Michael A. Rushanan

micharu1@cs.jhu.edu, micharu123@gmail.com, michaelrushanan.org

Research Interests: systems and application security

EDUCATION

Ph.D., Computer Science, Johns Hopkins University (JHU) Information Security Institute.
2011-Present. GPA: 3.8/4.0. Advisor(s): Dr. Aviel D. Rubin.
Expected Graduation: 2016

M.S., Computer Science, Johns Hopkins University (JHU).
2009-Present. GPA: 3.8/4.0. Avisor(s): Dr. Aviel D. Rubin.
Expected Graduation: 2013

M.S., Security Informatics, Johns Hopkins University (JHU) Information Security Institute.
2013-Present. GPA: 3.74/4.0. Avisor(s): Dr. Aviel D. Rubin.
Expected Graduation: 2014

B.S., Computer Science [minor Psychology], University of Maryland Baltimore County.
2005-2009.

EXPERIENCE

Research Assistant *Johns Hopkins University* August 2011-Present
Baltimore, MD

- Experimenting with a possible control flow integrity implementation that doesn't rely on binary rewriting.
- Researching the effects of using poorly implemented SSL/TLS protocols.
- Structuring an appropriate experimental methodology for learning what library version of OpenSSL a server is running.
- Experimenting with different semi-supervised, supervised approaches to determine how to achieve the best accuracy of OpenSSL library predictions.
- Reviewing different cryptographic implementations for securely and efficiently operating over medical images.
- Developing a possible research idea that considers public health surveys and anonymity.
- Provided focused development and testing of Charm, a framework for rapidly prototyping cryptosystems.
- Designed and implemented the database abstraction and analysis framework for SSLPrint, a modular tool for crawling web and identifying OpenSSL versions.
- Collaborated with subject matter experts in the field of medical imaging and public health.

Teaching Assistant *Johns Hopkins University* January 2012-May 2013
Baltimore, MD

- Provided teaching support for: Database Systems, Modern Cryptography, and UI and Mobile Application Development.
- General responsibilities included: delivering detailed lectures; providing consistent office hours; expanding accessibility through online tools such as Piazza; grading assignments

and exams; creating assignments, and; meeting with the course professor to gauge expectations and goals.
- Attended class frequently to facilitate a relationship with students and reinforce the material as presented by the professor.

So They Can Know *Sexual Health Innovations* September 2011-Present
Baltimore, MD

- Implemented an anonymous email system using SMTP, Python, and a randomized anonymous ID method that leverages encrypted cookies for safe data storage.
- Developed a robust database backend in PostgreSQL.
- Designed and implemented an external data client that can decrypt sensitive records downloaded from the server via a PBKDF.

Course Assistant *Johns Hopkins University* August 2010-May 2011
Baltimore, MD

- Provided course support for: Security and Privacy and Network Security.
- Managed consistent office hours with respect to the unavailability of other course assistants, in addition to assignment grading and creation.

Research Program Analyst *Johns Hopkins University* May 2009-May 2011
Baltimore, MD

- Configured tooling, cross-platform support, and linked library modularity to libfenc.
- Assisted in application design of an iOS based secure medical record application.
- Developed platform-dependent installers and cryptographic encryption schemes for Charm.

Department of Defense *National Security Agency* November 2003-November 2010
Ft. Meade, MD

- Managed a closed network infrastructure to facilitate staging and release of COTS software.
- Extended and provided in-house extensions to third-party software.
- Utilized multiple web-related technologies to enable streamlined and accessible support to external agencies.
- Collaborated and co-authored survey reports as a result of data collection per stakeholder request.
- Provided mentorship to three high school workstudies and one summer intern.

PUBLICATIONS

- Charm: A Framework for Rapidly Prototyping Cryptosystems. Joseph Akinyele, Christina Garman, Ian Miers, Matthew W. Pagano, Michael Rushanan, Matthew Green, Aviel D. Rubin. To appear in Journal of Cryptographic Engineering (JCEN), 2013.

PEER REVIEWED ABSTRACTS

- Initial Uptake of STI Partner Notification Website So They Can Know. Jessica Ladd, Jenny McManus, Stephan Adelson, Charlotte Gaydos, and Michael Rushanan. In submission to ISSTDR.
- An Efficient Encryption Framework for Medical Images. James Philbin, Matthew Green, Raphael Ning, Mahmoud Ismail, Michael Rushanan. In submission to SIIM.

TECHNICAL REPORTS

- None.

GRANTS

- None.

TECHNICAL SKILLS

- **Operating Systems:** Linux/Unix, Windows, and Mac OS X.
- **Virtualization Technologies:** VirtualBox, VMware, and QEMU.
- **Programming Languages:** C/C++, some C#, Java, Python, PHP, HTML, JavaScript, BASH, and some Perl.
- **Software Development Kits and Editors:** Eclipse, Xcode, gedit, Visual Studio, and VIM.

NON-PROFIT SOFTWARE PROJECTS

- So They Can Know (STCK): Lead backend developer for STCK, a partner notification website that provides numerous services for self-education, tips on communication, and anonymous email notification. Using the web framework Django, I have implemented the anonymous notification service and database backend.

OPEN-SOURCE SOFTWARE PROJECTS

- Functional Encryption Library (libfenc): A member of the team that developed an encryption library in C for experimentation with advanced cryptographic primitives such as attribute-based encryption variants. http://code.google.com/p/libfenc.
- Charm-Crypto Framework: A member of the team that developed a new cryptographic framework for rapidly prototyping cryptosystems. http://charm-cryptoc.com.

PROFESSIONAL SOCIETIES

- President of Upsilon Pi Epsilon, JHU Chapter, 2011-Present.
- Inducted into Upsilon Pi Epsilon, Spring 2011.

AWARDS AND HONORS

- Awarded second place in the Innovate for Healthcare Challenge, 2012.

ACTIVITIES

- External Reviewer for USENIX 2011, 2012.
- Technical blogging at http://michael-rushanan.blogspot.com/.

REFERENCES

- Dr. Aviel D. Rubin (rubin@jhu.edu).
- Paul D. Martin (pmartin@pauldmartin.org).
- Jessica H. Ladd (jladd@sexualhealthinnovations.org).