

Drew Springall

Auburn University
Computer Science & Software Engineering
Assistant Professor
<https://aaspring.com>
November 14, 2022

3101H Shelby Center
Auburn, AL 36849
(334) 844 - 6660 [office]
aaspring@auburn.edu
azs0249@auburn.edu

Research Overview

My research focuses on security and privacy, with an emphasis on defending users against nation-state adversaries, the world's most powerful class of attackers. My work has helped strengthen core Internet protocols (TLS, SSH, and IPsec) and improve the security of some of the most popular applications and Internet sites. I have had experience working on security problems in academia, in industry, and in government—a diversity of perspectives that helps me spot vulnerabilities (and solutions) that are hard to see from only one vantage point.

Positions

- Auburn University Auburn, AL
Assistant Professor, Department of Computer Science and Software Engineering 2020–present
Affiliated Faculty, Auburn Cyber Research Center (ACRC) 2020–present
Research Scientist, Cyber Security Sciences Institute (CSSI) 2020–present
Investigator, Biomimetic National Security Artificial Intelligence (BONSAI) Lab 2020–present
- Google Sunnyvale, CA
Software Engineer, Production Security Team Dec. 2017 – Oct. 2019
continued in Industry Experience

Education

- Ph.D. in Computer Science and Engineering, University of Michigan Apr. 2018
Advisor: J. Alex Halderman
Thesis: *Nation-State Attackers and their Effects on Computer Security*
Committee: Peter Honeyman, Atul Prakash, Florian Schaub
- M.S. in Computer Science and Engineering, University of Michigan Dec. 2015
- B.S. in Computer Science, University of Alabama May 2013

Honors and Awards

- Best Paper Award, ACM CCS 2015
- Pwnie Award for Most Innovative Research, Black Hat USA 2015
- Highest Rated Submission, ACM CCS 2014
- NSF Graduate Research Fellowship 2013

Publications

- **The Security Impact of HTTPS Interception**
Zakir Durumeric, Zane Ma, Drew Springall, Richard Barnes, Nick Sullivan, Elie Bursztein, Michael Bailey, J. Alex Halderman, and Vern Paxson
24th Network and Distributed System Security Symposium (NDSS), Feb. 2017.
Acceptance rate: 16%, 68/423.
- **Measuring the Security Harm of TLS Crypto Shortcuts**
Drew Springall, Zakir Durumeric, and J. Alex Halderman
16th ACM Internet Measurement Conference (IMC), Nov. 2016.
Acceptance rate: 25%, 46/184.
- **FTP: The Forgotten Cloud**
Drew Springall, Zakir Durumeric, and J. Alex Halderman
IEEE/IFIP Conference on Dependable Systems and Networks (DSN), Jun. 2016.
Acceptance rate: 22%, 58/259
- **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
22nd ACM Conference on Computer and Communications Security (CCS), Oct. 2015.
Acceptance rate: 19%, 128/659
 - ★ **Best Paper Award**
 - ★ **Pwnie Award for Most Innovative Research, Blackhat USA**
 - ★ **Selected as a “Research Highlight” by *Communications of the ACM*** (Jan. 2019 issue)
- **Security Analysis of the Estonian Internet Voting System**
Drew Springall, Travis Finkenauer, Zakir Durumeric, Jason Kitcat, Harri Hursti, Margaret MacAlpine, and J. Alex Halderman
21st ACM Conference on Computer and Communications Security (CCS), Nov. 2014.
Acceptance rate: 19%, 114/585
 - ★ **Highest ranked submission**

Teaching

- **Artificial Intelligence for Security (AI4Sec)**, COMP-7800/-7806 Spring 2021
Co-taught with Dr. Daniel Tauritz
A highly-collaborative, project-based graduate-level course mimicing the R&D lifecycle to apply AI concepts and techniques to security applications through small, mixed-background teams.
- **Computer and Network Security**, COMP-5370/-6370 Fall 2020/2021/2022
A mixed graduate/undergraduate introductory course designed to explore applied cryptography, network protocols, host-based techniques, and other issues in computer security.
- **Computer Security at the Fringes**, COMP-5970/6970/6979 Spring 2020
A mixed graduate/undergraduate Special Topics course which examines computer security at the edges of scale, ability, and understanding from both the offensive and defensive perspectives.

Advising and Mentoring

- Tripp Isbell — Ph.D. (in progress)
- Jarrod Hardy — Ph.D. (in progress)
- Ginny Genge — M.S. (in progress)
- Charlie Harper — M.S. (2022) now at Sandia National Laboratories

Speaking

- **Dominion ImageCast X CVEs and Reflections on CVD for Election Systems**
DEF CON 30, Aug. 2022
- **Election Forensics (panel)**
DEF CON 30, Aug. 2022

Professional Service

- Program Committee, USENIX Security Symposium 2021, 2022
- Program Committee, USENIX Workshop on Free and Open Communications on the Internet (FOCI) 2020–2022
- External reviewer, USENIX Security Symposium 2018–2020
- External reviewer, Network and Distributed System Security Symposium (NDSS) 2018

Non-Academic Experience

- **Google — Software Engineer III**
Production Security Team Dec. 2017 – Oct. 2019
Designed and built protections against highly privileged but rogue internal actors
Administered, maintained, and migrated the internal system of record for identity management used across all production infrastructure and services
- **Google — Software Engineering Intern**
Android SafetyNet Team May 2016 – Aug. 2016
Implemented new developer-facing Android APIs to provide application developers the ability to leverage Android SafetyNet’s anti-malware efforts within their own applications
- **Hewlett Packard — Software Engineering Intern**
ESS BIOS Development Team Jan. 2011 – Nov. 2012
Developed, improved, and maintained capabilities and functionality for Proliant server BIOS and UEFI firmware applications to improve customer ease-of-use and remote management
- **United States Marine Corps — Special Intelligence Communications Technician**
Sergeant (2651) 2004 – 2009
Served in many technical billets throughout the U.S., Iraq, and Afghanistan in support of the Marine Corps, National Security Agency, and Intelligence Community with regard to installation, administration, maintenance, and repair of security computer, radio, SATCOM, and telephone networks/equipment

Personal Highlights

- Discovered, reported, and successfully completed the first CVD of a major, actively-used voting system along with J. Alex Halderman resulting in CISA ICS Advisory ICSA-22-154-01
[CVE-2022-1739](#), [CVE-2022-1740](#), [CVE-2022-1741](#), [CVE-2022-1742](#), [CVE-2022-1743](#),
[CVE-2022-1744](#), [CVE-2022-1745](#), [CVE-2022-1746](#), and [CVE-2022-1747](#)
- Helped identify and prevent a DoS vulnerability in the TLS 1.3 RFC (pre-standardization) [1, 2]
- CVE-2017-15420: Chrome/Chromium URL-bar spoofing [[report](#), [release notes](#), [related](#)]
- Contributor to ZMap and Censys Internet-wide scanning projects [[ZMap](#), [Censys](#)]
- Research presented at 31st and 32nd Chaos Communications Congress [[31C3](#), [32C3](#)]
- Research covered in many publications outside of academia [[Wall Street Journal](#), [Washington Post](#), [Ars Technica](#), [The Guardian](#), [Playboy](#), [US-CERT](#), [NIST](#), [FBI Cyber Division](#)]

Funding Secured

- [EAGER: SaTC-EDU: Transformative Educational Approaches to Meld Artificial Intelligence and Cybersecurity Mindsets](#) May 2021–Apr. 2023
National Science Foundation, Division of Graduate Education (NSF-DGE)
- [Graduate Research Fellowship Award](#) Sept. 2013–Apr. 2018
National Science Foundation (NSF)