Editor in Chief: Roy Want ■ Intel Research ■ roy.want@intel.com

You're Not Paranoid; They Really Are Watching You!

Roy Want

Security and privacy are hot topics to consider when designing pervasive computing systems. Hot is the operative word, because if you compromise security or privacy, you'll likely upset a lot of people, and a heated discussion will ensue. I doubt many people would disagree with this observation. However, in practice, I've found that attention to security as well as interpretations of privacy vary a great deal.

SECURITY AS AN AFTERTHOUGHT

When designing any kind of computer system, it's common sense to consider security. However, many pervasive computing systems built under the guise of research don't start with a good security story. I've helped design and implement several such systems, so let me shed some light on the mindset.

A research project usually sets out to enable something that wasn't possible before. Designing such a system can be difficult, but the project's vision motivates the people involved and they're excited about actually using the resulting technology.

However, when it comes to security, we start thinking about ways to stop people from using this new capability. We create barriers that will stop the "bad guys" and, unfortunately, the good guys too when they forget their credentials. Even when a legitimate user has the correct credentials, security slows them down, requiring a password or similar authentication process. Security thus creates a negative mindset, and, for many of us, it's not why we joined the pervasive computing business.

Clearly, some researchers have staked their careers on pervasive computing security, and their important design contributions will help protect complex distributed systems. I don't wish to do anybody a disservice here; however, their motivation usually differs from that of the accompanying system builders. Consequently, we often don't architect secure systems, so we find ourselves adding security features only after we've accomplished the system's main goal.

PRIVACY AND CONTEXT

The work I am best known for from the '90s is the Active Badge project, which set out to find a way to automatically route telephone calls to the correct place in a building. To a new generation of researchers, this probably seems like a no-brainer; just buy everybody a cell phone!

However, at the time, there were no cell phones, and business phones were almost exclusively based on a Private Branch eXchange service (which many organizations still use). I wanted to automate the process of call-forwarding from an employee's default extension to the extension closest to the person's location. The solution I came up with was to have everybody wear an electronic badge that periodically beaconed a unique infrared signal. A network of low-cost infrared receivers distributed throughout the building would then record the signal, and a central server could collect all the data. A simple network service would let clients enter a name and look up the corresponding badge ID to determine the station where it was last sighted, along with the corresponding room and nearest extension.

As soon as we had built the system, we realized it was part of a far bigger pervasive computing story—thus the notion of context-aware computing was born. As you might expect, when shown publicly, the privacy issue was the main discussion point, inspiring a host of press articles with sensational titles such as "The Boss That Never Blinks" (*San Jose Mercury News*, West Magazine, 8. Mar. 1992) and "Orwellian Dream Come True: A Badge That Pinpoints You" (*The New York Times*, 12 Sept. 1992). Furthermore, all reporters inevitably asked

MISSION STATEMENT: *IEEE Pervasive Computing* is a catalyst for advancing research and practice in mobile and ubiquitous computing. It is the premier publishing forum for peer-reviewed articles, industry news, surveys, and tutorials for a broad, multidisciplinary community.

Published by the IEEE Computer Society ■ 1536-1268/07/$25.00 © 2007 IEEE

EDITORIAL BOARD MEMBERS

A number of board members have stepped down after considerable service to *IEEE Pervasive Computing*: Jean Bacon, Guerney Hunt, Mahmoud Naghshineh, Badri Nath, Dan Siewiorek, Thad Starner, Gaurav Sukhatme, and Jim Waldo. I thank them for their contributions, which have made the magazine a success and maintained our high publication standards.

We also welcome six new editorial board members this issue. I look forward to their contributions.

John Canny is the Paul and Stacy Jacobs Distinguished Professor of Engineering and a Professor in the Computer Science Division at the University of California, Berkeley. He received his PhD from the Massachusetts Institute of Technology for his thesis, "The Complexity of Robot Motion Planning." He received his MS from MIT and his BE in electrical engineering from Adelaide University, South Australia. Contact him at jfc@cs.berkeley.edu.

Ramón Cáceres is a research staff member at IBM Research. His research interests include computer systems and networks—in particular, mobile computing, pervasive/ubiquitous computing, wireless networking, network measurement, virtual machines, and security. He received his PhD and MS in computer science from UC Berkeley, and his B.Eng in electrical engineering from McGill University. Contact him at ramon@kiskeya.net.

Beverly L. Harrison is a senior scientist at Intel Research, Seattle. Her research interests include consumer research, the design and evaluation of novel user interface technologies, UI design, ubiquitous computing, and mobile technologies and applications. She received her PhD in industrial engineering, her MS in applied science from the University of Toronto, and her BS in mathematics from the University of Waterloo, Ontario. Contact her at beverly.harrison@intel.com.

Paul Lukowicz is a full professor of computer science and chair of the Embedded Systems Lab at the University of Passau Germany. He's also head of the research division for Pervasive Healthcare Systems, UMIT. His research interests include pervasive and ubiquitous computing. In particular, he's interested in activity and context recognition and wearable systems. He received his his PhD in computer science from the University of Karlsruhe, Germany and his MSc in computer science and in physics. Contact him at paul.lukowicz@uni-passau.de.

Natalia Marmasse is a software engineer for Google at the Haifa R&D Lab. Her research interests include mobile, ubiquitous, context-aware, and collaborative computing, with a focus on social-mobile applications, location-based services, and generally how computers can enhance human communication. She received her PhD from the Massachusetts Institute of Technology, her masters in media arts and science (also from MIT), and her BS in computer science from State University of New York. Contact her at nmarmas@gmail.com.

Bernt Schiele is a full professor in the computer science department at Darmstadt University of Technology. His main research interests are computer vision, perceptual computing, robotics, statistical learning methods, wearable computers, and integration of multimodal sensor data. He is particularly interested in developing methods that work under real-world conditions. He received his PhD in computer vision from INP Grenoble, France. Contact him at schiele@informatik.tu-darmstadt.de.

IEEE Computer Society Publications Office

10662 Los Vaqueros Circle, PO Box 3014
Los Alamitos, CA 90720-1314

STAFF

Lead Editor
Shani Murray
smurray@computer.org

Group Managing Editor
Crystal R. Shif
cshif@computer.org

Senior Editors
Dale Strok, Dennis Taylor, and Linda World

Assistant Editors
Molly Gamborg and Brooke Miner

Publications Administrator
Hilda Carman
pervasive@computer.org

Contributing Editors
Thomas Centrella and Joan Taylor

Production Editor
Jennie Zhu

Technical Illustrations
Alex Torres

Associate Publisher
Dick Price

Membership & Circulation Marketing Manager
Georgann Carter

Business Development Manager
Sandra Brown

Advertising Coordinator
Marian Anderson

Submissions: Access the IEEE Computer Society's Web-based system, Manuscript Central, at http://cs-ieee.manuscriptcentral.com/index.html. Be sure to select the right manuscript type when submitting. Articles must be original and should be approximately 5,000 words long, preferably not exceeding 10 references. Visit www.computer.org/pervasive for editorial guidelines.

Editorial: Unless otherwise stated, bylined articles as well as products and services reflect the author's or firm's opinion; inclusion does not necessarily constitute endorsement by the IEEE Computer Society or the IEEE.

IEEE pervasive COMPUTING
MOBILE AND UBIQUITOUS SYSTEMS

if we had sensors in the bathrooms and almost seemed disappointed when we told them we didn't.

Despite the external jibes at this location capability, the majority of my colleagues weren't deterred from wanting—and proudly wearing—the badges. On the whole, they viewed the project

FROM THE EDITOR IN CHIEF

as breaking new ground and embracing the ubicomp vision. Displaying a badge meant you were "in" because ubicomp was "in." The system was certainly useful, but I'm not sure it would have been as successful without the implication that you were also helping to build the ubicomp vision. After all, it contributed to a loss of personal privacy in the office, and individuals might not have considered the value-to-cost trade-off to be worth it. It's hard to know without a control experiment.

The lesson I learned is that our interpretation of right-to-privacy in the context of a new technology is very variable. What makes technology a good or bad thing is dramatically affected by the social setting in which it is used. In other words, there's no absolute standard for privacy that we can record in a rule book and follow when designing something new.

ISSUES FOR PERVASIVE COMPUTING

In a world that has embraced pervasive computing, everyone will carry mobile devices, and the surroundings will contain a rich network of computer systems that communicate with each other and share resources to support user tasks. While this vision is still some way off, we're getting closer each day. We've already moved from a static computation environment centered on work and home to a more mobile one.

Ensuring both pervasive security and ease of use is a challenge for our research community. One mitigating factor is that smaller mobile devices now have the potential to let us carry a personal, trusted computing device at all times, and we can use it to overcome the lack of trust we might have in our surroundings. The assumption, of course, is that our mobile computers haven't been compromised.

Fortunately, considerable effort is going into the design of mobile systems based on Trusted Processing Modules (TPM). These devices ensure a computer boots from a valid code image and can create a chain of trust from a root encryption key. TPMs can also authenticate remote parties and validate and decrypt content—all while maintaining the secrecy of their keys. Only a complex physical attack on such a device is likely to reveal its contents, so maintaining possession of the device offers a reasonable guarantee of security.

Despite progress in this regard, physical security and secure protocols are only one part of the story. Social attacks that trick people into revealing credentials when they shouldn't are more difficult to guard against and present an ongoing challenge.

Pervasive privacy will be even more difficult to achieve. The more I learn about the subject, the harder it is for me to believe we can make effective progress. The main problem is that everything in the real world is unique, so a skillful observation can reveal a signature that you can trace back to the owner. For example, consider a mobile device with cellular communication and the ability to use strong encryption with rotating media access control addresses to hide identity. Despite considerable effort to ensure that privacy is protected by the protocol, a radio frequency expert could carefully analyze the RF signature and find characteristics in the baseband signal that would be unique to the device (probably traced back to imperfections in the transistors or the crystal oscillator at the heart of the system). As the device's owner will probably go home at some point, you could trace the signal to a house address and use a simple Web search to determine a name. You could then link the owner to sightings at other locations, determine the time they were there, and determine the transactions that occurred.

Thus both security and privacy will continue to hold many special challenges for computer systems, which are amplified further when used to support the goals of pervasive computing. It will be interesting to see what guarantees, if any, we can make for the future users of these systems. P