

Michael R. Clarkson

Curriculum Vitae

August 11, 2017

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

Office phone: 607-255-0278
Fax: 607-255-9143
clarkson@cs.cornell.edu
<http://www.cs.cornell.edu/~clarkson/>

1 Current Position

Senior Lecturer, Cornell University

2 Education

- PhD in Computer Science, Cornell University, Ithaca, New York, minor in Music (organ), 2010.
- MS in Computer Science, Cornell University, Ithaca, New York, 2004.
- BS in Systems Analysis, Miami University, Oxford, Ohio, with departmental honors, *summa cum laude*, 1999.
- BM in Music Performance (piano), Miami University, Oxford, Ohio, *summa cum laude*, 1999.

3 Academic Employment

- Senior Lecturer, Cornell University, 2017–present.
- Lecturer, Cornell University, 2014–2017.
- Assistant Professor, George Washington University, 2011–2014.
- Postdoctoral Research Associate, Cornell University, 2009–2011.
- Instructor, Miami University, August 1999–December 1999.

4 Publications and Talks

4.1 Articles in Refereed Journals

1. Michael R. Clarkson and Fred B. Schneider. Quantification of integrity. *Mathematical Structures in Computer Science*, 25(2):207–258, 2015.
2. Michael R. Clarkson and Fred B. Schneider. Hyperproperties. *Journal of Computer Security*, 18(6):1157–1210, 2010.
3. Michael R. Clarkson, Andrew C. Myers, and Fred B. Schneider. Quantifying information flow with beliefs. *Journal of Computer Security*, 17(5):655–701, 2009.

4. Ann E. Kelley Sobel and Michael R. Clarkson. Formal methods application: An empirical tale of software development. *IEEE Transactions on Software Engineering*, 28(3):308–320, March 2002.

4.2 Articles in Refereed Conferences and Workshops

5. Kristopher Micinski, Jonathan Fetter-Degges, Jinseong Jeon, Jeffrey S. Foster, and Michael R. Clarkson. Checking interaction-based declassification policies for Android using symbolic execution. In *Proceedings of the European Symposium on Research in Computer Security (ESORICS)*, pages 520–538, September 2015.
6. Gurchetan S. Grewal, Mark D. Ryan, Liqun Chen, and Michael R. Clarkson. Du-vote: Remote electronic voting with untrusted computers. In *Proc. IEEE Computer Security Foundations Symposium (CSF)*, pages 155–169, July 2015.
7. Piotr Mardziel, Mário S. Alvim, Michael Hicks, and Michael R. Clarkson. Quantifying information flow for dynamic secrets. In *Proc. IEEE Symposium on Security and Privacy (Oakland)*, pages 540–555, May 2014.
8. Michael R. Clarkson, Bernd Finkbeiner, Masoud Koleini, Kristopher K. Micinski, Markus N. Rabe, and César Sánchez. Temporal logics for hyperproperties. In *Proc. Conference on Principles of Security and Trust (POST)*, pages 265–284, April 2014.
9. Andrew K. Hirsch and Michael R. Clarkson. Belief semantics of authorization logic. In *Proceedings of the ACM Conference on Computer and Communications Security (CCS)*, pages 561–572, November 2013.
10. Michael R. Clarkson and Fred B. Schneider. Quantification of integrity. In *Proc. IEEE Computer Security Foundations Symposium (CSF)*, pages 28–43, July 2010.
11. Michael R. Clarkson and Fred B. Schneider. Hyperproperties. In *Proc. IEEE Computer Security Foundations Symposium (CSF)*, pages 51–65, July 2008. One of three conference papers invited to special (peer-reviewed) issue of *Journal of Computer Security*.
12. Michael R. Clarkson, Stephen Chong, and Andrew C. Myers. Civitas: Toward a secure voting system. In *Proc. IEEE Symposium on Security and Privacy (Oakland)*, pages 354–368, May 2008.
13. Kevin R. O’Neill, Michael R. Clarkson, and Stephen Chong. Information-flow security for interactive programs. In *Proc. IEEE Computer Security Foundations Workshop (CSFW)*, pages 190–201, July 2006.
14. Michael R. Clarkson and Andrew C. Myers. Coercion-resistant remote voting using decryption mixes. Presented at *Workshop on Frontiers in Electronic Elections (FEE)*, September 2005.
15. Michael R. Clarkson, Andrew C. Myers, and Fred B. Schneider. Belief in information flow. In *Proc. IEEE Computer Security Foundations Workshop (CSFW)*, pages 31–45, June 2005. One of three conference papers invited to special (peer-reviewed) issue of *Journal of Computer Security*.
16. Nathaniel Nystrom, Michael R. Clarkson, and Andrew C. Myers. Polyglot: An extensible compiler framework for Java. In *Proc. Intl. Conference on Compiler Construction (CC)*, pages 138–152, April 2003.

4.3 Technical Reports

17. Ben Smyth, Steven Frink, and Michael R. Clarkson. Election verifiability: Cryptographic definitions and an analysis of helios and jcyj. Computing and Information Science Technical Report, <http://hdl.handle.net/1813/40575>, Cornell University, February 2017.
18. Adam M. Davis, Dmitri Chmelev, and Michael R. Clarkson. Civitas: Implementation of a threshold cryptosystem. Computing and Information Science Technical Report, <http://hdl.handle.net/1813/11661>, Cornell University, December 2008.
19. Michael Clarkson, Brian Hay, Meador Inge, abhi shelat, David Wagner, and Alec Yasinsac. Software review and security analysis of Scytl remote voting software. Report commissioned by Florida Division of Elections. Available from <http://election.dos.state.fl.us/voting-systems/pdf/FinalReportSept19.pdf>. Filed September 19, 2008.
20. Denis L. Bueno and Michael R. Clarkson. Hyperproperties: Verification of proofs. Computing and Information Science Technical Report, <http://hdl.handle.net/1813/11153>, Cornell University, July 2008.

4.4 Dissertation

21. Michael R. Clarkson. *Quantification and Formalization of Security*. PhD thesis, Cornell University, Ithaca, New York, February 2010. Nominated by Cornell for the ACM Doctoral Dissertation Award.

4.5 Keynote and Plenary Talks

22. *Mathematical Foundations for Computer Security Policies*. Conference on the Mathematical Foundations of Programming Semantics, University of Bath, June 7, 2012.
23. *Privacy in Electronic Voting*. FCS–PrivMod Workshop, University of Edinburgh, July 15, 2010.

4.6 Summer School Lectures

24. *Functional Programming*. SJTU International Workshop. Ithaca, NY, July 18–22, 2016.
25. *Hyperproperties and Civitas*. International School on Foundations of Security Analysis and Design (FOSAD). Bertinoro, Italy, September 3 and 4, 2015.
26. *Functional Programming*. SJTU International Workshop. Ithaca, NY, July 13–29, 2015.
27. *Software Foundations*. SJTU International Workshop. Ithaca, NY, July 8–15, 2014.
28. *Coq Bootcamp*. Oregon Programming Languages Summer School (OPLSS), University of Oregon, June 15, 2014.
29. *Hyperproperties*. Summer School on Formal Methods for the Science of Security, University of Illinois at Urbana-Champaign, July 25, 2013.
30. *Verifiability in Electronic Voting*. SecVote Summer School, Dagstuhl, Wadern, Germany, July 2012.
31. *Coercion-resistant Remote Voting: JCJ and Civitas*. SecVote Summer School, Bertinoro, Italy, September 3, 2010.

4.7 Invited Talks

32. *Cybersecurity Education*, panel chair. New England Security Day, Harvard University, April 28, 2016.
33. *Belief Semantics for Authorization Logic*. DC Anonymity, Privacy, and Security Seminar (DCAPS). University of Maryland, College Park, January 24, 2014.
34. *Foundations for Computer Security*. Tulane University. October 18, 2013.
35. *Hyperproperties*. DC Anonymity, Privacy, and Security Seminar (DCAPS). George Washington University, October 11, 2013.
36. *Civitas: Transparency and Security for Remote Voting*. Swiss E-Voting Workshop, September 6, 2010.
37. *Quantification of Integrity*. RADICAL Workshop, Microsoft Research Cambridge, May 10, 2010.
38. *Civitas*. Board Meeting on Electronic Voting at CRYPTO'08, International Association for Cryptologic Research, August 19, 2008.
39. *Civitas*. Dagstuhl Seminar on Frontiers of Electronic Voting, Wadern, Germany, July 31, 2007.

5 Grants and Contracts

- **Open-Audit Voting Systems—Protocol Models and Properties**, \$666k, September 2014–2017. NSF. PI: Poorvi Vora (George Washington University). co-PI: Michael Clarkson.
- **A Logical Foundation for Cybersecurity Built on Hyperproperties**, \$411k, September 2014–2017. AFOSR YIP. PI: Michael Clarkson.
- **Making Cybersecurity Quantifiable**, \$443k, July 2012–2015. AFOSR YIP. PI: Michael Clarkson.

6 Fellowships, Prizes, and Awards

- Cornell University College of Engineering Robert '55 and Vanne '57 Cowie Excellence in Teaching Award, 2015.
- AFOSR YIP Award, 2012.

7 Professional Activities

7.1 Refereeing

- Journals: *Computer Languages (Systems and Structures)*, *Computers and Security*, *Information and Computation*, *Information Processing Letters*, *IET Information Security*, *Journal of Computer and System Sciences*, *Journal of Computer Security*, *Journal of Systems and Software*, *Logical Methods in Computer Science*, *Mathematical Structures in Computer Science*, *Science of Computer Programming*, *Software: Practice and Experience*, *IEEE Transactions on Dependable and Secure Computing*, *IEEE Transactions on Knowledge and Data Engineering*, *ACM Transactions on Information and System Security*, *Transactions on Information Forensics and Security*, *ACM Transactions on Programming Languages and Systems*,

- Conferences and Workshops: ASIACCS, CSF, CSFW, DISC, ESORICS, EVT, EUROSYS, FAST, FM, FOSSACS, OOPSLA, OSDI, PLAS, PLDI, POPL, POST, Security and Privacy (Oakland), SIGCSE, TLDI, USENIX Security.
- Magazines: *IEEE Security and Privacy*.

7.2 Other

- Chair of panel on Cybersecurity Education at New England Security Day, Harvard University, April 28, 2016.
- Member of team commissioned by Florida Division of Elections for security review of Scytl Remote Voting Software, which was used by about 900 overseas voters in the 2008 U.S. General Election.

8 Teaching, Mentoring, and Advising

8.1 Cornell University

8.1.1 Courses Taught

Semester	Course	# Students
Spring 2017	CS 5430 System Security	94*
Spring 2017	CS 5431 Practicum in System Security	13*
Fall 2016	CS 3110 Data Structures and Functional Programming	305
Spring 2016	CS 5430 System Security	75
Spring 2016	CS 5431 Practicum in System Security	15
Fall 2015	CS 3110 Data Structures and Functional Programming	257
Spring 2015	CS 5430 System Security	79
Spring 2015	CS 3110 Data Structures and Functional Programming	129
Fall 2014	CS 3110 Data Structures and Functional Programming	279
Spring 2011	CS 5431 Practicum in System Security	22

* estimated

8.1.2 Course Development

- **CS 5431**, Practicum in Computer Security, Cornell University (Spring 2011). I developed this new practicum on computer security, focusing on defenses for real-world attacks and on security as part of software engineering.

8.1.3 PhD and MS Students Advised

- Steven Frink, August 2014–2016.
- Remy Jette, MS, 2016. Thesis title: *Automated assessment in a programming course*.

8.1.4 MEng Projects Supervised

- Nikhil Ravishankar, Spencer Steel, Andy Wang, and Drew Weymouth, MEng, 2015. Secure off-the-record chat.
- Chris Frommann, MEng, 2010. Coercion-resistant voting interface.
- Adam Davis and Dmitri Chemelev, MEng, 2008. Threshold cryptosystem for voting.
- Denis Bueno, MEng, 2008. Mechanized proofs for hyperproperties.

8.1.5 Undergraduate Research Projects Supervised

- Hunter Goldstein, 2015–2017. Deductive system for HyperLTL and verification in Coq.
- Ishaan Jhaveri, 2015. Mix-network tallying protocol for CERTUS.

8.2 George Washington University

8.2.1 Courses Taught

Semester	Course	# Students
Spring 2014	CSci 3907/6907 Software Foundations	4
Fall 2013	CSci 6545 Software Security	14
Spring 2013	CSci 4223/6223 Principles of Programming Languages	23
Fall 2012	CSci 3907/6907 Software Systems Security	10
Spring 2012	CSci 3907/6907 Advanced Security Seminar	5
Fall 2011	CSci 4531/6531 Computer Security	33

8.2.2 Course Development

- **CSci 4223/6223**, Principles of Programming Languages (Spring 2013). This new (to GW) course presented fundamental concepts underlying the design of programming languages. I based the course on one taught by Dan Grossman (U. Washington).
- **CSci 6545**, Software (Systems) Security (Fall 2012, 2013). I used my revised version of Computer Security (see below) as the basis for this new course. Software Security is at the intersection of computer security and software engineering. The course is designed to give students practical experience with building a software system and securing it.
- **CSci 3907/6907**, Advanced Security Seminar (Spring 2012). This research seminar focused on the nascent field of “Science of Security.” I developed the reading list and some lectures, but most of the lectures were given by students. I mentored each student in developing their lectures. Each student also engaged in a research project, including presenting a paper and a poster. I mentored those projects extensively.
- **CSci 4531/6531**, Computer Security (Fall 2011). I substantially revised the content of this course to be more systems oriented. I shifted away from a survey of the field of computer security and toward a focus on how to design and implement secure software. I redesigned the homework assignments to focus on more practical content. I added a major group software development project to the course, so that students could put into practice the material they learned.

8.2.3 Curriculum Development

- **CS PhD requirements** (2011–2012). I led a major update of the GW CS PhD requirements, including course work, qualifying/preliminary exams, and committee structures. The new requirements are substantially in line with requirements at top research universities.
- **MS in Cybersecurity in Computer Science** (2011–2012). I led the development of the curriculum for a new GW Master’s degree in cybersecurity, including working with faculty outside of CS to make the degree more interdisciplinary. A key feature of the curriculum is a common template that other departments could instantiate to offer their own cybersecurity degrees.

8.2.4 Postdocs Supervised

- Masoud Koleini, November 2012–May 2014.

8.2.5 PhD Students Advised

- Steven Frink, August 2013–August 2014.

8.2.6 PhD Committees

- Jinho Hwang, GW, proposed March 2013, defended November 2013.

8.2.7 Undergraduate Research Students Advised

- Andrew Hirsch, GW, Spring 2012–Spring 2013. Mechanized semantics for authorization logic.
- Michael Shick, GW, Spring 2012. Biometric authentication with hand geometry.
- Christopher Krawiec, GW, Spring 2012. Integrating mixnets with Helios voting.

9 Service

9.1 External

- PC Member, International Conference on Principles of Security and Trust (POST), 2016.
- PC Co-Chair, ACM Workshop on Programming Languages and Analysis for Security (PLAS), 2015.
- PC Member, European Symposium on Research in Computer Security (ESORICS), 2015.
- ERC Member, ACM Symposium on Principles of Programming Languages (POPL), 2015.
- PC Co-Chair, Workshop on Foundations of Computer Security (FCS), 2013, 2014.
- PC Member, Conference on Runtime Verification (RV), 2014.
- PC Member, ACM Symposium on Information, Computer, and Communications Security (ASIACCS), 2014.
- PC Member, Workshop on Quantitative Aspects in Security Assurance (QASA), 2013.

- Panelist, NSF SaTC, 2012.
- PC Member, IEEE Computer Security Foundations Symposium (CSF), 2012.
- Short Talks Chair, IEEE Computer Security Foundations Symposium (CSF), 2012.
- PC Member, Workshop on Formal Aspects in Security and Trust (FAST), 2011.
- PC Member, IEEE Computer Security Foundations Symposium (CSF), 2011.
- PC Member, Conference on E-Voting and Identity (VOTE-ID), 2009.
- Reviewer, Florida Division of Elections, 2008: Member of team commissioned by FL DoE for security review of Scytl Remote Voting Software, which was used by about 900 overseas voters in the 2008 U.S. General Election.
- PC Member, IAVoSS Workshop on Trustworthy Elections (WOTE) 2006.

10 Citizenship

Citizen of the United States