

Dilsun Kırılı Kaynar

Contact Information

Postdoctoral Fellow
Carnegie Mellon University
4720 Forbes Avenue
Collaborative Innovation Center
CyLab, 2119B
Pittsburgh, PA 15213, USA

Email: dilsun@cs.cmu.edu
Tel: 412 268 9297 (office)
Tel: 617 365 3950 (cell)
Fax: 412 268 5531
<http://www.cs.cmu.edu/~dilsun>

Education

- The University of Edinburgh, Edinburgh, Scotland, UK (1996 – 2001)
PhD in Computer Science, 2002
MSc in Computer Science, 1997

Advisor: Stephen Gilmore

PhD Thesis: *Mobile Computation with Functions*
Thesis also published as a book by Kluwer Academic Publishers.

MSc Thesis: *A Test-case Assessor for ML*
Received Distinction award from the University of Edinburgh.

- The Middle East Technical University, Ankara, Turkey (1992 – 1996)
BSc in Computer Engineering, 1996

Employment

- Carnegie Mellon University (2006 – present)
Postdoctoral Fellow
School of Computer Science and CyLab

Hosts: Jeannette Wing, Bruce Krogh, Anupam Datta

Projects: Attack Graphs, Model-based Test Generation, Foundations of Privacy

- Massachusetts Institute of Technology (2001 – 2006)
Postdoctoral Research Associate
Computer Science and Artificial Intelligence Laboratory
Theory of Distributed Systems Group

Host: Nancy Lynch

Projects: The IOA Language and Toolset, Modeling and Analysis of Timed Systems,
Security Protocol Analysis

- The University of Edinburgh (2000 – 2001)
Part-time Lecturer, School of Informatics
Part-time Research Assistant, Laboratory for Foundations of Computer Science

Course: Distributed Systems (CS4 and MSc)

Project: Type systems for Resource-bounded Programming and Compilation. Engineering and Physical Sciences Research Council (EPSRC) project led by Martin Hofmann and David Aspinall.

Research Interests

Distributed Computing, Security, Formal Modeling and Verification, Timed Systems, Programming Languages, Type Systems

Research Experience

Postdoctoral Research at CMU (2006 – present)

- Foundations of Privacy: The objective of this project is to develop principles and approaches for modeling systems that handle sensitive information, languages for specifying privacy policies, and practical logic-based methods for enforcing policy specifications. We are currently focusing on privacy in systems that contain large volumes of structured data such as database systems. We aim to formulate a quantitative notion of privacy that does not severely undermine utility.
- Model-based Test Generation: The objective of this project is to develop efficient test generation methods for timing-dependent systems such as embedded controllers from their design models. In particular, we focus on system designs that have formally been verified with respect to some assumptions about the environment, and view testing as a complementary mechanism to formal verification. We aim to generate tests to be applied to the system implementation in its real environment. The idea is to drive the real environment with our tests such that we can detect whether it violates the environmental assumptions used in formal verification.
- Attack Graphs (ended in Spring 2007): This project, based on Sheyner's PhD thesis, investigated automatic generation of network attack graphs that represent all possible ways a given security property can be violated in a network. The central idea of the project was to leverage model-checking technology in this context. Given a logic property, and a system model, a model-checker for that logic either verifies that the property is satisfied or yields a counterexample that demonstrates a violation. The automatic generation of attack graphs was done by exploiting a linear-time temporal logic (LTL) model-checker to generate all possible counterexamples for a given security property. My role was to investigate methods for improving scalability, adapting ideas from the compositional reasoning area to the setting of the project.

Postdoctoral Research at MIT (2001 – 2006):

- **Security Protocol Analysis:** The objective of this project is to develop high-level formal methods for modeling and reasoning about cryptographic security protocols without idealizing cryptography or computational capabilities of adversarial components. The accomplishments to date include the development of a probabilistic I/O automaton model suitable for modeling protocols and their requirements, and notions of simulation relations for proving security properties using multiple levels of abstraction. The current work, which I continue to be involved in, focuses on methods for the analysis of long-lived systems such as digital archives. An important characteristic of long-lived systems is that security needs to be guaranteed throughout the lifetime of the system even if some cryptographic primitives are compromised in due course. The analysis of such systems need to incorporate the notion of time, which is missing from existing analysis frameworks.
- **Modeling and Analysis of Timed Systems:** With my coauthors Lynch, Segala, and Vaandrager, I developed a new formal framework – the Timed I/O Automata Framework – which facilitates the precise description of behavior, including timing-dependent behavior, in distributed systems and provides mathematical methods for proving implementation relationships between systems and their specifications. This framework provides expressive modeling notions that extend those of the basic I/O automaton model (which is well-established in reasoning about untimed distributed algorithms) and subsumes many prior models for timed-systems. I also led the design of a modeling language – Tempo – based on this framework. This language extends the IOA Language, which was previously developed within the Theory of Distributed Systems Group to support description of untimed I/O automata. Currently, the focus of this project has shifted to the development of a toolset, including a simulator for Tempo programs and an interface to the theorem prover PVS. I am still involved in this project and am coauthoring a tutorial on modeling timed systems with Tempo.
- **The IOA Language and Toolset (ended in Fall 2002):** I participated in case studies aimed at establishing a verification methodology for distributed algorithms that employs the IOA Language and Toolset. I was involved in projects to enhance the capabilities of the IOA Toolset, for example, with support for dynamic invariant detection and debugging. I also worked on the design of a tool for automatically translating IOA models to distributed Java code in a way that preserves their semantics.

Doctoral Research (1997 – 2001):

- **Functional languages for distributed computing:** I explored distributed computation with functional languages that support code mobility through the mobility of functions between remote sites. I focused on the languages of the ML family and higher-order process calculi. The main motivation for focusing on these languages was that they are simple, well-founded, elegant, and lend themselves to rigorous analysis methods to reason about their potential behavior. I aimed at demonstrating that these characteristics made them particularly well-suited for mobile computation.

- Type systems for mobility: I investigated the use of annotated type and effect systems in statically analyzing potential behavior of programs. I introduced new analyses motivated by the nature of the mobile code setting, different from the traditional uses of annotated type and effect systems. For example, I designed type systems to predict which functions may become mobile at runtime, and to estimate their potential invocation sites in the system.
- Type systems for security: I investigated the use of annotated type and effect systems in controlling the flow of values in a system with users of different trust levels. For example, I designed a type system that enforces the confinement of values within a specified mobility region in the system, and a type system that detects whether a program is vulnerable to leaking sensitive information indirectly because of conditional branching on sensitive data.

EPSRC Project, 2001:

- Type systems for resource-bounded programming and compilation: The focus of the project was on the design of specialized type systems that allow one to check whether an algorithm and data structure falls into a certain desirable complexity class.

Teaching Experience

- Massachusetts Institute of Technology,
Computer Science and Artificial Intelligence Laboratory

Supervisor of Master's theses and undergraduate research projects:

- * Edward Solovey. *Simulation of Composite I/O Automata*, MEng Thesis, completed in 2003.
- * Christine Robson. *TIOA and UPPAAL*, MEng Thesis, completed in 2004.
- * Panayiotis Mavrommatis. *Simulation of Timed Input/Output Automata*, MEng Thesis, completed in 2006.
- * Toh Ne Win, Fivos Constantinou.
Undergraduate research students on the IOA project

- The University of Edinburgh, The School of Informatics

Lecturer for Distributed Systems (Senior and Master's level): Lectures covered major concepts and design issues for distributed systems, basic distributed algorithms. Had full responsibility for the course: prepared teaching materials, projects and exams.

Tutor for CS1, CS2 courses: Introduced basic concepts of computer science and software engineering process to students, taught programming and data structures using Java and Standard ML, logics and techniques for reasoning about programs.

Publications

Books

- Dilsun K. Kaynar, Nancy A. Lynch, Roberto Segala, and Frits W. Vaandrager. *The Theory of Timed I/O Automata*. In series Synthesis Lectures on Computer Science, Morgan and Claypool Publishers, 101pp, 2006. ISBN 159829010X.
- Dilsun Kırıl. *Mobile Computation with Functions*. In series Advances in Information Security. Kluwer Academic Publishers, 2002. ISBN 1-4020-7024-1. This monograph is based on my PhD thesis.

Journal Papers

- Ran Canetti, Ling Cheung, Dilsun Kaynar, Moses Liskov, Nancy Lynch, Olivier Pereira, and Roberto Segala. Analyzing Security Protocols Using Time-bounded Task-PIOAs. To appear in *Discrete Event Dynamic Systems: Theory and Practice*, 2008.
- Ran Canetti, Ling Cheung, Dilsun Kaynar, Moses Liskov, Nancy Lynch, Olivier Pereira, and Roberto Segala. Using Probabilistic I/O Automata to Improve the Analysis of Cryptographic Protocols. In *ERCIM News* 63: 40-41, October 2005.
- Toh Ne Win, Michael D. Ernst, Stephen J. Garland, Dilsun K. Kaynar, and Nancy Lynch. Using simulated execution in verifying distributed algorithms. In *Software Tools for Technology Transfer* 4: 1-10, 2003. Extended abstract appeared in *Proceedings of Fourth International Conference on Verification, Model Checking and Abstract Interpretation (VMCAI)*, New York, January 2003.
- Dilsun Kırıl. Distributed call-tracking for security. In *Computer Languages, Systems and Structures* 28: 129-154, 2002. Invited paper for the special issue on Computer Languages and Security.
- Chris Walton, Dilsun Kırıl, and Stephen Gilmore. An abstract machine model of dynamic module replacement. In *Future Generation Computer Systems*, 16(7): 793-808, May 2000.

Papers in Refereed Conferences and Workshops

- Ran Canetti, Ling Cheung, Dilsun Kaynar, Nancy Lynch, and Olivier Pereira. Compositional Security for Task-PIOAs. In *Proceedings of 20th IEEE Computer Security Foundations Symposium (CSF)*, pp. 125-139, Venice, Italy, 2007. IEEE Computer Society.
- Ran Canetti, Ling Cheung, Dilsun Kaynar, Moses Liskov, Nancy Lynch, Olivier Pereira, and Roberto Segala. Time-bounded Task-PIOAs: A Framework for Analyzing Security Protocols. In *Proceedings of the 20th International Symposium on Distributed Computing (DISC)*, Stockholm, Sweden, September 18-20, 2006. Invited paper.

- Ran Canetti, Ling Cheung, Dilsun Kaynar, Moses Liskov, Nancy Lynch, Olivier Pereira, and Roberto Segala. Task-Structured Probabilistic I/O Automata. In *Proceedings the 8th International Workshop on Discrete Event Systems (WODES)*, Ann Arbor, Michigan, July, 2006.
- Ran Canetti, Ling Cheung, Dilsun Kirli, Moses Liskov, Nancy Lynch, Olivier Pereira, Roberto Segala. Using Task-Structured Probabilistic I/O Automata to Analyze Cryptographic Protocols . In *Proceedings of the Workshop on Formal and Computational Cryptography (FCC)*, pp. 34-39, July 2006.
- Hongping Lim, Dilsun Kaynar, Nancy Lynch, and Sayan Mitra. Translating timed I/O automata specifications for theorem proving in PVS. In *Proceedings of International Conference on Formal Modelling and Analysis of Timed Systems (FORMATS)*, Volume 3829 of Lecture Notes on Computer Science, Uppsala, Sweden, September 26 - 28, 2005. Springer.
- Dilsun Kaynar, Nancy Lynch, and Sayan Mitra. Specifying and Proving Timing Properties with TIOA Tools. In *25th IEEE International Real-Time Systems Symposium, Work in Progress Session (RTSS WIP)*, Lisbon, Portugal, December 5-8 2004.
- Dilsun Kaynar and Nancy Lynch. Decomposing Verification of Timed I/O Automata. In *Proceedings of the Joint Conference on Formal Modelling and Analysis of Timed Systems (FORMATS) Formal Techniques in Real-Time and Fault Tolerant System (FTRTFT)*, Volume 3253 of Lecture Notes in Computer Science, pages 84-101, Grenoble, France, September, 2004. Springer.
- Dilsun K. Kaynar, Nancy Lynch, Roberto Segala, and Frits Vaandrager. Timed I/O Automata: A Framework for modeling and analyzing real-time systems. In *Proceedings of the 24th IEEE International Real-Time Systems Symposium (RTSS)*, pages 166-177. Cancun, Mexico, December 2003. IEEE Computer Society.
- Dilsun K. Kaynar, Anna Chefter, Laura Dean, Stephen Garland, Nancy Lynch, Toh Ne Win, and Antonio Ramirez. Simulating nondeterministic systems at multiple levels of abstraction. In *Proceedings of Tools Day*, held in conjunction with CONCUR, pages 44-60, Brno, Czech Republic, August 2002.
- Dilsun Kirli. Confined mobile functions. In *Proceedings of the 14th IEEE Computer Security Foundations Workshop (CSFW)*, pages 283-294, Nova Scotia, Canada, June 2001. IEEE Computer Society.
- Dilsun Kirli. Secure information flow for mobile functions. In *Proceedings of the Workshop on Issues in the Theory of Security (WITS)*, pages 30-35, Geneva, July 2000.
- Dilsun Kirli. A survey on functions, concurrency, distribution and mobility. In *Proceedings of the 1st Scottish Functional Programming Workshop*, pages 203-213, Stirling, UK, September 1999.

- Dilsun Kırılı. A static type system for detecting potentially transmissible functions. In P. Sewell and J. Vitek, editors, *Proceedings of the 5th Mobile Object Systems Workshop: Programming Languages for Wide Area Networks*, Lisbon, Portugal, June 1999.

In review

- Ran Canetti, Ling Cheung, Dilsun Kaynar, Moses Liskov, Nancy Lynch, Olivier Pereira, and Roberto Segala. Task-Structured Probabilistic I/O Automata. Submitted to *Information and Computation*.
- Ran Canetti, Ling Cheung, Dilsun Kaynar, Nancy Lynch, and Olivier Pereira. How to Model Bounded Computation in Timed Systems. Manuscript under revision.

Other

- Ran Canetti, Ling Cheung, Dilsun Kaynar, Moses Liskov, Nancy Lynch, Olivier Pereira, and Roberto Segala. Using Probabilistic I/O Automata to Analyze an Oblivious Transfer Protocol. Technical Report MIT-LCS-TR-1001a, MIT CSAIL, Cambridge, MA, August 2005. Also published as Cryptology ePrint Archive Report 2005/452.
- Dilsun K. Kaynar, Anna Chefter, Laura Dean, Stephen Garland, Nancy Lynch, Toh Ne Win, Antonio Ramirez. The IOA simulator manual. Technical Report MIT-LCS-TR-843, MIT Laboratory for Computer Science. Available at <http://theory.lcs.mit.edu/tds/ioa.html>.
- Dilsun Kırılı. A polymorphic type and effect system for detecting mobile functions. Technical Report ECS-LFCS-99-413, Laboratory for Foundations of Computer Science, Division of Informatics, University of Edinburgh, 1999.
- Stephen Gilmore, Dilsun Kırılı, and Chris Walton. Dynamic ML without dynamic types. Technical Report ECS-LFCS-97-378, Laboratory for Foundations of Computer Science, Department of Computer Science, The University of Edinburgh, 1998.
- Dilsun Kırılı. A test case assessor for ML. MSc Thesis. The University of Edinburgh, 1997.

Awards and Honors

- Overseas Research Student Award, UK (1997 – 2000)
- The University of Edinburgh, LFCS PhD Studentship (1997 – 2000)
- Distinction award for my Master of Science Degree (1997)
- British Council Chevening Scholarship (1996 – 1997)
- Turkish Education Foundation Scholarship (1992 – 1997)
- AFS Intercultural Exchange Student, Belgium (1991 – 1992)

References

- PhD Supervisor:** Stephen Gilmore
Laboratory for Foundations of Computer Science
The University of Edinburgh
Edinburgh EH9 3JZ, Scotland, UK
Tel: +44 131 650 5189
Fax: +44 131 667 7209
Email: Stephen.Gilmore@ed.ac.uk
- Postdoctoral Advisor:** Nancy Lynch
MIT Computer Science and Artificial Intelligence Laboratory
Stata Center, 32 Vassar Street, G668
Cambridge, MA 02139, USA
Tel: 617 253 7255
Fax: 617 258 8682
Email: lynch@csail.mit.edu
- Postdoctoral Advisor:** Bruce Krogh
Department of Electrical and Computer Engineering
Carnegie Mellon University
5000 Forbes Ave.
Pittsburgh, PA 15213-3890
Tel: 412 268 2472
Fax: 412 268 3890
Email: krogh@ece.cmu.edu
- Postdoctoral Advisor:** Anupam Datta
CyLab, Carnegie Mellon University
CIC Building, Room 2118
Tel: 617 268 4254
Fax: 617 268 5531
Email: danupam@cmu.edu
- Postdoctoral Advisor:** Jeannette Wing
Computer Science Department, Carnegie Mellon University
Assistant Director,
Computer and Information Science and Engineering Directorate
National Science Foundation
4201 Wilson Boulevard, Suite 1105
Arlington, VA 22230
Tel: 703 292 8900
Email: jwing@nsf.gov or wing@cs.cmu.edu

Research Collaborator: Alexander A. Shvartsman
Computer Science and Engineering
University of Connecticut
371 Fairfield Road, Unit 2155
Storrs, Connecticut 06269
Tel: 860 486 2672
Fax: 860 486 4817
Email: aas@cse.uconn.edu