Wilfredo (Will) Marrero

Contact

School of Computer Science
Carnegie Mellon University
Pittsburgh PA 15213-3891
(412) 268-3069
Email: marrero@cs.cmu.edu
WWW: http://www.cs.cmu.edu/∼marrero

or

5631 Northumberland Street
Pittsburgh PA 15217
(412) 422-0173

Personal

Birthdate:	May 24, 1970
Birthplace:	Los Angeles, California
Citizenship:	United States

Education

Carnegie Mellon University (September 1992 to present)

- Ph.D. Computer Science (Expected June 1999)
  Thesis: Model Checking for Security Protocols
  Advisor: Professor Edmund Clarke
- M.S. Computer Science (December 1994)

Columbia University (September 1988 to May 1992)

- B.A. Mathematics and Computer Science (May 1992)

Honors and Awards

John Jay Scholar, Columbia University, 1988-1992.
Minority Summer Research Fellowship, Columbia University 1991.
National Hispanic Scholarship, National Hispanic Scholarship Fund 1991-1992.
Russell C. Mills Computer Science Award, Columbia University, 1992.
Summa Cum Laude, Columbia University, 1992.
Phi Beta Kappa, Columbia University, 1992.

Research Interests

Computer Security: Security Protocols, Protocol Verification, Electronic Commerce, Information Survivability.

Formal Methods: System Modeling, Model Checking, Compositional Reasoning, Hardware Verification, Real-time and Hybrid Systems.

Thesis Summary

My thesis merges some of the ideas of formal methods, specifically model checking, with security protocol design and analysis. I have built a tool that performs a state space search of a security protocol model looking for traces that violate a specification given in a formal logic. This logic is rich enough to express a wide range of security properties. I have also exploited state reduction techniques including abstraction, symmetry, and partial order reduction to decrease the size of the state space that must be searched during model checking, resulting in a more efficient model checker.

Employment

Summer Research Intern — *Cadence*
June 1996–September 1996 — *Cadence Berkeley Labs, Berkeley, CA*
I worked with Dr. Jerry Burch trying to model and to verify a simple out of order execution processor. This was done using a model checker built to verify a pipelined processor. This work helped to uncover limitations in the model checker.

Summer Research Intern — *Intel Corporation*
May 1995–September 1995 — *Hillsboro, OR*
I worked with Manpreet Khaira and Xudong Zhao in modeling and verifying arithmetic units in the Pentium II processor. We used a model checker based on hybrid decision diagrams (HDDs) and helped to develop a methodology for verifying such large circuits. This experience also exposed me to the latest in microprocessor design and validation.

Summer Researcher — *Columbia University*
May 1992–August 1992 — *New York, NY*
I worked on the MARVEL project, a rule-based, object oriented programming environment. The principal investigator was Professor Gail Kaiser. My work dealt specifically with the problem of maintaining consistency of a database of objects in the presence of object evolution (changes in classes) and process evolution (changes in rules). This research led to a technical report.

Teaching

I have been a teaching assistant in a number of math and computer science classes both as a graduate student at Carnegie Mellon University and as an undergraduate at Columbia University.

Undergraduate Algorithms (Fall 1995, Carnegie Mellon)
Undergraduate Algorithms (Fall 1994, Carnegie Mellon)
Structure and Interpretation of Computer Programs (Spring 1992, Columbia)
Calculus (Spring 1992, Columbia)
Introduction to Computer Science (Fall 1991, Columbia)
Calculus (Fall 1991, Columbia)
Calculus (Spring 1991, Columbia)

Journal Publications

A. Browne, E. Clarke, S. Jha, D.E. Long, and W. Marrero, An improved algorithm for evaluation of fixpoint expressions, *Theoretical Computer Science*, Volume 178, 1997. A preliminary version appeared in CAV ’94.

Refereed Conferences and Workshops

E. M. Clarke and W. Marrero, Using formal methods for analyzing security, *Information Survivability Workshop*, 1998.

E. M. Clarke, S. Jha, and W. Marrero, A machine checkable logic of knowledge for specifying security properties of electronic commerce protocols, *Workshop on Formal Methods and Security Protocols*, 1998.

E. M. Clarke, S. Jha, and W. Marrero, Using state space exploration and a natural deduction style message derivation engine to verify security protocols, *Proceedings of the IFIP Working Conference on Programming Concepts and Methods (PROCOMET)*, 1998.

W. Marrero, E. M. Clarke, and S. Jha, A model checker for security protocols, *DIMACS Workshop on Design and Formal Verification of Security Protocols*, 1997.
A preliminary version appeared as technical report TR-CMU-CS-97-139, Carnegie Mellon University, May 1997.

S. Campos, E. Clarke, W. Marrero and M. Minea, Verus: a tool for quantitative analysis of finite-state real-time systems, *Workshop on Languages, Compilers and Tools for Real-Time Systems*, 1995.

S. Campos, E. Clarke, W. Marrero and M. Minea, Timing analysis of industrial real-time systems, *Workshop on Industrial Strength Formal Specification Techniques*, 1995.

S. Campos, E. Clarke, W. Marrero, M. Minea and H. Hiraishi, Computing quantitative characteristics of finite-state real-time systems, *IEEE Real-Time Systems Symposium*, 1994.

Technical Reports

S. Berezin, E. Clarke, S. Jha, W. Marrero, Model checking algorithms for the mu-calculus, Technical Report TR-CMU-CS-96-180, Carnegie Mellon University, September 1996.

G. Kaiser, I. Ben-Shaul, G. Heineman, W. Marrero, Process evolution for the Marvel environment, Technical Report CUCS-047-92, Columbia University, 1992

Presentations

E. M. Clarke and W. Marrero, Using formal methods for analyzing security, *Information Survivability Workshop*, 1998.

E. M. Clarke, S. Jha, and W. Marrero, A machine checkable logic of knowledge for specifying security properties of electronic commerce protocols, *Workshop on Formal Methods and Security Protocols*, 1998.

E. M. Clarke, S. Jha, and W. Marrero, Using state space exploration and a natural deduction style message derivation engine to verify security protocols, *IFIP Working Conference on Programming Concepts and Methods (PROCOMET)*, 1998.

W. Marrero, E. M. Clarke, and S. Jha, A model checker for security protocols, *DIMACS Workshop on Design and Formal Verification of Security Protocols*, 1997.

Languages Fluent in English and Spanish.
Conversational in French, Italian, and German.

References

Professor Edmund Clarke
School of Computer Science
Carnegie Mellon University
Pittsburgh, PA 15213-3891
(412) 268-2628
emc@cs.cmu.edu

Professor Jeannette Wing
School of Computer Science
Carnegie Mellon University
Pittsburgh, PA 15213-3891
(412) 268-3068
wing@cs.cmu.edu

Professor Doug Tygar
102 South Hall #4600
University of California
Berkeley, CA 94720-4600
(510) 643-7855
tygar@cs.berkeley.edu