

David Adrian

Contact Information

Ann Arbor, MI 48109
(650) 265-1193

davidcadrian@gmail.com
<https://dadrian.io>
[@dadrian](https://github.com/dadrian)

Education

University of Michigan, Ann Arbor, MI

PhD, Computer Science

Expected 2020

- ADVISOR: J. Alex Halderman
- RESEARCH FOCUS: Computer Security

Masters of Science in Engineering, Computer Science

Class of 2016

Bachelors of Science in Engineering, Computer Science

Class of 2014

- MINOR: Mathematics

Research Experience

Research Assistant, with Professor J. Alex Halderman

2013 - Present

- Computer security and Internet measurement research, concentrating on using global perspectives to gain insight into networks and cryptography.
- Created and maintain ZGrab, ZCrypto, and ZMap, open-source tools for high-speed Internet-wide measurement (available on GitHub).
- Released Censys, a search engine for Internet-wide measurement data.
- Codiscovered the Logjam and DROWN attacks on TLS.

Whisper Project, with Professor Robert P. Dick

2011 - 2013

- Released MANES, an Android prototyping framework for mobile ad-hoc networks
- Released Shout, a user-facing censorship-resistant communication application built using MANES

Work Experience

Cofounder and Principal Engineer, ZCorp/Censys

2017 - Present

- Cofounded a startup company to commercialize <https://censys.io>.

Software Engineering Intern, Google Chrome Security

Summer 2016

- Worked on the Chrome TLS and X.509 stack
- Implemented OCSP Expect-Staple in order to measure the feasibility of OCSP Must-Staple.

Software Engineering Intern, Duo Security

Summer 2013

- Two-factor authentication-as-a-service, using mobile phones as the second authentication factor and push notifications for login approval.
- Grew various Python backend subsystems to support new features; handled all bugs, feature requests, and security considerations for the Duo Unix client.
- Wrote a patch for OpenSSH to securely allow third-party authentication plugins.

Teaching Experience

Instructional Aide, EECS 280: Programming and Data Structures

Fall 2013

Instructional Aide, EECS 281: Data Structures and Algorithms

Winter 2014

Graduate Student Instructor, EECS 588: Computer Security

Winter 2015

Graduate Student Instructor, EECS 388: Intro to Computer Security

Fall 2015

Lecturer, EECS 388: Intro to Computer Security

Fall 2016

Computer Skills

Languages: C, C++, Go, Java, Javascript, Python, Rust

Platforms/Frameworks: Android, Celery, Node.js, OpenGL, POSIX, Pyramid, React, Tornado/Cyclone/Twisted, Unity3D

Datastores: Elasticsearch, Kafka, MySQL, MongoDB, Postgres, Redis, RocksDB

Infrastructure: Google Cloud, Grafana, Prometheus, Salt

**Conference
Publications**

Measuring small subgroup attacks against Diffie-Hellman

Luke Valenta, David Adrian, Antonio Sanso, Shaanan Cohney, Joshua Fried,
Marcella Hastings, J. Alex Halderman, and Nadia Heninger.
Proc. 24th Network NDSS Symposium (NDSS 17), February 2017.

An Internet-Wide View of ICS Devices

Ariana Mirian, Zane Ma, David Adrian, Matthew Tischer, Thasphon Chuenchujit,
Tim Yardley, Robin Bertheier, Josh Mason, Zakir Durumeric, J. Alex
Halderman, and Michael Bailey.
14th IEEE Conference on Privacy, Security, and Trust (PST 17), December 2016.

DROWN: Breaking TLS Using SSLv2

Nimrod Aviran, Sebastian Schinzel, Jura Somorovsky, Nadia Heninger, Maik Dankel,
Jens Steube, Luke Valenta, David Adrian, J. Alex Halderman, Viktor Dukhovni,
Emilia Käsper, Shaanan Cohney, Susanne Engels, Christof Paar, and Yuval
Shavitt
Proc. 25th USENIX Security Symposium, August 2016.

**Neither Snow Nor Rain Nor MITM. . . An Empirical Analysis of Email De-
livery Security**

Zakir Durumeric, David Adrian, Ariana Mirian, James Kasten, Kurt Thomas,
Vijay Eranti, Nicholas Lidzborski, Elie Bursztein, Michael Bailey, and J. Alex
Halderman
Proc. 15th ACM Internet Measurement Conference (IMC 15), October 2015.

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-Béguelin and Paul Zimmermann.
*Proc. 22nd ACM Conference on Computer and Communications Security
(CCS 15), October 2015.*

Best Paper Award!

A Search-Engine Backed by Internet-Wide Scanning

Zakir Durumeric, David Adrian, Ariana Mirian, Michael Bailey, and J. Alex
Halderman
*Proc. 22nd ACM Conference on Computer and Communications Security
(CCS 15), October 2015.*

**Performance and Energy Consumption Analysis of a Delay-Tolerant Net-
work for Censorship-Resistant Communication**

Yue Liu, David R. Bild, David Adrian, Gulshan Singh, Robert P. Dick,
Dan S. Wallach, and Z. Morley Mao
*Proc. ACM International Symposium on Mobile Ad Hoc Networking and Computing
2015 (MobiHoc 2015).*

The Matter of Heartbleed

Zakir Durumeric, Frank Li, James Kasten, Johanna Amann, Jethro Beekman,
Mathias Payer, Nicolas Weaver, David Adrian, Vern Paxson, Michael Bailey,
and J. Alex Halderman
Proc. 14th ACM Internet Measurement Conference (IMC '14).

Best Paper Award!

**Workshop
Publications**

Zipper ZMap: Internet-Wide Scanning at 10 Gbps

David Adrian, Zakir Durumeric, Gulshan Singh and J. Alex Halderman
8th USENIX Workshop on Offensive Technologies (WOOT '14)