Minimizing Security Risks in Ubicomp Systems

Jason I. Hong, Carnegie Mellon University

In the Internet’s early days, few people foresaw the emergence of spam, phishing schemes, and malware such as viruses, worms, Trojan horses, spyware, and key loggers that plague users today. We can likewise expect unprecedented privacy and security risks with the widespread deployment of sensor-based systems, wireless networking, and mobile and embedded devices.

In 2004, socialite Paris Hilton’s smart phone was hacked twice. The hackers publicly posted online intimate photos that she had taken, personal e-mail, and phone numbers of other celebrities in her address book, causing a great deal of inconvenience and embarrassment for all those involved. These incidents, while not yet commonplace, highlight the vulnerabilities of ubiquitous computing systems.

MORE PERSONAL DATA

The amount of intimate information that ubicomp systems capture and store is rapidly increasing. In the near future, such systems will monitor everything from purchase preferences to TV viewing habits, location history, emotional state, driving behavior, and medical status.

Such rich and alluring data could be used to create invasive, personalized advertising as well as for more sinister purposes. For example, stalkers, jilted lovers, abusive spouses, or blackmailers could use spyware that surreptitiously monitors a mobile user’s whereabouts not only to generate annoying location-based spam but also as a form of surveillance.

It’s safe to assume that ubicomp technologies will suffer from the same sorts of unforeseen vulnerabilities that have plagued the Internet. For example, Web cookies were originally intended to facilitate browsing, but they quickly became a pervasive vehicle for tracking online activities. However, given the unprecedented amount of data in ubicomp systems, the potential threat to users is far greater.

OVERBURDENED USERS

As ubicomp systems proliferate, the burden of security and privacy protection is increasingly falling on the user. In at least one instance, Ms. Hilton lost data not because of the attack’s sophistication but because the hacker correctly guessed the answer to her poorly chosen password retrieval question—namely, “What is the name of your pet?”—which was publicly known.

Ms. Hilton’s data might have been safe if she had selected a more obscure password, but she’s no guiltier than many users confronted with today’s dizzying array of systems and applications requiring their own usernames and passwords. This approach made sense in the mainframe era, when people only needed one or two passwords, but it isn’t sustainable as computing systems become part of the fabric of our lives.

A related problem is maintaining system integrity—installing an effective security package, downloading the latest software patches and updates, and configuring everything correctly. Hiring a dedicated administrator to carry out such tasks on multiple systems is commonplace in companies but simply beyond the means of average users. If current trends continue, keeping home-based ubicomp systems up to date will become practically impossible.

MOBILE DEVICES AND WIRELESS NETWORKS ARE MAKING EXISTING SECURITY MODELS OBSOLETE

Mobile devices and wireless networks are making existing security models obsolete. It’s likely that Ms. Hilton thought that she was practicing “safe computing” by not sending risqué photos to people she thought would forward them on to others. Little did she know that her smart phone allowed remote access.

However, even if Ms. Hilton was aware of this and the associated risks, it’s just as likely she wouldn’t have been able to configure the settings correctly. A recent usability study conducted by Cynthia Kuo and colleagues at Carnegie Mellon University showed that even highly technical users had significant trouble configuring Wi-Fi access points to support basic security
features and getting clients to connect properly.

Another problem with mobile devices is that they can be misplaced or stolen. Some phones in Japan and Scandinavia can be used to purchase items, enabling thieves to easily commit fraud. US federal laws currently cap liability for unauthorized use of a credit card to $50, but it’s not clear whether this includes smart phone transactions. There are no safeguards against the theft of electronic cash on such devices.

In the future, the loss or theft of mobile devices will put more than data, credit, or e-money at risk. Researchers have already prototyped systems that let mobile phone users remotely unlock the doors to their homes, control their ovens and thermostats, and get streaming video of webcams installed in various rooms.

A single unaccounted for mobile device can create massive problems for an organization that are difficult, expensive, and time-consuming to remedy. For example, because most laptops are configured to tunnel through corporate firewalls, a company would have to assume that a lost or stolen laptop could be used to breach network security.

In March 2005, a laptop containing personal data on nearly 100,000 UC Berkeley alumni was stolen. Fortunately, the laptop was eventually recovered, but the incident dramatically exposed the system’s vulnerability to large-scale identity theft—a vulnerability that many organizations share.

MINIMIZING THE RISKS

What can we do to minimize the privacy and security risks associated with ubicomp systems?

An obvious solution is to reduce the costs of accessing and maintaining multiple systems. For example, many popular PDA and PC-based “key rings” manage user passwords across multiple Web sites. Users need only remember one password to access their key ring and log in to all of their sites. This feature is also built into many Web browsers.

In addition, some banks have started using two-factor authentication—for example, combining a physical token with a numeric code key that periodically refreshes in conjunction with a single password.

New interaction models could also mitigate ubicomp privacy and security risks.

Biometrics completely eliminate the need for passwords. For example, some PDAs and laptops come with fingerprint scanners that make authentication quick and easy without forcing users to remember anything.

A combination of these techniques can be used to make logging in to a large number of mobile and embedded systems manageable.

Securing multiple systems—with different operating systems, configurable preferences, and user interfaces—and keeping their software up to date presents a greater challenge. One way to deal with this problem is to make it easier for users to configure systems correctly. For example, the study by Kuo and colleagues featured a simplified user interface that enabled even novices to successfully set up a Wi-Fi access point.

Another possibility is to have each device automatically update itself with the deployment of new software, shifting the burden of maintenance from users to device manufacturers and service providers.

Yet another option is to provide ways of running a single operation on multiple devices simultaneously. For example, by using standard naming conventions, it would be possible to aggregate a collection of lightbulbs and turn them all on or off using a single command rather than issuing that same command to individual bulbs.


New interaction models could also mitigate ubicomp privacy and security risks. For example, to prevent unauthorized access to certain services from a stolen or lost mobile device, the device would have to periodically return to a certain physical place and “prove” that it’s in that location.

Better detection and recovery methods must also be developed. For example, aggregating personal information that is shared with others across all devices would give users a uniform view of who is seeing what about them. In addition, a system like Computrace—a software-based laptop recovery service that enables law enforcement to recover stolen computers after they are connected to a phone line or the Internet—could be adapted for locating misplaced or stolen mobile devices.

We can’t account for every possible security and privacy risk in ubiquitous computing systems. We can, however, design such systems to reduce the burden on users as well as develop better security models and interaction techniques to prevent and minimize foreseeable threats.

Jason I. Hong is an assistant professor in the Human-Computer Interaction Institute at Carnegie Mellon University’s School of Computer Science. Contact him at jasonb@cs.cmu.edu.