Ben Kaiser

Address
312 Sherrerd Hall
Princeton, NJ 08544

Contact
bkaiser@princeton.edu

EDUCATION

Ph.D., Computer Science — September 2018 – Present
Princeton University, Princeton, NJ
Advisor: Professor Jonathan Mayer
GPA 3.93

M.S., Computer Science — September 2013 – May 2015
Rensselaer Polytechnic Institute, Troy, NY
Advisor: Professor Ana Milanova
GPA 3.67
Activities: Group and private tutor, TA, secretary of RPISEC security group

B.S., Computer Science — September 2011 – May 2015
Rensselaer Polytechnic Institute, Troy, NY
GPA 3.67

A.S., Computer Information Systems — September 2009 – May 2011
State University of New York at Cobleskill, Cobleskill, NY
GPA 3.59

EXPERIENCE

Graduate Researcher, Center for Information Technology Policy — September 2018 – Present
Princeton University, Princeton, NJ

- Conducting interdisciplinary research into online disinformation with researchers in Sociology and Politics. Project details provided below under *Ongoing Projects*.
- Led mixed methods research on the effectiveness of interstitial disinformation warnings. Published and presented at USENIX Security.
- Developing tool to scrape websites, replay their content for offline browsing, and facilitate annotation of those websites. The tool is to be used in HCI and UX studies and released publicly.
- Presented security research results to stakeholders at FCC, Senate offices, and an industry association to spur policy action on telecom security.
- Mentoring undergraduate and Master's researchers.
- Organizing weekly Work-in-Progress talk series.

Associate Technical Staff, Secure Resilient Systems and Technologies Group — June 2015 – August 2018
MIT Lincoln Laboratory, Lexington, MA

- As principal investigator, led a project to design and implement a formally verified, correct-by-construction secure software update tool for satellites. Delivered prototype tool to Air Force sponsor.
- Designed and implemented a decentralized cryptographic access control scheme to be used for cloud data security in the Department of Defense.
- Participated in a massive multi-stakeholder process developing an architecture design and requirements for a holistic security architecture to be deployed to 400+ Federal agencies.
- Surveyed over 100 analysis and research papers to systematize viable applications of blockchain technology for the Department of Defense.

Undergraduate Research Assistant September 2013 – May 2015
Rensselaer Polytechnic Institute, Troy, NY

- Developed a formal framework for reasoning about binary protection and program analysis. Proved impossibility of perfect binary obfuscation against program analysts. Published one paper at LATINCRYPT; published and presented a second at RAID.

PROJECTS

In Progress

- **B. Kaiser**, S. Sanovich, J. Mayer, A. Guess. Labeling Online Disinformation: Experts vs. Crowdworkers. Presented preliminary work at American Political Science Association 2021 Annual Meeting (APSA 2021).

  We aim to evaluate whether crowdworkers can efficiently and reliably classify news and disinformation websites using low-level features, and to establish which features correlate with experts' credibility assessments. Participants will use a custom-built annotation platform to browse and label normalized, recorded snapshots of over 3,000 news and disinformation websites.

- **B. Kaiser**, A. Kohlbrenner, and J. Mayer. Measuring Online News and Disinformation at Scale.

  In a large scale, browser-based naturalistic field experiment, we will measure exposure to and engagement with known sources of news and disinformation across the internet. Using minimized, anonymized browsing data contributed by participants, we will examine the pathways of exposures, visits, and social media shares for over 10,000 news and disinformation websites.

Peer Reviewed

- **B. Kaiser**, J. Wei, E. Lucherini, K. Lee, J. N. Matias, and J. Mayer (2021). Adapting Security Warnings to Counter Online Disinformation. 30th USENIX Security Symposium (SEC 2021).
- A. Hounsel, J. Holland, **B. Kaiser**, K. Borgolte, N. Feamster, and J. Mayer (2020). Identifying Disinformation Websites Using Infrastructure Features. 10th USENIX Workshop on Free and Open Communications on the Internet (FOCI 20).
- K. Lee, **B. Kaiser**, A. Narayanan, and J. Mayer (2020). An Empirical Study of Wireless Carrier Authentication for SIM Swaps. 16th Symposium on Usable Privacy and Security (SOUPS 2020).
- S. Ruoti, **B. Kaiser**, A. Yerukhimovich, J. Clark, and R. Cunningham (2019). Blockchain Technology: What Is It Good for? ACM Queue, Volume 17 Issue 5, December 2019.
- J. Blackthorne, **B. Kaiser**, B. Fuller, and B. Yener (2017). Environmental Authentication in Malware. 6th International Conference on Cryptology and Information Security in Latin America (LATINCRYPT 2017).
- J. Blackthorne, **B. Kaiser**, and B. Yener (2016). A Formal Framework for Environmentally Sensitive Malware. 19th International Symposium on Research in Attacks, Intrusions, and Defenses (RAID 2016).
- V. Gadepally, B. Hancock, **B. Kaiser**, J. Kepner, P. Michaleas, M. Varia, and A. Yerukhimovich, Computing on Masked Data to Improve the Security of Big Data (2015). 15th IEEE International Symposium on Technologies for Homeland Security (HST 2015).

Other Published Work

- **B. Kaiser**, J. Mayer, and J. N. Matias (2021). Warnings That Work: Combating Misinformation Without Deplatforming. Lawfare Blog.
- **B. Kaiser**, M. Jurado, and A. Ledger (2018). The Looming Threat of China: An Analysis of Chinese Influence on Bitcoin. arXiv preprint arXiv:1810.02466.

- G. Itkis, **B. Kaiser**, J. Coll, W. Smith, and R. Cunningham, Charting a Security Landscape in the Clouds: Data Protection and Collaboration in Cloud Storage. Technical Report 1210, MIT Lincoln Laboratory, 2016.
- **B. Kaiser** (2015). A Context-Sensitive Security Type System for Java (Master's Thesis). Available from ProQuest Dissertations and Theses database (UMI No. 1590111).

Prepublication

- T. Braje, A. Lee, A. Wagner, **B. Kaiser**, D. Park, M. Kalke, R. Cunningham, and A. Chlipala. Adversary Safety by Construction in a Language of Cryptographic Protocols. Preparing for submission to USENIX SEC 2022.

  We present the design and implementation of an executable protocol language that permits drastically simplified model checking for security properties. Our key insight is *abstracting away* adversary interference into safety rules, akin to type safety checks in other languages. The tool is implemented as a library within the Coq theorem prover.

TALKS AND PRESENTATIONS

See `https://benkaiser.org` for slides and recordings of public talks.

- Adapting Security Warnings to Counter Online Disinformation (2021). 30th USENIX Security Symposium (SEC).
- Labeling Online Disinformation: Experts vs. Crowdworkers (2020). American Political Science Association 2021 Annual Meeting (APSA 2021).
- Vulnerabilities in SIM Swap Authentication (2019). Presented to members of the Cellular Telecommunications and Internet Association (CTIA).
- Analyzing China's Influence over Bitcoin (2018). Cryptoeconomics Security Conference (CESC).
- Formally Verified Software Updates for Aircraft and Satellites (2017). New England Systems Verification Day (SVD).
- A Cryptographic Framework for Decentralized Access Control (2016). Volpe Cybersecurity Conference & Expo.
- A Formal Framework for Environmentally Sensitive Malware (2016). 19th International Symposium on Research in Attacks, Intrusions and Defenses (RAID).

VOLUNTEER

- Co-founded CodeCreative, a free summer program teaching basic computer science skills to students from underserved schools in Boston. Developed a curriculum from scratch, led weekly lessons, and mentored students through two 8-week sessions.
- Taught topics in theoretical cryptography to gifted high school students at LLCipher, a summer program coordinated by MIT Lincoln Laboratory.
- Taught information security fundamentals to the STEM club at Emma Willard, a private high school for girls in Troy, NY.