Patrick Drew McDaniel

William L. Weiss Professor of Information and Communications Technology
School of Electrical Engineering and Computer Science ◇ Pennsylvania State University
Office : W329 Westgate Building ◇ University Park, PA 16802 ◇ (814) 863-3599
email: mcdaniel@cse.psu.edu ◇ *Homepage*: `http://www.patrickmcdaniel.org/`

ACADEMIC AND RESEARCH APPOINTMENTS

William L. Weiss Professor of Information and Communications Technology 2017-present
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, Institute for Networking and Security Research 2016-present
College of Engineering, Pennsylvania State University, University Park, Pennsylvania

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

Program Manager, Cyber-Security Collaborative Research Alliance (CRA) 2013-2018
College of Engineering, Pennsylvania State University, University Park, Pennsylvania

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

EDUCATION

University of Michigan, Ann Arbor, MI 2001
- **Ph.D.**, Computer Science and Engineering
- Dissertation: *Policy Management in Secure Group Communication*
- Advisor: Dr. Atul Prakash

Ball State University, Muncie, IN 1991
- **M.S.**, Computer Science
- Thesis: The Analysis of D_i, a Detailed Design Metric on Large Scale Software

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

STUDENTS

Past Post-Docs

- *Vaibhav Rastogi*, graduated Northwestern University, joined
- *Robert Walls*, graduated University of Massachusetts, Amherst, joined

Past PhD Students

- *Z. Berkay Celik*, Spring 2019, now **Assistant Professor**, Purdue University
- *Nicolas Papernot*, Spring 2018, now **Assistant Professor**, University of Toronto
- *Wenhui Hu*, Fall 2016, now **Senior Member of Technical Staff**, Oracle
- *Devin Pohly*, Spring 2016, now **Assistant Professor**, Wheaton College
- *Damien Octeau*, Summer 2014, now **Software Engineer in Security**, 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 **Associate Professor**, North Carolina State University
- *Kevin Butler*, Summer 2010, now **Associate Professor**, University of Florida
- *Machigar Ongtang*, Summer 2010, now **Assistant Professor**, Dhurakij Pundit University
- *Patrick Traynor*, Spring 2008, now **Professor**, University of Florida, co-advisor
- *Fr. Boniface Hicks*, Fall 2007, now **Assistant Professor**, St. Vincent College

Current PhD Students : *Ryan Sheatsley*, Pennsylvania State University, Spring 2022 ⋄ *Bolor-Erdene Zolbayar*, Pennsylvania State University, Spring 2022

Past Masters Students : *Sushrut Shringarputale*, 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

TEACHING

- **CMPSC311 - Introduction to Systems Programming**
  Fall 2013, Fall 2014, Fall 2015, Fall 2016, Summer 2019, Spring 2020
- **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

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

AFFILIATIONS

Association for Computing Machinery (ACM), *Fellow*

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

USENIX Advanced Computing Systems Association (USENIX)

American Association for the Advancement of Science (AAAS)

HONORS, AWARDS, AND KEYNOTE ADDRESSES

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, April 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, November 2020*

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", November 2020*

J. D. Williams student paper award, Nuclear Security and Physical Protection division, *recognizing the best student papers by area in Proceedings of the Institute of Nuclear Materials Management Annual Meeting (INMM), July 2019*

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

Best Paper, 2017 EAI SECURECOMM 2018, *with Sayed M. Saghaian, Tom La Porta, Trent Jaeger and Z. Berkay Celik, August 2018*

Best Student Paper, 2017 ACM Symposium on SDN Research (SOSR), *with Stefan Achleitner, Thomas La Porta and Trent Jaeger, April 2017*

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

ACM Fellow, *for contributions to computer and mobile systems security, December 2015*

Science of Security Index of Significant Research in Cyber Security , *acknowledging paper 'Toward a Science of Secure Environments', Science of Security Virtual Organization (SOS-VO), August 2015*

IEEE Fellow, *for contributions to the security of mobile communications, November 2014*

Best Artifact Award, 20th International Symposium on the Foundations of Software Engineering (FSE), *with advisee Damien Octeau and collaborator Somesh Jha, November 2012*

Best Paper, 25th Annual Computer Security Applications Conference, *with advisees Machigar Ongtang, Stephen McLaughlin, and William Enck, December 2009*

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

Penn State Engineering Society Outstanding Research Award, *highly selective 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, March 2009*

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

Commendation for Exceptional Leadership and Achievement , *in recognition of efforts as PI of the EVEREST study, from Ohio Secretary of State Jennifer Brunner, August 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, August 2008*

National Science Foundation CAREER Award, *Faculty early career development grant, August 2007*

Penn State Computer Science and Engineering Outstanding Teaching Award, *Given to best teacher in the department as selected by students, March 2007*

ACM Certificate of Meritorious Service, *Certificate acknowledging exemplary service as associate editor of ACM Transactions on Internet Technologies, April 2007*

Best Student Paper, 22nd Annual Computer Security Applications Conference, *as advisor, with Boniface Hicks and Kiyan Ahmadizadeh, December 2006*

Best Paper, Innovations and Commercial Applications of Distributed Sensor Networks Symposia, *Awarded for best paper in conference, October 2005.*

Hartz Family Career Development Professor, *Endowed Professorship, Pennsylvania State University, Fall 2004-2007*

Bang for the Buck Award, DARPA Dynamic Coalitions Program, *Award for most feature-rich/useful software system, April 2002*

National Aeronautics and Space Administration, Kennedy Space Center Fellowship, *Research Fellowship, September 1997 - August 2000*

Electrical Engineering and Computer Science Summer Fellowship Award, *University of Michigan, June 1997*

Dean's Citation for Perfect Academic Record, *Ball State University, June 1991*

Keynote Addresses

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

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

3. 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.

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

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

6. The 25th International Conference on Computer Communication and Networks (ICCCN 2016), August, 2016, Waikoloa, Hawaii.

7. 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.

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

9. The Importance of Measurement and Decision Making to a Science of Security, 2015 IEEE Conference on Communications and Network Security (CNS), September 2015, Florence, Italy.

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

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

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

13. 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

14. 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.

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

16. Security Challenges and Solutions in Mobile Smartphone Applications, IEEE Computer Security Foundations (CSF 2011), Abbaye des Vaux de Cernay, France, June 2012.

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

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

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

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

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

5. 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.

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

7. Tracing the Arc of Smartphone Application Security. Celebrating 50 Years of Computer Science @ NC State, North Carolina State University, Raleigh, NC, October, 2017.

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

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

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

11. Tracing the Arc of Smartphone Application Security. Rochester Institute of Technology, College of Computing and Information Sciences, Rochester, NY, May 2017.

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

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

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

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

16. Six Years of Mobile Smartphone Security. Technische Universtat Darmstadt, Darmstadt Germany, July, 2015.

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

18. Security Challenges and Solutions in Mobile Smartphone Applications. Department of Software Information Systems College of Computing and Informatics, UNC Charlotte, Charlotte, NC, December, 2010.

PATENTS

U.S. Patent 8,732,293, System and method for tracking individuals on a data network using communities of interest, Patrick McDaniel, Subhabrata Sen, Oliver Spatschek, Jacobus E. Van de Merwe, May 20, 2014.

U.S. Patent 8,453,227, Reverse firewall with self-provisioning, William A. Aiello, Charles Robert Kalmanek, Jr., William J. Leighton, III, Patrick McDaniel, Subhabrata Sen, Oliver Spatscheck, Jacobus E. Van der Merwe, May 28, 2013.

U.S. Patent 7,975,044, Automated disambiguation of fixed-serverport-based applications from ephemeral applications, Oliver Spatscheck, Subhabrata Sen, Jacobus E. Van der Merwe, Patrick McDaniel, May 28, 2013.

U.S. Patent 7,873,350, End-to-end secure wireless communication for requesting a more secure channel, Patrick Drew McDaniel, Martin Joel Strauss, January 18, 2011.

RESEARCH SUPPORT

PI, *SaTC CORE: Frontier: Collaborative: End-to-End Trustworthiness of Machine-Learning Systems*, NSF (CNS), *$9,649,366* (PSU award $2,044,550), 8/15/2016-3/31/2017, 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*, 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

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

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

- *Member*–2019-present

Ohio University College of Engineering, Board of Vistors

- *Member*–2018-present

IEEE Computer Society's Technical Committee on Security and Privacy

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

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, 2010, 2011, 2012, 2014, 2015, 2016, 2017, 2018, 2019, 2020

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

IEEE European Symposium on Security and Privacy
- *Steering Committee*–2015-present
- *Program Committee*–2016, 2017

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

ACM Conference on Computer and Communications Security (CCS)
- *Program Committee*–2006, 2008, 2009, 2010, 2012, 2018, 2019, 2020, 2021
- *Industry and Government Track Chair*–2004, 2007
- *Program Committee-Industry and Government Track*–2003, 2005, 2006
- *Test of Time Committee*–2019, 2020

International Conference on Privacy, Security and Trust (PST)
- *Steering Committee*–2019-

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 Conference 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

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

International 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

MILCOM

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

The Five Nines Workshop on Designing and Managing High Availability Internet Services (INM 2007)

- *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)

Ahmed Abdou, Abbas Acar, Abbas Acar Hidayet Aksu, Stefan Achleitner, Gail-Joon Ahn, Hidayet Aksu, Alexander Alexeev, Raquel Alvarez, Alejandro Andrade Salazar, Manos Antonakakis, Ahmed Atya, Leonardo Babun, Michael Backes, Christopher Balbier, Z Berkay Celik, Z. Berkay Celik, Yohan Beugin, Dan Boneh, Thomas Bowen, Quinn Burke, Kevin Butler, Hasan Cam, Berkay Celik, Ritu Chada, Ritu Chadha, Joseph Choi, Adrien Cosson, David Dagon, Drew Davidson, Lorenzo De Carli, Kyle Denney, Matt Durbin, Matthew Durbin, Daniel E. Krych, Earlence Fernandes, Ian Goodfellow, Tristan Grieve, Kathrin Grosse, Jens Grossklags, Ting He, Diane Henshel, Blaine Hoak, Yunfeng Hong, Yongjian Hu, Rauf Izmailov, Andrew J. Grotto, Edward J. M. Colbert, Trent Jaeger, Somesh Jha, Engin Kirda, Srikanth Krishnamurthy, Padma Krishnaswamy, Amit Kumar Sikder, Alexey Kurakin, Thomas La Porta, Chun-Ming Lai, John Launchbury, Chaz Lever, Karl Levitt, Yu-Cheng Lin, Azaree Lintereur, David Lopez-Paz, Sayed M. Saghaian, Praveen Manoharan, Lisa Marvel, Yacin Nadji, Namitha

Nambiar, Iulian Neamtiu, Michael Norris, Nicolas Papernot, Yu Paul, Eric Pauley, Jonathan Petit, Giuseppe Petracca, Alexander Poylisher, Zhiyun Qian, Vaibhav Rastogi, Ahmad-Atamli Reineh, Brian Rivera, A Selcuk Uluagac, A. Selcuk Uluagac, Constantin Serban, Ryan Sheatsley, Tyler Shipp, Sushrut Shringarputale, Arunesh Sinha, Anand Sivasubramaniam, Chengyu Song, Shridatt Sugrim, Yuqiong Sun, Ananthram Swami, Gang Tan, Steve Templeton, Dave Tian, Florian Tramer, Dang Tu Nguyen, Selcuk Uluagac, Srikanth V. Krishnamurthy, Prasanna Venkatesh, Robert Walls, Xiaoyun Wang, Michael Weisman, Michael Wellman, Michael Wiesman, Felix Wu, Tian Xie, Mingli Yu, S. Zhao, Bolor-Erdene Zolbayar

CASES (Expert Witness)

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 Google Inc., United States Patent and Trademark Office, Case no. Patent No. 9,444,812.

Good Technology Corporation et al., v. AirWatch, LLC, Expert for defense, United States District Court for the Northern District of California, Case no. 5-12-cv-05827.

Inter Partes Review, Expert for Duo Security Inc., United States Patent and Trademark Office, Case no. IPR2017-01041.

Inter Partes Review, Expert for Duo Security Inc., United States Patent and Trademark Office, Case no. IPR2017-01064.

Frederick Whalen, et al., v. SEI/AARON'S, INC., Expert for defense, United States District Court for the Northern District of Georgia, Case no. 1:2014-cv-01209.

Certain Portable Electronic Communications Devices, Including Mobile Phones and Components Thereof, Expert for plaintiff, International Trade Commission.

Secure Axcess, LLC v. Bank of America Corp., et al., Expert for defense, United States District Court for the Eastern District of Texas, Tyler Division, Case no. 6-10-cv-00670.

Intellectual Ventures I LLC, v. Check Point et al., Expert for plaintiff, United States District Court for the District of Delaware, Case no. 1-10-cv-01067.

NetMonitor LLC, v. Compuware et al., Expert for plaintiff, United States District Court for the District of Delaware, Case no. 1-10-cv-01061.

Amdocs Ltd. v. Openet Telcom Ltd., Expert for defense, United States District Court for the Eastern District of Virginia, Alexandria Division, Case no. 1-10-cv-00910.

PSI Systems Inc. v. Stamps.com, Expert for defense, United States District Court for the Central District of California, Case no. 2-08-cv-05233.

Stamps.com v. Endicia, Expert for plaintiff, United States District Court for the Central District of California, Case no. 2-06-cv-07499.

Kara Technologies v. Stamps.com, Expert for defense, United States District Court for the Central District of California, Case no. 2-05-cv-01890.

Coinstar Inc. v. Coinxchange, Expert for defense, United States District Court for the Eastern District of Virginia, Richmond Division, Case no. 3-06-cv-00299.

VCode Holdings Inc. v. Stamps.com, Expert for defense, United States District Court for the Central District of California.

Inter Partes Review, Expert for Google Inc.,, United States Patent and Trademark Office, Case no. (Patent No. 8,489,868).

Inter Partes Review, Expert for Cisco Systems, Inc., , Case no. (Patent No. 7,536,598).

Vir2us v. Cisco Systems, INC and Sourcefire, LLC, Expert for defense, United States District Court for the Eastern District of Virginia, Case no. 51:16cv1095.

Zito Vault, LLC V. International Business Machines Corporation, and Softlayer Technologies, Inc., Expert for defense, , Case no. 3:16-CV-962-M.

PUBLICATIONS

Books

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

Book Chapters

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

Kevin Butler, William Enck, Patrick Traynor, Jennifer Plasterr, and Patrick McDaniel. Privacy Preserving Web-Based Email. *Algorithms, Architectures and Information Systems Security, Statistical Science and Interdisciplinary Research*, World Scientific Computing, pages 349-371. November 2008. *Editor*: Bhargab Bhattacharya, Susmita Sur-Kolay, Subhas Nandy and Aditya Bagchi. (extends iciss06b)

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

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

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

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

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

Columns

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

Patrick McDaniel, Brian Rivera, and Ananthram Swami, Toward a Science of Secure Environments. *IEEE Security & Privacy Magazine*, 12(4), July/August, 2014.

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

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

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 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.

Journal Publications

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

Mingli Yu, Tian Xie, Ting He, Patrick McDaniel, and Quinn Burke, Flow Table Security in SDN: Adversarial Reconnaissance and Intelligent Attacks. *IEEE/ACM Transactions on Networking*, 2021. (*to appear*).

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

Ryan Sheatsley, Matthew Durbin, Azaree Lintereur, and Patrick McDaniel, Improving Radioactive Material Localization by Leveraging Cyber-Security Model Optimizations. *IEEE Sensors*, 2021. (*to appear*).

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

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

Dan Boneh, Andrew J. Grotto, 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, 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, Earlence Fernandes, Eric Pauley, 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, Patrick McDaniel, Gang Tan, 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, Zhiyun Qian, Srikanth Krishnamurthy, Thomas La Porta, 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.

Daniel E. Krych and Patrick McDaniel, Exposing Android Social Applications: Linking Data Leakage to Privacy Policies. *Journal of Cyber Security Technology*, Taylor & Francis, 2019.

Ian Goodfellow, Patrick McDaniel, and Nicolas Papernot, Making machine learning robust against adversarial inputs. *Communications of the ACM*, ACM, 61(7):56-66, June/July, 2018.

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

Stefan Achleitner, Thomas La Porta, Patrick McDaniel, Shridatt Sugrim, Srikanth 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, Robert Walls, Yacin Nadji, David Dagon, 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 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, Daniel Luchaup, 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.

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

Zhenfu Cao, Keqiu Li, Xu Li, Patrick McDaniel, Radha Poovendran, 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):279-282, 2014.

William Enck, Peter Gilbert, Seungyeop Han, Vasant Tendulkar, Byung-Gon Chun, Landon Cox, Jaeyeon Jung, 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. (extends egc+10)

William Enck, Peter Gilbert, Byung-Gon Chun, Landon P. Cox, Jaeyeon Jung, Patrick McDaniel, and Anmol N. 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, Stephen McLaughlin, William Enck, and Patrick McDaniel, Semantically Rich Application-Centric Security in Android. *Security and Communication Networks*, 5(6):658-673, 2012.

Thomas Moyer, Kevin Butler, Joshua Schiffman, Patrick McDaniel, and Trent Jaeger, Scalable Web Content Attestation. *IEEE Transactions on Computers*, 61(5):686–699, April, 2011. (extends mbs+09)

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

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

Patrick Traynor, Chaitrali Amrutkar, Vikhyath Rao, Trent Jaeger, 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, Kevin Butler, William Enck, 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, Patrick Traynor, Patrick McDaniel, and Brent Waters, Secure Attribute-Based Systems. *Journal of Computer Security (JCS)*, 18(5):799–837, 2010. (extends ptmw06)

Boniface Hicks, Sandra Rueda, Luke St. Clair, Trent Jaeger, and Patrick McDaniel, A Logical Specification and Analysis for SELinux MLS Policy. *ACM Transactions on Information and System Security (TISSEC)*, 13(26), 2010. (extends hrs+07)

Kevin Butler, Toni Farley, 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, Sunam Ryu, 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. (extends rbtm07)

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

William Enck, Thomas Moyer, Patrick McDaniel, Shubho Sen, Panagiotis Sebos, Sylke Spoerel, Albert Greenberg, Yu-Wei Sung, 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. (extends ems+07)

Heesook Choi, William Enck, Jaesheung Shin, 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. (extends ces+05)

Patrick Traynor, William Enck, Patrick McDaniel, and Thomas La Porta, Exploiting Open Functionality in SMS-Capable Cellular Networks. *Journal of Computer Security*, 16(6):713-742, Febraury, 2009. (extends etml05)

Patrick Traynor, Michael Chien, Scott Weaver, Boniface Hicks, and Patrick McDaniel, Non-Invasive Methods for Host Certification. *ACM Transactions on Information and System Security (TISSEC)*, 11(3), 2008. (extends tcw+06)

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, William Enck, and Patrick McDaniel, TARP: Ticket-based Address Resolution Protocol. *Computer Networks*, Elsevier, 51(15):4322–4337, October, 2007. (extends lem05)

Patrick McDaniel and Avi Rubin, *Guest Editoral: 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. (extends mp02)

Patrick McDaniel, William Aiello, Kevin Butler, and John Ioannidis, Origin Authentication in Interdomain Routing. *Journal of Communication Networks*, Elsevier, 50(16):2953-2980, November, 2006. (extends aim03)

Matthew Pirretti, Sencun Zhu, Vijaykrishnan Narayanan, Patrick McDaniel, Mahmut Kandemir, and Richard Brooks, The Sleep Deprivation Attack in Sensor Networks: Analysis and Methods of Defense. *International Journal of Distributed Sensor Networks*, 2(3):267-287, June, 2005. (extends pzn+05)

Simon Byers, Lorrie Cranor, Eric Cronin, Dave Kormann, and Patrick McDaniel, Analysis of Security Vulnerabilities in the Movie Production and Distribution Process. *Telecommunications Policy*, 28(8):619-644, August, 2004. (extends bcc+03)

Conference Publications

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

Ryan Sheatsley, Blaine Hoak, Eric Pauley, Yohan Beugin, Michael Wiesman, 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, Ting He, Patrick McDaniel, and Namitha Nambiar. Attack Resilience of Cache Replacement Policies. *IEEE International Conference on Computer Communications (INFOCOM)*, IEEE, May 2021.

Adrien Cosson, Amit Kumar Sikder, Leonardo Babun, Z. Berkay Celik, 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.

Sayed M. Saghaian, Thomas La Porta, and Simone Silvestri 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, Patrick McDaniel, Thomas La Porta, 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, Leonardo Babun, Z. Berkay Celik, Abbas Acar Hidayet Aksu, Patrick McDaniel, 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, Ting He, Patrick McDaniel, and Quinn Burke. Flow Table Security in SDN: Adversarial Reconnaissance and Intelligent Attacks. *IEEE INFOCOM*, IEEE Conference on Computer Communications 2020. Beijing, China.

Michael Norris, Z. Berkay Celik, Prasanna Venkatesh, S. Zhao, Patrick McDaniel, 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.

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

Matt Durbin, Ryan Sheatsley, Christopher Balbier, Tristan Grieve, 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, Abbas Acar, Hidayet Aksu, Abbas Acar, Ryan Sheatsley, A. 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, 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, Chengyu Song, Zhiyun Qian, Srikanth V. Krishnamurthy, 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, Leonardo Babun, Amit Kumar Sikder, Hidayet Aksu, Gang Tan, Patrick McDaniel, and A. Selcuk Uluagac. Sensitive Information Tracking in Commodity IoT. *Proceedings of the 27th USENIX Security Symposium*, August 2018. Baltimore, MD.

Rauf Izmailov, Shridatt Sugrim, Ritu Chadha, 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, Thomas La Porta, Trent Jaeger, Z. Berkay Celik, and Patrick McDaniel. Mission-oriented

Security Model, Incorporating Security Risk, Cost and Payout. *Proceedings of EAI SECURECOMM 2018*, August 2018. (**best paper award**).

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

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

Nicolas Papernot, Patrick McDaniel, 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, Xiaoyun Wang, Yunfeng Hong, Yu-Cheng Lin, Felix Wu , 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, Nicolas Papernot, Praveen Manoharan, 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, David Lopez-Paz, and Patrick McDaniel. Patient-Driven Privacy Control through Generalized Distillation. *Proceedings of the Privacy-Aware Computing (PAC)*, IEEE 2017.

Abbas Acar, Z. Berkay Celik, Hidayet Aksu, A. 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, Drew Davidson, Lorenzo De Carli, 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. (acceptance rate=24%)

Yunfeng Hong, Yongjian Hu, Chun-Ming Lai, Felix Wu, Iulian Neamtiu, Yu Paul, Patrick McDaniel, 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, Patrick McDaniel, Ian Goodfellow, Somesh Jha, 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. (acceptance rate=209%)

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

Ahmed Atya, Zhiyun Qian, Srikanth V. Krishnamurthy, Thomas La Porta, Patrick McDaniel, and Lisa Marvel. Stealth Migration: Hiding Virtual Machines on the Network. *IEEE International Conference on Computer Communications (INFOCOM)*, IEEE 2017.

Stefan Achleitner, Thomas La Porta, Patrick McDaniel, Srikanth V. Krishnamurthy, Alexander Poylisher, and Constantin Serban. Malicious Co-Residency on the Cloud: Attacks and Defense. *IEEE International Conference on Computer Communications (INFOCOM)*, IEEE 2017.

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

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

IEEE 2016.

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

Devin J. 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, Robert Walls, Yacin Nadji, David Dagon, 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, Michael Backes, Sven Bugiel, Sascha Fahl, 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, Patrick McDaniel, Xi Wu, 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, Scott Brown, 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, Patrick McDaniel, Somesh Jha, Matt Fredrikson, 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, Somesh Jha, Matthew Dering, Patrick McDaniel, Alexandre Bartel, Li Li, 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 J. Pohly and Patrick McDaniel. MICSS: A Realistic Multichannel Secrecy Protocol. *IEEE Global Communications Conference (GLOBECOM)*, December 2015. San Diego, CA.

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

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

Berkay Celik, Robert Walls, 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, 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, Ahmed Atya, Trent Jaeger, Srikanth Krishnamurthy, Karl Levitt, Patrick McDaniel, 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, Stephen Lange-Maney, 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, Daniel Luchaup, Matthew Dering, 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, Alexandre Bartel, Tegawende Bissyande, Jacques Klein, Yves Le Traon, Steven Arzt, Siegfried Rasthofer,

Eric Bodden, 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.

Jing Tian, Kevin Butler, 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, Lorrie Cranor, 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, Damien Octeau, 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, Siegfried Rasthofer, Christian Fritz, Eric Bodden, Alexandre Bartel, Jacques Klein, Yves Le Traon, 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.

Phillip Koshy, 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, Barbados.

Stephen McLaughlin, Devin Pohly, 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, Patrick McDaniel, Somesh Jha, Alexandre Bartel, Eric Bodden, 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. (acceptance rate=16.2%)

Devin J. Pohly, Stephen McLaughlin, 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. (acceptance rate=18.9%)

Weining Yang, Ninghui Li, Yuan Qi, Wahbeh Qardaji, Stephen McLaughlin, and Patrick McDaniel. Minimizing Private Data Disclosures in the Smart Grid. *19th ACM Conference on Computer and Communications Security (CCS)*, October 2012. (acceptance rate=18.9%)

Eun Kyoung Kim, 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. (acceptance rate=30%)

Damien Octeau, 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 award**). (acceptance rate=17.4%)

Thomas Moyer, 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.* (extends mdd+10)

Stephen McLaughlin, 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. (acceptance rate=13.9%)

William Enck, Damien Octeau, Patrick McDaniel, and Swarat Chaudhuri. A Study of Android Application Security. *Proceedings of the 20th USENIX Security Symposium*, August 2011. San Francisco, CA. (acceptance rate=17.2%)

Kevin Butler, 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. (acceptance rate=16.3%)

Stephen McLaughlin, Dmitry Podkuiko, Adam Delozier, 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. (acceptance rate=16.3%)

Machigar Ongtang, 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. (acceptance rate=16.3%)

Patrick Traynor, Joshua Schiffman, Thomas La Porta, Patrick McDaniel, Abhrajit Ghosh, and Farooq Anjum. Constructing Secure Localization Systems with Adjustable Granularity. *IEEE Global Communications Conference (GLOBECOM)*, December 2010. Miami, FL. (acceptance rate=36%)

William Enck, Peter Gilbert, Byung-gon Chun, Landon P. Cox, Jaeyeon Jung, Patrick McDaniel, and Anmol N. 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. (acceptance rate=16.1%)

Toby Ehrenkranz, 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. (acceptance rate=25%)

Boniface Hicks, Sandra Rueda, David King, Thomas Moyer, Joshua Schiffman, Yogesh Sreenivasan, 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)*, pages 163-172, June 2010. Pittsburgh, PA.

Kevin Butler, Stephen McLaughlin, and Patrick McDaniel. Disk-Enabled Authenticated Encryption. *Proceedings of the 26th IEEE Symposium on Massive Storage Systems and Technologies (MSST)*, May 2010. (acceptance rate=45.5%)

Machigar Ongtang, Stephen McLaughlin, William Enck, and Patrick McDaniel. Semantically Rich Application-Centric Security in Android. *Proceedings of the 25th Annual Computer Security Applications Conference (ACSAC)*, pages 340-349, December 2009. Honolulu, Hawaii. (**best paper**). (acceptance rate=19.0%)

Thomas Moyer, Kevin Butler, Joshua Schiffman, Patrick McDaniel, and Trent Jaeger. Scalable Asynchronous Web Content Attestation. *Proceedings of the 25th Annual Computer Security Applications Conference (ACSAC)*, pages 95-104, December 2009. Honolulu, Hawaii. (acceptance rate=19.0%)

Joshua Schiffman, Thomas Moyer, Christopher Shal, Trent Jaeger, and Patrick McDaniel. Justifying Integrity Using a Virtual Machine Verifier. *Proceedings of the 25th Annual Computer Security Applications Conference (ACSAC)*, pages 83-92, December 2009. Honolulu, Hawaii. (acceptance rate=19.0%)

William Enck, Machigar Ongtang, and Patrick McDaniel. On Lightweight Mobile Phone App Certification. *Proceedings of the 16th ACM Conference on Computer and Communications Security (CCS)*, pages 235-245, November 2009. (acceptance rate=18.4%)

Patrick Traynor, Michael Lin, Machigar Ongtang, Vikhyath Rao, Trent Jaeger, 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)*, pages 223-234, November 2009. (acceptance rate=18.4%)

William Enck, Patrick McDaniel, and Trent Jaeger. PinUP: Pinning User Files to Known Applications. *Proceedings of the 24th Annual Computer Security Applications Conference (ACSAC)*, December 2008. (acceptance rate=24.3%)

William Enck, Kevin Butler, Thomas Richardson, Patrick McDaniel, and Adam Smith. Defending Against Attacks on Main Memory Persistence. *Proceedings of the 24th Annual Computer Security Applications Conference (ACSAC)*, December 2008. (acceptance rate=24.3%)

Kevin Butler, Stephen McLaughlin, and Patrick McDaniel. Rootkit-Resistant Disks. *Proceedings of the 15th ACM Conference on Computer and Communications Security (CCS)*, November 2008. Alexandria, VA. (acceptance rate=18.1%%)

Patrick Traynor, Kevin Butler, 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. (acceptance rate=17.7%%)

Luke St. Clair, Joshua Schiffman, Trent Jaeger, and Patrick McDaniel. Establishing and Sustaining System Integrity via Root of Trust Installation. *23rd Annual Computer Security Applications Conference (ACSAC)*, pages 19-29, December 2007. Miami, FL. (acceptance rate=21.9%)

Boniface Hicks, Tim Misiak, and Patrick McDaniel. Channels: Runtime System Infrastructure for Security-typed Languages. *23rd Annual Computer Security Applications Conference (ACSAC)*, pages 443-452, December 2007. Miami, FL. (acceptance rate=21.9%)

Dhananjay Bapat, Kevin Butler, and Patrick McDaniel. Towards Automated Privilege Separation. *Proceedings of 2nd International Conference on Information Systems Security (short paper)*, December 2007. Delhi, India. (acceptance rate=31.5%)

Lisa Johansen, Kevin Butler, Michael Rowell, and Patrick McDaniel. Email Communities of Interest. *Fourth Conference on Email and Anti-Spam (CEAS 2007)*, August 2007. Mountain View, California. (acceptance rate=18.9%)

Patrick Traynor, Patrick McDaniel, and Thomas La Porta. On Attack Causality in Internet-Connected Cellular Networks. *Proceedings of the 16th USENIX Security Symposium*, pages 1–16, August 2007. Boston, MA. (acceptance rate=12.28%)

Boniface Hicks, Sandra Rueda, 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. (acceptance rate=23.8%)

William Enck, Patrick McDaniel, Shubho Sen, Panagiotis Sebos, Sylke Spoerel, Albert Greenberg, 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. (acceptance rate=23.8%)

Boniface Hicks, Sandra Rueda, Luke St. Clair, Trent Jaeger, and Patrick McDaniel. A Logical Specification and Analysis for SELinux MLS. *12th ACM Symposium on Access Control Models and Technologies (SACMAT)*, ACM, June 2007. Sophia Antipolis, France. (acceptance rate=23.75%)

Anusha Sriraman, Kevin Butler, Patrick McDaniel, and Padma Raghavan. Analysis of IPv4 Address Space Delegation Structure. *12th IEEE Symposium on Computers and Communications (ISCC)*, July 2007. Aveiro, Portugal. (acceptance rate=40%)

Heesook Choi, Thomas La Porta, and Patrick McDaniel. Privacy Preserving Communication in MANETs. *Proceedings of Fourth Annual IEEE Communications Society Conference on Sensor, Mesh, and Ad Hoc Communications and Networks (SECON 07)*, June 2007. San Diego, CA. (acceptance rate=20%)

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

Sunam Ryu, Kevin Butler, Patrick Traynor, and Patrick McDaniel. Leveraging Identity-based Cryptography for Node ID Assignment in Structured P2P Systems. *Proceedings of the 3rd IEEE International Symposium on Security in Networks and Distributed Systems (SSNDS-07)*, June 2007. Niagra Falls, Canada. (acceptance rate=40%)

Hosam Rowaihy, William Enck, Patrick McDaniel, and Thomas La Porta. Limiting Sybil Attacks in Structured Peer-to-Peer Networks. *Proceedings of IEEE INFOCOM 2007 MiniSymposium*, May 2007. Anchorage, AK. (acceptance rate=25%)

Boniface Hicks, Kiyan Ahmadizadeh, and Patrick McDaniel. Understanding Practical Application Development in Security-Typed Languages. *22st Annual Computer Security Applications Conference (ACSAC)*, pages 153–164, December 2006. Miami, Fl. (**best student paper**). (acceptance rate=30.3%)

Luke St. Clair, Lisa Johansen, William Enck, Matthew Pirretti, Patrick Traynor, Patrick McDaniel, and Trent Jaeger. Password Exhaustion: Predicting the End of Password Usefulness. *Proceedings of 2nd International Conference on Information Systems Security (ICISS)*, pages 37–55, December 2006. Kolkata, India.

Kevin Butler, William Enck, Jennifer Plasterr, Patrick Traynor, and Patrick McDaniel. Privacy-Preserving Web-Based Email. *Proceedings of 2nd International Conference on Information Systems Security (ICISS)*, pages 116–131, December 2006. Kolkata, India. (acceptance rate=30.4%)

Matthew Pirretti, Patrick Traynor, Patrick McDaniel, and Brent Waters. Secure Attribute-Based Systems. *Proceedings of the 13th ACM Conference on Computer and Communications Security (CCS)*, pages 99-112, November 2006. Alexandria, VA. (acceptance rate=14.7%)

Kevin Butler, William Aiello, and Patrick McDaniel. Optimizing BGP Security by Exploiting Path Stability. *Proceedings of the 13th ACM Conference on Computer and Communications Security (CCS)*, pages 298-310, November 2006. Alexandria, VA. (acceptance rate=14.7%)

Patrick Traynor, William Enck, Patrick McDaniel, and Thomas La Porta. Mitigating Attacks on Open Functionality in SMS-Capable Cellular Networks. *Proceedings of the Twelfth Annual International Conference on Mobile Computing and Networking (MobiCom)*, pages 182-193, September 2006. Los Angeles, CA. (acceptance rate=11.7%)

Patrick Traynor, Michael Chien, Scott Weaver, Boniface Hicks, and Patrick McDaniel. Non-Invasive Methods for Host Certification. *Proceedings of the Second IEEE Communications Society/CreateNet International Conference on Security and Privacy in Communication Networks (SecureComm)*, August 2006. Baltimore, MD. (acceptance rate=25.4%)

Sophie Qiu, Patrick McDaniel, Fabian Monrose, and Avi Rubin. Characterizing Address Use Structure and Stability of Origin Advertisement in Interdomain Routing. *11th IEEE Symposium on Computers and Communications*, pages 489-496, June 2006. Pula-Cagliari, Sardinia, Italy. (acceptance rate=49.4%)

Patrick McDaniel, Shubho Sen, Oliver Spatscheck, Jacobus Van der Merwe, William Aiello, and Charles Kalmanek. Enterprise Security: A Community of Interest Based Approach. *Proceedings of Network and Distributed Systems Security 2006 (NDSS)*, February 2006. San Diego, CA. (acceptance rate=13.6%)

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

Wesam Lootah, William Enck, and Patrick McDaniel. TARP: Ticket-Based Address Resolution Protocol. *21st Annual Computer Security Applications Conference (ACSAC)*, pages 95-103, December 2005. Tuscon, AZ. (acceptance rate=19.2%)

William Enck, Patrick Traynor, Patrick McDaniel, and Thomas La Porta. Exploiting Open Functionality in SMS-Capable Cellular Networks. *Proceedings of the 12th ACM Conference on Computer and Communications Security (CCS)*, pages 393–404, November 2005. Alexandria, VA. (acceptance rate=15.0%)

Matthew Pirretti, Sencun Zhu, Vijaykrishnan Narayanan, Patrick McDaniel, 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 Symposia*, October 2005. Bethesda, Maryland. (**best paper**). (acceptance rate=27.2%)

Louis Kruger, Somesh Jha, and Patrick McDaniel. Privacy Preserving Clustering. *10th European Symposium on Research in Computer Security (ESORICS '05)*, September 2005. Milan, Italy. (acceptance rate=16.4%)

Heesook Choi, William Enck, Jaesheung Shin, Patrick McDaniel, and Thomas La Porta. Secure Reporting of Traffic Forwarding Activity in Mobile Ad Hoc Networks. *MobiQuitous 2005*, July 2005. San Diego, CA. (acceptance rate=35%)

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

William Aiello, John Ioannidis, and Patrick McDaniel. Origin Authentication in Interdomain Routing. *Proceedings of 10th ACM Conference on Computer and Communications Security (CCS)*, ACM, pages 165-178, October 2003. Washington, DC. (acceptance rate=13.8%)

Eric Cronin, Sugih Jamin, Tal Malkin, and Patrick McDaniel. On the Performance, Feasibility, and Use of Forward Secure Signatures. *Proceedings of 10th ACM Conference on Computer and Communications Security (CCS)*, ACM, pages 131-144, October 2003. Washington, DC. (acceptance rate=13.8%)

Patrick McDaniel. On Context in Authorization Policy. *8th ACM Symposium on Access Control Models and Technologies (SACMAT)*, ACM, pages 80-89, June 2003. Como, Italy. (acceptance rate=37.0%)

Geoff Goodell, William Aiello, Tim Griffin, John Ioannidis, Patrick McDaniel, and Avi Rubin. Working Around BGP: An Incremental Approach to Improving Security and Accuracy of Interdomain Routing. *Proceedings of Network and Distributed Systems Security 2003 (NDSS)*, Internet Society, pages 75-85, February 2003. San Diego, CA. (acceptance rate=20.5%)

Patrick McDaniel and Atul Prakash. Methods and Limitations of Security Policy Reconciliation. *2002 IEEE Symposium on Security and Privacy*, IEEE Computer Society Press, pages 73-87, May 2002. Oakland, CA. (acceptance rate=17.8%)

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

Hugh Harney, Andrea Colegrove, and Patrick McDaniel. Principles of Policy in Secure Groups. *Proceedings of Network and Distributed Systems Security 2001 (NDSS)*, Internet Society, pages 125-135, February 2001. San Diego, CA. (acceptance rate=24.2%)

Patrick McDaniel and Sugih Jamin. Windowed Certificate Revocation. *Proceedings of IEEE INFOCOM 2000*, IEEE, pages 1406-1414, March 2000. Tel Aviv, Israel. (acceptance rate=26%)

Patrick McDaniel and Avi Rubin. A Response to 'Can We Eliminate Certificate Revocation Lists?'. *Proceedings of Financial Cryptography 2000*, International Financial Cryptography Association (IFCA), February 2000. Anguilla, British West Indies. (acceptance rate=26.1%)

Andrwe Adamson, C.J. Antonelli, Kevin Coffman, Patrick McDaniel, and Jim Rees. Secure Distributed Virtual Conferencing. *Proceedings of Communications and Multimedia Security (CMS '99)*, pages 176-190, September 1999. Katholieke Universiteit, Leuven, Belgium. (acceptance rate=70%)

Patrick McDaniel, Atul Prakash, and Peter Honeyman. Antigone: A Flexible Framework for Secure Group Communication. *Proceedings of the 8th USENIX Security Symposium*, pages 99-114, August 1999. Washington, DC. (acceptance rate=26.8%)

Workshop Publications

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

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

Berkay Celik, 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, Thomas La Porta, Patrick McDaniel, Shridatt Sugrim, Srikanth 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, Trent Jaeger, Thomas La Porta, Nicolas Papernot, Robert Walls, Alexander Kott, Lisa Marvel, Ananthram Swami, Prasant Mohapatra, 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, Thomas Moyer, Hayawardh Vijayakumar, 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, Dmitry Podkuiko, Adam Delozier, Sergei Miadzvezhanka, and Patrick McDaniel. Embedded Firmware Diversity for Smart Electric Meters. *Proceedings of the 5th Workshop on Hot Topics in Security (HotSec*

'10), August 2010. Washington, DC. (acceptance rate=19.6%)

Patrick McDaniel, Kevin Butler, Stephen McLaughlin, Radu Sion, 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, Patrick McDaniel, 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, 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.

Matt 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, William Enck, Harri Hursti, Stephen McLaughlin, Patrick Traynor, and Patrick McDaniel. Systemic Issues in the Hart InterCivic and Premier Voting Systems: Reflections Following Project EVEREST. *In Proceedings of the 3rd USENIX/ACCURATE Electronic Voting Technology Workshop (EVT '08)*, July 2008.

Kevin Butler, 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. (acceptance rate=30%)

William Enck, Sandra Rueda, Yogesh Sreenivasan, Joshua Schiffman, Luke St. Clair, Trent Jaeger, and Patrick McDaniel. Protecting Users from "Themselves". *Proceedings of the 1st ACM Computer Security Architectures Workshop*, November 2007. Alexandria, VA. (acceptance rate=30%)

Boniface Hicks, 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. (acceptance rate=39%)

Boniface Hicks, Sandra Rueda, Trent Jaeger, and Patrick McDaniel. Integration of SELinux and Security-typed Languages. *Proceedings of the 2007 Security-Enhanced Linux Workshop*, March 2007. Baltimore, MD. (acceptance rate=75%)

Sophie Qiu, Fabian Monrose, 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. (acceptance rate=40%)

Shiva Chaitanya, Kevin Butler, Patrick McDaniel, and Anand Sivasubramaniam. Design, Implementation and Evaluation of Security in iSCSI-based Network Storage Systems. *Proceedings of 2nd International Workshop on Storage Security and Survivability (StorageSS 2006)*, October 2006. Alexandria, Virginia. (acceptance rate=68.7%)

Trent Jaeger, Patrick McDaniel, Luke St. Clair, Ramon Caceres, and Reiner Sailer. Shame on Trust in Distributed Systems. *Proceedings of the First Workshop on Hot Topics in Security (HotSec '06)*, July 2006. Vancouver, B.C., Canada. (acceptance rate=19.6%)

Kevin Butler, 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 Network Environments. *Proceedings of DETER Community Workshop*, June 2006. Arlington, VA.

Boniface Hicks, David King, Patrick McDaniel, and Michael Hicks. Trusted Declassification: High-level Policy for a Security-Typed Language. *Proceedings of ACM SIGPLAN Workshop on Programming Languages and Analysis for Security*, pages 65-74, June 2006. Ottawa, Canada. (acceptance rate=58.8%)

Ali Al-Lawati, Dongwon Lee, and Patrick McDaniel. Blocking in Private Information Matching. *Proceedings of Second International ACM SIGMOD Workshop on Information Quality in Information Systems*, June 2005. Baltimore, MD. (acceptance rate=42.3%)

William Aiello, Charles Kalmanek, Patrick McDaniel, Shubho Sen, Oliver Spatscheck, and Jacobus Van der Merwe. Analysis of Communities Of Interest in Data Networks. *Passive and Active Measurement Workshop 2005*, March 2005. Boston, MA. (acceptance rate=28.5%)

Simon Byers, Lorrie Cranor, David Kormann, and Patrick McDaniel. Searching for Privacy: Design and Implementation of a P3P-Enabled Search Engine. *Proceedings of 2004 Workshop on Privacy Enhancing Technologies (PETS)*, May 2004. Toronto, Canada. (acceptance rate=28.7%)

Hao Wang, Somesh Jha, Patrick McDaniel, and Miron Livny. Security Policy Reconciliation in Distributed Computing Environments. *Proceedings of 5th International Workshop on Policies for Distributed Systems and Networks (Policy 2004)*, IEEE Computer Society Press, pages 137-146, June 2004. Yorktown Heights, NY. (acceptance rate=20.6%)

Simon Byers, Lorrie Cranor, Eric Cronin, Dave Kormann, and Patrick McDaniel. Analysis of Security Vulnerabilities in the Movie Production and Distribution Process. *Proceedings of 2003 ACM Workshop on Digital Rights Management*, ACM, October 2003. Washington, DC, also appeared in Telecommunications Policy Research Conference – September 2003. (acceptance rate=40.0%)

Patents

Patrick McDaniel and Martin Strauss, End-to-end secure wireless communication for requesting a more secure channel. U.S. Patent 7,873,350, January 2011.

Oliver Spatscheck, Subhabrata Sen, Jacobus Van der Merwe, and Patrick McDaniel, Automated disambiguation of fixed-serverport-based applications from ephemeral applications. U.S. Patent 7,875,044, July 2011.

Patrick McDaniel and Martin Strauss, End-to-end secure wireless communication for requesting a more secure channel. U.S. Patent 8,175,580, May 2012.

William Aiello, Charles Kalmanek Jr, William Leighton III, Patrick McDaniel, Subhabrata Sen, Oliver Spatscheck, and Jacobus Van der Merwe, Reverse firewall with self-provisioning. U.S. Patent 8,453,227, May 2013.

Patrick McDaniel, Subhabrata Sen, Oliver Spatscheck, and Jacobus Van der Merwe, System and method for tracking individuals on a data network using communities of interest. U.S. Patent 8,732,293, May 2014.

William Aiello, Charles Kalmanek Jr, William Leighton III, Patrick McDaniel, Subhabrata Sen, Oliver Spatscheck, and Jacobus Van der Merwe, Reverse firewall with self-provisioning. U.S. Patent 8,813,213, August 2014.

Other Publications

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 & Artificial Intelligence Subcommittee, and the Special Cyber Operations Research and Engineering Subcommittee of the National Science and Technology Council 2020.

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

Nicolas Papernot, Patrick McDaniel, Ian Goodfellow, Somesh Jha, Berkay Celik, and Ananthram Swami, Practical Black-Box Attacks against Deep Learning Systems using Adversarial Examples. *arXiv preprint arXiv:1602.02697*, 2016.

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

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

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

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

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

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

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

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

Jim Irrer, Atul Prakash, and Patrick McDaniel. Antigone: Policy-Based Secure Group Communications Systems and AMirD: Antigone-Based Secure File Mirroring System. *Proceedings of DARPA Information Survivability Conference and Exposition III, Demo Summaries*, pages 44-46, April 2003.

Patrick McDaniel and Sugih Jamin, Windowed Key Revocation in Public Key Infrastructures. *NASA Tech Briefs*, pages 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, Hugh Harney, Andrea Colegrove, Atul Prakash, and P. Dinsmore, Multicast Security Policy Requirements and Building Blocks (*Draft).* Internet Research Task Force, Secure Multicast Research Group (SMuG), November 2000.

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

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

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

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

Technical Reports

Stefan Achleitner, Quinn Burke, Patrick McDaniel, Trent Jaeger, Thomas La Porta, and Srikanth 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.

Nicolas Papernot, Ian Goodfellow, Ryan Sheatsley, Reuben Feinman, and Patrick McDaniel, cleverhans v1.0.0: an adversarial machine learning library. Technical Report arXiv:1610.00768, arXiv preprint 2016.

Devin J. 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, Patrick McDaniel, Somesh Jha, Matt Fredrikson, 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 2015.

Wenhui Hu, Damien Octeau, 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 2014.

Devin J. Pohly, Stephen McLaughlin, 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 2012.

Damien Octeau, 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, 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, Dmitry Podkuiko, Adam Delozier, 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, 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, Thomas Moyer, Hayawardh Vijayakumar, 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, 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. Updated 13 July 2010.

Joshua Schiffman, Thomas Moyer, Christopher Shal, 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 2009.

Machigar Ongtang, Stephen McLaughlin, 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 2009.

Stephen McLaughlin, 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 2009.

William Enck, 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 2009.

Patrick Traynor, Michael Lin, Machigar Ongtang, Vikhyath Rao, 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 2009.

Boniface Hicks, Sandra Rueda, Yogesh Sreenivasan, Guruprasad Jakka, David King, 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, Thomas Moyer, Christopher Shal, 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.

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

Thomas Moyer, Kevin Butler, Joshua Schiffman, 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.

Boniface Hicks, Sandra Rueda, Luke St. Clair, 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, 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, Joshua Schiffman, Thomas La Porta, Patrick McDaniel, 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, Kevin Butler, 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, 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, Sandra Rueda, Joshua Schiffman, Yogesh Sreenivasan, Luke St. Clair, 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, 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, Kevin Butler, 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, Joshua Schiffman, Trent Jaeger, and Patrick McDaniel, Establishing and Sustaining System Integrity via Root 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, 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, 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, Sandra Rueda, Trent Jaeger, and Patrick McDaniel, A Logical Specification and Analysis for SELinux MLS Policy. 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, Sandra Rueda, Trent Jaeger, and Patrick McDaniel, From Trusted to Secure: Building and Executing Applications 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, Kevin Butler, William Enck, Patrick Traynor, and Patrick McDaniel, Grains of SANs: Building Storage Area Networks from Memory 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, Vikhyath Rao, Trent Jaeger, Patrick 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, Kevin Butler, Patrick McDaniel, and Padma 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, Joshua Schiffman, Trent Jaeger, and Patrick McDaniel, Sum of the Parts: Composing Trust from Validation Primitives. Technical Report NAS-TR-0056-2006, Network and Security Research Center, Department of Computer Science and Engineering, Pennsylvania State University, University Park, PA, USA, November 2006.

Sophie Qiu, 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, Sandra Rueda, Trent Jaeger, and Patrick 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, William Enck, Patrick McDaniel, and Thomas La Porta, Mitigating Attacks on Open Functionality in SMS-Capable Networks. 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, Kevin Butler, William Enck, 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, Sandra Rueda, 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, Kevin Butler, 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, 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. (extends lem05)

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, Patrick McDaniel, Luke St. Clair, 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, Kevin Butler, 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, Kiyan Ahmadizadeh, and Patrick McDaniel, From Languages to Systems: Understanding Practical Application 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, David King, Patrick McDaniel, and Michael Hicks, Trusted Declassification: High-level policy for a security-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, Patrick Traynor, Patrick McDaniel, 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, Kevin Butler, Thomas Richardson, and Patrick 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, Lisa Johansen, William Enck, Matthew Pirretti, Patrick Traynor, Patrick McDaniel, and Trent 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, 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, Vijaykrishnan Narayanan, Patrick McDaniel, 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, Michael Chien, Scott Weaver, Boniface 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, Patrick McDaniel, Fabian Monrose, and Avi Rubin, Characterizing Address Use Structure and Stabillity of Origin 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, William Enck, Patrick McDaniel, and Thomas 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, Patrick McDaniel, and Ali Hurson, Information Flow Control in Database Security: A Case Study 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, 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, Kevin Butler, William Enck, Jennifer Plasterr, Scott Weaver, John van Bramer, and Patrick McDaniel, 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, Patrick Traynor, Patrick McDaniel, and Thomas 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, David King, and Patrick McDaniel, Declassification with Cryptographic Functions in a Security-Typed Language. Technical Report NAS-TR-0004-2005, Network and Security Center, Department of Computer Science, Pennsylvania State University, January 2005. (*updated May 2005*).

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

Kevin Butler, Toni Farley, Patrick McDaniel, and J. Rexford, A Survey of BGP Security Issues and Solutions. Technical Report TD-5UGJ33, AT&T Labs - Research, Florham Park, NJ, February 2004. (*revised June 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, Johyn Ioannidis, and Patrick McDaniel, Origin Authentication in Interdomain Routing. Technical Report TD-5QHG2G, AT&T Labs - Research, Florham Park, NJ, August 2003.

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

Simon Byers, Lorrie Cranor, Eric Cronin, Dave Kormann, and Patrick McDaniel, Analysis of Security Vulnerabilities in the Movie Production and 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 Secure Group Communication. Technical Report CSE-TR-438-00, Electrical Engineering and Computer Science, University of Michigan, December 2000.

Patrick McDaniel and Atul Prakash, Lightweight Failure Detection in Secure Group Communication. Technical Report CSE-TR-428-00, Electrical Engineering and Computer Science, University of Michigan, June 2000.

Patrick McDaniel and Atul Prakash, Antigone: Implementing Policy in Secure Group Communication. Technical Report CSE-TR-426-00, Electrical Engineering and Computer Science, University of Michigan, May 2000.

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

Patrick McDaniel, 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 Revocation Lists?". Technical Report 99.8.1, AT&T Labs - Research, Florham Park, NJ, August 1999.

Andrew Adamson, C.J. Antonelli, Kevin Coffman, Patrick McDaniel, and Jim Rees, Secure Distributed Virtual Conferencing: Multicast or Bust. 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, University of Michigan 1998.

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

Patrick McDaniel, 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, Delores Zage, Patrick McDaniel, and Irshad Khan, Evaluating Design Metrics on Large-Scale Software. Technical Report SERC-TR-106-P, Software Engineering Resource Center, Purdue University, September 1991.

PUBLIC SPEAKING

Invited Talks

The Challenges of Machine Learning in Adversarial Settings: A Systems Perspective. *CACR Security Speaker Series, Indiana University*, Online, August, 2020.

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 & 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.

Huddle with the Faculty: The Challenges of Machine Learning in Adversarial Settings. *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 & 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, 2016.

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 for Assessment 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, 2013.

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.

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

Distinguished Speaker: 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 Systems College 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, Computer Science 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, 2009.

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 Security Research 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, 2008.

Ohio Voting Systems Integrity: The EVEREST Report. *Ohio State University*, Columbus, OH, February, 2008.

Ohio Voting Systems Integrity: The EVEREST Report. *Ohio University*, Athens, OH, February, 2008.

Ohio Voting Systems Integrity: The EVEREST Report. *Miami University, Ohio*, Oxford, OH, February, 2008.

Ohio Voting Systems Integrity: The EVEREST Report. *Bowling Green State University*, Bowling Green, OH, February, 2008.

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 Fall Showcase*, West Lafayette, IN, June, 2007.

Open Functionality in SMS/Cellular Networks. *Computer and Information Science, University of Oregon*, 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 Address–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 Address–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 Fall Showcase*, 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 Replayable Network Environments. *NSF/DETER Community Workshop*, Arlington, VA, June, 2006.

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

JifClipse: Extending Developer Tools for Security-Typed Languages. *Software Engineering Research Center Spring Showcase*, Shaumburg, IL, June, 2006.

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

Information Flow Revisited: Software Engineering to Provable 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.

Exploiting Open Functionality in SMS-Capable Cellular Networks. *Distinguished Lecture, 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, Computer Science and Engineering, Pennsylvania State University*, State College, PA, October, 2005.

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

Critical Infrastructure Security through Provably Secure Network Mediation. *2nd Japan/US Workshop on Critical Information Infrastructure 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 & Reliability (CQR) International Workshop*, St. Petersburg, FL, April, 2005.

Analysis of Security Vulnerabilities in the Movie Production 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 Science Department, University of Michigan*, Ann Arbor, MI, October, 2004.

Origin Authentication in Interdomain Routing. *Computer Science Department, University of Wisconsin*, Madison, MD, September, 2004.

Analysis of Security Vulnerabilities in the Movie Production 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 Movie Production and Distribution Process. *Information Systems Research Seminar, Stern School of Business, New York University*, New York, NY, April, 2004.

Analysis of Security Vulnerabilities in the Movie Production and Distribution Process. *Ball State University*, Muncie, IN, April, 2004. Distinguished Speaker.

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 of Massachusetts - Amherst*, Amherst, MA, March, 2004.

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

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

Origin Authentication in Interdomain Routing. *Computer Science Department, Northwestern University*, 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 Movie Production 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 Communications Security (CCS)*, Washington, DC, October, 2003.

Origin Authentication in Interdomain Routing. *Computer Science Department, Stevens Institute of Technology*, 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 Movie Production 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 and Technologies*, 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) / Laboratory for Computer Systems (LCS) seminar series, School of Computer Science, 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 Computer Science, 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 Study Defense. *Department of Electrical Engineering and Computer Science, University of Michigan*, Ann Arbor, MI, September, 1997.

Tutorials

Understanding Android's Security Framework. *ACM Conference on Computer and Communications Security (CCS)*, New York, NY, October, 2008. Joint tutorial with William Enck.

Web Security. *The Thirteenth International World Wide Web Conference (WWW2004)*, New York, NY, May, 2004.

Network and Information Security. *Regional Laboratory for Network Engineering Research and Training Institute, National Science Foundation,Jackson State University*, Jackson, MS, March, 2003.