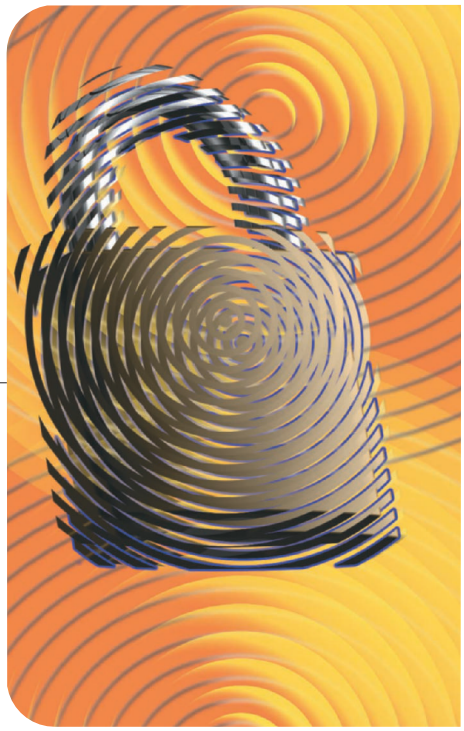
Wired on Wireless



Wireless technology is booming, and it's obvious why—everyone hates wires! Look under your desk lately? You'll likely find a "rat's nest" of cables for power, speakers, keyboard, mouse, the network, and maybe even the printer. No matter how organized or careful you are, the wires will become tangled over time, and you'll probably spend the majority of your time separating them the next time you move your equipment. Even having a laptop doesn't free you from wires: you still need your power, modem, and network cords, and possibly even a mouse. We just can't escape wires—or can we?

William A. Arbaugh
University of Maryland

New wireless technologies

In the past few years, we've seen wireless keyboards, mice, headsets, broadband networking, and even high-fidelity speakers. Radio frequency-based products' move toward the consumer space has greatly reduced the equipment's price, and this, in turn, has caused a groundswell of new consumer- and enterprise-oriented products that use wireless technology. This, however, creates the potential for security and privacy problems—the focus of this special issue.

New wireless technologies range from those that provide simple identifying information (such as radio frequency identification—RFID) to those that provide the wide-area broadband service Wi-Max, with Wi-Fi, Bluetooth, wireless USB (WUSB), and others in between. They all have great things to offer consumers and businesses alike. All, however, have some security or privacy concerns because the designers didn't pay attention to these issues in the design or implementation stages (as current and past analyses show) or because of how the technology can be used.

RFID is a simple protocol designed to "tag" items for tracking and accountability—a bar code that transmits. From tracking luggage as it moves around an airport, to tracking inventory in a store, or even prescriptions leaving the pharmacy, RFID's potential is significant. The problem is that RFID tags, unless removed, continue to operate after their intended use—after the consumer leaves the store, for example. Thus, you have the potential for the curious family "medicine cabinet snoop" (and every family has one) to get high tech: with the proper reader and close enough range to the tagged items, they might not even have to open the cabinet door, depending on the type of RFID tag.

Wi-Max, or IEEE 802.16, is a relatively new technology. It is designed to provide broadband wireless access (BWA) for wireless metropolitan area networks (WMANs). Wi-Max could potentially be used to solve the "last mile problem" of delivering high-speed broadband service to the home at a low enough cost to compete with DSL and cable broadband service. Unfortunately, as David Johnston and Jesse Walker show in their "Overview of IEEE 802.16 Security," Wi-Max has some serious security shortcomings that must be addressed before widespread adoption can be achieved.

The security of Wi-Fi, or IEEE 802.11, which provides wireless local area network service, has been the focus of numerous articles, headlines, and special issues. Fortunately, new IEEE standards have corrected several of the security problems discovered in the past few years. There are security risks, however, whenever you use wire-

less in sensitive environments; the installation, operation, and maintenance of the network must be monitored closely. In "Autonomic 802.11 Wireless LAN Security Auditing," Joel W. Branch and colleagues show us how the wireless infrastructure can be augmented with information from clients to provide a robust security monitoring system. While this degree of attention to security is not for everyone, it is essential to enterprises with high threat profiles.

Bluetooth is designed to connect peripherals and audio devices wirelessly. Fortunately, the Bluetooth special interest group that designed it considered security an important issue after some initial problems. Unfortunately, the technology does contain a few flaws that let attackers retrieve potentially sensitive information such as calendars, phone books, and even enough data to clone or copy the phone off of Bluetooth-enabled devices. It remains to be seen if these vulnerabilities exist due to a flaw in the protocol, its implementation, or even devices' user interfaces. These problems, however, drive home the fact that the threat to wireless-enabled equipment is significantly higher than to wired equipment because the attacker essentially has access to devices' communications simply by being within range of the targeted device.

With respect to security, the opposite end of the spectrum (no pun intended!) from Bluetooth is WUSB, a new initiative from Intel, Microsoft, and five other major electronics manufacturers. WUSB's goal is to be compatible with the wired USB 2.0; in this way, a WUSB-enabled device can bridge to legacy wired devices. Very little information is available about WUSB yet, but what is available raises concern from a security perspective. For example, WUSB's security goal is to provide the same level of security as wired USB.

While USB does have a security specification, I don't believe that any (or very few) actually implements it. But to be fair, I'll assume that proper authentication will always be used—whatever that means—in the context of WUSB. Unfortunately, authentication won't matter unless the channel is subsequently encrypted with a security association negotiated as part of or based on the authentication process. Attackers can easily hijack the channel or establish a man-in-the-middle attack when encryption is used properly. To their credit (or possibly discredit), the designers do offer the possibility of using encryption, but they leave it as an exercise for the application layer. Given the types of devices (keyboards, disk drives, and so on) that will use WUSB, my guess is that few vendors, if any, will bother to add encryption support.

What this means is that when you're using your WUSB keyboard at the airport, anyone within 10 meters will be able to receive your every keystroke—including passwords. Or, worse, anyone within 10 meters might be able to connect to your WUSB disk drive!

WUSB's designers might argue that WUSB devices' limited range will eliminate or mitigate any potential threat. Unfortunately, the effective range of wireless devices is often much larger than the specified range. Take Wi-Fi for example—most Wi-Fi devices' specified range is approximately 300 meters, yet stable connections are often made over much greater distances, often measured in kilometers, with the right antennas. Furthermore, there is one truism with technology: it will always be used in a manner that the designers never expected. As a result, even though the designers might feel that they have the security problems under control, users' creativity will identify problems the developers never thought of. Unless security is done right—designed in and reviewed throughout the lifecycle—the potential for problems is substantial.

Wireless security special issue

This special issue's articles cover just a small portion of the wireless security problem space. In addition to the two that I've introduced so far, which focus on specific wireless technologies, this section includes two articles that cover wireless in a more general fashion. Yih-Chun Hu and Adrian Perrig's article, "A Survey of Secure Wireless Ad Hoc Routing," provides an overview of ad-hoc network security. It is tremendously difficult to design effective security measures in this area because of the lack of a cohesive infrastructure on which security usually depends. The final feature, Jean-Pierre Hubaux, Srdjan Čapkun, and Jun Luo's "The Security and Privacy of Smart Vehicles," presents the many design challenges in developing a new technology that depends on wireless—specifically, automobile telematics. If you think the fact that someone standing near you can intercept your every keystroke is bad, how about someone driving beside you and deploying your air bag?!

With anything new, it is always easy to focus on the bad. I've tried not to do that here because I truly believe that we're just beginning to see the potential for wireless technology. However, that doesn't mean we should ignore problems. Instead, we must have frank and open debates on the problems as well as advantages so that the results benefit everyone. I hope this issue contributes to that goal. □

William A. Arbaugh *is an assistant professor at the University of Maryland. He received a PhD from the University of Pennsylvania, an MS in computer science from Columbia University, and a BS from the United States Military Academy. His research interests include wireless security and embedded systems. He is a member of the IEEE. Contact him at waa@cs.umd.edu.*