Bryan Parno

Collaborative Innovation Center, Office 2121, 4720 Forbes Avenue, Pittsburgh, PA 15213 parno@cmu.edu

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

Kavčić-Moura Professor, *Carnegie Mellon University*, Pittsburgh, PA. 4/2024 - Present
Professor, *Carnegie Mellon University*, Pittsburgh, PA. 7/2023 - 4/2024
Associate Professor, *Carnegie Mellon University*, Pittsburgh, PA. 1/2017 - 6/2023
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

IEEE Cybersecurity Award for Practice, 2024.
Intel's Hardware-Security Academic Test-of-Time Award, 2024.
Distinguished Paper, The Conference on Computer Aided Verification (**CAV**), 2024.
Test-of-Time Award, IEEE Symposium on Security and Privacy (**Oakland**), 2023.
IEEE Computer Society Golden Core Member, 2023.
Distinguished Paper Award, ACM **OOPSLA** Conference, 2022.
Best Paper Honorable Mention, ACM Conf. on Comp. & Communications Security (**CCS**), 2022.
Distinguished Paper Award, **USENIX Security** Symposium, 2022.
Second Prize ($75K) in the **USENIX Security** Internet Defense Prize competition, 2022.
Test-of-Time Award, IEEE Symposium on Security and Privacy (**Oakland**), 2020.
Distinguished Paper Award, ACM **PLDI** Conference, 2020.
The Joel and Ruth Spira Excellence in Teaching Award for 2019-2020.
Google Faculty Fellowship, 2018.
Sloan Research Fellowship, 2018.
Distinguished Paper Award, **USENIX Security** Symposium, 2017.
Research Highlight, Communications of the ACM, 2017.
Senior Member of ACM and IEEE, 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 (CMU 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

Degradation Attacks on Certifiably Robust Neural Networks.
Klas Leino, Chi Zhang, Ravi Mangal, Matt Fredrikson, Bryan Parno, and Corina Pasareanu.
Transactions on Machine Learning Research (**TMLR**), November, 2022.

Armada: Automated Verification of Concurrent Code with Sound Semantic Extensibility.
Jacob R. Lorch, Yixuan Chen, Manos Kapritsos, Haojun Ma, Bryan Parno,
Shaz Qadeer, Upamanyu Sharma, James R. Wilcox, and Xueyuan Zhao.
ACM Transactions on Programming Languages and Systems (**TOPLAS**), November, 2021.

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

Verus: A Practical Foundation for Systems Verification.
Andrea Lattuada, Travis Hance, Jay Bosamiya, Matthias Brun, Chanhee Cho, Hayley LeBlanc, Pranav Srinivasan, Reto Achermann, Tej Chajed, Chris Hawblitzel, Jon Howell, Jay Lorch, Oded Padon, Bryan Parno.
ACM Symposium on Operating Systems Principles (**SOSP**), October, 2024.

FlowCert: Translation Validation for Asynchronous Dataflow via Dynamic Fractional Permissions.
Zhengyao Lin, Joshua Gancher, Bryan Parno.
ACM Conference on Object-Oriented Programming Systems, Languages, and Applications (**OOPSLA**), October, 2024.

Context Pruning for More Robust SMT-based Program Verification.
Yi Zhou, Jay Bosamiya, Jessica Li, Marijn Heule, Bryan Parno.
Formal Methods in Computer-Aided Design (**FMCAD**) Conference, Oct., 2024.

CONFERENCES CONTINUED

Inductive Invariants That Spark Joy: Using Invariant Taxonomies to Streamline Distributed Protocol Proofs.
Tony Nuda Zhang, Travis Hance, Manos Kapritsos, Tej Chajed, Bryan Parno.
USENIX Symposium on Operating Systems Design and Implementation (**OSDI**), July, 2024.

A Framework for Debugging Automated Program Verification Proofs via Proof Actions.
Chanhee Cho, Yi Zhou, Jay Bosamiya, and Bryan Parno.
Conference on Computer Aided Verification (**CAV**), July, 2024.
Distinguished Paper Award.

Verus: Verifying Rust Programs using Linear Ghost Types.
Andrea Lattuada, Travis Hance, Chanhee Cho, Matthias Brun, Isitha Subasinghe, Yi Zhou, Jon Howell, Bryan Parno, and Chris Hawblitzel.
ACM Conference on Object-Oriented Programming Systems, Languages, and Applications (**OOPSLA**), October, 2023.

Leaf: Modularity for Temporary Sharing in Separation Logic.
Travis Hance, Jon Howell, Oded Padon, and Bryan Parno.
ACM Conference on Object-Oriented Programming Systems, Languages, and Applications (**OOPSLA**), October, 2023.

Galápagos: Developing Verified Low-Level Cryptography on Heterogeneous Hardwares.
Yi Zhou, Sydney Gibson, Sarah Cai, Menucha Winchell, and Bryan Parno.
ACM Conference on Computer & Communications Security (**CCS**), Nov., 2023.

Mariposa: Measuring SMT Instability in Automated Program Verification.
Yi Zhou, Jay Bosamiya, Yoshiki Takashima, Jessica Li, Marijn Heule, and Bryan Parno.
Formal Methods in Computer-Aided Design (**FMCAD**) Conference, Oct., 2023.

Algebraic Reductions of Knowledge.
Abhiram Kothapalli and Bryan Parno.
IACR **CRYPTO** Conference, August, 2023.

Sharding the State Machine: Automated Modular Reasoning for Complex Concurrent Systems.
Travis Hance, Yi Zhou, Andrea Lattuada, Reto Achermann, Alex Conway, Ryan Stutsman, Gerd Zellweger, Chris Hawblitzel, Jon Howell, and Bryan Parno.
USENIX Symposium on Operating Systems Design and Implementation (**OSDI**), July, 2023.

Owl: Compositional Verification of Security Protocols via an Information-Flow Type System.
Joshua Gancher, Sydney Gibson, Pratap Singh, Samvid Dharanikota, and Bryan Parno.
IEEE Symposium on Security and Privacy (**Oakland**), May, 2023.

MSWasm: Soundly Enforcing Memory-Safe Execution of Unsafe Code.
Alexandra E. Michael, Anitha Gollamudi, Jay Bosamiya, Evan Johnson, Aidan Denlinger, Craig Disselkoen, Conrad Watt, Bryan Parno, Marco Patrignani, Marco Vassena, and Deian Stefan.
ACM Symposium on Principles of Programming Languages (**POPL**), January, 2023.

FastVer2: A Provably Correct Monitor for Concurrent, Key-Value Stores.
Arvind Arasu, Tahina Ramananandro, Aseem Rastogi, Nikhil Swamy, Aymeric Fromherz, Kesha Hietala, Bryan Parno, and Ravi Ramamurthy.
ACM Conference on Certified Programs and Proofs (**CPP**), January, 2023.

Linear Types for Large-Scale Systems Verification.
Jialin Li, Andrea Lattuada, Yi Zhou, Jack Cameron, Jon Howell, Bryan Parno, Chris Hawblitzel.
ACM Conference on Object-Oriented Programming Systems, Languages, and Applications (**OOPSLA**), December, 2022.
Distinguished Paper Award.

CONFERENCES CONTINUED

Hammurabi: A Framework for Pluggable, Logic-based X.509 Certificate Validation Policies.
James Larisch, Waqar Aqeel, Christo Wilson, Alan Mislove, Taejoong Chung, Dave Levin, Bryan Parno, and Bruce Maggs.
ACM Conference on Computer & Communications Security (**CCS**), Nov., 2022.
Best Paper Honorable Mention.

Provably-Safe Multilingual Software Sandboxing using WebAssembly.
Jay Bosamiya, Benjamin Lim, and Bryan Parno.
USENIX Security Symposium, August, 2022.
Distinguished Paper Award and Second Place in the Internet Defense Prize Competition.

Transparency Dictionaries with Succinct Proofs of Correct Operation.
Ioanna Tzialla, Abhiram Kothapalli, Bryan Parno, and Srinath Setty.
Network and Distributed System Security Symposium (**NDSS**), April, 2022.

Fast Batched DPSS and its Applications.
Vipul Goyal, Abhiram Kothapalli, Elisaweta Masserova, Bryan Parno, and Yifan Song.
IACR Conference on Practice and Theory of Public-Key Cryptography (**PKC**), March, 2022.
Blockchains Enable Non-Interactive MPC.
Vipul Goyal, Elisaweta Masserova, Bryan Parno, and Yifan Song.
IACR Theory of Cryptography Conference (**TCC**), November, 2021.

Fast Geometric Projections for Local Robustness Certification.
Aymeric Fromherz, Klas Leino, Matt Fredrikson, Bryan Parno, and Corina Păsăreanu.
International Conference on Learning Representations (**ICLR**), Spotlight Presentation, May, 2021.

A Security Model and Fully Verified Implementation for the IETF QUIC Record Layer.
Antoine Delignat-Lavaud, Cedric Fournet, Bryan Parno, Jonathan Protzenko, Tahina Ramananandro, Jay Bosamiya, Joseph Lallemand, Itsaka Rakotonirina, and Yi Zhou.
IEEE Symposium on Security and Privacy (**Oakland**), May, 2021.

SoK: Computer-Aided Cryptography.
Manuel Barbosa, Gilles Barthe, Karthik Bhargavan, Bruno Blanchet, Cas Cremers, Kevin Liao, and Bryan Parno.
IEEE Symposium on Security and Privacy (**Oakland**), May, 2021.

HerQules: Securing Programs via Hardware-Enforced Message Queues.
Daming Chen, Wen Shih Lim, Mohammad Bakhshalipour, Phillip Gibbons, James C. Hoe, and Bryan Parno.
ACM Conference on Architectural Support for Programming Languages and Operating Systems (**ASPLOS**), April, 2021.

Finding Invariants of Distributed Systems: It's a Small (Enough) World After All.
Travis Hance, Marijn Heule, Ruben Martins, and Bryan Parno.
USENIX Symposium on Networked Systems Design and Implementation (**NSDI**), April, 2021

Don't Yank My Chain: Auditable NF Service Chaining.
Guyue Liu, Hugo Sadok, Anne Kohlbrenner, Bryan Parno, Vyas Sekar, and Justine Sherry.
USENIX Symposium on Networked Systems Design and Implementation (**NSDI**), April, 2021

CAPS: Smoothly Transitioning to a More Resilient Web PKI.
Stephanos Matsumoto, Jay Bosamiya, Yucheng Dai, Paul van Oorschot, and Bryan Parno.
ACSA Annual Computer Security Applications Conference (**ACSAC**), December, 2020.

Talek: Private Group Messaging with Hidden Access Patterns.
Raymond Cheng, William Scott, Elisaweta Masserova, Irene Zhang, Vipul Goyal, Thomas Anderson, Arvind Krishnamurthy, and Bryan Parno.
ACSA Annual Computer Security Applications Conference (**ACSAC**), December, 2020.

CONFERENCES CONTINUED

Storage Systems are Distributed Systems (So Verify Them That Way!).
Travis Hance, Andrea Lattuada, Chris Hawblitzel, Jon Howell, Rob Johnson, and Bryan Parno.
USENIX Symposium on Operating Systems Design & Implementation (**OSDI**), November, 2020.

Verified Transformations and Hoare Logic: Beautiful Proofs for Ugly Assembly Language.
Jay Bosamiya, Sydney Gibson, Yao Li, Bryan Parno, and Chris Hawblitzel.
Conference on Verified Software: Theories, Tools, and Experiments (**VSTTE**), July, 2020.

Armada: Low-Effort Verification of High-Performance Concurrent Programs.
Jacob R. Lorch, Yixuan Chen, Manos Kapritsos, Bryan Parno, Shaz Qadeer, Upamanyu Sharma, James R. Wilcox, and Xueyuan Zhao.
ACM Conference on Programming Language Design and Implementation (**PLDI**), June, 2020.
Distinguished Paper Award.

EverCrypt: A Fast, Verified, Cross-Platform Cryptographic Provider.
Jonathan Protzenko, Bryan Parno, Aymeric Fromherz, Chris Hawblitzel, Marina Polubelova, Karthikeyan Bhargavan, Benjamin Beurdouche, Joonwon Choi, Antoine Delignat-Lavaud, Cedric Fournet, Natalia Kulatova, Tahina Ramananandro, Aseem Rastogi, Nikhil Swamy, Christoph Wintersteiger, and Santiago Zanella-Beguelin.
IEEE Symposium on Security and Privacy (**Oakland**), May, 2020.

A Verified, Efficient Embedding of a Verifiable Assembly Language.
Aymeric Fromherz, Nick Giannarakis, Chris Hawblitzel, Bryan Parno, Aseem Rastogi, and Nikhil Swamy.
ACM Symposium on Principles of Programming Languages (**POPL**), January, 2019.

Komodo: Using Verification to Disentangle Secure-Enclave Hardware from Software.
Andrew Ferraiuolo, Andrew Baumann, Chris Hawblitzel, and Bryan Parno.
ACM Symposium on Operating Systems Principles (**SOSP**), October, 2017.

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.
USENIX Security Symposium, August, 2017.
Distinguished Paper Award.

Hash First, Argue Later: Adaptive Verifiable Computations on Outsourced Data.
Dario Fiore, Cedric Fournet, Esha Ghosh, Markulf Kohlweiss, Olya Ohrimenko, & Bryan Parno.
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.
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.
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.
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.
USENIX Symposium on Operating Systems Design and Implementation (**OSDI**), October, 2014.

CONFERENCES CONTINUED

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

Permacoin: Repurposing Bitcoin Work for Data Preservation.
Andrew Miller, Elaine Shi, Ari Juels, Bryan Parno, and Jonathan Katz.
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.
USENIX Annual Technical Conference (**ATC**), June, 2013.

Pinocchio: Nearly Practical Verifiable Computation.
Bryan Parno, Craig Gentry, Jon Howell, and Mariana Raykova.
IEEE Symposium on Security and Privacy (**Oakland**), May, 2013.
Best Paper Award.
Test-of-Time Award, 2023.

Quadratic Span Programs and Succinct NIZKs without PCPs.
Rosario Gennaro, Craig Gentry, Bryan Parno, and Mariana Raykova.
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.
EuroSys Conference, April, 2013.

Embassies: Radically Refactoring the Web.
Jon Howell, Bryan Parno, and John R. Douceur.
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.
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.
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.
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.
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.
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.
IACR **CRYPTO** Conference, August, 2010.

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

CONFERENCES CONTINUED

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

Unidirectional Key Distribution Across Time and Space with Applications to RFID Security.
Ari Juels, Ravikanth Pappu, and Bryan Parno.
USENIX Security Symposium, July, 2008.

Flicker: An Execution Infrastructure for TCB Minimization.
Jonathan M. McCune, Bryan Parno, Adrian Perrig, Michael K. Reiter, and Hiroshi Isozaki.
EuroSys Conference, April, 2008.
Intel's Hardware-Security Academic Test-of-Time Award, 2024.

SNAPP: Stateless Network-Authenticated Path Pinning.
Bryan Parno, Adrian Perrig, and David Andersen.
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.
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.
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.
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.
Conference on Future Networking Technologies (**CoNEXT**), December, 2006.

Phoolproof Phishing Prevention.
Bryan Parno, Cynthia Kuo, and Adrian Perrig.
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.
IEEE Symposium on Security and Privacy (**Oakland**), May, 2005.
Test-of-Time Award, 2020.

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

WORKSHOPS

No Root Store Left Behind.
James Larisch, Waqar Aqeel, Taejoong Chung, Eddie Kohler, Dave Levin, Bruce Maggs, Bryan Parno, and Christo Wilson.
ACM Workshop on Hot Topics in Networks (**HotNets**), November, 2023.

Self-correcting Neural Networks for Safe Classification.
Klas Leino, Aymeric Fromherz, Ravi Mangal, Matt Fredrikson, Bryan Parno, Corina Pasareanu.
Workshop on Formal Methods for ML-Enabled Autonomous Systems (**FoMLAS**), August, 2022.

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.
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.
Workshop on Hot Topics in Networks (**HotNets**), November, 2011.

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

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

TECHNICAL REPORTS

Burrow: Custom Read/Write Permissions for Custom Ghost State in Concurrent Separation Logic.
Travis Hance, Jon Howell, Oded Padon, and Bryan Parno.
CMU-CyLab-21-002, November, 2021.

Self-Repairing Neural Networks: Provable Safety for Deep Networks via Dynamic Repair.
Klas Leino, Aymeric Fromherz, Ravi Mangal, Matt Fredrikson, Bryan Parno, and Corina Păsăreanu.
arXiv:2107.11445 [cs.LG], July, 2021.

Poppins: A Direct Construction for Asymptotically Optimal zkSNARKs.
Abhiram Kothapalli, Elisaweta Masserova, and Bryan Parno.
ePrint Archive, Report 2020/1318, March, 2021.

A Note on the Unsoundness of vnTinyRAM's SNARK.
Bryan Parno.
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.
MSR-TR-2011-19, February, 2011.

Help Me Help You: Using Trustworthy Host-Based Information in the Network.
Bryan Parno, Zongwei Zhou, and Adrian Perrig.
CMU-CyLab-09-016, November, 2009.

Don't Talk to Zombies: Mitigating DDoS Attacks via Attestation.
Bryan Parno, Zongwei Zhou, and Adrian Perrig.
CMU-CyLab-09-009, June, 2009.

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

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.

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.

TEACHING

18-732: Secure Software Systems
Carnegie Mellon University — Spring, 2020 – present

15/18-330: Introduction to Computer Security
Carnegie Mellon University — Fall, 2019 – present

15/18-330: Introduction to Computer Security
Carnegie Mellon University — Fall, 2018
Co-taught with Vyas Sekar

18-732: Secure Software Systems
Carnegie Mellon University — Spring, 2018
Co-taught with Lujo Bauer

15-811: Verifying Complex Systems
Carnegie Mellon University — Spring, 2017

CSE599W: Verifying Software Systems
University of Washington — Spring, 2016
Co-taught with Zach Tatlock and Xi Wang

MENTORING

PhD Students Graduated

Lisa Masserova (co-advised with Vipul Goyal) 2018-2024
Postdoc with Elaine Shi (CMU) as of Fall 2024.

Travis Hance 2018-2024
Postdoc at MPI-SWS as of Fall 2024.

Jay Bosamiya 2017-2024
Senior Researcher at Microsoft Research as of Fall 2024.

Abhiram Kothapalli 2018-2024
Postdoc at UC Berkeley as of Fall 2024.

Aymeric Fromherz (co-advised with Corina Păsăreanu) 2017-2021
Permanent (tenured) Researcher at Inria, Paris.
Received the **A.G. Milnes Award** (Department award for the highest quality dissertation)
Received the **ACM SIGSAC Doctoral Dissertation Award**
(for Outstanding PhD Thesis in Computer and Information Security)

Steve Matsumoto, PhD, ECE, CMU. 2017-2019
Assistant Professor at Olin College as of Fall 2019.

Postdocs

Joshua Gancher	2021-2024
Assistant Professor at Northeastern University as of Fall 2024.	

PhD Advising

Sydney Gibson	2020-present
Zhengyao Lin	2022-present
Mike McLoughlin (co-advised with Fraser Brown)	2023-present
Amar Shah (co-advised with Marijn Heule)	2024-present
Pratap Singh	2022-present
Elanor Tang	2024-present
Yi Zhou	2019-present

Masters Advising

Yi Cai	2023-2024
Chanhee Cho	2021-2023
Samvid Dharanikota	2022
Benjamin Lim	2018-2020
Xueyuan Zhao	2018-2019
Mickael Laurant (visiting from ENS)	2018

Undergraduate Advising

Paul Hitchcox	REU 2024
Rory Brennan-Jones	REU 2024
Liz Austell	REU 2023
Alex Bai	REU 2023
Jessica Li	2023
Sarah Cai	REU 2021
Mimi Winchell	REU 2021
Jack Cameron	2020-2021
Valerie Choung	2020-2021
Yucheng Dai	2019-2020
Anne Kohlbrenner (co-advised with Justine Sherry)	2018-2019
Alisa Chang	2017-2018

PhD Thesis Committees

	Defense Date	*Advisor(s)*
Carnegie Mellon University		
Nikhil Vanjani		Elaine Shi
Mingxun Zhou		Elaine Shi
Hao Chung		Elaine Shi
Afonso Tinoco		Elaine Shi
Jenna Wise	11/2023	Jonathan Aldrich and Joshua Sunshine
Yifan Song	5/2022	Vipul Goyal
Kyle Soska	4/2021	Nicolas Christin
Ankush Das	4/2021	Jan Hoffmann
Soo-Jin Moon	9/2020	Vyas Sekar
Abelino Jiménez	6/2019	Bhiksha Raj
University of Michigan		
Tony Zhang		Manos Kapritsos
INRIA		
Son Ho		Karthik Bhargavan and Jonathan Protzenko
University of Burtsev		
Zhaofeng Li		Anton Burtsev
University of Illinois Urbana-Champagne		
Bolton Bailey	5/2024	Andrew Miller
University of Virginia		
Samee Zahur	4/2016	Dave Evans
University of Texas, Austin		
Srinath Setty	8/2014	Mike Walfish
University of North Carolina		
Yinqian Zhang	6/2014	Mike Reiter

Mentoring Continued

MS Thesis Committees

Monica Pardeshi, *Carnegie Mellon University*.	Defended July, 2023.
Keerthi Samhita Vempatti Venkatanaga, *Carnegie Mellon University*.	Defended April, 2023.
Cayden Codel, *Carnegie Mellon University*.	Defended April, 2022.

Interns Mentored, Microsoft Research 2011-2016

Benjamin Kreuter (*University of Virginia*)
Karthik Nagaraj (*Purdue University*)
Arjun Narayan (*University of Pennsylvania*)
Ashay Rane (*University of Texas, Austin*)
Mariana Raykova (*Columbia University*)
Joshua Schiffman (*Pennsylvania State University*)
Srinath Setty (*University of Texas, Austin*)
Sai Deep Tetali (*University of California, Los Angeles*)
Laure Thompson (*Cornell University*)
Doug Woos (*University of Washington*)
Xi Xiong (*Pennsylvania State University*)
Samee Zahur (*University of Virginia*)
Danfeng Zhang (*Cornell University*)

University Service

University RPT (non-tenure) Committee	August, 2017 – July, 2018
University Ad Hoc Committee on Childcare	July, 2019 – present
SCS Security Concentration Committee	March, 2017 – present
CyLab Education Steering Committee, **Chair**	February, 2020 – present
CyLab Education Steering Committee	April, 2019 – February, 2020
CyLab Student Professional Development Committee	April, 2019 – September, 2020
CyLab Director Search Committee	May, 2018 – December, 2018
CSD Hiring Committee	December 2023 – May, 2024
CSD Diversity, Equity, and Inclusion Committee, **Chair**	August, 2020 – October, 2023
CSD PhD Admissions Committee, **Chair**	May, 2019 – May, 2020
CSD PhD Admissions Committee	June, 2017 – December, 2018
CSD Speaking Skills Committee	March, 2018 – present
ECE Software Systems Course Coordinator	September, 2017 – August, 2019
ECE Junior Faculty Committee	May, 2019 – September, 2021
ECE Graduate Studies Committee	May, 2019 – present
ECE PhD Admissions Committee	June, 2017 – December, 2018

Professional Activities

Chair, IEEE Computer Society, Technical Committee on Security & Privacy, 2021-2023

Senior Program Committee, Privacy Enhancing Technologies Symposium (**PETS**), 2023

Program Committee, USENIX Symposium on Operating Systems Design and Implementation (**OSDI**), 2023

Review Panelist, NSF, 2023

Review Panelist, NSF, 2022

Program Committee, USENIX **Security** Symposium, 2022

Technical Advisor, CipherMode Labs (startup), 2021-present

Technical Advisory Committee, Algorand Foundation, 2019-2022

Review Panelist, NSF, 2021

Program Committee, USENIX Symposium on Operating Systems Design and Implementation (**OSDI**), 2020

Professional Activities Continued

External Review Committee, ACM Conference on Programming Language Design and Implementation (**PLDI**), 2020

Vice Chair, IEEE Computer Society, Technical Committee on Security & Privacy, 2020-2021

Program Committee, Network and Distributed System Security Symposium (**NDSS**), 2020

Program Committee, USENIX Symp. on Networked Systems Design & Impl. (**NSDI**), 2020

Review Panelist, NSF, 2019

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

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

Review Panelist, NSF, 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, 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, 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.

Selected Invited Talks

Building Fast and Provably Secure Systems
Cloudflare, October, 2024

Verus: Developing Verified and Performant Software
Collins Aerospace, Formal Methods Community of Practice, May, 2024

Formally Verifying the Rust Standard Library with Verus
The High Confidence Software and Systems Conference (HCSS), May, 2024

Verus: Developing Verified and Performant Software
Amazon, July, 2023

Panel: Challenges and Opportunities in Implementation and Verification of Cryptography
IEEE SecDev Conference, October, 2021

Developing High-Performance Mechanically-Verified Code – **Distinguished Lecture**
ETH Zurich, November, 2020

SELECTED INVITED TALKS CONTINUED

Developing High-Performance Mechanically-Verified Cryptographic Code – **Keynote**
Workshop on Foundations of Computer Security, June, 2020

Developing High-Performance Mechanically-Verified Cryptographic Code – **Invited Talk**
IACR Conference on Cryptographic Hardware and Embedded Systems, August, 2019

Developing High-Performance Mechanically-Verified Cryptographic Code – **Keynote**
Workshop on Foundations of Computer Security, June, 2020

Developing High-Performance Mechanically-Verified Cryptographic Code – **Invited Talk**
IACR Conference on Cryptographic Hardware and Embedded Systems, August, 2019

Provably Secure, Provably Isolated Code – **Invited Talk**
DARPA ISAT Principled Hardware/Software Interfaces (PHI) Workshop, February, 2019.

Full Verification of Complex Systems
ETH Zurich, June, 2018.

Making Verifiable Computation Useful – **Invited Talk**
DIMACS Workshop on Outsourcing Computation Securely, July, 2017.

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.

Fully Verified Outsourced Computation
CalTech, CMU, Columbia, Harvard, MIT, Princeton,
Stanford, UCLA, University of Washington, Yale. February - April, 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.

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.