Piotr (Peter) Mardziel

253 Dudley Oxford Rd
Dudley, MA 01571
USA

piotrm@gmail.com
http://www.cs.umd.edu/~piotrm
+1 (508)873-5439

Education

2008-2014	•	**University of Maryland**, College Park, Maryland
		Ph.D. In Computer Science (GPA: 3.8/4.0)
2005-2007	•	**Worcester Polytechnic Institute**, Worcester, Massachusetts
		M.S. In Computer Science (GPA: 3.8/4.0 overall, 4.0/4.0 in Computer Science)
2002-2005	•	**Worcester Polytechnic Institute**, Worcester, Massachusetts
		B.S. In Computer Science (GPA: 4.0/4.0)

Research/Work Experience

2010-present • **University of Maryland**, College Park, Maryland

2015-present **Faculty Research Assistant** (postdoc)

Probabilistic programming: Developing techniques and tools for probabilistic inference for models written in a programming language, with emphasis on soundness relative to security concerns. The project aims to extent the work below with richer languages and more efficient inference.

2010-2014 **Graduate Research Assistant**, supervised by Prof. Michael Hicks

Information flow in dynamic systems: I developed a model for measuring the information flow of systems with time-varying secrets against adversaries that have the ability to decide when they attack adaptively [1, 2].

Knowledge in secure multi-party computation: I developed and formalized techniques for knowledge inference to improve the efficiency of secure multi-party computation [4]. I analyzed and quantified the release of information in secure computations among multiple parties each protecting their secrets [5].

Knowledge-based security policies: I developed techniques for static analysis of information flow within programs using probabilistic abstract interpretation [6, 3].

This work included the design and implementation of a probabilistic abstract interpreter for a simple imperative language. The interpreter is composed of almost 10,000 lines of OCaml code.

Summer 2012 • **IMDEA Software Institute**, Madrid, Spain

Research intern, supervised by Boris Köpf. I worked on the expression of information flow metrics as games among competing parties as opposed to purely information theoretic quantities. This work inspired the models I later developed for information flow for dynamic secrets and allowed such them to easily take into account important aspects of real-world scenarios that are beyond the scope of simple channels.

2005-2007 • **Worcester Polytechnic Institute**, Worcester, Massachusetts

M.S. research project, supervised by Prof. Daniel Dougherty:

"Noninterference in Concurrent Game Structures": I designed a formulation of noninterference based on concurrent game structures and explored the benefits of such a formulation over existing works on noninterference with particular focus on nontransitive information flow policies. (pdf)

2004-2005 • **Worcester Polytechnic Institute**, Worcester, Massachusetts

B.S.research project, supervised by Prof. Carolina Ruiz:

"Improved Two-Dimensional Warping": I analytically and experimentally studied a polynomial time approximation algorithm for 2-dimensional warping. I described a time complexity improvement of said algorithm from $O(N^6)$ to $O(N^4)$. I developed an extension of the algorithm for 3D and potential higher-dimensional applications. (pdf)

Research/Work Experience (Continued)

2002-2004 • KIWI Computer
Software Engineer
Developed official event software for the FIRST Robotics Competition. This software was used at 29 official competitions internationally and many other unofficial and off-season events. Project involved development of GUI, database storage of scoring and match information, automated upgrades and database/web-site synchronization, software to interface with field electronics, printed reports, real-time scoring, and animated graphical displays. Used FreeBSD, MySQL, Apache, Macromedia (now Adobe) Flash / Actionscript, GTK, unix shell scripting, and Perl.

Publications

2014 [1] • Piotr Mardziel, Mário S. Alvim, and Michael Hicks. "Adversary Gain vs Defender Loss in Quantified Information Flow". In: *Workshop on Foundations of Computer Security (FCS)*. July 2014. (pdf)

[2] • Piotr Mardziel, Mario Alvim, Michael Hicks, and Michael Clarkson. "Quantifying Information Flow for Dynamic Secrets". In: *Proceedings of the IEEE Symposium on Security and Privacy (S&P)*. May 2014. (pdf)

2013 [3] • Piotr Mardziel, Stephen Magill, Michael Hicks, and Mudhakar Srivatsa. "Dynamic Enforcement of Knowledge-based Security Policies using Abstract Interpretation". In: *Journal of Computer Security* 21.4 (Jan. 2013), pp. 463–532. (pdf)

[4] • Aseem Rastogi, Piotr Mardziel, Matthew Hammer, and Michael Hicks. "Knowledge Inference for Optimizing Secure Multi-party Computation". In: *Proceedings of the ACM SIGPLAN Workshop on Programming Languages and Analysis for Security (PLAS)*. June 2013. (pdf)

2012 [5] • Piotr Mardziel, Michael Hicks, Jonathan Katz, and Mudhakar Srivatsa. "Knowledge-Oriented Secure Multiparty Computation". In: *Proceedings of the ACM SIGPLAN Workshop on Programming Languages and Analysis for Security (PLAS)*. June 2012. (pdf)

2011 [6] • Piotr Mardziel, Stephen Magill, Michael Hicks, and Mudhakar Srivatsa. "Dynamic Enforcement of Knowledge-based Security Policies". In: *Proceedings of the IEEE Computer Security Foundations Symposium (CSF)*. June 2011. (pdf)

Talks

- **Modeling, Measuring, and Limiting Adversary Knowledge**
  - presented at the Applied Communication Sciences, January 2015
  - presented for the Applied Logic and Security group at Worcester Polytechnic Institute, January 2015
  - presented at Microsoft Research, Cambridge UK, February 2015
  - presented at the JHU Applied Physics Laboratory, February 2015

- **Adversary Gain vs. Defender Loss in Quantified Information Flow**
  - presented at 2014 Workshop on Foundations of Computer Security, Vienna, Austria

- **Quantifying Information Flow for Dynamic Secrets**
  - presented at the 2014 IEEE Symposium on Security & Privacy, San Jose, CA
  - presented at the 2014 meeting of the International Technology Alliance, Cardiff, UK

- **Probabilistic Computation for Information Security**
  - presented at the 2012*NIPS Workshop on Probabilistic Programming, Lake Tahoe, NV

- **Dynamic Enforcement of Knowledge-based Security Policies**
  - presented at the 2011 Symposium on Computer Security Foundations, Paris, France
  - presented at the April 2011 NJ Programming Languages and Systems Seminar, Princeton, NJ
  - presented at the George Washington University Computer Security Seminar

Professional Activities

(sub)reviewer • CSF 2013, CSF 2014, POPL 2013, JCSS, S&P 2015

Awards

2006 • **Provost's MQP Award**
Top CS undergraduate thesis among 46 completed that year.
2005 • **Computer Science Outstanding Junior Award**
Top CS junior of that year.

Technology Experience

Languages • OCaml, Perl; Familiar with: C, Haskell, Python, C++, Java, Javascript, Scheme
Systems • OS X; Familiar with Linux, FreeBSD, Windows
Media • Photoshop, Illustrator, Flash, 3D Studio MAX
Other • MySQL, HTML, LaTeX, Actionscript, OpenGL

Relevant Coursework

PL • CMSC631 Program Analysis and Understanding (website)
Mathematics • MATH712 Mathematical Logic I (syllabus),
MATH713 Mathematical Logic II (syllabus)
Theory • CMSC752 Concrete Complexity (book),
CMSC754 Computational Geometry (website),
CMSC858C Probabilistic Method (website)
AI • CMSC723 Computational Linguistics I (website),
CMSC828D Introduction to Game Theory (website)

Other Activities

2001-2004 • **FIRST Robotics Team at WPI** (team 190)
Led initial development of an inertial navigation system including micro-controller software and design which resulted, in part, in several awards presented to the team during competitions. Also was the main contributor of graphical materials (t-shirt designs, team web-site, etc.). Held the position of "Chief of Graphics" and was responsible for the team's visual identity and web-site.

Miscellaneous

Languages • English (fluent), Polish (native)
Citizenship • USA, Poland (EU)

Piotr (Peter) Mardziel

253 Dudley Oxford Rd
Dudley, MA 01571
USA

piotrm@gmail.com
http://www.cs.umd.edu/~piotrm
+1 (508)873-5439

References

1 <u>Dr. Michael Hicks</u>, Professor of Computer Science at University of Maryland, College Park

Department of Computer Science
University of Maryland
A.V. Williams Building
College Park, MD 20742

email: mwh@cs.umd.edu voice: +1-301-405-2710
website: http://www.cs.umd.edu/~mwh

2 <u>Dr. Mudhakar Srivatsa</u>, Research scientist at IBM T.J. Watson Research Center

IBM T.J. Watson Research Center
1101 Kitchawan Road
Yorktown Heights, NY 10598

email: msrivats@us.ibm.com voice: +1-914-945-3766
website: http://researcher.watson.ibm.com/researcher/view.php?person=us-msrivats

3 <u>Dr. Michael R. Clarkson</u>, Lecturer of Computer Science at Cornell University

Department of Computer Science
Cornell University
461 Gates Hall
107 Hoy Road
Ithaca, NY 14853

email: clarkson@cs.cornell.edu voice: +1-607-255-0278
website: http://www.cs.cornell.edu/~clarkson