Eric Wustrow

Assistant Professor
University of Colorado Boulder
Electrical, Computer, and Energy Engineering
425 UCB · Boulder, CO 80309

Web: https://ericw.us/trow
Email: ewust@colorado.edu
Phone: 734.330.8702

Appointments

University of Colorado Boulder 2016-present
Assistant Professor of Electrical, Computer, and Energy Engineering (ECEE)

Education

University of Michigan
Ph.D. in Computer Science, November 2015
Advisor: J. Alex Halderman

University of Michigan
B.S.E. in Computer Engineering, May 2010

Research

My research focuses on **computer security** from a systems perspective. Much of my work focuses on network security and censorship resistance. I have **created and deployed censorship circumvention systems** that get around Internet censorship in countries like Iran and China, studied new ways that governments block circumvention tools, and built tools to combat new censorship methods. Beyond censorship, I also work on Internet protocol security, architecture security, and cryptocurrencies.

Publications

A Global Measurement of Routing Loops on the Internet
Abdulrahman Alaraj*, Kevin Bock, Dave Levin, Eric Wustrow
To appear in *Passive and Active Measurement Conference*
(**PAM 2023**), March 2023. Acceptance Rate: 34% (27/80)

Chasing Shadows: A security analysis of the ShadowTLS proxy
Gaukas Wang*, Anonymous, Jackson Sippe*, Hai Chi, Eric Wustrow
To appear in *Workshop on Free and Open Communications on the Internet*
(**FOCI 2023**), March 2023.
Acceptance rate: 64% (7/11)

Where have all the paragraphs gone? Detecting and Exposing Censorship in Chinese Translation
Mizhang Streisand, Eric Wustrow, Amir Houmansadr
To appear in *Workshop on Free and Open Communications on the Internet*
(**FOCI 2023**), March 2023.
Acceptance rate: 64% (7/11)

* denotes University of Colorado graduate student

Open to a fault: On the passive compromise of TLS keys via transient errors
George Sullivan, Jackson Sippe*, Nadia Heninger, Eric Wustrow
In Proc. 31st USENIX Security Symposium
(**USENIX Security 2022**), August 2022.

Throttling Twitter: An Emerging Censorship Technique in Russia
Diwen Xue, Reethika Ramesh, ValdikSS, Leonid Evdokimov, Andrey Viktorov, Arham Jain, Eric Wustrow, Simone Basso, and Roya Ensafi
In *Proc. of the 2021 Internet Measurement Conference*
(**IMC 2021**), November 2021.
Acceptance rate: 28% (54/196)

Weaponizing Middleboxes for TCP Reflected Amplification
Kevin Bock, Abdulrahman Alaraj*, Yair Fax, Kyle Hurley, Eric Wustrow, and Dave Levin
In *Proc. 30th USENIX Security Symposium*
(**USENIX Security 2021**), August 2021.
⋆ Awarded Distinguished Paper. ⋆ Internet Defense Prize (Third place).
Acceptance rate: 19%

Improving Signal's Sealed Sender
Ian Martiny*, Gabriel Kaptchuk, Adam Aviv, Dan Roche, and Eric Wustrow
In *Proc. of Network and Distributed System Security Symposium*
(**NDSS 2021**), February 2021.
Acceptance rate: 16%

Investigating Large Scale HTTPS Interception in Kazakhstan
Ram Sundara Raman, Leonid Evdokimov, Eric Wustrow, J. Alex Halderman, and Roya Ensafi
In *Proc. of the 2020 Internet Measurement Conference*
(**IMC 2020**), November 2020.
Acceptance rate: 25% (53/216)

HTTPT: A Probe-Resistant Proxy
Sergey Frolov*, and Eric Wustrow
In *Proc. of USENIX Workshop on Free and Open Communications on the Internet*
(**FOCI 2020**), August 2020.
Acceptance rate: 55% (11/20)

Running Refraction Networking for Real
Ben VanderSloot, Sergey Frolov*, Jack Wampler*, Sze Chuen Tan, Irv Simpson, Michalis Kallitsis, J. Alex Halderman, Nikita Borisov, and Eric Wustrow
In *Proc. on Privacy Enhacning Technologies*
(**PETS 2020**), July 2020.
Acceptance rate: 23% (78/339)

Detecting Probe-resistant Proxies
Sergey Frolov*, Jack Wampler*, and Eric Wustrow
In *Proc. of Network and Distributed System Security Symposium*

(**NDSS 2020**), February 2020.
Acceptance rate: 17% (88/506)

Conjure: Summoning Proxies from Unused Address Space
Sergey Frolov*, Jack Wampler*, Sze Chuen Tan, J. Alex Halderman, Nikita Borisov, and Eric Wustrow
In *Proc. 26th ACM Conference on Computer and Communications Security*
(**CCS 2019**), November 2019.
Acceptance rate: 16% (117/722)

This is Your President Speaking: Spoofing Alerts in 4G LTE Networks
Gyuhong Lee*, Jihoon Lee*, Jinsung Lee*, Youngbin Im*, Max Hollingsworth*, Eric Wustrow, Dirk Grunwald, and Sangtae Ha
In *Proc. of the 17th ACM International Conference on Mobile Systems, Applications and Services*
(**MobiSys 2019**), July 2019.
⋆ **Awarded Best Paper.**
Acceptance rate: 23% (40/172)

ExSpectre: Hiding Malware in Speculative Execution
Jack Wampler*, Ian Martiny*, and Eric Wustrow
In *Proc. of Network and Distributed System Security Symposium*
(**NDSS 2019**), February 2019.
Acceptance rate: 17% (89/521)

The use of TLS in Censorship Circumvention
Sergey Frolov* and Eric Wustrow
In *Proc. of Network and Distributed System Security Symposium*
(**NDSS 2019**), February 2019.
Acceptance rate: 17% (89/521)

Breaking the Trust Dependence on Third Party Processes for Reconfigurable Secure Hardware
Aimee Coughlin*, Greg Cusack*, Jack Wampler*, Eric Keller, and Eric Wustrow
In *Proc. 27th ACM/SIGDA International Symposium on Field-Programmable Gate Arrays*
(**FPGA 2019**), February 2019.

The Proof is in the Pudding - Proofs of Work for Solving Discrete Logarithms (Short paper)
Marcella Hastings, Nadia Heninger, and Eric Wustrow
In *Proc. 23rd Intl. Conference on Financial Cryptography and Data Security*
(**FC 2019**), February 2019.
Acceptance rate: 22% (40/178)

Proof-of-Censorship: Enabling Centralized Censorship-resistant Content Providers
Ian Martiny*, Ian Miers, and Eric Wustrow

In *Proc. 22nd Intl. Conference on Financial Cryptography and Data Security* (**FC 2018**), February 2018.
Acceptance rate: 26% (29/109)

Initial Measurements of the Cuban Street Network (Short paper)
Eduardo E P Pujol, Will Scott, Eric Wustrow, J Alex Halderman
In *Proc. of the 2017 Internet Measurement Conference* (**IMC 2017**), November 2017.
Acceptance rate: 23% (42/179)

An ISP-scale deployment of TapDance
Sergey Frolov*, Fred Douglas, Will Scott, Allison McDonald, Benjamin VanderSloot, Rod Hynes, Adam Kruger, Michalis Kallitsis, David G Robinson, Steve Schultze, Nikita Borisov, Alex Halderman, and Eric Wustrow
In *Proc. of USENIX Workshop on Free and Open Communications on the Internet* (**FOCI 2017**), August 2017.
Acceptance rate: 55% (10/18)

Trusted click: Overcoming security issues of NFV in the cloud
Michael Coughlin*, Eric Keller, and Eric Wustrow
In *Proc. of the ACM International Workshop on Security in Software Defined Networks & Network Function Virtualization* (**SDN-NFVSec**), March 2017.
⋆ **Awarded Best Paper.**

DDoSCoin: Cryptocurrency with a Malicious Proof-of-Work
Eric Wustrow, and Benjamin VanderSloot
In *Proc. of the 10th USENIX Workshop on Offensive Technologies* (**WOOT 2016**), August 2016.
Acceptance rate: 47% (21/44)

Imperfect Forward Secrecy: How Diffie-Hellman Fails in Practice
David Adrian, Karthikeyan Bhargavan, Zakir Durumeric, Pierrick Gaudry, Matthew Green, J. Alex Halderman, Nadia Heninger, Drew Springall, Emmanuel Thomé, Luke Valenta, Benjamin VanderSloot, Eric Wustrow, Santiago Zanella-Béguelink, and Paul Zimmermann
In *Proc. 22nd ACM Conference on Computer and Communications Security* (**CCS 2015**), October 2015.
⋆ **Awarded Best Paper.**
Acceptance rate: 20% (128/646)

Replication Prohibited: Attacking Restricted Keyways with 3D Printing
Ben Burgess, Eric Wustrow, and J. Alex Halderman
In *Proc. of the 9th USENIX Workshop on Offensive Technologies* (**WOOT 2015**), August 2015.
Acceptance rate: 35% (20/57)

Security Analysis of a Full-Body Scanner
Keaton Mowery, Eric Wustrow, Tom Wypych, Corey Singleton, Chris Comfort, Eric Rescorla, Stephen Checkoway, J. Alex Halderman, and Hovav Shacham

In *Proc. 23rd USENIX Security Symposium*
(**USENIX Security 2014**), August 2014.
Acceptance rate: 19% (67/350)

TapDance: End-to-Middle Anticensorship without Flow Blocking
Eric Wustrow, Colleen M. Swanson, and J. Alex Halderman
In *Proc. 23rd USENIX Security Symposium*
(**USENIX Security 2014**), August 2014.
Acceptance rate: 19% (67/350)

Elliptic Curve Cryptography in Practice
Joppe W. Bos, J. Alex Halderman, Nadia Heninger, Jonathan Moore, Michael Naehrig, and Eric Wustrow
In *Proc. 18th Intl. Conference on Financial Cryptography and Data Security*
(**FC 2014**), March 2014.
Acceptance rate: 22% (31/138)

ZMap: Fast Internet-wide Scanning and its Security Applications
Zakir Durumeric, Eric Wustrow, and J. Alex Halderman
In *Proc. 22nd USENIX Security Symposium*
(**USENIX Security 2013**), August 2013.
Acceptance rate: 16% (45/277)

CAge: Taming Certificate Authorities by Inferring Restricted Scopes
James Kasten, Eric Wustrow, and J. Alex Halderman
In *Proc. 17th Intl. Conference on Financial Cryptography and Data Security*
(**FC 2013**), April 2013.

Mining Your Ps and Qs: Widespread Weak Keys In Network Devices
Nadia Heninger, Zakir Durumeric, Eric Wustrow, and J. Alex Halderman
In *Proc. 21st USENIX Security Symposium*
(**USENIX Security 2012**), August 2012.
⋆ **Awarded Best Paper.**
Acceptance rate: 19% (43/222)

Attacking the Washington, D.C. Internet Voting System
Scott Wolchok, Eric Wustrow, Dawn Isabel, and J. Alex Halderman
In *Proc. 16th Financial Cryptography and Data Security*
(**FC 2012**), February 2012.
Acceptance rate: 26% (33/88)

Telex: Anticensorship in the Network Infrastructure
Eric Wustrow, Scott Wolchok, Ian Goldberg and J. Alex Halderman
In *Proc. 20th USENIX Security Symposium*
(**USENIX Security 2011**), August 2011.
⋆ **PET Award Runner-up.**
Acceptance rate: 17% (35/204)

Internet Background Radiation Revisited
Eric Wustrow, Manish Karir, Michael Bailey, Farnam Jahanian and

Geoff Houston
In *Proc. 10th Internet Measurement Conference*
(**IMC 2010**), November 2010.
Acceptance rate: 22% (47/211)

Security Analysis of India's Electronic Voting Machines
Scott Wolchok, Eric Wustrow, J. Alex Halderman, Hari K. Prasad, Arun Kankipati, Sai Krishna Sakhamuri, Vasavya Yagati, and Rop Gonggrijp
In *Proc. 17th ACM Conference on Computer and Communications Security*
(**CCS 2010**), October 2010.
⋆ **Highest Rated Submission.**
Acceptance rate: 17% (55/320)

PE-ARP: Port Enhanced ARP for IPv4 Address Sharing
Manish Karir, Eric Wustrow, Jim Rees
Merit Networks Technical Report, July 2009.

Broader Impact

TLS fingerprints in Censorship Circumvention (2018)
In this ongoing study, we collect real-world Internet traffic and compare the TLS "fingerprints" of censorship circumvention tools to real-world implementations. This is useful for finding and fixing tools at risk of being blocked by censors, and helped guide design of our purpose-built library (uTLS) for mimicking TLS implementations.

Refraction Networking (2018-)
We have deployed a fundamentally new form of censorship circumvention tool that places proxies in the middle of the network, at Internet service providers (ISPs) outside censoring countries. We partnered with university and research ISPs, as well as a popular censorship circumvention tool, and are currently providing ongoing Internet access to tens of thousands of users in censored regions.

Analysis of a Full Body Scanner (2014)
We revealed that X-ray backscatter full-body scanners previously used in airports were insufficient to detect the non-metallic threats they were specifically intended to find. This work raised serious questions about TSA's procedures for purchasing and deploying security technologies.

ZMap Internet-Wide Scanner (2013)
ZMap is an open-source, Internet-wide network scanner tool that is able to probe the entire IPv4 address space in under 45 minutes, over 1000 times faster than previous approaches. Now a major open-source project, it has been adopted widely by researchers performing Internet security measurement.

Detection of Widespread Weak Keys in Network Devices (2012)
By scanning the Internet for TLS and SSH hosts, we discovered that millions of embedded networked devices had generated weak cryptographic keys using insufficient entropy sources. We disclosed vulnerabilities to more than 60 network device makers and spawned major changes to the Linux kernel's random

number generator.

Telex Anticensorship System (2011)
Telex is a fundamentally new form of censorship circumvention that places proxies in the middle of the network, at Internet service providers (ISPs) outside censoring countries. This makes them difficult for censors to block without blocking large amounts of unrelated traffic. I'm now working with a large ISP to deploy a Telex testbed.

Analysis of India's E-Voting System (2010)
We demonstrated low-tech attacks that could compromise India's nation-wide electronic voting machines, showing that the system was not tamperproof as the government claimed. As a result, India is working to deploy new machines that add a paper audit trail, changing how the country votes.

Funding

CAREER: Combating Censorship from within the Network
Source: NSF
Award Amount: $569,911 (PI)
05/01/2022 – 04/31/2027

EAGER: SaTC-EDU: Integrating Cybersecurity into Artificial Intelligence Education
Source: NSF
Award Amount: $297,000 (co-PI)
05/01/2021 – 04/31/2023

Facilitating and Supporting Transport protocols That Result in Advanced Circumvention Capabilities (FAST TRACC)
Source: Psiphon, Inc. Award Amount: $128,500 (co-PI)
08/01/2021 – 7/31/2023

Studying the Impact of IPv6 on Information Controls and Censorship Circumvention
Source: NSF
Award Amount: $399,923 (PI; total award: $1,206,509)
10/01/2020 – 09/31/2024

Refraction Networking Operationalization (ReNO)
Source: Psiphon, Inc.
Award Amount: $200,000 (co-PI)
10/01/2020 – 08/01/2022

SDR LTE Network Testbed and RESPONS
Source: Public Saftey Communications Research (PSCR) Division - NIST
Award Amount: $1,502,796 (co-PI)
06/01/2017 – 05/31/2020

Decoy Routing: Internet Freedom in the Network's Core
Source: United States Department of State
Award Amount: $485,696 (co-PI; total award: $4,000,026)

04/01/2016 – 09/31/2019

Honors and Awards

Distinguished Paper of USENIX Security 2021 for "Weaponizing Middleboxes for TCP Reflected Amplification."

USENIX/Facebook Internet Defense Prize 2021 (Third Place) for "Weaponizing Middleboxes for TCP Reflected Amplification." ($40,000 Prize)

Holland Teaching Excellence Award 2021 ($2,000 Prize)

Best Paper of Mobisys 2019 for "This is Your President Speaking: Spoofing Alerts in 4G LTE Networks."

Best Paper of CCS 2015 for "Imperfect Forward Secrecy: How Diffie-Hellman Fails in Practice."

Best Paper of USENIX Security 2012 for "Mining Your Ps and Qs: Detection of Widespread Weak Keys in Network Devices."

Runner-up for 2012 PET Award for Outstanding Research in Privacy Enhancing Technologies for "Telex: Anticensorship in the Network Infrastructure."

NSF Graduate Research Fellowship for research in combating Internet censorship by state-level actors (2011-2015).

OpenITP Fellowship at the New American Foundation for research in the area of Internet Freedom and anticensorship (2013–14).

Invited Talks and Panels

Censorship Circumvention
University of Colorado Technology, Cybersecurity, and Policy (TCP) seminar, January 2021

Refraction Networking: Deploying next-generation censorship circumvention
RightsCon (Tunis), June 2019

Panel: Technologist Reactions and Perspectives
The Legal Pitfalls of Ethical Hacking - Silicon Flatirons (Denver), December 2018

Understanding Cryptocurrencies
Association of Certified Anti-Money Laundering Specialists (ACAMS) Colorado Chapter (Denver), June 2018

Deploying Anticensorship in the Network
CyLab (CMU, Pittsburgh), March 2018
SUMIT 2017 (Ann Arbor), October 2017

Panel: Censorship Circumvention, From Academia to Practice
Annual Computer Security Applications Conference (ACSAC - Los Angeles), December 2016

Replication Prohibited: 3D Printed key attacks
32nd Chaos Communication Congress (Hamburg), December 2015

Security Analysis of a Full-Body Scanner
31st Chaos Communication Congress (Hamburg), December 2014

Anticensorship in the Network Infrastructure
RIPE 68 (Warsaw), May 2014

Finding Whom to Blame: Network Tools
Michigan Hackers Tech Talk (Ann Arbor), October 2012

Telex: Anticensorshp in the Network Infrastructure
Boston Freedom in Online Communication, March 2013
RightsCon Circumvention Tech Summit (Rio de Janeiro), May 2012
NANOG 54 (San Diego), February 2012

Professional Service

Department:
Cybersecurity Faculty Search Committee 2021-2022
Curriculum Committee 2020-2022
Computer Engineering Faculty Search Committee 2019-2020
Chair Search Committee 2018-2019
Graduate Committee 2018-2019
Big Data / Machine Learning / Security Faculty Search Committee 2017-2018
Computer Science Faculty Search Committee 2016-2017
Computer Engineering Faculty Search Committee 2016-2017
Graduate Committee 2015-2016

Program committee member:
Internet Measurement Conference (IMC) 2019, 2020, 2022
USENIX Security Symposium 2018, 2019, 2021, 2022
Financial Cryptography (FC) 2017, 2018, 2019, 2020
TheWebConf (formerly WWW) 2017, 2019
Research in Attacks, Intrusions and Defenses (RAID) 2018
USENIX Workshop on Free and Open Communications on the Internet (FOCI) 2013, 2016, 2018, 2020.

External reviewer:
USENIX Security Symposium 2014, ACM Conference on Computer and Communications Security (CCS) 2012–15, ACM Internet Measurement Conference (IMC) 2015, IEEE/ACM Transactions on Networking 2012.

Co-Chair:
Free and Open Communications on the Internet (FOCI) 2021.

PhD Students

Sergey Frolov (graduated 2020; Google)
Ian Martiny (graduated 2022; Facebook)

Jack Wampler (expected graduation 2023)
Abdulrahman Alaraj
Jackson Sippe
Gaukas Wang

Teaching

ECEN 2350: Digital Logic (Spring 2022, Spring 2023) *ECEN 4133: Computer Security Fundamentals* (Spring 2020, Spring 20201, Fall 2022)
ECEN 5032: Cryptocurrency Security (Spring 2019)
ECEN 3350: Programming Digital Systems (Fall 2018, Fall 2019, Fall 2020)
ECEN 5003: Censorship Circumvention (Fall 2017)
ECEN 5032: Introduction to Computer Security (Fall 2016, Spring 2017, Spring 2018)
ECEN 5014: Computer Security and Privacy (Spring 2016)
EECS 388: Introduction to Computer Security (U. Michigan co-instructor, Spring 2015)