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.
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.  

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.  
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.  

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 Rousopoulos.  

James Larisch, Waqar Aqeel, Christo Wilson, Alan Mislove, Taejoong Chung, Dave Levin, Bryan Parno, and Bruce Maggs.  
To Appear in ACM Conference on Computer & Communications Security (CCS), Nov., 2022.

Linear Types for Large-Scale Systems Verification.  
Jialin Li, Andrea Lattuada, Yi Zhou, Jack Cameron, Jon Howell, Bryan Parno, Chris Hawblitzel.  
To Appear in the ACM Conference on Object-Oriented Programming Systems, Languages, and Applications (OOPSLA), November, 2022.

Provably-Safe Multilingual Software Sandboxing using WebAssembly.  
Jay Bosamiya, Benjamin Lim, and Bryan Parno.  
To Appear in the USENIX Security Symposium, August, 2022.

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.  
CONFERENCES CONTINUED

Blockchains Enable Non-Interactive MPC.
Vipul Goyal, Elisaweta Masserova, Bryan Parno, and Yifan Song.

Fast Geometric Projections for Local Robustness Certification.
Aymeric Fromherz, Klas Leino, Matt Fredriksson, Bryan Parno, and Corina Păsăreanu.

A Security Model and Fully Verified Implementation for the IETF QUIC Record Layer.

SoK: Computer-Aided Cryptography.
Manuel Barbosa, Gilles Barthe, Karthik Bhargavan, Bruno Blanchet, Cas Cremers, Kevin Liao, and Bryan Parno.

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.

Don’t Yank My Chain: Auditable NF Service Chaining.
Guyue Liu, Hugo Sadok, Anne Kohlbrenner, Bryan Parno, Vyas Sekar, and Justine Sherry.

CAPS: Smoothly Transitioning to a More Resilient Web PKI.
Stephanos Matsumoto, Jay Bosamiya, Yucheng Dai, Paul van Oorschot, and Bryan Parno.

Talek: Private Group Messaging with Hidden Access Patterns.

Storage Systems are Distributed Systems (So Verify Them That Way!).
Travis Hance, Andrea Lattuada, Chris Hawblitzel, Jon Howell, Rob Johnson, and Bryan Parno.

Verified Transformations and Hoare Logic: Beautiful Proofs for Ugly Assembly Language.
Jay Bosamiya, Sydney Gibson, Yao Li, Bryan Parno, and Chris Hawblitzel.

Armada: Low-Effort Verification of High-Performance Concurrent Programs.
Jacob R. Lorch, Yixuan Chen, Manos Kapritsoc, Bryan Parno, Shaz Qadeer, Upamanyu Sharma, James R. Wilcox, and Xueyuan Zhao.

A Verified, Efficient Embedding of a Verifiable Assembly Language.
Aymeric Fromherz, Nick Giannarakis, Chris Hawblitzel, Bryan Parno, Aseem Rastogi, and Nikhil Swamy.

Komodo: Using Verification to Disentangle Secure-Enclave Hardware from Software.
Andrew Ferraiuolo, Andrew Baumann, Chris Hawblitzel, and Bryan Parno.

Vale: Verifying High-Performance Cryptographic Assembly Code.
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.

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.

Geppetto: Versatile Verifiable Computation.
IEEE Symposium on Security and Privacy (Oakland), May, 2015.

Chris Hawblitzel, Jon Howell, Jacob R. Lorch, Arjun Narayan, Bryan Parno, Danfeng Zhang, and Brian Zill.

Missive: Fast Application Launch From an Untrusted Buffer Cache.

Permacoin: Repurposing Bitcoin Work for Data Preservation.

How to Run POSIX Apps in a Minimal Picoprocess.
Jon Howell, Bryan Parno, and John R. Douceur.

Pinocchio: Nearly Practical Verifiable Computation.
Bryan Parno, Craig Gentry, Jon Howell, and Mariana Raykova.
Best Paper Award.

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

Resolving the Conflict Between Generality and Plausibility in Certified Computation.
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.

Lockdown: A Safe and Practical Environment for Security Applications.
Amit Vasudevan, Bryan Parno, Ning Qu, Virgil Gligor, and Adrian Perrig.

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.
Best Practical Paper Award.

How to Delegate and Verify in Public: Verifiable Computation from Attribute-based Encryption.
Bryan Parno, Mariana Raykova, and Vinod Vaikuntanathan.

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.

Bootstrapping Trust in Commodity Computers.
Bryan Parno, Jonathan M. McCune, and Adrian Perrig.

CLAMP: Practical Prevention of Large-Scale Data Leaks.
Bryan Parno, Jonathan M. McCune, Dan Wendlandt, David G. Andersen, and Adrian Perrig.

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

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

SNAPP: Stateless Network-Authenticated Path Pinning.
Bryan Parno, Adrian Perrig, and David Andersen.

Jonathan M. McCune, Bryan Parno, Adrian Perrig, Michael K. Reiter, and Arvind Seshadri.

Countermeasures against Government-Scale Monetary Forgery.
Alessandro Acquisti, Nicolas Christin, Bryan Parno, and Adrian Perrig.
<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Test-of-Time Award, 2020.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Technical Reports</td>
<td>Algebraic Reductions of Knowledge.</td>
<td>Abhiram Kothapalli and Bryan Parno.</td>
<td></td>
</tr>
</tbody>
</table>
Memoir—Formal Specs and Correctness Proofs.
John R. Douceur, Jacob R. Lorch, Bryan Parno, James Mickens, and Jonathan M. McCune.

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.

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

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

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

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

Jonathan M. McCune, Adrian Perrig, Anupam Datta, Virgil Gligor, Yanlin Li, Bryan Parno, Amit Vasudevan, and Ning Qu.
#8,627,414 – January, 2014

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

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

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

18-732: Secure Software Systems
Carnegie Mellon University
Spring, 2020, 2021, 2022

15/18-330: Introduction to Computer Security
Carnegie Mellon University
Fall, 2019, 2020, 2021

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
PhD Students Graduated
Aymeric Fromherz (co-advised with Corina Păsăreanu) 2017-2021
Postdoc at Inria, Paris as of Fall 2021.
Received the A.G. Milnes Award (Department award for the highest quality dissertation)
Steve Matsumoto, PhD, ECE, CMU. 2017-2019
Assistant Professor at Olin College as of Fall 2019.

Postdocs
Joshua Gancher 2021-present

PhD Advising
Jay Bosamiya 2017-present
Sydney Gibson 2020-present
Travis Hance 2018-present
Abhiram Kothrapali 2018-present
Lisa Masserova (co-advised with Vipul Goyal) 2018-present
Yi Zhou 2019-present

Masters Advising
Chanhee Cho 2021-present
Benjamin Lim 2018-2020
Xueyuan Zhao 2018-2019
Mickael Laurant (visiting from ENS) 2018

Undergraduate Advising
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 2018

PhD Thesis Committees
Bolton Bailey, University of Illinois, Urbana-Champaign.
Jenna Wise, Carnegie Mellon University.
Samee Zahur, University of Virginia. Defended April, 2016.
Srinath Setty, University of Texas, Austin. Defended August, 2014.

MS Thesis Committees
Cayden Codel, Carnegie Mellon University. Defended April, 2022

Interns Mentored, Microsoft Research
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)
Selected Invited Talks

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

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
ACR Conference on Cryptographic Hardware and Embedded Systems, August, 2019

Provably Secure, Provably Isolated Code – Invited Talk

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

Making Verifiable Computation Useful – Invited Talk

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

Bootstrapping Cloud Security – Invited Plenary Talk

Verifying Computation – Special ECE Graduate Seminar

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.

Non-Interactive Verifiable Computation.

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.
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
Program Committee, USENIX Security Symposium, 2022
Technical Advisor, CipherMode Labs (startup), 2021-present
Technical Advisory Committee, Algorand Foundation, 2019-present
Program Committee, USENIX Symposium on Operating Systems Design and Implementation (OSDI), 2020
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
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.
**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 Diversity, Equity, and Inclusion Committee, Chair
  - August, 2020 – present
- 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