Ethan Heilman (Ph.D)

Cryptologist
https://github.com/EthanHeilman

December 1, 2024
Ethan.R.Heilman@gmail.com
https://www.ethanheilman.com/

Education

- **Boston University** — Boston, MA
  Ph.D. Computer Science, Advised by Sharon Goldberg and Leonid Reyzin — *2022*
- **Bridgewater State University** — Bridgewater, MA
  B.S. Computer Science — *2007*

Research Areas:

As a Network Security researcher I investigate the security of Bitcoin, blockchains and other deployed global scale networks. My work employs tools from system-building, measurement, modeling and simulation, network security and cryptology.

Employment

- **Cloudflare** — Boston, MA
  Principal Systems Engineer — *2024 - present*
- **OpenPubkey** — Linux Foundation
  Technical Steering Committee Chair — *2024 - present*
- **BastionZero/Arwen/Commonwealth Crypto** — Boston, MA
  Co-founder and Chief Technology Officer — *2017 - 2024*
- **Boston University** — Boston, MA
  Research Fellow — *2013 - present*
- **Pubget Inc** — Bost, MA
  Senior Software Engineer — *2011 - 2013*
- **Broad Institute** — Cambridge, MA
  Software Engineer — *2008 - 2011*
- **Jumptap Inc** — Cambridge, Ma
  Software Engineer — *2007 - 2008*

Recent Awards, Grants & Honors

BastionZero Runner Up for the RSAC Innovation Sandbox Contest 2022
Nominated for a Pwnie Award (Best Cryptographic Attack) 2018
ETHEREUM Bounty Program (10000 pts) 2018
IETF Applied Networking Research Prize (ANRP) 2014
MIT Bitcoin Evangelism Award. 2014
Financial Crypto'14 Travel Grant 2014
Google Security Honorable Mention 2012
Juniper Networks Travel Support for ECRYPT II Hash Workshop 2011

Publications

1. 2024 **ColliderScript: Covenants in Bitcoin via 160-bit hash collisions**, E. Heilman, V. Kolobov, A. Levy, A. Poelstra
2. 2023 **OpenPubkey: Augmenting OpenID Connect with User-held Signing Keys**, E. Heilman, L Mugnier, A. Filippidis, S. Goldberg, S. Lipman, Y. Marcus, M. Milano, S. Premkumar, C. Unrein
3. 2020 **Cryptanalysis of curl-p and other attacks on the IOTA cryptocurrency**, IACR Transactions on Symmetric Cryptology 2020, E Heilman, N Narula, G Tanzer, J Lovejoy, M Colavita, M Virza, T Dryja
4. 2020 **The Arwen Trading Protocols**, International Conference on Financial Cryptography and Data Security 2020, E. Heilman, S. Lipmann, S. Goldberg
5. 2018 **Low-Resource Eclipse Attacks on Ethereum's Peer-to-Peer Network**, Y. Marcus, E. Heilman, S. Goldberg
6. 2018 **The rewards of selfish mining: technical perspective**, Communications of the ACM, S. Goldberg, E. Heilman
7. 2018 **An Empirical Analysis of Traceability in the Monero Blockchain**, Proceedings on Privacy Enhancing Technologies, M. Möser, K. Soska, E. Heilman, K. Lee, H. Heffan, S. Srivastava, K. Hogan, J. Hennessey, A. Miller, A. Narayanan, N. Christin
8. 2017 **Atomically trading with roger: Gambling on the success of a hardfork**, International Workshop on Data Privacy Management Cryptocurrencies and Blockchain Technology, P. McCorry, E. Heilman, A. Miller
9. 2017 **TumbleBit: An Untrusted Bitcoin-Compatible Anonymous Payment Hub**, Network and Distributed System Security Symposium (NDSS 2017), E. Heilman, L. Alshenibr, F. Baldimtsi, A. Scafuro, S. Goldberg
10. 2016, **Blindly Signed Contracts: Anonymous On-Blockchain and Off-Blockchain Bitcoin Transactions**, 3rd Workshop on Bitcoin and Blockchain Research at 20th International Conference of Financial Cryptography, E. Heilman, F. Baldimtsi, S. Goldberg
11. 2015, **Eclipse Attacks on Bitcoin's Peer-to-Peer Network**, USENIX Security'15, E. Heilman, A. Kendler, A. Zohar, S. Goldberg
12. 2014, **From the Consent of the Routed: Improving the Transparency of the RPKI**, SIGCOMM'14, E. Heilman, D. Cooper, L. Reyzin and S. Goldberg
13. 2014, **One Weird Trick to Stop Selfish Miners: Fresh Bitcoins, A Solution for the Honest Miner.**, E Heilman, Poster at FC'14
14. 2013, **On the risk of misbehaving RPKI authorities**, Proceedings of the Twelfth ACM Workshop on Hot Topics in Networks, D Cooper, E Heilman, K Brogle, L Reyzin, S Goldberg
15. 2011, **Restoring the Differential Resistance of MD6', EuroCrypt II Hash Workshop**, E. Heilman
16. 2009 **Attacks Against PermuteTransformXor Compression Functions and Spectral Hash Collisions**, NIST mailing list, Cryptology ePrint Archive Report, E. Heilman

17. 2007, **Poster: Developing lowcost AVL and Web Mapping for Real Time Intermodal Customer Information Using a GPS Cell Phones and Google Maps** , U Shama, L Harman, E Heilman, J Baltikauskas

18. 2006, **Metrowest Suburban Mobility Research, Development and Technology Project**, Office of Transportation Planning, Executive Oce Of Transportation, Draft., E. Heilman, U. Shama and L. Harman

Selected Presentations

1. **OpenPubkey: Augmenting OpenID Connect with User held Signing Keys**
   - Cloudflare Research, Remote, 2024
   - Cloudflare Eng Presents, Remote, 2024
   - BSides Cambridge, Belmont, Massachusetts, 2023
2. **OP_CAT**
   - OP_NEXT, Fidelity Center for Applied Technology (FCAT), Boston, Massachusetts, 2024
   - MIT Media Lab Digital Currency Initiative (Research Talk), Cambridge, Massachusetts, 2024
3. **Signing Docker Official Images Using OpenPubkey (youtube)**
   - DockerCon, Los Angeles, California, 2023
4. **An Exploration of Bitcoin's P2P Network and its Security**
   - Bitcoin Research Day, New York, New York, 2023
5. **Cryptanalysis of Curl-P and Other Attacks on the IOTA Cryptocurrency**
   - 27th annual Fast Software Encryption conference (remote), Athens, Greece, 2020
   - BlackHat USA, Los Vegas, 2018,
   - Boston Blockchain Network, Boston, 2017
6. **Near Misses: What Could've Gone Wrong**
   - Cryptoeconomic Systems Summit, Cambridge, MA, 2019
7. **Bitcoin Eclipse Attacks (Survey)**
   - Chaincode Labs, New York, 2018
8. **xCrow Protocol for Fast Crosschain Atomic Swaps**
   - Binary District "Off the chain" workshop, Berlin, 2018
9. **Cross-Chain Swaps**
   - Dev++ Bitcoin Edge/BC-2, Keio University, Japan, 2018
   - Dev++ Bitcoin Edge, Stanford University, 2017
   - BC-2, Tokyo, 2017

10. **Atomically trading with roger: Gambling on the success of a hardfork**
    - Scaling Bitcoin, Stanford, 2017
11. **TumbleBit: An Untrusted Bitcoin-Compatible Anonymous Payment Hub**
    - NDSS'17: The Network and Distributed System Security Symposium (2017)
    - The New Context Conference, San Francisco (2016)
    - The Scaling Bitcoin Workshop, Milan (2016)
    - University of Illinois, Urbana-Champaign (2016)
    - MIT Media Lab Digital Currency Initiative Blockchain Seminar (2016)
    - MACS Project Meeting (2016)
    - MIT Security Seminar (2016)
12. **Blindly Signed Contracts: Anonymous On-Blockchain and Off-Blockchain Bitcoin Transactions**
    - BITCOIN'16 (2016)
    - Cornell Systems Lunch (2016)
    - MIT Security Seminar (2016)
13. **Eclipse Attacks on Bitcoin's Peer-to-Peer Network**
    - USENIX Security'15 (2015)
    - UMass, Amherst (2015 and 2016)
    - UPenn Seminar (2015)
    - Princeton Bitcoin Workshop (2015)
    - University of Maryland Syschat (2015)
    - MIT Security Seminar (2015)
14. **From the Consent of the Routed: Improving the Transparency of the RPKI**
    - SIGCOM'14 (2014)
    - New England Networking and Systems Day (2014)
    - Boston University Security Seminar (2014)
    - Hubspot Tech Talks (2014)
15. **Restoring the Differential Security of MD6**
    - ECRYPT II Hash Workshop, Estonia (2011)
    - MIT Crypto Group (2011)
16. **Developing lowcost AVL and Web Mapping for Real Time Intermodal Customer Information Using a GPS Cell Phones and Google Maps**
    - Transportation Research Symposium Institute of Transportation Engineers Massachusetts Chapter (MAITE) (2007)
    - 23rd National Conference on Undergraduate Research (2007)

Teaching Assistant (Boston University)

Probability in Computer Science (94 Students) 2016
Network Security (59 Students) 2015
Network Security (53 Students) 2014

Academic Service

Program Chair

Scaling Bitcoin: "Scaling the Edge" 2017

Session Chair

NDSS'17: The Network and Distributed System Security Symposium 2017

Program Committee

AFT'24: The fifth international conference on Advances in Financial Technologies 2024
CES Spring 23: Cryptoeconomic Systems 2023
AFT'23: The fifth international conference on Advances in Financial Technologies 2023
FC'23: Financial Cryptography and Data Security 2023
CES Fall 21: Cryptoeconomic Systems 2021
CBT 2021: 3th International Workshop on Cryptocurrencies and Blockchain Technology) . . 2021
DeFi 21: 1st Workshop on Decentralized Finance 2021
CVCBT 2021 Crypto Valley Conference on Blockchain Technology) 2021
AFT 2021: 3rd Conference on Advances in Financial Technology 2021
FC'21: Financial Cryptography and Data Security 2021
FC'20: Financial Cryptography and Data Security 2020
S&P'20: IEEE Symposium on Security and Privacy (Oakland) 2020
CES'20: Cryptoeconomic Systems 2020
CVC'20: Crypto Valley Conference 2020
CVCBT'19: Crypto Valley Conference on Blockchain Technology 2019
Cryptocurrency Implementers Workshop 2019
FC'19: Financial Cryptography and Data Security 2019
IEEE S&B: Security and Privacy on the Blockchain Workshop 2018
BlockSEA: Workshop on Blockchain and Sharing Economy Applications 2018
Scaling Bitcoin: "Kaizen" 2018
BITCOIN 2018: 5th Workshop on Bitcoin and Blockchain Research 2018
IEEE S&B: Security and Privacy on the Blockchain Workshop 2017
BITCOIN 2017: 4th Workshop on Bitcoin and Blockchain Research 2017
BITCOIN 2016: 3rd Workshop on Bitcoin and Blockchain Research 2016
SAT 2015: Workshop on Surveillance and Technology 2015

External Reviewer

CyberSec-2020: the Journal of Cybersecurity 2020
S&P'20: IEEE Symposium on Security and Privacy (Oakland) 2020
FC 2017: Financial Cryptography and Data Security 2017 2017
CRYPTO 2016: 36th International Cryptology Conference 2016
IMC 2016: ACM Internet Measurement Conference 2016
NSDI 15: USENIX Symposium on Networked and Systems Design and Implementation . . . 2015

Selected Open Source Software Projects

1. **OpenPubkey**: An implementation in go-lang of the OpenPubkey protocol. Currently a project under the Linux Foundation. This project is based on an implementation of OpenPubkey I wrote. I am currently the main contributor and chair of the technical steering committee.
2. **Bitcoin Peer Forger (BPF)**: BPF is a network security research tool which allows an on-path party to connect to a Bitcoin node from a large number of spoofed IP addresses.
3. **TumbleBit**: Implements TumbleBit protocol as part of TumbleBit research publication. Used as a reference for development of nTumbleBit open source project.
4. **RPKI Downgrade Detector**: RPKI transparency tool released as part of RPKI and secure routing publications. Used at NIST for RPKI anomaly detection.
5. **Flip It**: Javascript implementation of a research game designed to model Advanced Persistent Threats (APT). While not developed for this purpose, a research team had people play my implementation of Flip It to explore the psychology of computer security.
6. **Differential Pattern Search Program for MD6**: This software is used to reestablish the differential resistance of MD6. It uses a classification system of differential weight patterns that allows us to extend previous analysis to prove that MD6 is resistant to differential cryptanalysis.
7. **Contributions to bitcoin-core**: As shown below I have made ten contributions to the Bitcoin-core open-source project ranging from security improvements to the peer-to-peer networking layer to bugfixes and unittests. These contributions have been included downstream in projects such as Zcash, Bitcoin-ABC, Litecoin and many others.

Selected Open Source Software Contributions

1. **Bitcoin Improvement Proposals** BIP-347 OP_CAT **(Proposed Standard: Draft)**
2. **Memguard** Removes drop based finalizer **(merged)**
3. **VtNetCore** Fixes a bug in OSC-112 control sequences **(merged)**
4. **Bitcoin-Core** random: fixes read buffer resizing in RandAddSeedPerfmon **(merged)**
5. **Bitcoin-Core** Limit the number of IPs we use from each DNS seeder **(merged)**
6. **Bitcoin-Core** Add test-before-evict discipline to addrman **(merged)**
7. **Bitcoin-Core** Feeler connections to increase online addrs in the tried table **(merged)**

8. **Bitcoin-Core** Remove non-determinism which is breaking net_tests **(merged)**
9. **Bitcoin-Core** Fix de-serialization bug where AddrMan is left corrupted **(merged)**
10. **Bitcoin-Core** Adds unittests for CAddrMan and CAddrinfo, removes source of non-determinism **(merged)**
11. **Bitcoin-Core** Creates unittests for addrman, makes addrman testable **(merged)**
12. **python-bitcoinlib** Adding IPv6 support to addr messages with example code **(merged)**

Selected Trade Press and Media

Media Quotes and Interviews

- North Korea, NFTs and a hit video game: inside a $500m cryptocurrency theft (Carly Olson, The Guardian, 2022)
- Mt. Gox bitcoin debacle: huge heist or sloppy glitch (Jeremy Wagstaff, Reuters, 2014)

Collider Script

- ColliderScript: A $50M Bitcoin Covenant With No New Opcodes (Andrew Poelstra, Bitcoin Magazine, 2024)
- Bitcoin Developers Working With StarkWare, Blockstream Claim Breakthrough on New Features (Bradley Keoun, Coindesk, 2024)
- ColliderScript: Advancing Bitcoin covenants without a fork (Macauley Peterson, Blockworks, 2024)

OpenPubkey

- Latest OpenPubkey Project Initiative Makes SSH More Secure (Michael Vizard, Security Boulevard, 2024)
- Enhancing Security with OpenPubkey (Varnesh Gawde, vulnerx, 2023)
- New cryptographic protocol aims to bolster open-source software security, (ZDNet, 2023)
- SD Times Open-Source Project of the Week: OpenPubkey, (Jenna Barron, SD Times, 2023)

BIP-347: Proposed OP_CAT improvement to Bitcoin

- OP_CAT Proposal to Bring Smart Contracts to Bitcoin Finally Gets a 'BIP Number' This marks the first step towards reintroducing functionality removed from Bitcoin by creator Satoshi Nakamoto in 2010. (Daniel Kuhn, Coindesk, 2024)
- OP_CAT Proposal Assigned BIP-347, Aims to Enhance Bitcoin With Ethereum-Style Smart Contracts (SHINOBIJAN, Bitcoin Magazine, 2024)
- OP_CAT proposal for covenants on Bitcoin receives official BIP number (Bitcoin.com, 2024)
- MIT BITCOIN Expo: Member of the Covenants Panel MIT BITCOIN Expo, 2024)
- TO MEME, OR NOT TO MEME: THE CAT (SHINOBIJAN, Bitcoin Magazine, 2024)
- Satoshi-Era Bitcoin Function 'OP_CAT' Dusted Off as Development Fervor Grows Developers Ethan Heilman and Armin Sabouri view OP_CAT as a simple opcode that offers some of the general purpose functionality currently missing in Bitcoin (Jamie Crawley, Coindesk, 2024)

- What Is the OP_CAT Bitcoin Improvement Proposal? (Unchained, 2024)
- The History of OP_CAT and the Evolution of the Bitcoin Network (Trust Machines, 2023)

BastionZero

- BastionZero releases SplitCert for password-free authentication and access (Michael Hill, CSO Online, 2023)
- BastionZero Recognized for Innovative Cryptographic Approach to Zero-Trust Infrastructure Access (yahoo, 2022)
- BastionZero launches zero-trust cloud platform for engineering teams (Tim Keary, Venture Beat, 2022)
- Security startups to watch for 2022 (CSO staff, www.csoonline.com, 2022)
- Meet the 10 Finalists in the RSA Conference Innovation Sandbox (Karen Spiegelman, DarkReading, 2022)

The Arwen Trading Protocols

- Their goal: make cryptocurrency less scary (Scott Kirsner, Boston Globe)
- Layer 2 blockchain protocol Arwen raises $3.3M to streamline trade settlement with atomic swaps (Celia Wan, The Block)
- This Startup Is Fixing The Biggest Security Hole In Bitcoin Exchanges (Kyle Torpey, Forbes)
- Crypto Startup Wants You to Trade on Exchanges Without Trusting Them (Nikhilesh De, CoinDesk)
- Arwen Enables Self-Custody for Traders of Centralized Crypto Exchanges (Avi Mizrahi, Bitcoin.com)

Low-Resource Eclipse Attacks on Ethereums Peer-to-Peer Network

- Ethereum Was Significantly Less Secure Than Bitcoin Until Last Month (Daniel Oberhaus, Motherboard)
- Researchers Explore Eclipse Attacks on the Ethereum Blockchain (Amy Castor, Bitcoin Magazine/Nasdaq)
- Ethereum fixes serious “eclipse” flaw that could be exploited by any kid (Dan Goodin, Ars Technica)

Cryptanalysis of Curl-P and Other Attacks on the IOTA Cryptocurrency

- MIT And BU Researchers Uncover Critical Security Flaw In $2B Cryptocurrency IOTA (Amy Castor, Forbes)
- Cryptographers Urge People to Abandon IOTA After Leaked Emails (Morgen Peck, IEEE spectrum)
- FUD, inglorious FUD (Jemima Kelly, Alphaville - Financial Times)
- A $5 Billion Cryptocurrency Has Enraged Cryptographerss (Daniel Oberhaus, Jordan Pearson, Motherboard)
- Cryptographers Urge People to Abandon IOTA After Leaked Emails (Morgen Peck, IEEE Spectrum)
- IOTA: The $3.7 Billion Crypto Developers Love to Hate (Alyssa Hertig, CoinDesk)

- Blockchain bug hunters feature prominently at this year's Pwnie Awards (David Canellis, TheNextWeb)

Atomically trading with roger: Gambling on the success of a hardfork

- Gambling on a Hard Fork: Will Roger Ver Take up a High-Stakes Bitcoin Wager? (Amy Castor, CoinDesk)

An Empirical Analysis of Traceability in the Monero Blockchain

- The Dark Web's Favorite Currency is Less Untraceable Than it Seems (Andy Greenberg, Wired Magazine)
- Cryptojacker's choice coin Monero might be trackable (Chris Burns, SlashGear)
- Attacks that unmask anonymous blockchain transactions can be used against everyone who ever relied on the defective technique (Cory Doctorow, BoingBoing)

TumbleBit: An Untrusted Bitcoin-Compatible Anonymous Payment Hub

- With TumbleBit, Bitcoin Mixing May Have Found Its Winning Answer (Bitcoin Magazine/Nasdaq)
- Tumblebit - zdecentralizowany mikser bitcoinów (bitcoin.pl)
- Bitcoin Price Prediction for 2017: 6 Major Events to Impact Bitcoin Value (CoinTelegraph)
- Blockchain Surveillance is Accelerating Privacy Tool Development (Bitcoin.com)
- Investment Bank Praises Bitcoin Core Scaling Roadmap in Price Report (CoinJournal)
- Ensuring Bitcoin Fungibility in 2017 (CoinDesk)
- E021: TumbleBit, Drones, and Peaceful Protests (podcast - Bitcoin and Markets)
- TumbleBit improves Bitcoin privacy and scalability (video - KNC news)
- Meet Tumblebit: The Unlinkable Payment Hub (Bitcoin News)
- How TumbleBit Builds On CoinSwap To Improve Bitcoin Privacy And Fungibility (Cryptocoins News)
- TumbleBit Part 1: How Does This Bitcoin Privacy Proposal Compare to Monero and Zcash?
  TumbleBit Part 2: How Does This Bitcoin Privacy Improvement Compare with CoinJoin and CoinShuffle?
  TumbleBit Part 3: Potential Privacy Improvements for Bitcoin's Lightning Network (coindesk)

Eclipse Attacks on Bitcoin's Peer-to-Peer Network

- The Top 10 Cryptocurrency Research Papers of 2015 (CoinDesk)

(Blog Entry) Is PlayStation 4 Network Traffic Especially Difficult to Decrypt?

- PlayStation Network Encryption? It's Not That Good (Forbes)

(Project) Potlucky Bitcoin Payment System

- MIT Bitcoin Project Names Final Winners of $15k App Contest (CoinDesk)

Selected Blog Posts

1. The Terminal Escape Sequences Ocean is Deep and Dark: Debugging a Virtual Terminal
2. The Design of Arwen's Ethereum Escrow Smart Contract
3. Definitions of COLLECTION within the Intelligence Community and the Law.
4. A Brief History of NSA Backdoors.
5. Are IP Address Allocations Property?
6. On the NSA's Thinking Behind the Decision to Backdoor a US Cryptographic Standard.
7. A Review of William Liscum Borden's 'There Will Be No Time: The Revolution in Strategy'.
8. Is PlayStation 4 Network Traffic Especially Difficult to Decrypt?
9. A Brief Examination of Hacking Team's Crypter: core-packer.

Students Mentored

High School Students

- Shashvat Srivastava (Intern 2017)
  Monero privacy research.
  Semifinalist in 2017 Siemens Competition.
  Started as an undergraduate at MIT in 2019.
- Henry Heffan (Intern 2017)
  Monero privacy research.
  Semifinalist in 2017 Siemens Competition.
- Yuval Marcus (Intern Summer 2016)
  Ethereum and blockchain networking research.
- Hristo Stoyanov (Intern Summer 2014)
  RPKI vulnerability mitigations.
  Finalist in the International Science and Engineering Fair 2015.
  Started as an undergraduate at Stanford in Fall 2015.

Undergraduate Students

- Danny Cooper (B.A. Boston University 2014)
  RPKI research. Awarded IETF/IRTF Applied Networking Research Prize. (2014)
  Boston University Computer Science Undergraduate Research Award (2014)
  Started as a security researcher at Akamai.
- AJ Trainor (B.A. Boston University 2016)
  Research on low multiplicative complexity hash function design(Spring-Summer 2016).
  Started as a software engineer at Cambridge Blockchain.
- Alison Kendler. (B.A. Boston University 2016)
  Research on Bitcoin networking attacks and countermeasures (Summer 2015).
  Finalist for 2016 CRA undergraduate research award.
  Started as a security researcher at MITRE.

- Ann Ming Samborski (B.A. Boston University 2017)
  Research on Bitcoin micropayment networks (Spring 2016).
  Interned on a security team at Cisco (Summer 2016).
- Leen AlShenibr (B.A. Boston University 2017)
  Research on Bitcoin privacy improvements (Spring-Summer 2016).
  Presented research at Scaling Bitcoin Milan (2016).
- Daniel Gould. (B.A. Boston University 2019)
  Research on TumbleBit, 2017.
- Ezequiel Gomez. (B.A. BU expected 2019)
  Research on TumbleBit, 2017.