

Drew Springall

aaspring@umich.edu

<https://aaspring.com>

Overview

I am a software engineer, academic researcher, and night/weekend tinkerer interested in improving the security and privacy of the Internet as a whole. I am currently working on Google's Production Security team to secure internal infrastructure and protect against insider threats. Before that, I received a Ph.D. in Computer Science and Engineering from the University of Michigan where I focused on analyzing highly-privileged and well-resourced attackers, such as nation-state intelligence agencies, as well as identifying and quantifying Internet-scale vulnerabilities.

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, and Florian Schaub
- M.S. in Computer Science and Engineering, University of Michigan Dec 2015
- B.S. in Computer Science, University of Alabama May 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
Proc. 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
Proc. 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
Proc. 46th 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
Proc. 22nd ACM Conference on Computer and Communications Security (CCS), Oct. 2015.
Acceptance rate: 19%, 128/659
 - ★ **Best Paper Award**
 - ★ **Pwnie for Most Innovative Research**

- **Security Analysis of the Estonian Internet Voting System**
 Drew Springall, Travis Finkenauer, Zakir Durumeric, Jason Kitcat, Harri Hursti, Margaret MacAlpine, and J. Alex Halderman
Proc. 21st ACM Conference on Computer and Communications Security (CCS), Nov. 2014.
 Acceptance rate: 19%, 114/585
 ★ **Highest ranked submission**

Work Experience

- **Google — Software Engineer** (Mountain View, CA)
 Production Security Team, Dec 2017 – Present
 - Identify, monitor, and reduce insider threats caused by over-privileged entities, cross-domain privilege interaction, and legacy organizational processes
 - Migrate and transform internal identity management infrastructure while maintaining backwards compatibility with existing APIs, clients, and workflows
 - Investigate and design new core infrastructure to defend against legitimate, but rogue, insiders
- **Google — Software Engineering Intern** (Mountain View, CA)
 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
 - Drafted public documentation and internal design documentation for Android SafetyNet APIs
- **Hewlett Packard — Software Engineering Co-op Intern** (Houston, TX)
 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
 - Created a suite of developer-centric tools allowing intelligent reporting, maintenance, updating, and collaboration of development and bug trackers
- **United States Marine Corps — Special Intelligence Communications Technician**
 Sergeant (2651), 2004 – 2009
 - Installed, administered, maintained, and repaired secure computer, radio, SATCOM, and telephone networks and equipment
 - Served in many technical billets throughout the US, Iraq, and Afghanistan in support of the Marine Corps, National Security Agency, and multinational Intelligence Community

Teaching Experience

- **Introduction to Computer Security** (University of Michigan)
 Graduate Student Instructor, EECS 388, Spring 2017
 - Taught Binary Exploitation and Control Flow Hijacking lectures
 - Led weekly recitation to reinforce lecture material with real-world examples
 - Held weekly office hours to provide assistance with concepts, projects, and homeworks
- **Introduction to Computer Security** (University of Michigan)
 Guest Lecturer, EECS 388, Fall 2017

- Taught Binary Exploitation, Control Flow Hijacking, and Government Surveillance/Post-Snowden Era lectures
- **Securing Digital Democracy** (Coursera)
Graduate Student Assistant, Fall 2013
 - Assisted in administrating and coordinating a massive, open online course that explored the security risks—and future potential—of electronic and Internet voting

Professional Service

- External reviewer, USENIX Security 2018
- External reviewer, Network and Distributed System Security Symposium (NDSS) 2018
- External reviewer, ACM Conference on Computer and Communications Security (CCS) 2017
- External reviewer, Network and Distributed System Security Symposium (NDSS) 2017
- External reviewer, USENIX Security 2016

Other Personal Highlights

- Research presented at 31st and 32nd Chaos Communications Congress [[31C3](#), [32C3](#)]
- 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](#)]
- Recipient of a 2013 National Science Foundation Graduate Research Fellowship [[NSF GRFP](#)]
- Research covered by and cited in many publications outside of academia [[The Wall Street Journal](#), [The Washington Post](#), [Ars Technica](#), [The Guardian](#), [US-CERT](#), [NIST](#), [FBI Cyber Division](#)]
- Research discussed and pictured in Playboy (fully-clothed) [[article](#)]