Ben Weintraub

Contact Information

Email: ben@weintraub.xyz — Boston, MA
GitHub: github.com/iowaguy — Website: ben-weintraub.com

Research Interests

Network security, network measurements, protocol analysis, distributed ledgers

Education

Northeastern University, Boston, MA

PhD in Computer Science **September 2019 – present**

- Expected Graduation: June 2025
- Advisor: Dr. Cristina Nita-Rotaru

Northeastern University, Boston, MA

MS in Computer Science **September 2018 – September 2019**

University of Iowa, Iowa City, IA

BS in Electrical Engineering **September 2008 – June 2013**

Professional Experience

Northeastern University, Boston, MA **May 2019 – present**
Research Assistant, Networks and Distributed Systems Security Lab

- *Security of Layer 2 Blockchain Protocols:* Measurements and evaluations of layer-two blockchain protocols including payment channels and rollups.
- *DNSSEC Optimizations:* Evaluating the feasibility of using DNSSEC for enabling clients to trust DNS resolvers.
- *Intent-based Networking Security* Studying temporal vulnerabilities in SDN.
- *Differential Fuzzing of Policy Engines* Investigating methods for testing access control policy engines.

MIT-Lincoln Laboratory, Remote **June 2023 – August 2023, June 2024 – August 2024**
Research Intern

- *Intent-based Networking:* Measuring SDN controller-switch interactions for timing related vulnerabilities.

Cloudflare, Remote **June 2022 – August 2022**
Research Intern

- *Name Resolution for IPFS:* Designed a method for using DNSSEC to enable clients to download data from public IPFS gateways without trusting the DNS resolution of the gateways themselves.

BlueTalon, Sunnyvale, CA **March 2015 – July 2018**
Software Engineer

- *Access Control:* Worked on policy enforcement proxies for Postgres, Impala, Hive, and HDFS. Built infrastructure for deployment of distributed software.

IBM, Kansas City, MO **June 2013 – March 2015**
Software Engineer

- *Distributed Databases:* Developed fault tolerance features for the Netezza Data Warehouse, and hardened code to pass government security standards.

University of Iowa, Iowa City, IA **December 2011 – June 2013**
Research Assistant

- *Digital Circuit Board Modeling:* Optimized 3D rendering algorithm for integrated circuit component thermal analysis.

Syncbak, Inc., Marion, IA **June 2011 – August 2011**
Software Engineering Intern

- *Broadcast Reliability:* Developed code for testing reliability of experimental methods for digital television signal transmission.

Publications

Ben Weintraub, Satwik Prabhu Kumble, Cristina Nita-Rotaru, and Stefanie Roos. 2024. Payout Races and Congested Channels: A Formal Analysis of Security in the Lightning Network. In Proceedings of the 2024 ACM SIGSAC Conference on Computer and Communications Security (CCS '24), October 14–18, 2024, Salt Lake City, UT, USA. ACM, New York, NY, USA, 15 pages. https://doi.org/10.1145/3658644.3670315

Ben Weintraub, Jiwon Kim, Ran Tao, Cristina Nita-Rotaru, Hamed Okhravi, Dave (Jing) Tian, and Benjamin E. Ujcich. 2024. Exploiting Temporal Vulnerabilities for Unauthorized Access in Intent-Based Networking. In Proceedings of the 2024 ACM SIGSAC Conference on Computer and Communications Security (CCS '24), October 14–18, 2024, Salt Lake City, UT, USA. ACM, New York, NY, USA, 15 pages. https://doi.org/10.1145/3658644.3670301

Christof Ferreira Torres, Albin Mamuti, **Ben Weintraub**, Cristina Nita-Rotaru, and Shweta Shinde. 2024. Rolling in the Shadows: Analyzing the Extraction of MEV Across Layer-2 Rollups. In Proceedings of the 2024 ACM SIGSAC Conference on Computer and Communications Security (CCS '24), October 14–18, 2024, Salt Lake City, UT, USA. ACM, New York, NY, USA, 15 pages. https://doi.org/10.1145/3658644.3690259

Iffat Anjum, Jessica Sokal, Hafiza Ramzah Rehman, **Ben Weintraub**, Ethan Leba, William Enck, Cristina Nita-Rotaru, & Bradley Reaves. (2023). MSNetViews: Geographically Distributed Management of Enterprise Network Security Policy. Proceedings of the 28th ACM Symposium on Access Control Models and Technologies, 121–132. https://doi.org/10.1145/3589608.3593836

Ben Weintraub, Christof Ferreira Torres, Cristina Nita-Rotaru, Radu State. (2022). A Flash(bot) in the Pan: Measuring Maximal Extractable Value in Private Pools. Proceedings of the 22nd ACM Internet Measurement Conference (IMC '22). Internet Measurement Conference, Nice, France.

Kyle Hogan, Sacha Servan-Schreiber, Zachary Newman, **Ben Weintraub**, Cristina Nita-Rotaru, Srini Devadas. ShorTor: Improving Tor Network Latency via Multi-hop Overlay Routing. IEEE Symposium on Security & Privacy 2022.

Maria Pacheco, Max von Hippel, **Ben Weintraub**, Cristina Nita-Rotaru, Dan Goldwasser. (2022). Automated Attack Synthesis by Extracting Finite State Machines from Protocol Specification Documents. IEEE Security & Privacy 2022, 18.

Ben Weintraub, Cristina Nita-Rotaru, and Stefanie Roos. (2021). Structural Attacks on Local Routing in Payment Channel Networks. Workshop on Security & Privacy on the Blockchain, 362–374. https://doi.org/10.1109/EuroSPW54576.2021.00046

Ben Goerdt, Ibrahim Ozbolat, Amer Dababneh, **Ben Weintraub**, et al. (2013, 15-21 November). Integration of a Reliability Model Within a Virtual Analysis System For Printed Circuit Boards. Paper presented at the ASME International Mechanical Engineering Congress and Exposition, San Diego, California USA

Patents

Weintraub, Benjamin L. "Consensus-based policy management." U.S. Patent No. 11,005,889. 11 May 2021.

Weintraub, Benjamin L., and Pratik Verma. "Policy management, enforcement, and audit for data security." U.S. Patent No. 10,091,212. 2 Oct. 2018.

Weintraub, B., Verma, P., Mujumdar, P., Microsoft. "Policy enforcement for search engines." U.S. Patent No. 11,146,563. 12 Oct. 2021.

Teaching

Northeastern University, Boston, MA

- CS7610: Distributed Systems, Fall 2024
- CY4930: Cybersecurity Capstone, Spring 2024
- CS4730: Distributed Systems, Spring 2023
- CS4730: Distributed Systems, Fall 2023

Service

- S&P Program Committee, 2025
- IMC Poster Program Committee, 2024
- Northeastern joint committee for planning transition of Cybersecurity and Privacy Institute to new building, 2022-2024

Talks

Exploiting Temporal Vulnerabilities for Unauthorized Access in Intent-Based Networking
ACM Computer and Communication Security, October 2024

Payout Races and Congested Channels: A Formal Analysis of Security in the Lightning Network
ACM Computer and Communication Security, October 2024

A Flash(bot) in the Pan: Measuring Maximal Extractable Value in Private Pools
Syracuse University, April 2024 MIT Digial Currency Initiative, April 2024 ACM Internet Measurement Conference, October 2022

Structural Attacks on Local Routing in Payment Channel Networks
IEEE Security & Privacy on the Blockchain, August 2021
Boston Computation Club, July 2021

How To Avoid Blockchains, and Is That Even Safe?
Carnegie Mellon University, Blockchain Fundamentals course, November 2020

Exploiting Centrality: Attacks in Payment Channel Networks with Local Routing
MIT Security Seminar, February 2021

Relevant Courses

Distributed Systems, Networking, Operating Systems, Network Security, Algorithms, Programming Languages, Data Structures, Machine Learning

Awards and Leadership

Best Paper, 2nd place, SACMAT 2023
Best Presentation, 2nd place, Northeastern University Systems Day (2023)
Best Project in Distributed Systems class as voted on by peers (2018)
VP of Membership, Toastmasters – Stanford University chapter (2015-2016)
Recipient, University of Iowa National Scholars Award (2008-2012)
Recipient, Engineering Excellence Award (2009)
Captain, Iowa Men's Ultimate Frisbee Team (2012-2013)