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

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. My work has spanned censorship resistance, Internet protocol security, and embedded systems security.

I have exposed vulnerabilities in insecure electronic voting systems in the U.S. and abroad, developed detection techniques that uncovered weaknesses in widespread cryptographic protocol implementations, and created systems for circumventing large-scale Internet censorship in countries such as Iran and China.

Publications

DDoSCoin: Cryptocurrency with a Malicious Proof-of-Work
Eric Wustrow, 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

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.

Honors and Awards

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

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

Program committee member: USENIX Workshop on Free and Open Communications on the Internet (FOCI) 2013, 2016.

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.

Teaching

ECEN 5032: Introduction to Computer Security (2016)

ECEN 5014: Computer Security and Privacy (2016)

EECS 388: Introduction to Computer Security (2015)
Co-instructor of undergraduate security course, with Professor Z. Morley Mao. Responsible for teaching half of lecture sections and developing curriculum.

EECS 588: Computer and Network Security (2011–2014)
Served as teaching assistant, guest lectured, and advised course project groups.

Camp CAEN: Computer programming summer camp (2008)
Taught middle- and high-school students HTML, CSS, Javascript, and Java.

Relevant Internships

Square, Inc. — Software Security Intern (2014)
Implemented new secure channel for next-generation credit card reader.

Qualcomm — Software Intern (2010)
Worked with CDMA Technologies team testing LTE software functionality.

Merit Networks — Network Engineering Intern (2009)
Modified Linux kernel to support new IPv4 sharing concepts.

Radio Aurora Explorer (RAX) Satellite (2009)
Designed hardware and software for orbital experiments.