Bryan Parno

parno@cmu.edu

Collaborative Innovation Center, Office 2121
4720 Forbes Avenue
Pittsburgh, PA 15213

Research Interests

My research is primarily focused on investigating long-term, fundamental improvements in how to design and build secure systems. As a result, my work combines theory and practice to provide formal, rigorous security guarantees about concrete systems, with an emphasis on creating solid foundations for practical solutions.

Professional Appointments

Associate Professor, *Carnegie Mellon University*, Pittsburgh, PA. 1/2017 - Present
Computer Science and Electrical & Computer Engineering Departments

Researcher, *Microsoft Research*, Redmond, WA. 8/2010 - 12/2016

Education

Carnegie Mellon University, Pittsburgh, PA. 8/2004 - 5/2010
Ph.D. in Electrical and Computer Engineering
Dissertation: *Trust Extension as a Mechanism for Secure Code Execution on Commodity Computers*
Recipient of the ACM Doctoral Dissertation Award
Advisor: Adrian Perrig

Master's Degree in Electrical and Computer Engineering 6/2005
Thesis: *Distributed Detection of Node Replication Attacks in Sensor Networks*

Harvard University, Cambridge, MA. 9/2000 - 6/2004
Summa Cum Laude with a BA in Computer Science and Citation in Spanish
Phi Beta Kappa, Junior 24
Senior Thesis: *Subverting LOCKSS*

Honors

Research Highlight, Communications of the ACM, 2017.

Research Highlight, Communications of the ACM, 2016.

Best Paper Award, IEEE Symposium on Security and Privacy (**Oakland**), 2013.

Best Paper Award, USENIX Symposium on Networked Systems Design & Impl. (**NSDI**), 2013.

Best Practical Paper Award, IEEE Symposium on Security and Privacy (**Oakland**), 2012.

Forbes' 30-Under-30: Science List, 2011

ACM Doctoral Dissertation Award, 2010

A.G. Milnes Award (departmental award for the dissertation of highest quality), 2010

National Defense Science and Engineering Graduate Fellowship, 2004

National Science Foundation Graduate Fellowship, 2004

Department of Homeland Security Graduate Fellowship, 2004

John Harvard Scholarship for "Academic achievement of the highest distinction", 2002

Eagle Scout, 1998

Books & Chapters

Trust Extension as a Mechanism for Secure Code Execution on Commodity Computers.
Bryan Parno.
ACM, 2014.

Bootstrapping Trust in Modern Computers.
Bryan Parno, Jonathan M. McCune, and Adrian Perrig.
Springer, August, 2011.

Browser Enhancements for Preventing Phishing Attacks.
Bryan Parno, Cynthia Kuo, and Adrian Perrig.
In Phishing and Counter-Measures: Understanding the Increasing Problem of Electronic Identity Theft., Markus Jakobsson and Steven Myers, Ed. Wiley-Interscience, 2006.

JOURNALS

IronFleet: Proving Practical Distributed Systems Correct.
Chris Hawblitzel, Jon Howell, Manos Kapritsos, Jacob R. Lorch, Bryan Parno, Michael L. Roberts, Srinath Setty, and Brian Zill.
Communications of the ACM (**CACM**), July, 2017.
Research Highlight.

Pinocchio: Nearly Practical Verifiable Computation.
Bryan Parno, Craig Gentry, Jon Howell, and Mariana Raykova.
Communications of the ACM (**CACM**), February, 2016.
Research Highlight.

Network Adversary Attacks against Secure Encryption Schemes.
Virgil D. Gligor, Bryan Parno, and Ji Sun Shin.
IEICE Transactions on Communications, February, 2015.

Monetary Forgery in the Digital Age: Will Physical-Digital Cash Be a Solution?
Nicolas Christin, Alessandro Acquisti, Bryan Parno, and Adrian Perrig.
I/S: A Journal of Law and Policy for the Information Society, 7(2), 2012.

Trust Extension for Commodity Computers.
Bryan Parno.
Communications of the ACM (**CACM**), 55(6), June, 2012.

Defending a P2P Digital Preservation System.
Bryan Parno and Mema Rousoppoulos.
IEEE Transactions on Dependable and Secure Computing (**IEEE TDSC**), 1(4), December, 2004.

CONFERENCES

Vale: Verifying High-Performance Cryptographic Assembly Code.
Barry Bond, Chris Hawblitzel, Manos Kapritsos, K. Rustan M. Leino, Jacob R. Lorch, Bryan Parno, Ashay Rane, Srinath Setty, and Laure Thompson.
Proceedings of the **USENIX Security** Conference, August, 2017.

Hash First, Argue Later: Adaptive Verifiable Computations on Outsourced Data.
Dario Fiore, Cedric Fournet, Esha Ghosh, Markulf Kohlweiss, Olya Ohrimenko, & Bryan Parno.
Proceedings of the ACM Conference on Computer & Communications Security (**CCS**), 2016.

Cinderella: Turning Shabby X.509 Certificates into Elegant Anonymous Credentials with the Magic of Verifiable Computation.
Antoine Delignat-Lavaud, Cedric Fournet, Markulf Kohlweiss, and Bryan Parno.
Proceedings of the IEEE Symposium on Security and Privacy (**Oakland**), May, 2016.

IronFleet: Proving Practical Distributed Systems Correct.
Chris Hawblitzel, Jon Howell, Manos Kapritsos, Jacob R. Lorch, Bryan Parno, Michael L. Roberts, Srinath Setty, and Brian Zill.
Proceedings of the ACM Symposium on Operating Systems Principles (**SOSP**), October, 2015.

Geppetto: Versatile Verifiable Computation.
Craig Costello, Cedric Fournet, Jon Howell, Markulf Kohlweiss, Benjamin Kreuter, Michael Naehrig, Bryan Parno, and Samee Zahur.
Proceedings of the IEEE Symposium on Security and Privacy (**Oakland**), May, 2015.

Ironclad Apps: End-to-End Security via Automated Full-System Verification.
Chris Hawblitzel, Jon Howell, Jacob R. Lorch, Arjun Narayan, Bryan Parno, Danfeng Zhang, and Brian Zill.
Proceedings of the USENIX Symposium on Operating Systems Design and Implementation (**OSDI**), October, 2014.

Missive: Fast Application Launch From an Untrusted Buffer Cache.
Jon Howell, Jeremy Elson, Bryan Parno, and John R. Douceur.
Proceedings of the USENIX Annual Technical Conference (**ATC**), June, 2014.

CONFERENCES CONTINUED

Permacoin: Repurposing Bitcoin Work for Data Preservation.
Andrew Miller, Elaine Shi, Ari Juels, Bryan Parno, and Jonathan Katz.
Proceedings of the IEEE Symposium on Security and Privacy (**Oakland**), May, 2014.

How to Run POSIX Apps in a Minimal Picoprocess.
Jon Howell, Bryan Parno, and John R. Douceur.
Proceedings of the USENIX Annual Technical Conference (**ATC**), June, 2013.

Pinocchio: Nearly Practical Verifiable Computation.
Bryan Parno, Craig Gentry, Jon Howell, and Mariana Raykova.
Proceedings of the IEEE Symposium on Security and Privacy (**Oakland**), May, 2013.
Best Paper Award.

Quadratic Span Programs and Succinct NIZKs without PCPs.
Rosario Gennaro, Craig Gentry, Bryan Parno, and Mariana Raykova.
Proceedings of the IACR **Eurocrypt** Conference, May, 2013.

Resolving the Conflict Between Generality and Plausibility in Certified Computation.
Srinath Setty, Benjamin Braun, Victor Vu, Andrew Blumberg, Bryan Parno, and Michael Walfish.
Proceedings of the **EuroSys** Conference, April, 2013.

Embassies: Radically Refactoring the Web.
Jon Howell, Bryan Parno, and John R. Douceur.
Proceedings of the USENIX Symposium on Networked Systems Design and Implementation (**NSDI**), April, 2013.
Best Paper Award.

Shroud: Enabling Private Access to Large-Scale Data in the Data Center.
Jacob R. Lorch, Bryan Parno, James Mickens, Mariana Raykova, and Joshua Schiffman.
Proceedings of the USENIX Conference on File and Storage Technologies (**FAST**), Feb., 2013.

Lockdown: A Safe and Practical Environment for Security Applications.
Amit Vasudevan, Bryan Parno, Ning Qu, Virgil Gligor, and Adrian Perrig.
Proceedings of the Conference on Trust & Trustworthy Computing (**TRUST**), June, 2012.

User-Driven Access Control: Rethinking Permission Granting in Modern Operating Systems.
Franziska Roesner, Tadayoshi Kohno, Alexander Moshchuk, Bryan Parno, Helen J. Wang, and Crispin Cowan.
Proceedings of the IEEE Symposium on Security and Privacy (**Oakland**), May, 2012.
Best Practical Paper Award.

How to Delegate and Verify in Public: Verifiable Computation from Attribute-based Encryption.
Bryan Parno, Mariana Raykova, and Vinod Vaikuntanathan.
Proceedings of the IACR Theory of Cryptography Conference (**TCC**), March, 2012.

Memoir: Practical State Continuity for Protected Modules.
Bryan Parno, Jacob R. Lorch, John R. Douceur, James Mickens, and Jonathan M. McCune.
Proceedings of the IEEE Symposium on Security and Privacy (**Oakland**), May, 2011.

Non-Interactive Verifiable Computation: Outsourcing Computation to Untrusted Workers.
Rosario Gennaro, Craig Gentry, and Bryan Parno.
Proceedings of the IACR **CRYPTO** Conference, August, 2010.

Bootstrapping Trust in Commodity Computers.
Bryan Parno, Jonathan M. McCune, and Adrian Perrig.
Proceedings of the IEEE Symposium on Security and Privacy (**Oakland**), May, 2010.

CLAMP: Practical Prevention of Large-Scale Data Leaks.
Bryan Parno, Jonathan M. McCune, Dan Wendlandt, David G. Andersen, and Adrian Perrig.
Proceedings of the IEEE Symposium on Security and Privacy (**Oakland**), May, 2009.

CONFERENCES CONTINUED

Unidirectional Key Distribution Across Time and Space with Applications to RFID Security.
Ari Juels, Ravikanth Pappu, and Bryan Parno.
Proceedings of the **USENIX Security** Conference, July, 2008.

Flicker: An Execution Infrastructure for TCB Minimization.
Jonathan M. McCune, Bryan Parno, Adrian Perrig, Michael K. Reiter, and Hiroshi Isozaki.
Proceedings of the **EuroSys** Conference, April, 2008.

SNAPP: Stateless Network-Authenticated Path Pinning.
Bryan Parno, Adrian Perrig, and David Andersen.
Proceedings of the ACM Symposium on Information, Computer and Communications Security (**ASIACCS**), March, 2008.

How Low Can You Go?: Recommendations for Hardware-Supported Minimal TCB Code Execution.
Jonathan M. McCune, Bryan Parno, Adrian Perrig, Michael K. Reiter, and Arvind Seshadri.
Proceedings of the Conference on Architectural Support for Programming Languages and Operating Systems (**ASPLOS**), March, 2008.

Countermeasures against Government-Scale Monetary Forgery.
Alessandro Acquisti, Nicolas Christin, Bryan Parno, and Adrian Perrig.
Proceedings of the Financial Cryptography and Data Security Conference (**FC**), January, 2008.

Portcullis: Protecting Connection Setup from Denial-of-Capability Attacks.
Bryan Parno, Dan Wendlandt, Elaine Shi, Yih-Chun Hu, Bruce Maggs, and Adrian Perrig.
Proceedings of ACM **SIGCOMM**, August, 2007.

Minimal TCB Code Execution (Extended Abstract).
Jonathan M. McCune, Bryan Parno, Adrian Perrig, Michael K. Reiter, and Arvind Seshadri.
Proceedings of the IEEE Symposium on Security and Privacy (**Oakland**), May, 2007.

Secure Sensor Network Routing: A Clean-Slate Approach.
Bryan Parno, Mark Luk, Evan Gaustad, and Adrian Perrig.
Proceedings of the Conference on Future Networking Technologies (**CoNEXT**), December, 2006.

Phoolproof Phishing Prevention.
Bryan Parno, Cynthia Kuo, and Adrian Perrig.
Proceedings of the Financial Cryptography and Data Security Conference (**FC**), February, 2006.

Distributed Detection of Node Replication Attacks in Sensor Networks.
Bryan Parno, Adrian Perrig, and Virgil Gligor.
Proceedings of the IEEE Symposium on Security and Privacy (**Oakland**), May, 2005.

An Analysis of Database-Driven Mail Servers.
Nick Elprin and Bryan Parno.
Proceedings of the Large Installation Systems Administration Conference (**LISA**), October, 2003.

WORKSHOPS

Pinocchio Coin: Building Zerocoin from a Succinct Pairing-based Proof System.
George Danezis, Cedric Fournet, Markulf Kohlweiss, and Bryan Parno.
Workshop on Language Support for Privacy Enhancing Technologies, November, 2013.

Using Trustworthy Host-Based Information in the Network – **Invited Paper**.
Bryan Parno, Zongwei Zhou, and Adrian Perrig.
Proceedings of the Workshop on Scalable Trusted Computing (**STC**), October, 2012.

The Web Interface Should Be Radically Refactored.
John R. Douceur, Jon Howell, Bryan Parno, Michael Walfish, and Xi Xiong.
Proceedings of the Workshop on Hot Topics in Networks (**HotNets**), November, 2011.

Bootstrapping Trust in a "Trusted" Platform.
Bryan Parno.
Proceedings of the Workshop on Hot Topics in Security (**HotSec**), July, 2008.

Challenges in Securing Vehicular Networks.
Bryan Parno and Adrian Perrig.
Proceedings of the Workshop on Hot Topics in Networks (**HotNets**), November, 2005.

TECHNICAL REPORTS

A Note on the Unsoundness of vnTinyRAM's SNARK.
Bryan Parno.
Technical Report, ePrint Archive, Report 2015/437, May, 2015.

Memoir—Formal Specs and Correctness Proofs.
John R. Douceur, Jacob R. Lorch, Bryan Parno, James Mickens, and Jonathan M. McCune.
Technical Report MSR-TR-2011-19, February, 2011.

FANFARE for the Common Flow.
Elaine Shi, Bryan Parno, Adrian Perrig, Yih-Chun Hu, and Bruce Maggs.
Technical Report CMU-CS-05-148, February, 2005.

Professional Activities

PC Co-Chair, IEEE Symposium on Security and Privacy (**Oakland**), 2018

PC Co-Chair, IEEE Symposium on Security and Privacy (**Oakland**), 2017

Program Committee, ACM Conference on Computer & Communications Security (**CCS**), 2016

Program Committee, IEEE European Symposium on Security and Privacy (**EuroS&P**), 2016

Program Committee, IACR International Cryptology Conference (**CRYPTO**), 2015

Program Committee, IEEE Symposium on Security and Privacy (**Oakland**), 2015

Program Committee, IEEE Symposium on Security and Privacy (**Oakland**), 2014

Program Committee, ACM Conf. on Security & Privacy in Wireless Networks (**WiSec**), 2014

PC Co-Chair, ACM Cloud Computing Security Workshop (**CCSW**), 2013

Workshop Organizer, Language Support for Privacy-Enhancing Technologies (**PETShop**), 2013

Program Committee, ACM Conference on Computer & Communications Security (**CCS**), 2013

Program Committee, Conference on Trust and Trustworthy Computing (**TRUST**), 2013

Program Committee, IEEE Symposium on Security and Privacy (**Oakland**), 2013

Program Committee, Network and Distributed System Security Symposium (**NDSS**), 2013

Program Committee, ACM Conference on Computer & Communications Security (**CCS**), 2012

Program Committee, ACM Cloud Computing Security Workshop (**CCSW**), 2012

Program Committee, Conference on Trust and Trustworthy Computing (**TRUST**), 2012

Program Committee, ACM Symposium on Mobile Ad Hoc Networking (**MobiHoc**), 2012

Program Committee, Network and Distributed System Security Symposium (**NDSS**), 2012

Program Committee, Conference on Cryptology and Network Security (**CANS**), 2011

Program Committee, Network and Distributed System Security Symposium (**NDSS**), 2011

Program Committee, IACR Conference on Public Key Cryptography (**PKC**), 2011

Program Committee, APWG eCrime Researchers Summit, 2010

Program Committee, The MobiSys Conference PhD Forum, 2010

Program Committee, APWG eCrime Researchers Summit, 2009

Program Committee, Financial Cryptography and Data Security Conference (**FC**), 2009

External Reviewer (100+ Reviews) for:

- 25 conferences and workshops, including CCS, CRYPTO, EuroCrypt, EuroSys, NDSS, NSDI, OSDI, SenSys, SIGCOMM, SOSP, SRDS, SRUTI, USENIX Security, and WiSe.
- 12 journals, including ACM CACM, IACR JoC, IEEE/ACM ToN, ACM SIGCOMM CCR, ACM TOIT, IEEE TMC, ACM ToCC, ACM ToCS, and IEEE TDSC.

TEACHING EXPERIENCE

Thesis Committees
Samee Zahur, *University of Virginia*. Defended April, 2016.
Srinath Setty, *University of Texas, Austin*. Defended August, 2014.
Yinqian Zhang, *University of North Carolina*. Defended June, 2014.

Interns Mentored 2011-2015
Benjamin Kreuter (*UVa*), Karthik Nagaraj (*Purdue*), Arjun Narayan (*U.Penn*), Ashay Rane (*UT Austin*), Mariana Raykova (*Columbia*), Joshua Schiffman (*Penn. State*), Srinath Setty (*UT Austin*), Sai Deep Tetali (*UCLA*), Laure Thompson (*Cornell*), Doug Woos (*UW*), Xi Xiong (*Penn. State*), Samee Zahur (*UVa*), and Danfeng Zhang (*Cornell*)

15-811: Verifying Complex Systems (graduate seminar)
Carnegie Mellon University Spring, 2017
- Covered the tools and techniques for verifying the correctness, security, and reliability of complex systems.

CSE599W: Verifying Software Systems (graduate seminar)
University of Washington Spring, 2016
- Covered the tools and techniques for verifying the correctness, security, and reliability of complex systems.
- Co-instructor with Zach Tatlock and Xi Wang.

English as a Second Language (ESL)
Chester County OIC, Pennsylvania Summer, 2001
- Developed and implemented an English curriculum for a class of recent immigrants from Mexico, adapting instruction to accommodate a wide range of skill levels.

PATENTS

Providing Consistent Security Information. #9,432,401 – August, 2016
John Douceur, Bryan Parno, and Robert Reeder.

End-to-End Security via Secure Hardware Running Verified Software. #9,363,087 – June, 2016
Chris Hawblitzel, Jon Howell, Jacob R. Lorch, Bryan Parno, and Brian Zill.

Utilization of a Protected Module to Prevent Offline Dictionary Attacks. #9,294,281 – March, 2016
Stuart Schechter, David Molnar, Jacob R. Lorch, Barry Bond, Bryan Parno.

Personal Identification Combining Proximity Sensing With Biometrics. #9,152,868 – October, 2015
Chris Smowton, Ronnie Chaiken, Weidong Cui, Oliver Foehr, Jacob R. Lorch, David Molnar, Bryan Parno, Stefan Saroiu, Alec Wolman.

User-Driven Access Control. #9,106,650 – August, 2015
Franziska Roesner, Tadayoshi Kohno, Alexander Moshchuk, Bryan Parno, Helen Jiahe Wang.

Methods for User-Verifiable Execution of Security-Sensitive Code. #8,627,414 – January, 2014
Jonathan M. McCune, Adrian Perrig, Anupam Datta, Virgil Gligor, Yanlin Li, Bryan Parno, Amit Vasudevan, and Ning Qu.

Method and Apparatus for Secure Online Transactions. #8,352,738 – January, 2013
Bryan Parno, Cynthia Kuo, and Adrian Perrig.

Securing Anti-Virus Software with Virtualization. #8,307,443 – October, 2012
Helen Wang, Jacob R. Lorch, and Bryan Parno.

Key Distribution in Unidirectional Channels with Applications to RFID. #8,031,875 – October, 2011
Ari Juels and Bryan Parno.

SELECTED INVITED TALKS

Ironclad: Full Verification of Complex Systems – **Keynote**
The 10th Layered Assurance Workshop, December, 2016.

Ironclad: Full Verification of Complex Systems – **Invited Talk**
Workshop on Formal Methods and Security (FMS), June, 2016.

Ironclad: Full Verification of Complex Systems – **Invited Talk**
Conference on Verification, Model Checking, and Abstract Interpretation (VMCAI), Jan., 2016.

Ironclad: Full Verification of Complex Systems – **Invited Talk**
Stanford Security Seminar, December, 2015.

Bootstrapping Cloud Security – **Invited Plenary Talk**
Conference on Applied Cryptography and Network Security (ACNS), June, 2013.

Verifying Computation – **Special ECE Graduate Seminar**
Carnegie Mellon University, Pittsburgh, PA, October, 2012.

Building Trusted Systems with Protected Modules.
University of Texas, Austin, February, 2012.
University of Cambridge, October, 2011.

Bootstrapping Trust 101.
Trusted Infrastructure Workshop, Pittsburgh, PA, June, 2010.

Privacy and Technology.
Washington County Bar Association Winter Meeting, Washington, PA, January, 2010.

Non-Interactive Verifiable Computation.
Crypto in the Clouds Workshop, Cambridge, MA, August, 2009.

Techniques for Securing Sensor Networks.
University of Porto, Portugal, December, 2006.
New University of Lisbon, Portugal, December, 2006.

Distributed Detection of Node Replication Attacks in Sensor Networks.
ARO Workshop on Localization in Wireless Sensor Networks, Seattle, WA, June, 2005.