In the Internet’s early days, few people foresaw the emergence of spam, phishing, and malware such as the viruses, worms, Trojan horses, spyware, and key loggers that plague users today. The widespread deployment of sensor-based systems, wireless networking, mobile and embedded devices, and other pervasive computing technologies poses even greater risks to security and privacy. Devices can be overrun, revealing information about their physical operating environment. Furthermore, new wireless networking technologies might be susceptible to eavesdropping and thus could expose personal information about their users. Even when the technological foundations are secure, users might still reject a system simply because they don’t feel comfortable or safe using it.

Fortunately, the research community has been facing these challenges head on—even the Palo Alto Research Center’s original papers on ubiquitous computing noted security and privacy concerns. Since then, researchers have continued to discuss how to effectively secure pervasive computing systems and maintain appropriate levels of privacy for users (see the “Related Resources” sidebar). Security and privacy concerns touch on all aspects of pervasive computing, including hardware, operating systems, networks, databases, user interfaces, and applications. The seven articles that we selected for this special issue draw on ideas from many of these fields and provide a flavor of the kinds of security and privacy challenges and opportunities in pervasive computing.

Security for mobile computing

Ensuring security and privacy will require significant advances in pervasive computing’s technological underpinnings. Currently, most of us carry around all of our data and computational power. In contrast, two articles discuss the development of a small, mobile device that can leverage the computing infrastructure already in the environment.

In “Securing Pocket Hard Drives,” Nishkam Ravi, Chandra Narayanaswami, Mandayam Raghunath, and Marcel-Catalin Rosu introduce the idea of portable storage-based personalization. Users carry a pocket hard drive and then boot a borrowed PC from this device. In “Rapid Trust Establishment for Pervasive Personal Computing,”
Related Resources

A great deal of work has examined the issue of security and privacy for pervasive computing. Here, we highlight a few resources that are good starting points.

**Articles**

There have been several special issues in the past focusing on privacy and security. *IEEE Pervasive Computing* published five articles looking at technical issues in its Jan.–March 2003 issue. The following year, *Personal and Ubiquitous Computing* (vol. 8, no. 6) contained five articles examining social issues, design challenges, and user evaluations of systems with respect to privacy.

Giovanni Iachello and Jason Hong have a forthcoming article, “End-User Privacy in Human-Computer Interaction,” which will appear in *Foundations and Trends*. This article surveys privacy with respect to design and evaluation across HCI.

**Workshops**

There have also been a series of privacy workshops held at the International Conference on Ubiquitous Computing:

- Ubicomp Communities: Privacy as Boundary Negotiation (Ubicomp 03): http://guir.berkeley.edu/pubs/ubicomp2003/privacyworkshop/
- Intimate Computing (Ubicomp 03): www.paulos.net/intel/lab/ubicomp03/Workshop
- Privacy Workshop (Ubicomp 04): www.cs.berkeley.edu/~jfc/ubicomp-privacy2004
- Ubicomp Privacy: Privacy in Context (Ubicomp 05): http://people.ischool.berkeley.edu/~jensg/ubicomp2005
- Ubicomp Privacy: Technologies, Users, and Policy (Ubicomp 07): www.vs.inf.ethz.ch/events/uc07/privacy

**The user experience**

The user interface for security and privacy functions is another important consideration when designing pervasive computing systems. Today’s desktop computers typically identify and authenticate users by requesting a username and password. However, this doesn’t work well in pervasive computing environments, because a person will likely use multiple systems in a given day and text input is difficult in such environments.

Biometrics, which identifies people on the basis of such features as their fingerprint, iris, or face, is one possible solution to this problem. In “Palmprint Verification for Controlling Access to Shared Computing Resources,” Maylor Leung, A.C.M. Fong, and Siu Cheung Hui evaluate a new algorithm for identifying people on the basis of palmprints, with promising results.

Another important aspect of the user experience is how the system lets people manage their privacy. “Physical Access Control for Captured RFID Data,” by Travis Kriplean, Evan Welbourne, Nodira Khousainova, Vibhor Rastogi, Magdalena Balazinska, Gaetano Borriello, Tadayoshi Kohno, and Dan Suciu, discusses the deployment of a building-wide RFID infrastructure that can track people and objects. It also presents a model for physical access control, restricting what historical information a person can see on the basis whether that person was physically present when that information was recorded.

We also need user studies to deepen our understanding of how people use and perceive pervasive computing systems. A key problem in this area is understanding what leads people to accept or reject a pervasive computing system. In “Physical, Social, and Experiential Knowledge in Pervasive Computing Environments,” Gillian Hayes, Erika Shehan Poole, Giovanni Iachello, Andrea Grimes, Gregory Abowd, and Khai Truong summarize their evaluation of a pervasive computing system for recording everyday experiences in an informal space. Drawing on these experiences, they present a model for how users use physical, social, and experiential knowledge to decide what level of utility and privacy a new technology offers.

Another open question is, “What kind of personal information is a person willing to share and under what conditions?” In “Privacy in Location-Aware Computing Environments,” Denise Anthony, Tristan Henderson, and David Kotz present intriguing results from their study of privacy preferences for location

Ajay Surie, Adrian Perrig, Mahadev Satyanarayanan, and David Farber describe their work on Trust-Sniffer, a user-carried device that can verify secure applications and incrementally expand a user’s list of trusted applications.

Improvements in wireless networking can also help address security and privacy concerns. “Multichannel Security Protocols,” by Ford Long Wong and Frank Staiano, describes how to use multiple wireless channels simultaneously to improve overall security. Their insight is that different channels have different security properties, so we can develop new protocols that combine the best of each.
information. The results suggest that important factors include how users define where they are, what they’re currently doing, and who they’re with.

This issue’s articles represent only a snapshot of the ongoing research in privacy and security for pervasive computing. We look forward to practitioners and researchers continuing their attempts to overcome security and privacy challenges so that the grand vision of pervasive computing can come to fruition.

The results suggest that important factors include how users define where they are, what they’re currently doing, and who they’re with.

This issue’s articles represent only a snapshot of the ongoing research in privacy and security for pervasive computing. We look forward to practitioners and researchers continuing their attempts to overcome security and privacy challenges so that the grand vision of pervasive computing can come to fruition.

OCTOBER–DECEMBER 2007

PERVASIVE computing

CALL FOR PAPERS

IEEE PERVERSIVE COMPUTING

Pervasive User-Generated Content

User-generated content can range from content created explicitly by the user and uploaded to help shape their ubicomp experience through to small contributions from large numbers of distributed contributors that can subsequently be mined and analyzed. The theme of this special issue spans data collection, processing, presentation, and evaluation. We welcome submissions on all aspects of this topic, including:

- Networked data-gathering from large populations
- Data mining and machine learning from distributed sources
- Tracking multitudes of everyday objects
- Mashups/overlays of user data with other artifacts such as maps
- Users as computing platforms and intelligent data sources
- Games/other schemes for gathering data from large populations
- Usability aspects for efficient data contribution
- Applications and displays of pervasively generated content

Guest Editors: John Krumm, Microsoft Research; Chandra Narayanaswami, IBM Research; Nigel Davies, Lancaster University

Submissions should be 4,000 to 6,000 words and should follow the magazine’s guidelines on style and presentation (see www.computer.org/pervasive/author.htm). All submissions will be anonymously reviewed in accordance with normal practice for scientific publications.

In addition to full-length submissions, we also invite work-in-progress submissions of 250 words or less (submit to mgamborg@computer.org) by 11 Aug. 2008. These will not be peer reviewed but will be reviewed by the Department Editor.

Jason Hong is an assistant professor at Carnegie Mellon University’s Human Computer Interaction Institute. His research interests include location-based services and usable security and privacy. He received his PhD in computer science from the University of California at Berkeley. Contact him at jasonh@cs.cmu.edu.

Mahadev Satyanarayanan is the Carnegie Group Professor of Computer Science at Carnegie Mellon University. His research interests include mobile computing, pervasive computing, and distributed systems. He received his PhD in computer science from Carnegie Mellon University. He’s a fellow of the ACM and IEEE and the founding editor in chief of IEEE Pervasive Computing. Contact him at the Computer Science Dept., Carnegie Mellon Univ., Wean Hall 4212, 5000 Forbes Ave., Pittsburgh, PA 15213; satya@cs.cmu.edu.

George Cybenko is the Dorothy and Walter Gramm Professor of Engineering at Dartmouth College. His research interests include distributed information, control systems, computer security, and signal processing. He received his PhD in mathematics from Princeton University. He’s a fellow of the IEEE and a member of the Society for Industrial and Applied Mathematics, and he serves on the boards of the IEEE Computer Society and the Computing Research Association. He was the founding editor in chief of IEEE Security & Privacy. Contact him at gvc@dartmouth.edu.

CALL FOR PAPERS

IEEE PERVERSIVE COMPUTING

Pervasive User-Generated Content

User-generated content can range from content created explicitly by the user and uploaded to help shape their ubicomp experience through to small contributions from large numbers of distributed contributors that can subsequently be mined and analyzed. The theme of this special issue spans data collection, processing, presentation, and evaluation. We welcome submissions on all aspects of this topic, including:

- Networked data-gathering from large populations
- Data mining and machine learning from distributed sources
- Tracking multitudes of everyday objects
- Mashups/overlays of user data with other artifacts such as maps
- Users as computing platforms and intelligent data sources
- Games/other schemes for gathering data from large populations
- Usability aspects for efficient data contribution
- Applications and displays of pervasively generated content

Guest Editors: John Krumm, Microsoft Research; Chandra Narayanaswami, IBM Research; Nigel Davies, Lancaster University

Submissions should be 4,000 to 6,000 words and should follow the magazine’s guidelines on style and presentation (see www.computer.org/pervasive/author.htm). All submissions will be anonymously reviewed in accordance with normal practice for scientific publications.

In addition to full-length submissions, we also invite work-in-progress submissions of 250 words or less (submit to mgamborg@computer.org) by 11 Aug. 2008. These will not be peer reviewed but will be reviewed by the Department Editor.

Jason Hong is an assistant professor at Carnegie Mellon University’s Human Computer Interaction Institute. His research interests include location-based services and usable security and privacy. He received his PhD in computer science from the University of California at Berkeley. Contact him at jasonh@cs.cmu.edu.

Mahadev Satyanarayanan is the Carnegie Group Professor of Computer Science at Carnegie Mellon University. His research interests include mobile computing, pervasive computing, and distributed systems. He received his PhD in computer science from Carnegie Mellon University. He’s a fellow of the ACM and IEEE and the founding editor in chief of IEEE Pervasive Computing. Contact him at the Computer Science Dept., Carnegie Mellon Univ., Wean Hall 4212, 5000 Forbes Ave., Pittsburgh, PA 15213; satya@cs.cmu.edu.

George Cybenko is the Dorothy and Walter Gramm Professor of Engineering at Dartmouth College. His research interests include distributed information, control systems, computer security, and signal processing. He received his PhD in mathematics from Princeton University. He’s a fellow of the IEEE and a member of the Society for Industrial and Applied Mathematics, and he serves on the boards of the IEEE Computer Society and the Computing Research Association. He was the founding editor in chief of IEEE Security & Privacy. Contact him at gvc@dartmouth.edu.