.04435, arXiv preprint, 2016.

Nicolas Papernot and Patrick McDaniel and Ian Goodfellow, *Transferability in Machine Learning: from Phenomena to Black-Box Attacks using Adversarial Samples*, Technical Report arXiv:1605.07277, arXiv preprint, 2016.

Nicolas Papernot and Patrick McDaniel and Ananthram Swami and Richard Harang, *Crafting Adversarial Input Sequences for Recurrent Neural Networks*, Technical Report arXiv:1604.08275, arXiv preprint, 2016.

Z. Berkay Celik and Patrick McDaniel and Rauf Izmailov and Nicolas Papernot and Ryan Sheatsley and Raquel Alvarez and Ananthram Swami, *Detection under Privileged Information*, Technical Report arXiv:1603.09638,

arXiv preprint, 2016.

Vaibhav Rastogi and Drew Davidson and Lorenzo De Carli and Somesh Jha and Patrick McDaniel, *Towards Least Privilege Containers with Cimplifier*, Technical Report arXiv:1602.08410, arXiv preprint, 2016.

Nicolas Papernot and Patrick McDaniel and Ian Goodfellow and Somesh Jha and Z. Berkay Celik and Ananthram Swami, *Practical Black-Box Attacks against Machine Learning*, Technical Report arXiv:1602.02697, arXiv preprint, 2016.

Nicolas Papernot and Patrick McDaniel and Somesh Jha and Matthew Fredrikson and Z. Berkay Celik and Ananthram Swami, *The Limitations of Deep Learning in Adversarial Settings*, Technical Report arXiv:1511.07528, arXiv preprint, 2015.

Nicolas Papernot and Patrick McDaniel and Xi Wu and Somesh Jha and Ananthram Swami, *Distillation as a Defense to Adversarial Perturbations against Deep Neural Networks*, Technical Report arXiv:1511.04508, arXiv preprint, 2015.

Alexander Kott and Ananthram Swami and Patrick McDaniel, *Six Potential Game-Changers in Cyber Security: Towards Priorities in Cyber Science and Engineering*, Technical Report arXiv:1511.00509, arXiv preprint, 2015.

Li Li and Alexandre Bartel and Jacques Klein and Yves Le Traon and Steven Arzt and Siegfried Rasthofer and Eric Bodden and Damien Octeau and Patrick McDaniel, *I know what leaked in your pocket: uncovering privacy leaks on Android Apps with Static Taint Analysis*, Technical Report arXiv:1404.7431, arXiv preprint, 2014.

Devin Pohly and Patrick McDaniel, *Modeling Privacy and Tradeoffs in Multichannel Secret Sharing Protocols*, Technical Report NAS-TR-0188-2016, Institute of Networking and Security Research, Department of Computer Science and Engineering, Pennsylvania State University, University Park, PA, USA, January, 2016.

Nicolas Papernot and Patrick McDaniel and Somesh Jha and Matthew Fredrikson and Z. Berkay Celik and Ananthram Swami, *The Limitations of Deep Learning in Adversarial Settings*, Technical Report NAS-TR-0172-2014, Network and Security Research Center, Department of Computer Science and Engineering, Pennsylvania State University, University Park, PA, USA, October, 2016.

Wenhui Hu and Damien Octeau and Patrick McDaniel and Peng Liu, *Duet: Library Integrity Verification for Android Applications*, Technical Report NAS-TR-0172-2014, Network and Security Research Center, Department of Computer Science and Engineering, Pennsylvania State University, University Park, PA, USA, February, 2016.

Devin Pohly and Stephen McLaughlin and Patrick McDaniel and Kevin Butler, *Hi-Fi: Collecting High-Fidelity Whole-System Provenance*, Technical Report NAS-TR-0160-2012, Network and Security Research Center, Department of Computer Science and Engineering, Pennsylvania State University, University Park, PA, USA, June, 2016.

Damien Octeau and Somesh Jha and Patrick McDaniel, *Retargeting Android Applications to Java Bytecode*, Technical Report NAS-TR-0150-2011, Network and Security Research Center, Department of Computer Science and Engineering, Pennsylvania State University, University Park, PA, USA, September, 2011.

Stephen McLaughlin and Patrick McDaniel, *Protecting Consumer Privacy from Electric Load Monitoring*, Technical Report NAS-TR-0147-2011, Network and Security Research Center, Department of Computer Science and Engineering, Pennsylvania State University, University Park, PA, USA, March, 2011.

William Enck and Patrick McDaniel, *Federated Information Flow Control for Mobile Phones*, Technical Report NAS-TR-0136-2010, Network and Security Research Center, Department of Computer Science and Engineering, Pennsylvania State University, University Park, PA, USA, July, 2010.

Kevin Butler and Stephen McLaughlin and Patrick McDaniel, *Kells: A Protection Framework for Portable Data*, Technical Report NAS-TR-0134-2010, Network and Security Research Center, Department of Computer Science

and Engineering, Pennsylvania State University, University Park, PA, USA, June, 2010.

Stephen McLaughlin and Dmitry Podkuiko and Adam Delozier and Sergei Miadzvezhanka and Patrick McDaniel, *Multi-vendor Penetration Testing in the Advanced Metering Infrastructure*, Technical Report NAS-TR-0133-2010, Network and Security Research Center, Department of Computer Science and Engineering, Pennsylvania State University, University Park, PA, USA, June, 2010.

Machigar Ongtang and Kevin Butler and Patrick McDaniel, *Porscha: Policy Oriented Secure Content Handling in Android* , Technical Report NAS-TR-0132-2010, Network and Security Research Center, Department of Computer Science and Engineering, Pennsylvania State University, University Park, PA, USA, June, 2010.

Joshua Schiffman and Thomas Moyer and Hayawardh Vijayakumar and Trent Jaeger and Patrick McDaniel, *Seeding Clouds with Trust Anchors*, Technical Report NAS-TR-0127-2010, Network and Security Research Center, Department of Computer Science and Engineering, Pennsylvania State University, University Park, PA, USA, April, 2010.

William Enck and Machigar Ongtang and Patrick McDaniel, *TaintDroid: An Information-Flow Tracking System for Realtime Privacy Monitoring on Smartphones*, Technical Report NAS-TR-0120-2010, Network and Security Research Center, Department of Computer Science and Engineering, Pennsylvania State University, University Park, PA, USA, February, 2010.

Joshua Schiffman and Thomas Moyer and Christopher Shal and Trent Jaeger and Patrick McDaniel, *Justifying Integrity Using a Virtual Machine Verifier*, Technical Report NAS-TR-0119-2009, Network and Security Research Center, Department of Computer Science and Engineering, Pennsylvania State University, University Park, PA, USA, August, 2010.

Machigar Ongtang and Stephen McLaughlin and William Enck and Patrick McDaniel, *Semantically Rich Application-Centric Security in Android*, Technical Report NAS-TR-0116-2009, Network and Security Research Center, Department of Computer Science and Engineering, Pennsylvania State University, University Park, PA, USA, June, 2010.

Stephen McLaughlin and Dmitry Podkuiko and Patrick McDaniel, *Energy Theft in the Advanced Metering Infrastructure*, Technical Report NAS-TR-0115-2009, Network and Security Research Center, Department of Computer Science and Engineering, Pennsylvania State University, University Park, PA, USA, June, 2010.

Kevin Butler and Stephen McLaughlin and Thomas Moyer and Joshua Schiffman and Patrick McDaniel and Trent Jaeger, *Firma: Disk-Based Foundations for Trusted Operating Systems*, Technical Report NAS-TR-0114-2009, Network and Security Research Center, Department of Computer Science and Engineering, Pennsylvania State University, University Park, PA, USA, April, 2010.

William Enck and Machigar Ongtang and Patrick McDaniel, *On Lightweight Mobile Phone App Certification*, Technical Report NAS-TR-0113-2009, Network and Security Research Center, Department of Computer Science and Engineering, Pennsylvania State University, University Park, PA, USA, April, 2010.

Patrick Traynor and Michael Lin and Machigar Ongtang and Vikhyath Rao and Thomas La Porta and Patrick McDaniel, *On Cellular Botnets: Measuring the Impact of Malicious Devices on the Network Core*, Technical Report NAS-TR-0110-2009, Network and Security Research Center, Department of Computer Science and Engineering, Pennsylvania State University, University Park, PA, USA, March, 2010.

Boniface Hicks and Sandra Rueda and Yogesh Sreenivasan and Guruprasad Jakka and David King and Trent Jaeger and Patrick McDaniel, *An Architecture for Enforcing End-to-End Security Over Web Applications*, Technical Report NAS-TR-0104-2009, Network and Security Research Center, Department of Computer Science and Engineering, Pennsylvania State University, University Park, PA, USA, January, 2009.

Joshua Schiffman and Thomas Moyer and Christopher Shal and Trent Jaeger and Patrick McDaniel, *No Node Is an Island: Shamon Integrity Monitoring Approach*, Technical Report NAS-TR-0103-2009, Network and Security

Research Center, Department of Computer Science and Engineering, Pennsylvania State University, University Park, PA, USA, February, 2009.

Patrick Traynor and Michael Lin and Machigar Ongtang and Vikhyath Rao and Trent Jaeger and Thomas La Porta and Patrick McDaniel, *On Cellular Botnets: Measuring the Impact of Malicious Devices on the Network Core*, Technical Report NAS-TR-0099-2008, Network and Security Research Center, Department of Computer Science and Engineering, Pennsylvania State University, University Park, PA, USA, Novemeber, 2008.

Kevin Butler and Stephen McLaughlin and Thomas Moyer and Patrick McDaniel and Trent Jaeger, *SwitchBlade: Policy-Driven Disk Segmentation*, Technical Report NAS-TR-0098-2008, Network and Security Research Center, Department of Computer Science and Engineering, Pennsylvania State University, University Park, PA, USA, November, 2008.

Thomas Moyer and Kevin Butler and Joshua Schiffman and Patrick McDaniel and Trent Jaeger, *Scalable Asynchronous Web Content Attestation*, Technical Report NAS-TR-0095-2008, Network and Security Research Center, Department of Computer Science and Engineering, Pennslyvania State University, University Park, PA, USA, September, 2008.

William Enck and Machigar Ongtang and Patrick McDaniel, *Automated Cellphone Application Certification in Android (or) Mitigating Phone Software Misuse Before It Happens*, Technical Report NAS-TR-0094-2008, Network and Security Research Center, Department of Computer Science and Engineering, Pennslyvania State University, University Park, PA, USA, September, 2008.

Boniface Hicks and Sandra Rueda and Luke St. Clair and Trent Jaeger and Patrick McDaniel, *A Logical Specification and Analysis for SELinux MLS Policy*, Technical Report NAS-TR-0091-2008, Network and Security Research Center, Department of Computer Science and Engineering, Pennslyvania State University, University Park, PA, USA, July, 2008.

Kevin Butler and Stephen McLaughlin and Patrick McDaniel, *Rootkit-Resistant Disks*, Technical Report NAS-TR-0089-2008, Network and Security Research Center, Department of Computer Science and Engineering, Pennslyvania State University, University Park, PA, USA, April, 2008.

Patrick Traynor and Joshua Schiffman and Thomas La Porta and Patrick McDaniel and Abhrajit Ghosh and Farooq Anjum, *Constructing Secure Localization Systems with Adjustable Granularity*, Technical Report NAS-TR-0084-2007, Network and Security Research Center, Department of Computer Science and Engineering, Pennslyvania State University, University Park, PA, USA, December, 2007.

Stephen McLaughlin and Kevin Butler and William Enck and Patrick McDaniel, *Genbd - A Generic Block Device*, Technical Report NAS-TR-0082-2007, Network and Security Research Center, Department of Computer Science and Engineering, Pennslyvania State University, University Park, PA, USA, November, 2007.

Kevin Butler and Stephen McLaughlin and Patrick McDaniel, *Non-Volatile Memory and Disks: Avenues for Policy Architectures*, Technical Report NAS-TR-0074-2007, Network and Security Research Center, Department of Computer Science and Engineering, Pennslyvania State University, University Park, PA, USA, June, 2007.

William Enck and Sandra Rueda and Joshua Schiffman and Yogesh Sreenivasan and Luke St. Clair and Trent Jaeger and Patrick McDaniel, *Protecting Users From "Themselves"*, Technical Report NAS-TR-0073-2007, Network and Security Research Center, Department of Computer Science and Engineering, Pennslyvania State University, University Park, PA, USA, June, 2007.

Dhananjay Bapat and Kevin Butler and Patrick McDaniel, *Towards Automated Privilege Separation*, Technical Report NAS-TR-0071-2007, Network and Security Research Center, Department of Computer Science and Engineering,Pennslyvania State University, University Park, PA, USA, May, 2007.

Patrick Traynor and Kevin Butler and William Enck and Patrick McDaniel, *Realizing Massive-Scale Conditional Access Systems Through Attribute-Based Cryptosystems*, Technical Report NAS-TR-0070-2007, Network and Security Research Center, Department of Computer Science and Engineering, Pennslyvania State University, University Park, PA, USA, May, 2007.

Luke St. Clair and Joshua Schiffman and Trent Jaeger andPatrick McDaniel, *Establishing and Sustaining System Integrity viaRoot of Trust Installation*, Technical Report NAS-TR-0067-2007, Network and Security Research Center, Department of Computer Science and Engineering,Pennslyvania State University, University Park, PA, USA, April, 2007.

Boniface Hicks and David King and Patrick McDaniel, *Jifclipse: Development Tools for Security-Typed Language*, Technical Report NAS-TR-0065-2007, Network and Security Research Center, Department of Computer Science and Engineering, Pennslyvania State University, University Park, PA, USA, April, 2007.

William Enck and Patrick McDaniel and Trent Jaeger, *Protecting User Files by Reducing Application Access*, Technical Report NAS-TR-0063-2007, Network and Security Research Center, Department of Computer Science and Engineering, Pennsylvania State University, University Park, PA, USA, February, 2007.

Boniface Hicks and Sandra Rueda and Trent Jaeger andPatrick McDaniel, *A Logical Specification and Analysis for SELinux MLSPolicy*, Technical Report NAS-TR-0058-2007, Network and Security Research Center, Department of Computer Science and Engineering,Pennsylvania State University, University Park, PA, USA, January, 2007.

Boniface Hicks and Sandra Rueda and Trent Jaeger andPatrick McDaniel, *From Trusted to Secure: Building and ExecutingApplications that Enforce System Security*, Technical Report NAS-TR-0061-2007, Network and Security Research Center, Department of Computer Science and Engineering,Pennsylvania State University, University Park, PA, USA, January, 2007.

Lisa Johansen and Kevin Butler and William Enck andPatrick Traynor and Patrick McDaniel, *Grains of SANs: Building Storage Area Networks fromMemory Spots*, Technical Report NAS-TR-0060-2007, Network and Security Research Center, Department of Computer Science and Engineering,Pennsylvania State University, University Park, PA, USA, January, 2007.

Patrick Traynor and Vikhyath Rao and Trent Jaeger andPatrick McDaniel and Thomas La Porta, *From Mobile Phones to Responsible Devices*, Technical Report NAS-TR-0059-2007, Network and Security Research Center, Department of Computer Science and Engineering,Pennsylvania State University, University Park, PA, USA, January, 2007.

Anusha Sriraman and Kevin Butler and Patrick McDaniel andPadma Raghavan, *Analysis of the IPv4 Address Space Delegation Structure*, Technical Report NAS-TR-0057-2006, Network and Security Research Center, Department of Computer Science and Engineering,Pennsylvania State University, University Park, PA, USA, December, 2006.

Luke St. Clair and Joshua Schiffman and Trent Jaeger andPatrick McDaniel, *Sum of the Parts: Composing Trust from Validation Primitives*, Technical Report NAS-TR-0056-2006, Network and Security Research Center, Department of Computer Science and Engineering,Pennsylvania State University, University Park, PA, USA, November, 2006.

Sophie Qiu and Patrick McDaniel and Fabian Monrose, *Toward Valley-Free Inter-domain Routing*, Technical Report NAS-TR-0054-2006, Network and Security Research Center, Department of Computer Science and Engineeering, Pennsylvania State University, University Park, PA, USA, October, 2006.

Boniface Hicks and Sandra Rueda and Trent Jaeger andPatrick McDaniel, *Integrating SELinux with Security-typed Languages*, Technical Report NAS-TR-0052-2006, Network and Security Research Center, Department of Computer Science and Engineering,Pennsylvania State University, University Park, PA, USA, October, 2006.

Patrick Traynor and William Enck and Patrick McDaniel andThomas La Porta, *Mitigating Attacks on Open Functionality in SMS-CapableNetworks*, Technical Report NAS-TR-0051-2006, Network and Security Research Center, Department of Computer Science and Engineering,Pennsylvania State University, University Park, PA, USA, October, 2006.

Patrick Traynor and Kevin Butler and William Enck and Kevin Borders and Patrick McDaniel, malnets*: Large-Scale Malicious Networks via Compromised Wireless Access Points*, Technical Report NAS-TR-0048-2006, Network and Security Research Center, Department of Computer Science and Engineering, Pennsylvania State University, University Park, PA, USA, September, 2006.

Boniface Hicks and Sandra Rueda and Trent Jaeger and 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, Pennsylvania State University, University Park, PA, USA, September, 2006.

Sunam Ryu and Kevin Butler and Patrick Traynor and Patrick McDaniel, *Leveraging Identity-based Cryptography for Node ID Assignment in Structured P2P Systems*, Technical Report NAS-TR-0043-2006, Network and Security Research Center, Department of Computer Science and Engineering, Pennsylvania State University, University Park, PA, USA, August, 2006.

Wesam Lootah and William Enck and Patrick McDaniel, *TARP: Ticket-based Address Resolution Protocol (extended version)*, Technical Report NAS-TR-0046-2006, Network and Security Research Center, Department of Computer Science and Engineering, Pennsylvania State University, University Park, PA, USA, August, 2006.

Patrick McDaniel, *Understanding Equivalance in High-Level and Information Flow Policy*, Technical Report NAS-TR-0042-2006, Network and Security Research Center, Department of Computer Science and Engineering, Pennsylvania State University, University Park, PA, USA, July, 2006.

Trent Jaeger and Patrick McDaniel and Luke St. Clair and Ramon Caceres and Reiner Sailer, *Shame on Trust in Distributed Systems*, Technical Report RC239664 (W0605-129), IBM Research Division, Yorktown Heights, NY, May, 2006.

Lisa Johansen and Kevin Butler and Michael Rowell and Patrick McDaniel, *Email Communities of Interest*, Technical Report NAS-TR-0040-2006, Network and Security Research Center, Department of Computer Science and Engineering,Pennsylvania State University, University Park, PA, USA, May, 2006.

Boniface Hicks and Kiyan Ahmadizadeh and Patrick McDaniel, *From Languages to Systems: Understanding PracticalApplication Development in Security-typed Languages*, Technical Report NAS-TR-0035-2006, Network and Security Research Center, Department of Computer Science and Engineering,Pennsylvania State University, University Park, PA, USA, April, 2006.

Boniface Hicks and David King and Patrick McDaniel andMichael Hicks, *Trusted Declassification: High-level policy for asecurity-typed language*, Technical Report NAS-TR-0033-2006, Network and Security Research Center, Department of Computer Science and Engineering,Pennsylvania State University, University Park, PA, USA, March, 2006.

Matthew Pirretti and Patrick Traynor and PatrickMcDaniel and Brent Waters, *Secure Attribute-Based Systems*, Technical Report NAS-TR-0028-2006, Network and Security Research Center, Department of Computer Science and Engineering,Pennsylvania State University, University Park, PA, USA, February, 2006.

William Enck and Kevin Butler and Thomas Richardson andPatrick McDaniel, *Securing Non-Volatile Main Memory*, Technical Report NAS-TR-0029-2006, Network and Security Research Center, Department of Computer Science and Engineering,Pennsylvania State University, University Park, PA, USA, February, 2006.

Luke St. Clair and Lisa Johansen and William Enck andMatthew Pirretti and Patrick Traynor and Patrick McDaniel andTrent Jaeger, *Password Exhaustion: Predicting the End of Password Usefulness*, Technical Report NAS-TR-0030-2006, Network and Security Research Center, Department of Computer Science and Engineering, Pennsylvania State University, University Park, PA, USA, February, 2006.

Heesook Choi and Patrick McDaniel and Thomas La Porta, *Privacy Preserving Communication in MANETs*, Technical Report NAS-TR-0031-2006, Network and Security Research Center, Department of Computer Science and Engineering, Pennsylvania State University, University Park, PA, USA, December, 2005.

Matthew Pirretti and Vijaykrishnan Narayanan and PatrickMcDaniel and Bharat Madan, *SLAT: Secure Localization with Attack Tolerance*, Technical Report NAS-TR-0024-2005, Network and Security Research Center, Department of Computer Science and Engineering,Pennsylvania State University, University Park, PA, USA, August, 2005.

Patrick Traynor and Michael Chien and Scott Weaver andBoniface Hicks and Patrick McDaniel, *Non-Invasive Methods for Host Certification*, Technical Report NAS-TR-0025-2005, Network and Security Research Center, Department of Computer Science and Engineering,Pennsylvania State University, University Park, PA, USA, September, 2005.

Sophie Qiu and Patrick McDaniel and Fabian Monrose andAvi Rubin, *Characterizing Address Use Structure and Stabillity ofOrigin Advertizement in Interdomain Routing*, Technical Report NAS-TR-0018-2005, Network and Security Research Center, Department of Computer Science and Engineering,Pennsylvania State University, University Park, PA, USA, July, 2005.

Hosam Rowaihy and William Enck and Patrick McDaniel andThomas La Porta, *Limiting Sybil Attacks in Structured Peer-to-Peer Networks*, Technical Report NAS-TR-0017-2005, Network and Security Research Center, Department of Computer Science and Engineering,Pennsylvania State University, University Park, PA, USA, July, 2005.

Boniface Hicks and Patrick McDaniel and Ali Hurson, *Information Flow Control in Database Security: A CaseStudy for Secure Programming with Jif*, Technical Report NAS-TR-0011-2005, Network and Security Research Center, Department of Computer Science and Engineering,Pennsylvania State University, Uni versity Park, PA, USA, April, 2005.

Wesam Lootah and William Enck and Patrick McDaniel, *TARP: Ticket-Based Address Resolution Protocol*, Technical Report NAS-TR-0010-2005, Network and Security Research Center, Department of Computer Science and Engineering,Pennsylvania State University, University Park, PA, USA, June, 2005.

Patrick Traynor and Kevin Butler and William Enck andJennifer Plasterr and Scott Weaver and John van Bramer and PatrickMcDaniel, *Privacy-Preserving Web-Based Email*, Technical Report NAS-TR-0009-2005, Network and Security Research Center, Department of Computer Science and Engineering,Pennsylvania State University, University Park, PA, USA, June, 2005.

William Enck and Patrick Traynor and Patrick McDaniel andThomas La Porta, *Exploiting Open Functionality in SMS-Capable Cellular Networks*, Technical Report NAS-TR-0007-2005, Network and Security Center, Department of Computer Science, Pennsylvania State University, May, 2005.

Boniface Hicks and David King and Patrick McDaniel, *Declassification with Cryptographic Functions in aSecurity-Typed Language*, Technical Report NAS-TR-0004-2005, Network and Security Center, Department of Computer Science, Pennsylvania State University, January, 2005.

William Aiello and Kevin Butler and Patrick McDaniel, *Path Authentication in Interdomain Routing*, Technical Report TR NAS-TR-0002-2004, Network and Security Center, Department of Computer Science and Engineering, Penn State University, November, 2004.

Dan Pei and William Aiello and Anna Gilbert and PatrickMcDaniel, *Origin Disturbances in BGP*, Technical Report TD-62TJJF8, AT&T Labs - Research, Florham Park, NJ, July, 2004.

Kevin Butler and Toni Farley and Patrick McDaniel andJennifer Rexford, *A Survey of BGP Security Issues and Solutions*, Technical Report TD-5UGJ33, AT&T Labs - Research, Florham Park, NJ, February, 2004.

Patrick McDaniel and Atul Prakash, *Securing Distributed Applications Using a Policy-based Approach*, Technical Report TD-5UDKVD, AT&T Labs - Research, Florham Park, NJ, December, 2003.

William Aiello and John Ioannidis and Patrick McDaniel, *Origin Authentication in Interdomain Routing*, Technical Report TD-5QHG2G, AT&T Labs - Research, Florham Park, NJ, August, 2003.

Eric Cronin and Sugih Jamin and Tal Malkin and PatrickMcDaniel, *On the Performance, Feasibility, and Use of Forward SecureSignatures*, Technical Report TD-5QHGBK, AT&T Labs - Research, Florham Park, NJ, August, 2003.

Simon Byers and Lorrie Cranor and Eric Cronin and DaveKormann and Patrick McDaniel, *Analysis of Security Vulnerabilities in the Movie Productionand Distribution Process*, Technical Report TD-5N6SJ4, AT&T Labs - Research, Florham Park, NJ, August, 2003.

Patrick McDaniel, *On Context in Authorization Policy*, Technical Report TD-5JCJCK, AT&T Labs - Research, Florham Park, NJ, January, 2003.

Patrick McDaniel and Atul Prakash, *An Architecture for Security Policy Enforcement*, Technical Report TD-5C6JFV, AT&T Labs - Research, Florham Park, NJ, July, 2002.

Patrick McDaniel and Atul Prakash, *Methods and Limitations of Security Policy Reconciliation*, Technical Report TD57-PAW, AT&T Labs - Research, Florham Park, NJ, February, 2002.

Patrick McDaniel and Atul Prakash, *Ismene: Provisioning and Policy Reconciliation in SecureGroup Communication*, Technical Report CSE-TR-438-00, Electrical Engineering and Computer Science, Universityof Michigan, December, 2000.

Patrick McDaniel and Atul Prakash, *Lightweight Failure Detection in Secure GroupCommunication*, Technical Report CSE-TR-428-00, Electrical Engineering and Computer Science, Universityof Michigan, June, 2000.

Patrick McDaniel and Atul Prakash, *Antigone: Implementing Policy in Secure GroupCommunication*, Technical Report CSE-TR-426-00, Electrical Engineering and Computer Science, Universityof Michigan, May, 2000.

Patrick McDaniel and Sugih Jamin, *Windowed Certificate Revocation*, Technical Report CSE-TR-413-99, Electrical Engineering and Computer Science, Universityof Michigan, November, 1999.

Patrick McDaniel and Atul Prakash and Peter Honeyman, *Antigone: A Flexible Framework for Secure Group Communication*, Technical Report 99-2, Center for Information Technology Integration, September, 1999.

Patrick McDaniel and Avi Rubin, *A Response to "Can We Eliminate Certificate RevocationLists?"*, Technical Report 99.8.1, AT&T Labs - Research, Florham Park, NJ, August, 1999.

Andrew Adamson and Charles J. Antonelli and Kevin Coffman andPatrick McDaniel and Jim Rees, *Secure Distributed Virtual Conferencing: Multicast orBust*, Technical Report 99-1, Center for Information Technology Integration, January, 1999.

Patrick McDaniel and Sugih Jamin, *Windowed Key Revocation in Public Key Infrastructures*, Technical Report CSE-TR-376-98, Electrical Engineering and Computer Science, Universityof Michigan, , 1998.

Patrick McDaniel and Sugih Jamin, *A Scalable Key Distribution Hierarchy*, Technical Report CSE-TR-366-98, Electrical Engineering and Computer Science, Universityof Michigan, , 1998.

Patrick McDaniel and Peter Honeyman and Atul Prakash, *Lightweight Secure Group Communication*, Technical Report 98-2, Center for Information Technology Integration,University of Michigan, April, 1998.

Wayne Zage and Delores Zage and Patrick McDaniel and IrshadKhan, *Evaluating Design Metrics on Large-Scale Software*, Technical Report SERC-TR-106-P, Software Engineering Resource Center, PurdueUniversity, September, 1991.

PUBLIC SPEAKING

When is it Ok for AI to Be Wrong?, AI Meets Society Symposium (AIMS), Morgridge Hall, Madison, WI, February, 2026.

What Does AI Mean for Our Future?, AFSCME Retirees Subchapter 52 (Badger Talk), Madison Labor Temple, Madison, WI, October, 2025.

How to Read a Paper, CS900, University of Wisconsin-Madison, Madison, WI, September, 2025.

What Does AI Mean for Our Future?, Wisconsin Public Library Systems / Winnefox Library System (Virtual Badger Talk), Virtual, September, 2025.

The Security of AI (what you need to know), Day of Learning Program, Class of 1975, UW-Madison Gordon Commons, Madison, WI, September, 2025.

The Security of AI (what you need to know), Alumni College, Red Crown Lodge, Woodriff, WI, June, 2025.

What Does AI Mean to Our Future? (what you need to know), PBS AI Series Badger Talk, PBS Wisconsin, Golden Rondelle Theater, Racine, WI, May, 2025.

Keynote, *Adversarial Machine Learning: A 10-year Perspective*, US-Taiwan Workshop on Cybersecurity, National Science Foundation, Arlington, VA, March, 2025.

Distinguished Lecture, *Adversarial Machine Learning: A 10-year Perspective*, Department of Electrical and Computer Engineering, Iowa State University, Ames, IA, January, 2025.

Distinguished Lecture, *Adversarial Machine Learning: A 10-year Perspective*, NSF ACTION AI Institute Distinguished Lecture Series, Virtual, December, 2024.

Distinguished Lecture, *Adversarial Machine Learning: A 10-year Perspective*, Department of Electrical and Computer Engineering, University of Illinois, Champaign-Urbana, Champaign, IL, November, 2024.

Security and its Role in Achieving Sustainability, Workshop on the Architecture of Green Energy Systems: The Underlying Problem and Its Challenge, Institute for Mathematical and Statistical Innovation, University of Chicago, Chicago, IL, June, 2024.

Distinguished Lecture, *The Challenges of Machine Learning in Adversarial Settings: A Systems Perspective*, Department of Electrical and Computer Engineering, University of California, Los Angeles, Los Angeles, CA, December, 2023.

The Security of AI (what organizations need to know), TEDxUWMadison, Madison, WI, November, 2023.

Distinguished Lecture, *The Challenges of Machine Learning in Adversarial Settings: A Systems Perspective*, Computer Science Department, Michigan State University, Lansing, MI, November, 2023.

The Security of AI (what organizations need to know), Greater Madison Chamber of Commerce, Madison, WI, September, 2023.

Securitys Role in Achieving Sustainability, Center for Sustainability and the Global Environment, Madison, WI, February, 2023.

Keynote, *Securitys Role in Achieving Sustainability*, 29th ACM Conference on Computer and Communications Security (CCS), Los Angeles, CA, November, 2022.

Keynote, *Security, Game Theory, and Their Role in Achieving Sustainability*, Conference on Decision and Game Theory for Security, Pittsburgh, PA, October, 2022.

NSF Funding: Why, What and How, School of Computer, Data and Information Sciences, UW-Madison, Madison, WI, October, 2022.

Keynote, *Prognosticating the Future of IoT Security*, 2022 IEEE SafeThings Workshop, San Francisco, CA, May, 2022.

Distinguished Lecture, *The Challenges of Machine Learning in Adversarial Settings: A Systems Perspective*, Temple University, Philadelphia, PA, March, 2022.

The Challenges of Machine Learning in Adversarial Settings: A Systems Perspective, CACR Security Speaker Series, Indiana University, Online, August, 2021.

Keynote, *The Challenges of Machine Learning in Adversarial Settings: A Systems Perspective*, Robustness of AI Systems to Adversarial Attacks (RAISA3), Online, August, 2020.

Distinguished Lecture, *The Challenges of Machine Learning in Adversarial Settings: A Systems Perspective*, Computer Science Department, University of Wisconsin-Madison, Madison, WI, February, 2020.

Shutterstock Distinguished Lecture, *The Challenges of Machine Learning in Adversarial Settings*, Computer Science Department, Stonybrook University, Stonybrook, NY, December, 2019.

Distinguished Blockchain Lecture, *The Challenges of Machine Learning in Adversarial Settings*, Cylab Security and Privacy Institute, Carnegie Mellon University, Pittsburgh, PA, December, 2019.

The Challenges of Machine Learning in Adversarial Settings, S2ERC, Ball State University, Muncie, IN, November, 2019.

Keynote, *The Challenges of Machine Learning in Adversarial Settings*, Triangle Area Privacy and Security Day, Durham, NC, October, 2019.

AI-Cybersecurity Workshop Briefing to the NITRD and MLAI Subcommittees, NITRD and MLAI Subcommittees Quarterly Meeting, Washington, DC, July, 2019.

Workshop on the Security and Privacy of Machine Learning, Workshop on the Security and Privacy of Machine Learning, International Conference on Machine Learning, Long Beach, CA, June, 2019.

Keynote, *The Challenges of Machine Learning in Adversarial Settings*, 2019 Subversion and Assurance of AI Workshop, US National Reconnaissance Office, Washington, DC, March, 2019.

The Challenges of Machine Learning in Adversarial Settings, National Science Foundation, Alexandria, VA, March, 2019.

Convergence of AI and IoT, Intelligence Community Studies Board, Division on Engineering and Physical Sciences, The National Academy of Sciences/Engineering, Washington, DC, February, 2019.

Tracing the Arc of Smartphone Application Security, Duke University, Durham, NC, February, 2019.

Distinguished Speaker Series, *The Challenges of Machine Learning in Adversarial Settings*, Department of Computer Science, University at Buffalo, Buffalo, NY, November, 2018.

Samuel D. Conte Distinguished Lecture Series, *The Challenges of Machine Learning in Adversarial Settings*, Department of Computer Science, Purdue University, West Lafeyette, Indiana, November, 2018.

The Challenges of Machine Learning in Adversarial Settings, Computer Science Department, Indiana University of Pennsylvania, Indiana, PA, October, 2018.

The Challenges of Machine Learning in Adversarial Settings, Huddle with the Faculty, Penn State University Alumni Association, University Park, PA, September, 2018.

Distinguished Lecture, *The Challenges of Machine Learning in Adversarial Settings*, Department of Software and Information Systems, University of North Carolina at Charlotte, Charlotte, NC, February, 2018.

Tracing the Arc of Smartphone Application Security, School of Electrical and Computer Engineering, Georgia Tech University, Atlanta, GA, December, 2017.

Tracing the Arc of Smartphone Application Security, Department of Electrical Engineering and Computer Science, Ohio University, Athens, OH, October, 2017.

Keynote, *Attacks, Defenses, and Impacts of Machine Learning in Adversarial Settings*, 2017 Conference on Security and Privacy in Communication Networks (SecureComm), Niagara Falls, Canada, October, 2017.

Distinguished Lecture, *Attacks, Defenses, and Impacts of Machine Learning in Adversarial Settings*, Celebrating 50 Years of Computer Science @ NC State, North Carolina State University, Raleigh, NC, October, 2017.

Distinguished Lecture, *Tracing the Arc of Smartphone Application Security*, Computer Science Department and the Electrical and Computer Engineering Department Seminar Series, Colorado State University, Fort Collins, CO, October, 2017.

Distinguished Lecture, *Tracing the Arc of Smartphone Application Security*, Rochester Institute of Technology, College of Computing and Information Sciences, Rochester, NY, September, 2017.

Distinguished Lecture, *Tracing the Arc of Smartphone Application Security*, University of Texas-Dallas, Department of Computer Science, Dallas, TX, May, 2017.

Keynote, *Tracing the Arc of Smartphone Application Security*, 2017 ACM on International Workshop on Security And Privacy Analytics, Scottsdale, AZ, March, 2017.

Distinguished Lecture, *Tracing the Arc of Smartphone Application Security*, The Ohio State University, Department of Computer Science and Engineering, Columbus, OH, March, 2017.

Distinguished Lecture, *Tracing the Arc of Smartphone Application Security*, University of California-Irvine, Computer Science Department, Irvine, CA, March, 2017.

Distinguished Lecture, *Tracing the Arc of Smartphone Application Security*, Virginia Technical University, Department of Computer Science, Blacksburg, VA, March, 2017.

Keynote, *Tracing the Arc of Smartphone Application Security*, 12th International Conference on Information Systems Security , Jaipur, India, December, 2016.

Tracing the Arc of Smartphone Application Security, University of Michigan, Ann Arbor, Ann Arbor, MI, November, 2016.

Machine Intelligence in Adversarial Settings, Developing a Normative Framework for Cyberwarfare, United States Naval Academy, Annapolis, MD, September, 2016.

Eight Years of Mobile Smartphone Security, University of Pittsburgh, Pittsburgh, PA, September, 2016.

Eight Years of Mobile Smartphone Security, New Jersey Institute of Technology, Newark, NJ, September, 2016.

Setting a Cyber-Security Baseline for Physical Systems: Terminology, Technologies, and Goals, Pacific Northwest Clean Water Association, webinar, August, 2016.

Keynote, *The Limitations of Machine Learning in Adversarial Settings*, 25th International Conference on Computer Communication and Networks (ICCCN 2016), Waikoloa, HI, August, 2016.

Keynote, *Learning from Ourselves: Where are we and where can we go in mobile systems security?*, Mobile Security Technologies (MOST) 2016 Workshop, IEEE Computer Society Security and Privacy Workshops, San Jose, CA, May, 2016.

Keynote, *Eight Years of Mobile Smartphone Security*, Center for Secure and Dependable Systems (CSDS) Cybersecurity Symposium, Coeur d'Alene, April, 2016.

Eight Years of Mobile Smartphone Security, University of Idaho, Moscow, ID, April, 2016.

Army Installation 2035: Cyber Challenges and Opportunities, US Department of Defense, Arlington, VA, April, 2016.

The Limitations of Machine Learning in Adversarial Settings, Florida Institute on National Security Assured Autonomy Workshop, Fort Myers, FL, February, 2016.

SABOT: Specification-based Payload Generation for Programmable Logic Controllers, Messaging, Malware and Mobile Anti-Abuse Working Group (M3AAWG) , San Francisco, CA, February, 2016.

Seven Years of Mobile Smartphone Security, Computer and Information Sciences Department, Temple University, Philadelphia, PA, January, 2016.

Seven Years of Mobile Smartphone Security, Massachusetts Institute of Technology–Lincoln Labs, Lexington, MA, January, 2016.

Six Years of Mobile Smartphone Security, Information Trust Institute, University of Illinois at Urbana-Champaign, Urbana-Champaign, IL, September, 2015.

Keynote, *The Importance of Measurement and Decision Making to a Science of Security*, 2015 IEEE Conference on Communications and Network Security, Florence, Italy, September, 2015.

Keynote, *The Importance of Measurement and Decision Making to a Science of Security*, 3rd International Symposium on Resilient Cyber Systems, Philadelphia, PA, August, 2015.

Distinguished Lecture, *Six Years of Mobile Smartphone Security*, CISPA Distinguished Lecture Series, Max Planck Institute/Saarland University, Saarbrucken Germany, July, 2015.

Distinguished Lecture, *Six Years of Mobile Smartphone Security*, Technische Universtat Darmstadt, Darmstadt Germany, July, 2015.

Estimating Attack Intent and Mission Impact From Detection Signals, Workshop on Cyber Attack Detection, Forensics and Attribution forAssessment of Mission Impact, NATO Science and Technology Organization, Information Systems Technology Panel, Istanbul, Turkey, June, 2015.

Keynote, *The Importance of Measurement and Decision Making to a Science of Security*, 2015 Symposium and Bootcamp on the Science of Security (Hotsos), University of Illinois at Urbana-Champaign, April, 2015.

Keynote, *Security and Science of Agility*, First ACM Workshop on Moving Target Defense (MTD 2014), Scottsdale, AZ, November, 2014.

Evaluating Mobile Smartphone Security: The First Five Years, Computer Science Colloquium Series, Harvard School of Engineering and Applied Sciences, Harvard University, Boston, MA, October, 2014.

Keynote, *A Secondary Internet Revolution: How the Smart Device has Changed the Information Security Landscape*, IEEE New Technology Industry Seminar (NTIS '13), Everett, WA, August, 2013.

Geotargeting: Mobile Device Privacy and Security, National Academy of Sciences, Washington DC, February, 2013.

Authentication and Web Security, Security and Privacy in IT-EMTM 604 Guest Lecture, University of Pennsylvania, Philadelphia, PA, February, 2013.

The Realities of Voting: A Retrospective of Ten Years of Information Security and Electronic Voting Systems, 2012 Information Assurance Day, Computer Science Department, Indiana University of Pennsylvania, Indiana, PA, November, 2012.

Keynote, *Permission-based Application Governance; A Step Forward or Backward?*, 26th Annual WG 11.3 Conference on Data and Applications Security and Privacy (DBSec'12), Paris, France, July, 2012.

Evaluating Mobile Smartphone Security: The First Four Years, Carnegie Mellon University, Pittsburgh, PA, April, 2012.

Keynote, *Scalable Integrity-Guaranteed AJAX*, The 14th Asia-Pacific Web Conference (APWeb), Kunming, China, April, 2012.

Evaluating Mobile Smartphone Application Security, Singapore Management University, Singapore, September, 2011.

Evaluating Mobile Smartphone Application Security, Computer Security Foundations Symposium, Florham Park, NJ, July, 2011.

Keynote, *Security Challenges and Solutions in Mobile Smartphone Applications*, Computer Security Foundations Symposium, Domaine de l'Abbaye des Vaux de Cernay, France, June, 2011.

Distinguished Lecture, *Security Challenges and Solutions in Mobile Smartphone Applications*, Computer and Information Science Department, University of Oregon, Eugene, OR, April, 2011.

Identifying (and Addressing) Security and Privacy Issues in Smart Electric Meters, Center for Non-Linear Studies, Los Alamos, NM, February, 2011.

Distinguished Lecture, *Security Challenges and Solutions in Mobile Smartphone Applications*, Department of Software Information SystemsCollege of Computing and Informatics, UNC Charlotte, Charlotte, NC, December, 2010.

Security Challenges and Solutions in Mobile Smartphone Applications, Computer Science Department, Indiana University of Pennsylvania, Indiana, PA, December, 2010.

Security Challenges and Solutions in Mobile Smartphone Applications, Computer Science Department, Georgetown University, Washington D.C., November, 2010.

Security Challenges and Solutions in Mobile Smartphone Applications, Networking and Security Research Center, ComputerScience and Engineering, Pennsylvania State University, University Park, PA, October, 2010.

Security Challenges and Solutions in Mobile Smartphone Applications, Security Day Seminar, Penn State University, University Park, PA, October, 2010.

The Changing Vulnerability Landscape, Association for Computing Machinery, Penn State Student Chapter, University Park, PA, September, 2010.

The Changing Vulnerability Landscape, ExxonMobil, Falls Church, VA, March, 2010.

The Impact of Supply Chain on Information and Communications Technology Security, The 1st Workshop on Telecommunications Infrastructure Protection and Security, Honolulu, HI, December, 2000.

Energy Theft in the Advanced Metering Infrastructure, Networking and Security Research Center, Computer-Science and Engineering, Pennsylvania State University, State College, PA, October, 2009.

Secure Provenance in High-End Computing Systems, NSF HECURA FSIO PI Meeting, Arlington, VA, August, 2009.

Missing Glue: Architectural Support for Security Annotations, National Science Foundation Security Driven Architecture Workshop, Arlington, VA, July, 2009.

Scalable Integrity-Justified Content Provenance, NSERC ISSNet Workshop, Ottawa, Canada, June, 2009.

Utility Grid Automation and Risk Management, Clean Technology Conference and Expo, Houston, Texas, May, 2009.

Scalable Integrity-Justified Content Provenance, Center for Applied Cybersecurity Research, Indiana University, Bloomington, IN, April, 2009.

Scalable Integrity-Justified Content Provenance, Department of Electrical Engineering and Computer Science, University of Michigan, Ann Arbor, MI, April, 2009.

What is Security, Dickenson Law School, Penn State University, State College, PA, April, 2009.

Scalable Integrity-Justified Content Provenance, Department of Computer Science and Engineering, Notre Dame University, South Bend, IN, April, 2009.

Electronic Voting: The Good, the Bad, and the Reality, Software Engineering Research Center Showcase, Muncie, IN, November, 2008.

Ohio Voting Systems Integrity: The EVEREST Report, Networking and Security Research Center, Computer-Science and Engineering, Pennsylvania State University, State College, PA, October, 2008.

Data Provenance: Challenges and Technology, Cyber Physical System Security Forum, Cyber SecurityResearch and Development Review, Washington DC, October, 2008.

System-Wide Information Flow Enforcement, NICIAR PI Meeting, Washington DC, September, 2008.

Presto: Configuration Management at Massive Scale, NSF Workshop on Assurable and Usable Security Configuration, George Mason University, Fairfax, VA, August, 2008.

Asymmetry in Performance and Security Requirements for I/O in High-end Computing, NSF HECURA FSIO PI Meeting, Arlington, VA, August, 2008.

Authentication and Web Security, Security and Privacy in IT-EMTM 604 Guest Lecture,University of Pennsylvania, Philadelphia, PA, May, 2008.

SPAM and SPAM Mitigation, Computer Science Department, St. Vincent's University, Latrobe, PA, April, 2008.

Phones, The Press, Research and Grad School … or how to make trouble and have fun doing it, Computer Science Department, St. Vincent's University, Latrobe, PA, April, 2008.

Applications and Services in Telecommunications Networks, NSF Wireless Security Workshop, Georgia Institute of Technology, Atlanta, GA, March, 2008.

Vulnerabilities and Opportunities in SMS-Capable Cellular Networks, Computer Science Department, Carleton University, Ottawa, Canada, March, 2008.

Ohio Voting Systems Integrity: The EVEREST Report, Case-Western Reserve University, Cleveland, OH, February, 2007.

Ohio Voting Systems Integrity: The EVEREST Report, Ohio State University, Columbus, OH, February, 2007.

Ohio Voting Systems Integrity: The EVEREST Report, Ohio University, Athens, OH, February, 2007.

Ohio Voting Systems Integrity: The EVEREST Report, Miami University, Ohio, Oxford, OH, February, 2007.

Ohio Voting Systems Integrity: The EVEREST Report, Bowling Green State University, Bowling Green, OH, February, 2007.

Vulnerabilities and Opportunities in SMS-Capable Cellular Networks, Computer Science Department, Indiana University of Pennsylvania, Indiana, PA, September, 2007.

Asymmetry in Performance and Security Requirements for I/O in High-End Computing, HECIWG FSIO 2007 Workshop, NSF, Arlington, VA, August, 2007.

Toward Valley-Free Interdomain Routing, IEEE International Conference on Communications (ICC) 2007, Glasgow, Scotland, June, 2007.

Extending Developer Tools for Security-Typed Languages, Software Engineering Research Center FallShowcase, West Lafayette, IN, June, 2007.

Open Functionality in SMS/Cellular Networks, Computer and Information Science, University ofOregon, Eugene, OR, May, 2007.

Open Functionality in SMS/Cellular Networks, Computer Security Symposium, St. Cloud State University, St. Cloud, MN, May, 2007.

Authentication and Web Security, Security and Privacy in IT-EMTM 604 Guest Lecture,University of Pennsylvania, Philadelphia, PA, April, 2007.

Grains of SANs: Building Storage Area Networks from Memory Spots, CISCO Remote Faculty Seminar, University Park, PA, April, 2007.

Grains of SANs: Building Storage Area Networks from Memory Spots, 2007 IEEE Security and Privacy Crystal Ball Workshop, Hawthorne, NY, January, 2007.

Keynote, *Password Exhaustion: Predicting the End of Password Usefulness*, 2nd International Conference on Information Systems Security , Kolkata, India, December, 2006.

Privacy Preserving Web-based Email, 2nd International Conference on Information Systems Security, Kolkata, India, December, 2006.

Keynote, *Physical and Digital Convergence: Where the Internet is the Enemy*, Eighth International Conference on Information and Communications Security (ICICS '06), Raleigh, NC, December, 2006.

Extending Developer Tools for Security-Typed Languages, Software Engineering Research Center FallShowcase, Muncie, IN, November, 2006.

Open Functionality in SMS/Cellular Networks, Johns Hopkins University, Computer Science Department, Baltimore, MD, September, 2006.

Open Functionality in SMS/Cellular Networks, George Mason University, Computer Science Department, Fairfax, VA, September, 2006.

Exploiting Open Functionality in SMS-Capable Cellular Networks, Motorola Security Symposium, Itasca, Il, September, 2006.

lseb: Testing Large Scale BGP Security in ReplayableNetwork Environments, NSF/DETER Community Workshop, Arlington, VA, June, 2006.

BGPRV: A Library for Fast and Efficient Routing DataManipulation, NSF/DETER Community Workshop, Arlington, VA, June, 2006.

JifClipse: Extending Developer Tools for Security-TypedLanguages, Software Engineering Research Center SpringShowcase, Shaumburg, IL, June, 2006.

Trends in Security: Critical Engineering in the Large, Schlumberger InnovateIT! 2006, Cambridge, MA, May, 2006.

Information Flow Revisited: Software Engineering toProvable Security, Network Center of Excellence, Motorola Labs, Shaumburg, IL, May, 2006.

Authentication and Web Security, Security and Privacy in IT-EMTM 604 Guest Lecture,University of Pennsylvania, Philadelphia, PA, April, 2006.

Exploiting Open Functionality in SMS-Capable Cellular Networks, InfraGard Pittsburgh Chapter General Meeting, Pittsburgh, PA, March, 2006.

Distinguished Lecture, *Exploiting Open Functionality in SMS-Capable Cellular Networks*, Computer Science Department, University of Virginia, Charlottesville, VA, January, 2006.

Software Engineering Tools for Security-Typed Languages:Using Eclipse to Make Secure Programming Practical, Software Engineering Research Center Showcase, Muncie, IN, November, 2005.

Exploiting Open Functionality in SMS-Capable Cellular Networks, AT&T IP Services Security Council, Middletown, NJ, October, 2005.

Exploiting Open Functionality in SMS-Capable Cellular Networks, Computer Science Department, Carnegie Mellon University, Pittsburgh, PA, October, 2005.

Exploiting Open Functionality in SMS-Capable Cellular Networks, Computer Science Department, Yale University, New Haven, CT, October, 2005.

Exploiting Open Functionality in SMS-Capable Cellular Networks, Computer Science Department, SUNY-Stony Brook, Stony Brook, NY, October, 2005.

Exploiting Open Functionality in SMS-Capable Cellular Networks, Networking and Security Research Center, ComputerScience and Engineering, Pennsylvania State University, State College, PA, October, 2005.

lseb: Trace Driven Modeling of Internet-Scale BGP Attacksand Countermeasures, 2nd Annual DETER/EMIST Workshop, Newport Beach, CA, September, 2005.

Critical Infrastructure Security through Provably SecureNetwork Mediation, 2nd Japan/US Workshop on Critical InformationInfrastructure Protection (CIIP), Tokyo, Japan, June, 2005.

Extending Developer Tools for Security-typed Languages, Software Engineering Research Center Showcase, West Lafayette, IN, June, 2005.

Origin Authentication in Interdomain Routing, 2005 IEEE Communications Quality and Reliability (CQR)International Workshop, St. Petersburg, FL, April, 2005.

Analysis of Security Vulnerabilities in the MovieProduction and Distribution Process, Messiah College, Senior Seminar Series, Grantham, PA, April, 2005.

Origin Authentication in Interdomain Routing, Intel Research, Folsom CA, April, 2005.

Key Distribution Strategies For Low-Power Wireless Networks, Network Center of Excellence, Motorola Labs, Shaumburg, IL, April, 2005.

Policy Evolution: Autonomic Environmental Security, Software Engineering Research Center Showcase, Muncie, IN, December, 2004.

Information Assurance for Enterprise Networks, BAE Systems, Networking Seminar, Reston, VA, November, 2004.

Origin Authentication in Interdomain Routing, Computer Science Department, Purdue University, West Lafayette, IN, October, 2004.

Origin Authentication in Interdomain Routing, Electrical Engineering and Computer ScienceDepartment, University of Michigan, Ann Arbor, MI, October, 2004.

Origin Authentication in Interdomain Routing, Computer Science Department, University ofWisconsin, Madison, MD, September, 2004.

Analysis of Security Vulnerabilities in the MovieProduction and Distribution Process, Computer Science and Engineering Student Organization, University Park, PA, September, 2004.

Useless Metaphors? Why Specifying Policy is So Hard, Workshop on Usable Privacy and Security Software,Center for Discrete Mathematics and Theoretical Computer Science(DIMACS), New Brunswick, New Jersey, July, 2004.

Analysis of Security Vulnerabilities in the MovieProduction and Distribution Process, Information Systems Research Seminar, Stern School ofBusiness, New York University, New York, NY, April, 2004.

Analysis of Security Vulnerabilities in the MovieProduction and Distribution Process, Ball State University, Muncie, IN, April, 2004.

Origin Authentication in Interdomain Routing, Computer Science Department, University of Illinois, Champaign, IL, March, 2004.

Origin Authentication in Interdomain Routing, Computer Science and Engineering Department,University of Minnesota, Minneapolis, MN, March, 2004.

Origin Authentication in Interdomain Routing, Computer Science Department, Johns Hopkins University, Baltimore, MD, March, 2004.

Origin Authentication in Interdomain Routing, Department of Computer Science, University ofMassachusetts - Amherst, Amherst, MA, March, 2004.

Origin Authentication in Interdomain Routing, Computer Science and Engineering Department, PennState University, University Park, PA, March, 2004.

Origin Authentication in Interdomain Routing, School of Electrical Engineering and ComputerScience, Oregon State University, Corvallis, OR, February, 2004.

Origin Authentication in Interdomain Routing, Computer Science Department, NorthwesternUniversity, Evanston, IL, February, 2004.

Origin Authentication in Interdomain Routing, Computer Science Department, SUNY-Stony Brook, Stony Brook, NY, February, 2004.

Attack Profiling and Simulation in Interdomain Routing, P2INGS Quarterly Meeting, Tempe, AZ, February, 2004.

Analysis of Security Vulnerabilities in the MovieProduction and Distribution Process, AT&T Finance Lunch, Morristown, NJ, January, 2004.

Origin Authentication in Interdomain Routing, AT&T IP Security Conference, Middletown, NJ, November, 2003.

Origin Authentication in Interdomain Routing, 10th ACM Conference on Computer and CommunicationsSecurity (CCS), Washington, DC, October, 2003.

Origin Authentication in Interdomain Routing, Computer Science Department, Stevens Institute ofTechnology, Hoboken, NJ, October, 2003.

Origin Authentication in Interdomain Routing, Computer Science Department, Arizona State University, Mesa, AZ, September, 2003.

Analysis of Security Vulnerabilities in the MovieProduction and Distribution Process, 31st Technology Policy Research Conference (TPRC), Arlington, VA, September, 2003.

On Context in Authorization Policy, 8th ACM Symposium on Access Control Models andTechnologies, Como, Italy, June, 2003.

The Antigone Project, DARPA Principal Investigator Meeting, San Antonio, TX, January, 2003.

Methods and Limitations of Security Policy Reconciliation, 2002 IEEE Symposium on Security and Privacy, Oakland, CA, May, 2002.

Policy Management in Distributed Systems, Cigital, Washington, DC, April, 2002.

Antigone: Policy Management in Secure Group Communication, School of Computer Science, Carnegie Mellon University, Pittsburgh, PA, April, 2001.

Antigone: Policy Management in Secure Group Communication, Computer Science Department, University of Wisconsin, Madison, MD, April, 2001.

Antigone: Policy Management in Secure Group Communication, Computer Science Department, University of Maryland, College Park, MD, April, 2001.

Antigone: Policy Management in Secure Group Communication, Computer Science Department, University of North Carolina, Chapel Hill, Chapel Hill, NC, April, 2001.

Antigone: Policy Management in Secure Group Communication, Computer Science Department, Johns Hopkins University, Baltimore, MD, March, 2001.

Antigone: Policy Management in Secure Group Communication, AT&T Shannon Laboratory, Florham Park, NJ, February, 2001.

Antigone: Policy Management in Secure Group Communication, Telcordia Applied Research Laboratory, Morristown, NJ, February, 2001.

Policy Problem Area 3 - Overview and Requirements, Internet Engineering Task Force MSEC BOF, San Diego, CA, December, 2000.

Multicast Security Policy Requirements and Building Blocks, Quarterly Secure Multicast Research Group Meeting (SMuG), San Diego, CA, December, 2000.

Antigone: Implementing Policy in Secure Multiparty Communication, Systems Design and Implementation (SDI) / Laboratoryfor Computer Systems (LCS) seminar series, School of ComputerScience, Carnegie Mellon University, Pittsburgh, PA, November, 2000.

Secure Group Communication in Antigone 2.0, 11th Annual IPoCSE Research Symposium, Ann Arbor, MI, October, 2000.

Antigone Secure Group Communication, Bi-Annual DARPA Visit, Software System Research Laboratory, Ann Arbor, MI, September, 2000.

Problem Area 3: Policy, Quarterly Secure Multicast Research Group Meeting (SMuG), Pittsburgh, PA, July, 2000.

Windowed Certificate Revocation, IEEE INFOCOM 2000, Tel Aviv, Israel, March, 2000.

A Response to 'Can We Eliminate Certificate Revocation Lists?', Financial Cryptography 2000, Anguilla, British West Indies, February, 2000.

Multicast Security Policy Definition, Quarterly Secure Multicast Research Group Meeting (SMuG), Washington, DC, November, 1999.

Antigone: A Flexible Framework for Secure Group Communication, Quarterly Secure Multicast Research Group Meeting (SMuG, NAI Labs, Baltimore, MD, September, 1999.

Antigone: A Flexible Framework for Secure Group Communication, 10th Annual IPoCSE Research Symposium, Ann Arbor, MI, September, 1999.

Antigone: A Flexible Framework for Secure Group Communication, 8th USENIX Security Symposium, Washington, DC, August, 1999.

Antigone: A Flexible Framework for Secure Group Communication, IBM Watson Security Seminar, Westchester County, NY, July, 1999.

Windowed Revocation in Public Key Infrastructures, Department of Electrical Engineering and ComputerScience, University of Michigan, Ann Arbor, MI, September, 1998.

Scalable Key Distribution Hierarchy, 9th Annual IPoCSE Research Symposium, Ann Arbor, MI, March, 1998.

JavaLauncher Applet Platform, NASA, Kennedy Space Center Security Seminar, Kennedy Space Center, FL, January, 1998.

Secure High Performance Group Communication, Directed StudyDefense, Department of Electrical Engineering and ComputerScience, University of Michigan, Ann Arbor, MI, September, 1997.