Dilsun Kırlı Kaynar

Contact Information

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

Email: dilsun@cs.cmu.edu
Phone (office): 412 268 9297
Phone (mobile): 617 365 3950
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 and Research Staff
  School of Computer Science and CyLab

  Hosts: Jeannette Wing, Anupam Datta

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

  Host: Nancy Lynch

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

Research Interests

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

Research Experience

Postdoctoral Research at CMU (2006 – present)

- Foundations of Privacy (current): The objective of this project is to develop principles for modeling systems that handle sensitive information, languages for specifying privacy policies, and algorithms for their enforcement. Specifically, we focus on logic-based languages for specifying privacy policies, where privacy policies may refer to aggregate information as well as information about individuals. We aim at leveraging methods based on model-checking, proof theory, and process equivalence in the context of privacy policy enforcement. We have completed full logical specifications of the disclosure-relevant portions of the Health Insurance Portability and Accountability Act (HIPAA) for healthcare providers and the Gramm-Leach-Bliley Act (GLBA) for financial institutions. These are the first full formalizations of real laws. This effort produced a logic – PrivacyLFP – suitable for expressing a large class of privacy regulations in practice and revealed the need for enforcement techniques that combine proactive access control and post-hoc audits with human input. We are currently working on the development of such techniques and their application in providing end-to-end privacy guarantees for organizational processes such as workflows in a healthcare system. Since such processes typically handle both individual and aggregate anonymized information obtained from a database, in a complementary line of work, westudy database privacy notions and investigate how they can be integrated into a formal framework for analyzing privacy properties for interactive processes that use databases as a component. As a first step we have developed a verification technique for differential privacy, which is a probabilistic notion of data privacy that has gained wide attention in the private data analysis community.

- Secure Systems (current): This project involves the development of a general framework for modeling systems, systematically specifying adversary classes, defining security properties, and proving that a given system satisfies a security property in the presence of adversaries. Our target systems include security hypervisors, virtual machine monitors, trusted computing systems, Web browsers, and network protocols. Our first accomplishment has been the development of a logic – the Logic of Secure Systems (LS^2) – with a sound proof system that allows proving security properties for system models in the presence of an adversary that can use both the network and the local system to launch an attack. We used this logic to characterize the Trusted Platform Module and Trusted Computing primitives, and proved code and execution integrity properties of remote attestation protocols. Proof system for LS^2 assumes a powerful yet fixed adversary model, which implies that its proof system cannot be used to prove properties for those systems that are designed to be secure against adversaries that do not fit in this model. Our wish for further generality led us to extend this work based on the

observation that modeling a system in terms of the interfaces exposed by the resources and defining adversaries as interface-confined and otherwise unknown programs yields a generic adversary model. The interface-based view of systems allows us to develop a proof system that is not tied to a specific domain with a fixed adversary model. We have some initial results that confirm the generality of our approach: we can express a large class of systems and properties of interest and preserve the basic compositional reasoning principles associated with LS^2, now to reason parametrically over adversary models. We are interested in extending our theory to enable the comparison of different adversary models with respect to their strength and of systems with respect to their security.

- 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 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 was 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 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 against polynomial-time-bounded adversaries, using multiple levels of abstraction. As an extension to this basic probabilistic model, the project also produced a novel modeling and analysis paradigm for long-lived systems such as digital archives in which security needs to be guaranteed throughout the lifetime of the system, which is not necessarily bounded by a polynomial, even if some cryptographic primitives are compromised in due course.

- 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. This project has also produced a toolset, including a simulator for Tempo programs and an interface to the theorem prover PVS, which is used for teaching purposes at some academic institutions.

- 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 Interests

Distributed Systems, Computer and Network Security, Programming Languages, Modeling and Verification, Data Structures and Algorithms, Discrete Mathematics, Logic for Computer Science, Theory of Computation

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.
    Undergradute 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.

Awards and Honors

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

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. The second edition is to appear in series Synthesis Lectures on Distributed Computing Theory.

- Dilsun Kırlı. *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

- Anupam Datta, Deepak Garg, Jason Franklin, Limin Jia, and Dilsun Kaynar. On Adversary Models and Compositional Security. Accepted for publication in *IEEE Security and Privacy*, Special Issue on Science of Security, 2011.

- Ran Canetti, Ling Cheung, Dilsun Kaynar, Moses Liskov, Nancy Lynch, Olivier Pereira, and Roberto Segala. Analyzing Security Protocols Using Time-bounded Task-PIOAs. *Discrete Event Dynamic Systems: Theory and Practice* Volume 18 (1): 111-159, 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, 2004. Extended abstract appeared in *Proceedings of Fourth International Conference on Verification, Model Checking and Abstract Interpretation (VMCAI)*, New York, January 2003.

- Dilsun Kırlı. 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 Kırlı, 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

- Henry DeYoung, Deepak Garg, Limin Jia, Dilsun Kaynar, and Anupam Datta. Experiences in the Logical Specification of the HIPAA and GLBA Privacy Laws. In *Proceedings of 9th ACM Workshop on Privacy in the Electronic Society (WPES)*, October 2010. ACM.

- Anupam Datta, Jason Franklin, Deepak Garg, and Dilsun Kaynar. Compositional System Security with Interface-Confined Adversaries. In *Proceedings of 26th Annual Conference on Mathematical Foundations of Programming Semantics (MFPS)*, Electronic Notes in Theoretical Computer Science, pages 49-71, May 2010. Invited paper. Elsevier.

- Anupam Datta, Jason Franklin, Deepak Garg, and Dilsun Kaynar. A Logic of Secure Systems and its Application to Trusted Computing. In *Proceedings of the 30th IEEE Symposium on Security and Privacy (Oakland)*, pages 221-236, May 2009. IEEE Computer Society.

- Ran Canetti, Ling Cheung, Dilsun Kaynar, Nancy Lynch, and Olivier Pereira. Modeling Computational Security in Long-Lived Systems. In *Proceedings of the 19th International Conference on Concurrency Theory (CONCUR)*, Volume 5201 of Lecture Notes on Computer Science, pages 114-130, Toronto, Canada, July 2008. Springer.

- Deepak Garg, Jason Franklin, Dilsun Kaynar, and Anupam Datta. A Logic for Reasoning About Networked Secure Systems . In *Proceedings of the Joint Workshop on Foundations of Computer Security, Automated Reasoning for Security Protocol Analysis and Issues in the Theory of Security (FCS-ARSPA-WITS)*, pages 143-161, Pittsburgh, Pennsylvania. June, 2008.

- 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)*, pages. 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)*, pages 238-253, Stockholm, Sweden, September 18-20, 2006. Invited paper. Springer.

- 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. IEEE.

- 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)*, pages 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, pages 17-31, 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.
- Toh Ne Win, Michael D. Ernst, Stephen J. Garland, Dilsun K. Kaynar, and Nancy Lynch. Using simulated execution in verifying distributed algorithms. In *Proceedings of Fourth International Conference on Verification, Model Checking and Abstract Interpretation (VMCAI)*,Volume 2575 of Lecture Notes in Computer Science, pages 283-297, New York, January 2003. Springer.
- 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 Kırlı. 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 Kırlı. 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 Kırlı. 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 Kırlı. 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.

Technical Reports

- Henry DeYoung, Deepak Garg, Dilsun Kaynar, Anupam Datta. Privacy Policy Specification and Audit in a Fixed-Point Logic - How to enforce HIPAA, GLBA and all that. Technical report CMU-CyLab-10-008, 2010.

- Henry DeYoung, Deepak Garg, Dilsun Kaynar, Anupam Datta. Logical Specification of the GLBA and HIPAA Privacy Laws. Technical report CMU-CyLab-10-007, 2010.
- Michael Tschantz, Anupam Datta, and Dilsun Kaynar. Differential Privacy for Probabilistic Systems. Technical Report CMU-CyLab-09-008, May, 2009.
- Deepak Garg, Jason Franklin, Dilsun Kaynar, and Anupam Datta. Towards a Theory of Secure Systems. Technical Report CMU-Cylab-08-003, February, 2008.
- Ran Canetti, Ling Cheung, Dilsun Kaynar, Nancy Lynch, and Olivier Pereira. Modeling Computational Security in Long-Lived Systems, Version 2. Technical Report MIT-CSAIL-TR-2008-068, Computer Science and Artificial Intelligence Laboratory, Massachusetts Institute of Technology, Cambridge, MA, November 2008.
- Pratyusa K. Manadhata, Dilsun K. Kaynar, and Jeannette M. Wing. A Formal Model for A System's Attack Surface. CMU Technical Report CMU-CS-07-144, July 2007.
- Ran Canetti, Ling Cheung, Dilsun Kaynar, Moses Liskov, Nancy Lynch, Olivier Pereira, and Roberto Segala. Using Task-Structured Probabilistic I/O Automata to Analyze an Oblivious Transfer Protocol. MIT-CSAIL-TR-2006-047, June 2006. This report is a revision of MIT-CSAIL-TR-2006-019, March 2006.
- 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 Kırlı. 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 Kırlı, 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.

Other

- Ran Canetti, Ling Cheung, Dilsun Kaynar, Moses Liskov, Nancy Lynch, Olivier Pereira, and Roberto Segala. Task-structured Probabilistic I/O Automata. Under revision.
- Michael Tschantz, Anupam Datta, and Dilsun Kaynar. Formal Verification of Differential Privacy. September 2010. Submitted.

- Nancy Lynch, Stephen Garland, Dilsun Kaynar, Laurent Michel, Alex Shvartsman. The Tempo Language User Guide and Reference Manual. 2007. Available at `http://www.veromodo.com/tempo/`.
- Dilsun Kırlı. A test case assessor for ML. MSc Thesis. The University of Edinburgh, 1997.

References

PhD Supervisor:
Stephen Gilmore
Reader, School of Informatics
The University of Edinburgh
Room 3.47, Informatics Forum
10 Crichton Street
Edinburgh EH8 9AB, Scotland, UK
Phone: +44 131 650 5189
Fax: +44 131 667 7209
Email: Stephen.Gilmore@ed.ac.uk

Postdoctoral Advisor:
Nancy Lynch
Professor of Electrical Engineering and Computer Science
MIT Computer Science and Artificial Intelligence Laboratory
Stata Center, 32 Vassar Street, G668
Cambridge, MA 02139, USA
Phone: 617 253 7255
Fax: 617 258 8682
Email: lynch@csail.mit.edu

Postdoctoral Advisor:
Jeannette Wing
Professor of Computer Science
Computer Science Department, Carnegie Mellon University
5000 Forbes Avenue
Pittsburgh, PA 15213
Phone: 412-268-3068 (office), 412-260-8926 (cell)
Email: wing@cs.cmu.edu

Postdoctoral Advisor:
Anupam Datta
Assistant Research Professor, CyLab
Carnegie Mellon University
4720 Forbes Avenue
Collaborative Innovation Center, Room 2118
Phone: 617 268 4254
Fax: 617 268 5531
Email: danupam@cmu.edu

Research Collaborator:
Bruce Krogh
Professor of Electrical and Computer Engineering
Carnegie Mellon University
5000 Forbes Avenue, B26 Porter Hall
Pittsburgh, PA 15213-3890
Phone: 412 268 2472
Fax: 412 268 3890
Email: krogh@ece.cmu.edu

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