POLICY 2010 PROGRAM

Wednesday, July 21

9:00 am *Welcome*

Conference Chairs

9:15 am *Invited Presentation* (Session Chair: Marianne Winslett)

Lorrie Faith Cranor, Carnegie Mellon University

"Building a Better Privacy Policy"

Abstract: Today's online privacy policies are failing consumers because they are difficult to understand and take too long to read. At the CyLab Usable Privacy and Security Laboratory at Carnegie Mellon University, we've developed and evaluated new ways of making privacy policies more usable for consumers. One approach is to distill privacy policy information into a simple privacy rating, and display this rating as an annotation to search engine results. Our laboratory studies have demonstrated that by including privacy ratings in search results consumers are motivated to seek out websites with better privacy policies and pay a small premium for better privacy. We've also conducted studies comparing a number of existing and new privacy policy formats to determine which are most usable, and developed and evaluated a new privacy "nutrition label" format based on concepts from standardized food labels. We've developed tools to generate our privacy nutrition labels automatically for websites that have Platform for Privacy Preferences (P3P) computer-readable privacy policies, and integrated this into the privacyfinder.org, a search engine run by our lab. We've also collected a large cache of P3P policies, which we've been able to mine for data about P3P and privacy policy trends. In this talk, I will review our approach to building a better privacy policy, discuss our studies, and highlight the lessons learned.

Biography: Lorrie Faith Cranor is an Associate Professor of Computer Science and of Engineering and Public Policy at Carnegie Mellon University where she is director of the CyLab Usable Privacy and Security Laboratory (CUPS). She is also Chief Scientist of Wombat Security Technologies, Inc. She has authored over 80 research papers on online privacy, phishing and semantic attacks, spam, electronic voting, anonymous publishing, usable access control, and other topics. She has played a key role in building the usable privacy and security research community, having co-edited the seminal book Security and Usability (O'Reilly 2005) and founded the Symposium On Usable Privacy and Security (SOUPS). She also chaired the Platform for Privacy Preferences Project (P3P) Specification Working Group at the W3C and authored the book Web Privacy with P3P (O'Reilly 2002). She has served on a number of boards, including the Electronic Frontier Foundation Board of Directors, and on the editorial boards of several journals. In 2003 she was named one of the top 100 innovators 35 or younger by Technology Review magazine. She was previously a researcher at AT&T-Labs Research and taught in the Stern School of Business at New York University.

10:30 am *Contributed Papers* (Session Chair: Naranker Dulay)

Social Networking and Usability

"Collaborative Privacy Policy Authoring in a Social Networking Context"
Ryan Wishart, Imperial College London
Domenico Corapi, Imperial College London
Srdjan Marinovic, Imperial College London

Morris Sloman, Imperial College London

"User Centric Policy Management in Online Social Networks"
Mohamed Shehab, University of North Carolina at Charlotte
Gorrell Cheek, University of North Carolina at Charlotte
Hakim Touati, University of North Carolina at Charlotte
Anna Squicciarini, The Pennsylvania State University
Pau-Chen Cheng, IBM T.J. Watson Research Center.

"A Policy Based Infrastructure for Social Data Access with Privacy"
Palanivel Kodeswaran, University of Maryland, Baltimore County
Evelyne Viegas, Microsoft Research

"Usable Policy Template Authoring for Iterative Policy Refinement"
Maritza Johnson, Columbia University
John Karat, IBM TJ Watson Research Center Hawthorne
Clare-Marie Karat, IBM TJ Watson Research Center Hawthorne
Keith Grueneberg, IBM TJ Watson Research Center Hawthorne

12:00 noon *Lunch*

1:30 pm *Contributed Papers* (Session Chair: Jeffrey Mark Bradshaw)

Usage Control

"Downstream Usage Control"
Laurent Bussard, European Microsoft Innovation Center
Gregory Neven, IBM Zurich Research Laboratory
Franz-Stefan Preiss, IBM Zurich Research

"Coordinating Data Usage Control in Loosely-Connected Networks"
Giovanni Russello, Create-Net
Enrico Scalavino, Imperial College London
Naranker Dulay, Imperial College London
Emil Lupu, Imperial College London

Debugging Policies

"ACPT: A Tool for Modeling and Verifying Access Control Policies"
JeeHyun Hwang, North Carolina State University
Tao Xie, North Carolina State University
Vincent Hu, NIST
Mine Altunay, Fermi National Laboratory

"An Intelligent Network for Federated Testing of NetCentric Systems"
Edward Chow, Jet Propulsion Laboratory
Mark James, Jet Propulsion Laboratory
Hsin-Ping Chang, Jet Propulsion Laboratory
Farrokh Vatan, Jet Propulsion Laboratory

Gurusham Sudhir, Jet Propulsion Laboratory

3:20 pm *Contributed Papers* (Session Chair: Dave Eyers)

Policy Applications I

"Mobile PAES: Demonstrating Authority Devolution for Policy Evaluation in Crisis Management Scenarios"
Enrico Scalavino, Imperial College London
Vaibhav Gowadia, Imperial College London
Rudi Ball, Imperial College London
Emil Lupu, Imperial College London
Giovanni Russello, Create-Net

"Teleo-Reactive Policies in Ponder2"
Kevin Twidle, Imperial College London
Srdjan Marinovic, Imperial College London
Naranker Dulay, Imperial College London

"Policy-Based Management for Resource-Constrained Devices and Systems"
Anna Litvina, MATERNA GmbH
Christoph Fiehe, MATERNA GmbH
Ingo Lueck, MATERNA GmbH
Franz-Josef Stewing, MATERNA GmbH
Jan Krueger, TU Dortmund University
Oliver Dohndorf, TU Dortmund University
Heiko Krumm, TU Dortmund University

4:20 pm *End of Scheduled Events*

Thursday, July 22

9:00 am *Invited Presentation* (Session Chair: Ken Moody)

Reagan Moore, University of North Carolina at Chapel Hill

"Policy-based Data Management"

Abstract: The organization of distributed data into sharable collections requires highly extensible systems capable of enforcing and evolving management policies. The integrated Rule Oriented Data System (iRODS) provides a framework within which policies can be defined, enforced, and audited for a wide variety of data management systems, ranging from data grids, to digital libraries, to processing pipelines, to persistent archives. Each application is characterized by a different set of policies and procedures, by a different set of assessment criteria, and by a different preferred access mechanism. The iRODS data grid installs a rule engine at each site where data will be stored, enforces local policies that must be met before data can leave the storage, and enforces global policies that apply to the shared collection. The open source software is provided under a BSD license from http://irods.diceresearch.org.

Biography: Reagan Moore is a Professor in the School of Information and Library Science at the

University of North Carolina at Chapel Hill, Chief Scientist for Data Intensive Cyber Environments at the Renaissance Computing Institute, and Director of the Data Intensive Cyber Environments Center at UNC. He coordinates research efforts in development of data grids, digital libraries, and preservation environments. Developed software systems include the Storage Resource Broker data grid and the integrated Rule-Oriented Data System. Supported projects include the National Archives and Records Administration Transcontinental Persistent Archive Prototype, and science data grids for seismology, oceanography, climate, high-energy physics, astronomy, and bio-informatics. An ongoing research interest is use of data grid technology to automate execution of management policies and validate trustworthiness of repositories.

Moore's previous roles include: Director of the DICE group at the San Diego Supercomputer Center, and Manager of production services at SDSC. He previously worked as a computational plasma physicist at General Atomics on equilibrium and stability of toroidal fusion devices. He has a Ph.D. in plasma physics from the University of California, San Diego, (1978) and a B.S. in physics from the California Institute of Technology (1967).

10:15 am *Contributed Papers* (Session Chair: Peter Linington)

Policy Applications II

"Automated Policy Generation Framework for Large-Scale Storage Infrastructures"
Ramani Routray, IBM Research - Almaden
David Eyers, University Of Cambridge
Peter Pietzuch, Imperial College London
Rui Zhang, IBM Research - Almaden
Prasenjit Sarkar, IBM Research - Almaden
Douglas Wilcocks, Imperial College London

"Linking Policies to the Spatial Environment"
David Evans, University of Cambridge
David Eyers, University of Cambridge
Jean Bacon, University of Cambridge

"QoP and QoS Policy Cognizant Module Composition"
Paul Seymer, George Mason University
Angelos Stavrou, George Mason University
Duminda Wijesekera, George Mason University
Sushil Jajodia, George Mason University

"Automatic Policy Mapping to Management System Configurations"
Abdelnasser Ouda, University of Western Ontario
Michael Bauer, University of Western Ontario
Hanan Lutfiyya, University of Western Ontario

12:05 pm *Lunch*

1:30 pm *Invited Presentation* (Session Chair: Marianne Winslett)

Annie Antón, North Carolina State University

"Compliance with Policies and Regulations"

Abstract: Properly protecting information is in all our best interests, but it is a complex undertaking. The fact that regulation is often written by non-technologists, introduces additional challenges and obstacles. Moreover, those who design systems that collect, store, and maintain sensitive information have an obligation to design systems holistically within this broader context of regulatory and legal compliance.

There are questions that should be asked when developing new requirements for information systems. For example: How do we build systems to handle data that must be kept secure and private when relevant regulations tie your hands? When building a system that maintains health or financial records for a large number of people, what do we need to do to protect the information against theft and abuse, keep the information private, *and* at the same time, satisfy all governing privacy laws and restrictions? Moreover, how do we know that we've satisfied those laws? How do we monitor for compliance while ensuring that we're monitoring the right things? And, how do you accomplish all this in a way that can be expressed clearly to end-users and legislators (or auditors) so they can be confident you are doing the right things?

We've been working on technologies to make these tasks simpler, and in some senses, automatic. In this talk, I will describe some of the research that we have been conducting to address these problems. The results of some of our studies pose interesting ethical questions for industry and society at large, and help illustrate the complexity of the problems.

Biography: Annie Antón is a Professor in the Computer Science Department of the College of Engineering at North Carolina State University (NCSU), where she is a member of the NCSU Cyber Defense Lab. Her research focuses on methods and tools to support the specification of complete, correct behavior of software systems used in environments that pose risks of loss as a consequence of failures and misuse. This includes Web-based and e-commerce systems in which the security of personal and private information is particularly vulnerable. Antón is the founder and director of ThePrivacyPlace.org, a research group of students and faculty at NCSU, Georgia Tech and Purdue. She is leading this group in the development of technology to assist practitioners and policy makers in meeting the challenge of eliciting and expressing policies (a form of requirements). These tools help ensure that privacy policies are aligned with the software systems that they govern.

Antón is co-founder of the Symposium on Requirements Engineering for Information Security (SREIS), which has bridged the gap between the software engineering and information security research communities. In 2002 she coordinated NC State's successful application for a National Security Agency Center of Academic Excellence in Information Assurance Education, involving the participation of faculty in three Colleges. She is an associate editor for IEEE Transactions on Software Engineering, the cognitive issues subject area editor for the Requirements Engineering Journal, and a member of the International Board of Referees for Computers & Security. Antón currently serves on the DHS Data Privacy and Integrity Advisory Committee and the CRA Board of Directors. She is a former member of the NSF CISE Advisory Council, IDA/DARPA Defense Science Study Group, Microsoft Research's University Relations Faculty Advisory Board, the Georgia Tech Advisory Board (GTAB) and the CRA-W Board.

2:45 pm *Contributed Papers* (Session Chair: Dave Eyers)

Authorization

" DAuth: Fine-grained Authorization Delegation for Distributed Web Application Consumers"
Joshua Schiffman, Pennsylvania State University
Xinwen Zhang, Samsung Information Systems America

Simon Gibbs, Samsung Information Systems America

"Toward Self-contained Authorization Policies"
Romain Laborde, IRIT/SIERA
Marwan Cheaito, University Paul Sabatier
Barrère François, IRIT/SIERA
Benzekri Abdelmalek, IRIT/SIERA

"A Small But Non-negligible Flaw in the Android Permission Scheme"
Wook Shin, KDDI R&D Laboratories, Inc.
Sanghoon Kwak, Dept. of EECS, Seoul National University
Shinsaku Kiyomoto, KDDI R&D Laboratories, Inc.
Kazuhide Fukushima, KDDI R&D Laboratories, Inc.
Toshiaki Tanaka, KDDI R&D Laboratories, Inc.

"A Model for the Governance of Federated Healthcare Information Systems"
Naftaly Minsky, Rutgers University

Policy Models and Languages

"Toward Policy-Based Data Downgrading: Semantic Framework and Automated Tools to Balance Need-To-Protect and Need-To-Share Policies"
Grit Denker, SRI International
Ashish Gehani, SRI International
Minyoung Kim, SRI International
David Hanz, SRI International

"JTAM - A Joint Threshold Administration Model"
Ashish Kamra, Purdue University
Elisa Bertino, Purdue University

5:15 pm *End of Scheduled Events*

Friday, July 23

9:00 am *Invited Presentation* (Session Chair: Ken Moody)

Boon Thau Loo, University of Pennsylvania

"Declarative Policy-based Networking"

Abstract: Declarative networking is a programming methodology that enables developers to concisely specify network protocols and services using a distributed recursive query language, which are directly compiled to a dataflow framework that executes the specifications. This approach provides ease and compactness of specification, and offers additional benefits such as optimizability and the potential for safety checks.

The declarative networking agenda started in 2005 with an initial goal of enabling safe extensible routers. Since we began our work on this topic, there has been increasing evidence that declarative, data-centric programming has much broader applicability. Researchers have expanded in multiple directions from our initial work on routing, to encompass low-level network issues at the wireless link layer, to higher-level logic including both overlay networks, robotics, distributed machine learning, and applications like code dissemination and content distribution.

This talk will first present an overview of declarative networking research and a broad survey of use cases in this field. I will next describe two specific instances relevant to policy-based networking. The first instance is in the security domain where security extensions to declarative networking enables the integration of security policies and distributed systems within a common declarative framework. The second instance utilizes declarative networking to implement adaptive hybrid protocols, where policy-driven adaptation of network protocols are specified in a generic set of declarative rule-based policies.

I will conclude with a discussion of ongoing research work, as well as a number of open challenges in declarative networking.

Biography: Boon Thau Loo is an Assistant Professor in the Computer and Information Science department at the University of Pennsylvania. He received his Ph.D. degree in Computer Science from the University of California at Berkeley in 2006. Prior to his Ph.D., he received his M.S. degree from Stanford University in 2000, and his B.S. degree with highest honors from UC Berkeley in 1999. His research focuses on distributed data management systems, Internet-scale query processing, and the application of data-centric techniques and formal methods to the design, analysis and implementation of networked systems. He was awarded the 2006 David J. Sakrison Memorial Prize for the most outstanding dissertation research in the Department of EECS at UC Berkeley, and the 2007 ACM SIGMOD Dissertation Award. He is a recipient of the NSF CAREER award (2009). He was also the program co-chair for the CoNEXT 2008 Student Workshop and the NetDB 2009 workshop co-located with SOSP.

10:15 am *Contributed Papers* (Session Chair: Duminda Wijesekera)

Networking and Virtual Organizations

"A Negotiation Framework for Negotiation of Coalition Policies"
Mandis Beigi, IBM Research
Jorge Lobo, IBM Research
Keith Grueneberg, IBM Research
Seraphin Calo, IBM Research
John Karat, IBM Research

"Enforcement of Data-Plane Policies in Next-Generation Networks"
Shashank Shanbhag, University of Massachusetts, Amherst
Tilman Wolf, University of Massachusetts, Amherst

"Towards Autonomous Administrations of Decentralized Authorization for Inter-domain Collaborations"
Hannah K. Lee, SVA, TU-HH

"Efficient Policy Checking Across Administrative Domains"
David Evans, University of Cambridge
David Eyers, University of Cambridge

11:45 am *Lunch*

1:15 pm *Conference Ends*