Bryan Parno

parno@cmu.edu

Research Interests

My research is 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

Amazon Scholar, *Amazon Web Services*, Seattle, WA. 3/2025 - Present

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*

Selected Honors

Jay Lepreau Best Paper Award, USENIX Symposium on Operating Systems Design and Impl., 2025.
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.
Distinguished Paper Award, **USENIX Security** Symposium, 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.
Sloan Research Fellowship, 2018.
Distinguished Paper Award, **USENIX Security** Symposium, 2017.
Senior Member of ACM and IEEE, 2017.
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

Selected Publications

OwlC: Compiling Security Protocols to Verified, Secure, High-Performance Libraries.
Pratap Singh, Joshua Gancher, Bryan Parno.
USENIX Security Symposium, August, 2025.

Vest: Verified, Secure, High-Performance Parsing and Serialization for Rust.
Yi Cai, Pratap Singh, Zhengyao Lin, Jay Bosamiya, Joshua Gancher, Milijana Surbatovich, and Bryan Parno.
USENIX Security Symposium, August, 2025.

Basilisk: Using Provenance Invariants to Automate Proofs of Undecidable Protocols.
Tony Zhang, Keshav Singh, Tej Chajed, Manos Kapritsos, Bryan Parno.
USENIX Symposium on Operating Systems Design and Implementation (**OSDI**), July, 2025.

AlphaVerus: Bootstrapping Formally Verified Code Generation through Self-Improving Translation and Treefinement.
Pranjal Aggarwal, Bryan Parno, Sean Welleck.
International Conference on Machine Learning (**ICML**), July, 2025.

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.

Publications Continued

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.

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 **OOPSLA**, October, 2023.

Leaf: Modularity for Temporary Sharing in Separation Logic.
Travis Hance, Jon Howell, Oded Padon, and Bryan Parno.
ACM **OOPSLA**, October, 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.

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.

Linear Types for Large-Scale Systems Verification.
Jialin Li, Andrea Lattuada, Yi Zhou, Jack Cameron, Jon Howell, Bryan Parno, Chris Hawblitzel.
ACM **OOPSLA**, December, 2022.

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.

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.

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.

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.

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.

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.

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

Selected 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, 2023
Technical Advisor, CipherMode Labs (startup), 2021-present
Technical Advisory Committee, Algorand Foundation, 2019-2022
PC Co-Chair, IEEE Symposium on Security and Privacy (**Oakland**), 2018
PC Co-Chair, IEEE Symposium on Security and Privacy (**Oakland**), 2017
PC Co-Chair, ACM Cloud Computing Security Workshop (**CCSW**), 2013
Workshop Organizer, Language Support for Privacy-Enhancing Technologies (**PETShop**), 2013