Matthew Fredrikson

Computer Science Department, Institute for Software Research
Carnegie Mellon University, Pittsburgh, PA 15213 USA

Email: mfredrik@cs.cmu.edu
Web: http://mattfredrikson.com

Positions

September 2015–Present. *Assistant Professor*, Carnegie Mellon University, Pittsburgh, PA.
Computer Science Department,
Institute for Software Research,
Electrical and Computer Engineering (Courtesy).

October 2012 – February 2013. *Research Intern*. Microsoft Research, Redmond, WA.
Research in Software Engineering (RiSE) Group. *Mentor:* Benjamin Livshits.

May 2010 – August 2010. *Research Intern*. Microsoft Research, Redmond, WA.
Research in Software Engineering (RiSE) Group. *Mentor:* Benjamin Livshits.

May 2009 – August 2009. *Research Intern*. SRI International, Menlo Park, CA.
Computer Science Laboratory. *Mentor:* Phillip Porras.

May 2008 – August 2008. *Research Intern*. IBM T.J. Watson Research Center, Hawthorne, NY.
Global Security Analysis Laboratory. *Mentor:* Mihai Christodorescu.

Education

University of Wisconsin – Madison, Madison, WI.

Ph.D. in Computer Sciences, August 2015.
Advisor: Professor Somesh Jha

M.S. in Computer Sciences, December 2009.

Duquesne University, Pittsburgh, PA.

B.S. in Computer Science, May 2007

B.A. in Mathematics, May 2007.

Publications

Peer-Reviewed Articles

V. Ngo, M. Dehesa-Azuara, M. Fredrikson, and J. Hoffmann. Verifying and Synthesizing Constant-Resource Implementations with Types. In *2017 IEEE Symposium on Security & Privacy (Oakland) (to appear)*, May 2017. *Acceptance rate: 12.9% (60 of 463)*

X. Wu, M. Fredrikson, S. Jha, and J. F. Naughton. A Methodology for Formalizing Model-Inversion Attacks. Jun 2016. *Acceptance rate: 35.6% (31 of 87)*

N. Papernot, P. McDaniel, S. Jha, M. Fredrikson, Z. B. Celik, and A. Swami. The limitations of deep learning in adversarial settings. In *IEEE European Symposium on Security and Privacy*, 2016. *Acceptance rate: 19.5% (38 of 194)*

M. Fredrikson, S. Jha, and T. Ristenpart. Model inversion attacks that exploit confidence information and basic countermeasures. In *ACM Conference on Computer and Communications Security (CCS)*, 2015. *Acceptance rate: 19.8% (128 of 646)*

M. Fredrikson, E. Lantz, S. Jha, S. Lin, D. Page, and T. Ristenpart. Privacy in pharmacogenetics: An end-to-end case study of personalized warfarin dosing. In *USENIX Security*, 2014. *Acceptance rate: 19.1% (67 of 350)* **Best Paper Award**.

S. Checkoway, M. Fredrikson, R. Niederhagen, M. Green, T. Lange, T. Ristenpart, D. J. Bernstein, J. Maskiewicz, and H. Shacham. On the practical exploitability of Dual EC DRBG in TLS implementations. In *USENIX Security*, 2014. *Acceptance rate: 19.1% (67 of 350)*

M. Fredrikson and B. Livshits. Zø: An optimizing zk compiler. In *USENIX Security*, 2014. *Acceptance rate: 19.1% (67 of 350)*

D. Davidson, M. Fredrikson, and B. Livshits. MoRePriv: Mobile os support for application personalization and privacy. In *Annual Computer Security Applications Conference (ACSAC)*, 2014. *Acceptance rate: 19.9% (47 of 236)*

M. Fredrikson and S. Jha. Satisfiability modulo counting: A new approach for analyzing privacy properties. In *Joint Meeting of Computer Science Logic and Logic in Computer Science (LICS)*, 2014. *Acceptance rate: 34.9% (74 of 212)*

M. Fredrikson, R. Joiner, S. Jha, T. Reps, P. Porras, H. Saïdi, and V. Yegneswaran. Efficient runtime policy enforcement using counterexample-guided abstraction refinement. In *Computer Aided Verification (CAV)*. 2012. *Acceptance rate: 20.5% (38 of 185)*

M. Fredrikson and B. Livshits. RePriv: Re-imagining content personalization and in-browser privacy. In *IEEE Symposium on Security and Privacy (Oakland)*, 2011. *Acceptance rate: 11.1% (34 of 306)*

A. Guha, M. Fredrikson, B. Livshits, and N. Swamy. Verified security for browser extensions. In *IEEE Symposium on Security and Privacy (Oakland)*, 2011. *Acceptance rate: 11.1% (34 of 306)*

M. Fredrikson, M. Christodorescu, and S. Jha. Dynamic behavior matching: A complexity analysis and new approximation algorithms. In *23rd Annual Conference on Automated Deduction (CADE)*, 2011.

M. Fredrikson, D. Davidson, S. Jha, and B. Livshits. Towards enforceable data-driven privacy policies. In *Web 2.0 Workshop on Security and Privacy (W2SP)*, 2011.

R. Paleari, L. Martignoni, E. Passerini, D. Davidson, M. Fredrikson, J. T. Giffin, and S. Jha. Automatic generation of remediation procedures for malware infections. In *USENIX Security*, 2010. *Acceptance rate: 14.8% (30 of 202)*

M. Fredrikson, S. Jha, M. Christodorescu, R. Sailer, and X. Yan. Synthesizing near-optimal malware specifications from suspicious behaviors. In *IEEE Symposium on Security and Privacy (Oakland)*, 2010. *Acceptance rate: 10.9% (20 of 237)*

C. Chen, C. X. Lin, M. Fredrikson, M. Christodorescu, X. Yan, and J. Han. Mining graph patterns efficiently via randomized summaries. In *Conference on Very Large Data Bases (VLDB)*, 2009. *Acceptance rate: 16.7% (51 of 305)*

L. Martignoni, E. Stinson, M. Fredrikson, S. Jha, and J. C. Mitchell. A layered architecture for detecting malicious behaviors. In *Recent Advances in Intrusion Detection (RAID)*, 2008. *Acceptance rate: 25.0% (20 of 80)*

Book Chapters and Technical Reports

X. Wu, M. Fredrikson, W. Wu, S. Jha, and J. F. Naughton. Revisiting Differentially Private Regression: Lessons From Learning Theory and their Consequences. *ArXiv e-prints*, Dec 2015.

B. Schneier, M. Fredrikson, T. Kohno, and T. Ristenpart. Surreptitiously weakening cryptographic systems. Cryptology ePrint Archive, Report 2015/097, 2015.

M. Christodorescu, M. Fredrikson, S. Jha, and J. Giffin. End-to-end software diversification of internet services. In S. Jajodia, A. Ghosh, V. Swarup, C. Wang, and X. S. Wang, editors, *Moving Target Defense*, pp. 117–130. Springer New York, 2011.

M. Fredrikson, M. Christodorescu, J. Giffin, and S. Jhas. A declarative framework for intrusion analysis. In S. Jajodia, P. Liu, V. Swarup, and C. Wang, editors, *Cyber Situational Awareness*, pp. 179–200. Springer New York, 2010.

Panels and Invited Talks

Panels

Panel on *Genomic Privacy*.
Symposium on "Big Privacy": Policy Meets Data Science
Center for Predictive Computational Phenotyping (CPCP), Madison, WI, October 2015.

Panel on *De-Identification and Anonymity*.
Workshop on Privacy-by-Design
Organized by the Computing Community Consortium (CCC), Pittsburgh, PA, August 2015.

Talks

Security, Privacy, and Inference: New Approaches for Dealing with Uncertain Adversaries.
University of Pittsburgh, Pittsburgh, PA, March 2016.

Does Publishing a Predictive Model for Precision Medicine Put Patient Privacy at Risk?
Center for Predictive Computational Phenotyping, Madison, WI, October 2015.

Practical De-Identification.
CCC Privacy-by-Design Workshop, Pittsburgh, PA, August 2015.

Privacy in Pharmacogenetics: An End-to-End Case Study of Personalized Warfarin Dosing.
USENIX Annual Technical Conference "Best of the Rest" Track, Santa Clara, CA, July 2015.

Inference Attacks: Understanding Privacy in the era of "Privacy is Dead".
Purdue, December 2014.
Cornell, February 2015.
University of Chicago, February 2015.
University of Michigan, February 2015.
Duke, February 2015.
Yale, February 2015.

Princeton, February 2015.
University of Iowa, March 2015.
Northeastern, March 2015.
Johns Hopkins, March 2015.
Brown, March 2015.
University of Illinois at Urbana-Champaign, March 2015.
Rice, March 2015.
University of Texas at Austin, March 2015.
Carnegie Mellon, March 2015.
University of California, San Diego, April 2015.
University of Southern California, April 2015.
University of Utah, April 2015.
Stanford, April 2015.
University of Massachussetts, Amherst, April 2015.
Microsoft Research, April 2015.

The Technology and Impact of Recent NSA and GCHQ Revelations (with Steve Weis and Eleanor Saitta).
Computers, Freedom, and Privacy 2014, Warrenton, VA. June 2014.

Technology and Implications of the DUAL EC Random Number Generator.
Techno Activism Third Mondays, Madison, WI. June 2014.

Synthesizing Near-Optimal Malware Specifications from Suspicious Behaviors (with Somesh Jha).
Malware 2013, San Juan, Puerto Rico. October 2013.

RePriv: Re-imagining content personalization and in-browser privacy.
Google Inc., Madison, WI. January 2011.

Students Advised

Current

Gihyuk Ko, *PhD* (ECE) *(co-advised with Prof. Anupam Datta)*
Klas Leino, *PhD*
Brandon Price, *CS undergraduate*
Ryan Wagner, *PhD (co-advised with Prof. David Garlan)*
Sam Yeom, *PhD*

Teaching

15-316 (*with Prof. Jean Yang*) *Software Foundations of Security and Privacy*.
Spring 2017.
12 units.

15-414 *Bug Catching: Automated Program Verification and Testing*.
Fall 2016.
12 units.

08-602 (*with Prof. Norman Sadeh*) *Current Topics in Privacy Seminar*.
Fall 2016.
10 students, 3 units. Overall evaluation: 5.0/5 (6 responding)

15-811/18-739 (*with Prof. Limin Jia*) *Special Topics: Formal Foundations of Software Security*.
Spring 2016.
14 students, 12 units.

08-602 (*with Prof. Lorrie Cranor*) *Current Topics in Privacy Seminar*.
Fall 2015.
10 students, 3 units. Overall evaluation: 5.0/5 (6 responding)

Service

External

Consulting:
Confidentiality Expert. Centers for Disease Control and Prevention, NHANES Program. 2015

Program Chair:
Workshop on Web 2.0 Security & Privacy, 2012

General Chair:
Workshop on Web 2.0 Security & Privacy, 2013 – 2014

Poster Chair:
IEEE Symposium on Security & Privacy, 2017

Program Committee:
IEEE Symposium on Security & Privacy (Oakland) 2017
ISOC Conference on Network and Distributed System Security (NDSS) 2017
ACM Conference on Computer and Communications Security (CCS) 2016
IEEE Computer Security Foundations Symposium (CSF) 2016
ACM Conference on Programming Language Design & Implementation (PLDI) 2016
USENIX Security Symposium 2015, 2016, 2017
EAI Conference on Security and Privacy in Communication Networks (SECURECOMM) 2015
Annual Computer Security Applications Conference (ACSAC) 2013 – 2015
ACM CCS Workshop on Security and Privacy in Smartphones and Mobile Devices (SPSM) 2014
ACM Symposium on Information, Computer and Communications Security (ASIACCS) 2014
International Symposium on Engineering Secure Software and Systems (ESSoS) 2013
Foundations of Software Engineering (FSE) New Ideas Track 2013
Workshop on Web 2.0 Security & Privacy (W2SP) 2013-2014

External Review Committee:
USENIX Security Symposium, 2014

External Reviewer:
Computer Aided Verification (CAV) 2013 – 2014
ACM Conference on Computer and Communications Security (CCS) 2011 – 2014
IEEE Computer Security Foundations Symposium (CSF) 2014
Network and Distributed System Security Symposium (NDSS) 2014
Conference on Principles of Security and Trust (POST) 2014
IEEE Symposium on Security and Privacy (Oakland) 2008 – 2011, 2013

USENIX Security Symposium 2010 – 2011
European Symposium on Programming (ESOP) 2012
Financial Cryptography (FC) 2012

Journal Reviewer:
Proceedings of the National Academy of Sciences (PNAS)
Journal of Machine Learning Research (JMLR)
Journal of Computer Security (JCS)
ACM Transactions on Information and System Security (TISSEC)
International Journal of Information Security.

Internal

PhD Admissions Committee, *Computer Science Department*. 2016/2017
Corporate Partners Conference Committee, *CyLab*. Jan 2016 – Present
Speaking Skills Committee, *Computer Science Department*. Oct. 2015 – Present
Faculty Hiring Committee, *Computer Science Department*. 2015/2016
Faculty Hiring Committee, *ISR Societal Computing*. 2015/2016
PhD Admissions Committee, *ISR Societal Computing*. 2015/2016

Honors & Awards

University of Wisconsin Computer Sciences "Outstanding Graduate Student Research Award", 2015.

USENIX Security Symposium Best Paper Award, 2014.

Microsoft Research Graduate Fellowship Award, 2011-2012.

Funding

AFOSR: *Accountable Predictive Systems*.
w/ Prof. Anupam Datta (PI)
Amount: $600,000

DARPA: *Reconciling Purpose, Data Privacy, and User Preferences: A Holistic Approach to Managing Privacy*.
w/ Prof. Jason Hong (PI) and Prof. Yuvraj Agarwal (co-PI)
Amount: $2,998,896