

Benjamin VanderSloot

Graduate Student
University of Michigan
Computer Science & Engineering
2260 Hayward Street
Ann Arbor, MI 48109

Web: <https://benvds.com>
Email: benvds@umich.edu
Phone: (269) 903-1612

Education

University of Michigan
Ph.D. in Computer Science, Expected Spring 2020
Advisor: J. Alex Halderman

University of Michigan
M.S. in Computer Science, Spring 2018

University of Michigan
B.S.E. in Computer Science, Minor in Mathematics, Spring 2015
summa cum laude

Research

My research focuses on computer security and privacy, with a focus on systems that benefit typical users. I have helped detect and evade censorship, measured geoblocking, helped uncover issues in widespread Internet protocols, and helped prevent certificate misissuance. I am also interested in answering questions about practical properties of privacy systems and understanding the concrete improvement in security with different practices.

Publications

403 Forbidden: A Global View of CDN Geoblocking

Allison McDonald, Matthew Bernhard, Luke Valenta, **Benjamin VanderSloot**, Will Scott, Nick Sullivan, J. Alex Halderman, Roya Ensafi
In *Proceedings of the ACM Internet Measurement Conference (IMC'18)*, November 2018.

Quack: Scalable Remote Measurement of Application-Layer Censorship

Benjamin VanderSloot, Allison McDonald, Will Scott, J. Alex Halderman, Roya Ensafi
In *Proceedings of the USENIX Security Symposium (Sec'18)*, July 2018.

An ISP-Scale Deployment of TapDance

Sergey Frolov, Fred Douglas, Will Scott, Allison McDonald, **Benjamin VanderSloot**, Rod Hynes, Adam Kruger, Michalis Kallitsis, David G. Robinson, Steve Schultze, Nikita Borisov, J. Alex Halderman, and Eric Wustrow
In *Proceedings of the USENIX Workshop on Free and Open Communications on the Internet (FOCI'17)*, August 2017.

A Security Analysis of Police Computer Systems

Benjamin VanderSloot, Stuart Wheaton, and J. Alex Halderman
In *Proceedings of the IEEE Annual Conference on Privacy, Security, and Trust (PST'17)* , December 2017.

Towards a Complete View of the Certificate Ecosystem

Benjamin VanderSloot, Johanna Amann, Matthew Bernhard, Zakir Durumeric, Michael Bailey, J. Alex Halderman
In *Proceedings of the ACM Internet Measurement Conference (IMC'16)* , November 2016.

DDoScoin: Cryptocurrency with a Malicious Proof-of-Work

Eric Wustrow and **Benjamin VanderSloot**
In *Proceedings of the USENIX Workshop on Offensive Technologies (WOOT'16)* , August 2016.

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 ThomÃ, Luke Valenta, **Benjamin VanderSloot**, Eric Wustrow, Santiago Zanella-Beguelin, and Paul Zimmermann
In *Proceedings of the ACM Conference on Computer and Communications Security (CCS'15)* , October 2015.
—**Best Paper Award**

A Memory Rename Table to Reduce Energy and Improve Performance

Joseph Pusdesris, **Benjamin VanderSloot**, Trevor Mudge
In *Proceedings of the ACM/IEEE International Symposium on Low Power Electronics and Design (ISLPED'14)* , August 2014.

Teaching

Teaching Philosophy

To be an effective teacher you need to provide significance beyond transactional grading.

Lecturer, Introduction to Computer Security (Winter 2018)

EECS 388, University of Michigan

One of three instructors for a 380 student course. Delivered lectures, held office hours, and deployed improvements to this long-standing course.

Graduate Student Instructor, Introduction to Computer Security (Fall 2017)

EECS 388, University of Michigan

Delivered binary exploitation and control flow integrity lectures, conducted weekly discussion sections, held office hours, and released and graded multiple projects and homeworks.

Guest Lecturer, Introduction to Computer Security (Winter 2016)

EECS 388, University of Michigan

Delivered lectures on physical security and Cyberconflict from an international policy perspective.

Guest Lecturer, Computer and Network Security (Fall 2015)

EECS 588, University of Michigan

Delivered a lecture on cryptography fundamentals to provide background for systems security

Broader Impact

New Methods for Censorship Measurement (2018)

Censored Planet is a project that monitors censorship globally using existing Internet infrastructure, without coordinating volunteers in-country. We developed a new technique to monitor application-layer censorship. The project has observed changes in censorship practices around geopolitical events.

Continuous Deployment of Anticensorship Tools (2018)

Decoy Routing techniques are a fundamentally different form of censorship circumvention that were initially developed in 2011. However, they require ISPs to deploy hardware on their network. We have an ongoing deployment in a partner ISP that provides open Internet access to users in censored countries.

Protecting a Local Police Department (2016)

We demonstrated attacks against a local police department's computer systems that could have compromised the confidentiality and integrity of criminal justice information. This was performed with the permission of the department we analyzed and all vulnerabilities were corrected..

Honors and Awards

NSF Graduate Research Fellowship, Honorable Mention (2016) for research in measuring cryptographic vulnerabilities in network traffic

Best Paper of CCS 2015 for "Imperfect Forward Secret: How Diffie-Hellman Fails in Practice"

2015 Most Innovative Research Pwnie for "Imperfect Forward Secret: How Diffie-Hellman Fails in Practice"

Rackham Merit Fellowship (2015)

Invited Talks

Censored Planet: Measuring Internet Censorship Globally and Continuously at 2018 International Conference on Cyber Security (ICCS'18), January 2018.

Professional Service

Shadow Reviewer

— ACM Internet Measurement Conference (IMC) 2018

External Reviewer

— ACM Conference on Computer and Communications Security (CCS) 2017

— Internet Society Network and Distributed System Security Symposium (NDSS) 2017

**University
Service**

Tor Exit Node Operator, May 2018 – present

Vice President and Treasurer, Computer Science and Engineering Graduate student organization, University of Michigan, May 2016 – May 2017

Dissonance Speaker Series, Founding Committee Member

Chapter President, Eta Kappa Nu (IEEE Honor Society), May 2014 – December 2014

Patents

United States Patent No. 9,471,480 for Data processing apparatus with memory rename table for mapping memory addresses to registers.

Internships

Microsoft, Windows OS Services Group — SDE Intern (2014)

Designed redundant storage layer for reliability in memcached-like service

Qualcomm Incorporated, Windows 8 Group — Software Engineer Intern (2012)

Designed a new fuzzing framework for GUI-driven applications