

Michael Clarkson

Curriculum Vitae

October 9, 2009

Department of Computer Science
Cornell University
4112 Upson Hall
Ithaca, NY 14853
Office phone: 607-254-7465
Fax: 607-255-4428

700 Warren Rd. Apt. 21-3A
Ithaca, NY 14850
Home phone: 607-257-9329
Mobile: 607-280-6913
clarkson@cs.cornell.edu
<http://www.cs.cornell.edu/people/clarkson>

EDUCATION

Cornell University, Ithaca, New York
Ph.D. in Computer Science, August 2009
M.S. in Computer Science, January 2004
Advisors: Prof. Andrew Myers and Prof. Fred B. Schneider
Dissertation title: *Quantification and Formalization of Security*

Miami University, Oxford, Ohio
B.S. in Systems Analysis with honors, *summa cum laude*, December 1999
B.M. in Music Performance, *summa cum laude*, December 1999
GPA 4.0/4.0

RESEARCH INTERESTS

Security: Electronic voting, information flow, and cryptography

Programming languages: Semantics, logics, and language-based security; specification and verification of programs

HONORS

- Intel Foundation Fellowship, 2007–2009
- National Science Foundation Graduate Research Fellowship, 2001–2005
- Four Outstanding Teaching Assistant Awards, Cornell Computer Science:
Functional Programming and Data Structures, 2008; System Security, 2004;
Advanced Programming Languages, 2003; Introduction to Compilers, 2001
- Cornell University Fellowship, 2000

RESEARCH EXPERIENCE

Postdoctoral Associate, Cornell University, 2009–present
Supervised by Prof. Fred B. Schneider

Research Assistant, Cornell University, 2000–2009
Advised by Prof. Andrew Myers and Prof. Fred B. Schneider

Developed a new mathematical framework of hyperproperties for expressing and verifying security policies. Designed and implemented Civitas, a secure remote electronic voting system. Created a new model for quantitative information flow.

Undergraduate Research Assistant, Miami University, 1999
Advised by Prof. Ann E. K. Sobel

Analyzed artifacts from an experimental curriculum that integrated formal methods and software engineering. Discovered evidence that study of formal methods improved students' skill at solving complex problems.

TEACHING EXPERIENCE

Instructor, Cornell University, Summer 2000, *CS 99, Fundamental Programming Concepts*: Full responsibility for class. Supervised one teaching assistant.

Instructor, Miami University, Fall 1999, *SAN 163, Introduction to Computer Concepts and Programming*: Full responsibility for class.

Teaching Assistant, Cornell University, periodically 2000–2008:

- *CS 312, Functional Programming and Data Structures*, with Prof. Andrew Myers, Spring 2008: Taught two recitation sections each week, developed four new recitation topics, and created a program verification logic that the class employed. Received CS Outstanding TA Award. Guest lecturer: Spring 2007 (recursive datatypes).
- *CS 513, System Security*, with Prof. Fred B. Schneider, Spring 2004, Fall 2007: Gave three or four lectures each term on access control, information flow, or electronic voting. Received CS Outstanding TA Award Spring 2004. Guest lecturer: Fall 2004, Fall 2005, and Fall 2006 (same topics).
- *CS 611, Advanced Programming Languages*, with Prof. Radu Rugina, Fall 2003: Received CS Outstanding TA Award. Guest lecturer: Fall 2005 and Fall 2006 (axiomatic semantics, lambda calculus).
- *CS 412, Introduction to Compilers*, with Prof. Andrew Myers, Spring 2001: Received CS Outstanding TA Award.
- *CS 211, Computers and Programming*, with instructor Paul Chew, Fall 2000: Head TA, managed course staff of nine other TAs.

Master's Project Supervisor, Cornell University, 2008. Directly supervised two projects:

- *Threshold cryptosystem*. Two Master's students extended my voting system (Civitas) to support threshold cryptography, including a sophisticated key generation protocol.

- *Proof verification*. A Master’s student formally verified several proofs from my work on hyperproperties, using a theorem prover.

Seminar Organizer, Cornell Security Discussion Group, 2005–2007. Founded weekly reading group on computer security. Chose papers and scheduled speakers.

Placement Exam Assistant, Cornell Computer Science, 2001, 2005–2008. Developed and graded departmental undergraduate placement exam.

SERVICE

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.

Program Committees: IAVoSS Workshop on Trustworthy Elections (WOTE) 2006, Conference on E-Voting and Identity (VOTE-ID) 2009.

Referee: *Information Processing Letters, Logical Methods in Computer Science, Software: Practice and Experience, IEEE Transactions on Knowledge and Data Engineering, ACM Transactions on Programming Languages and Systems*. CSFW, FAST, OOPSLA, OSDI, PLDI, POPL, Security and Privacy (Oakland), USENIX Security.

PUBLICATIONS

REFEREED JOURNAL AND CONFERENCE PAPERS

1. Michael R. Clarkson and Fred B. Schneider. Hyperproperties. *Journal of Computer Security*. Accepted for publication, March 2009; in press, August 2009. Computing and Information Science Technical Report, <http://hdl.handle.net/1813/11660>, Cornell University, December 2008.
2. Michael R. Clarkson and Fred B. Schneider. Hyperproperties. In *Proc. IEEE Computer Security Foundations Symposium*, pages 51–65, July 2008. One of three conference papers invited to special (peer-reviewed) issue of *Journal of Computer Security*.
3. Michael R. Clarkson, Stephen Chong, and Andrew C. Myers. Civitas: Toward a secure voting system. In *Proc. IEEE Symposium on Security and Privacy*, pages 354–368, May 2008.
4. Michael R. Clarkson, Andrew C. Myers, and Fred B. Schneider. Quantifying information flow with beliefs. *Journal of Computer Security*. Accepted for publication, December 2006. In press, January 2009. Computing and Information Science Technical Report, <http://hdl.handle.net/1813/5766>, Cornell University, March 2007.
5. Kevin R. O’Neill, Michael R. Clarkson, and Stephen Chong. Information-flow security for interactive programs. In *Proc. IEEE Computer Security Foundations Workshop*, pages 190–201, July 2006.
6. Michael R. Clarkson, Andrew C. Myers, and Fred B. Schneider. Belief in information flow. In *Proc. IEEE Computer Security Foundations Workshop*, pages 31–45, June 2005. One of three conference papers invited to special (peer-reviewed) issue of *Journal of Computer Security*.

7. Nathaniel Nystrom, Michael R. Clarkson, and Andrew C. Myers. Polyglot: An extensible compiler framework for Java. In *Proc. Intl. Conference on Compiler Construction*, pages 138–152, April 2003.
8. 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.

OTHER PAPERS AND REPORTS

9. Michael R. Clarkson. *Quantification and Formalization of Security*. PhD thesis, Cornell University, Ithaca, New York, August 2009.
10. 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.
11. 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.
12. 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.
13. Michael R. Clarkson and Andrew C. Myers. Coercion-resistant remote voting using decryption mixes. Presented at *Workshop on Frontiers in Electronic Elections*, September 2005.

INVITED TALKS

1. *Civitas*. Board Meeting (at CRYPTO'08) on Electronic Voting, International Association for Cryptologic Research, August 19, 2008.
2. *Civitas*. Dagstuhl Seminar on Frontiers of Electronic Voting, Wadern, Germany, July 31, 2007.
3. *Belief in Information Flow*. Colloquium, School of Computing Science, Newcastle University, July 3, 2006.

REFERENCES

- Prof. Andrew Myers
Cornell University
andru@cs.cornell.edu
607-255-8597
- Prof. Fred B. Schneider
Cornell University
fbs@cs.cornell.edu
607-255-9221