Drew Springall

Website: **https://aaspring.com** June 30, 2019

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.

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

- Honorable Mention for Graduate Student Instructor Award — 2017
- **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 Experience

– **Introduction to Computer Security** University of Michigan
Graduate Student Instructor, 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 homework

– **Introduction to Computer Security** University of Michigan
Guest Lecturer, Fall 2016
  – Taught "Binary Exploitation", "Control Flow Hijacking", and "Post-Snowden Era" lectures

– **Securing Digital Democracy** Coursera / University of Michigan
Graduate Student Assistant, Fall 2013
  – Assisted in administrating and coordinating a massive, open, online course (MOOC) that explored the security risks—and future potential—of electronic and Internet voting

– **New Member Onboarding** Deployable Communications Operations,
Lead Instructor, Jan. 2009 – Apr. 2009 National Security Agency
  – Trained incoming personnel on general and unit-specific equipment and processes
  – Developed course curriculum, schedule, and objectives
  – Led classroom and practical application periods of instruction

Work Experience

- **Auburn University — Assistant Professor**
  Department of Computer Science and Software Engineering, Starting Jan. 2020
- **Google — Software Engineer III**
  Production Security Team, Dec. 2017 – Present
  - Design and implement protections against highly privileged but rogue actors
  - 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
- **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
  - Team Leader for Department of Homeland Security quick-react team
  - Installed, administered, maintained, and repaired secure computer, radio, SATCOM, and telephone networks and equipment
  - Served in many technical billets throughout the U.S., Iraq, and Afghanistan in support of the Marine Corps, National Security Agency, and multinational Intelligence Community

Professional Service

- External reviewer, USENIX Security Symposium 2016, 2018, 2019
- External reviewer, Network and Distributed System Security Symposium (NDSS) 2017, 2018
- External reviewer, ACM Conference on Computer and Communications Security (CCS) 2017

Other Personal Highlights

- 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]