James D. Kasten, Jr.

1780 Broadway Street, Apt S230, Ann Arbor, MI 48105
(419) 706-6285   jdkasten@umich.edu

CURRICULUM VITAE

I am a sixth year Ph.D. student in the Computer Science and Engineering Department at the University of Michigan. My focus is on computer security with a particular interest in creating practical security solutions. Through my work, I hope to make security accessible and usable in applications for the masses. I am advised by Professor J. Alex Halderman.

EDUCATION

University of Michigan, Ann Arbor, Michigan, August 2010 – December 2015
- Ph.D. Candidate in Computer Science and Engineering
- Thesis: Server Authentication on the Past, Present, and Future Internet
- M.S. Computer Science and Engineering, May 2012
- GPA: 4.000 / 4.000
- STIET Research Fellow, 2010 – 2012

Vanderbilt University, Nashville, Tennessee, August 2006 – May 2010
- B.A. Double Major in Economics and Computer Science, *summa cum laude*
- GPA: 3.964 / 4.000
- Member of Gamma Beta Phi – National Honor and Service Society
- Computer Science Program Award, 2010

CONFERENCE PUBLICATIONS

Neither Snow Nor Rain Nor MITM... An Empirical Analysis of Mail Delivery Security
Zakir Durumeric, David Adrian, Ariana Mirian, James Kasten, Kurt Thomas, Vijay Eranti,
Nicholas Lidzborski, Elie Bursztein, Michael Bailey, J. Alex Halderman
To Appear: ACM Internet Measurement Conference (IMC'15), November 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 Internet Measurement Conference (IMC '14), Barcelona, Spain, October 2014 – **Best Paper Award***

Analysis of the HTTPS Certificate Ecosystem
Zakir Durumeric, James Kasten, Michael Bailey, and J. Alex Halderman
*Proc. 13th Internet Measurement Conference (IMC '13), Barcelona, Spain, October 2013 – **Best Paper Nomination***

CAge: Taming Certificate Authorities by Inferring Restricted Scopes
James Kasten, Eric Wustrow, J. Alex Halderman
Proc. 17th Intl. Conference on Financial Cryptography and Data Security (FC), Okinawa, Japan, April 2013

OTHER PUBLICATIONS

Automated Certificate Management Environment (ACME)
Richard Barnes, Jacob Hoffman-Andrews, James Kasten
IETF Internet-Draft, July 2015

SELECTED TALKS

Let's Encrypt: A Certificate Authority to Encrypt the Entire Web
- DEF CON, August 2015
- Yahoo Trust UnConference, April 2015

Let's Encrypt: Applications for NDN
- NDN Retreat, February 2015

CAge: Taming Certificate Authorities by Inferring Restricted Scopes
- Financial Cryptography, April 2013
- STIET Research Workshop, May 2012

Web of Trust for Android Applications
- STIET Research Workshop, May 2012

WORK EXPERIENCE

Google, Software Engineer
Mountain View, California, November 2015 – Present
- Production Security Development Team

Electronic Frontier Foundation, Consultant
San Francisco, California, November 2014 – July 2015
- Core developer of the Let's Encrypt client for the ISRG CA
- Project automatically configures and enables HTTPS for webservers with trusted certificates

Raytheon SI Government Solutions Inc., Computer Network Operations Intern
Annapolis Junction, Maryland, June 2013 – September 2013
- Designed and developed networking tools for use throughout Raytheon

TEACHING EXPERIENCE

University of Michigan, Advanced Compilers GSI, Introduction to Computer Security GSI
Ann Arbor, Michigan, Fall 2012 and Fall 2013
- Consulted on student projects and homework
- Taught multiple lectures and discussion sections
- GSI Award, Fall 2013

Vanderbilt University, Economic Statistics Recitation Leader
Nashville, Tennessee, Fall 2008
- Prepared and executed lesson plans for weekly class sections
- Answered all student inquiries and graded class projects and tests

SELECTED PRESS COVERAGE

Washington Post: Encrypting Web site traffic could become easier next year
CNET: Privacy Push Means Free Encryption for Websites
Freedom to Tinker: Let's Encrypt: Bringing HTTPS to Every Web Site
PC World: EFF, Mozilla back new certificate authority that will offer free SSL certificates
GCN: U. Michigan fronts effort to push HTTPS net security

RELEVANT GRADUATE SCHOOL PROJECTS

Rogue Wireless Access Point: Modified a router to insert trojans into all executables downloaded over HTTP
Dynamic Taint Analysis: Implemented dynamic taint analysis within LLVM
Browser Security Modes: Implemented a browser extension to change the security properties based on user-intention
Web of Trust for Applications: Designed and tested a web of trust rating system for Android applications