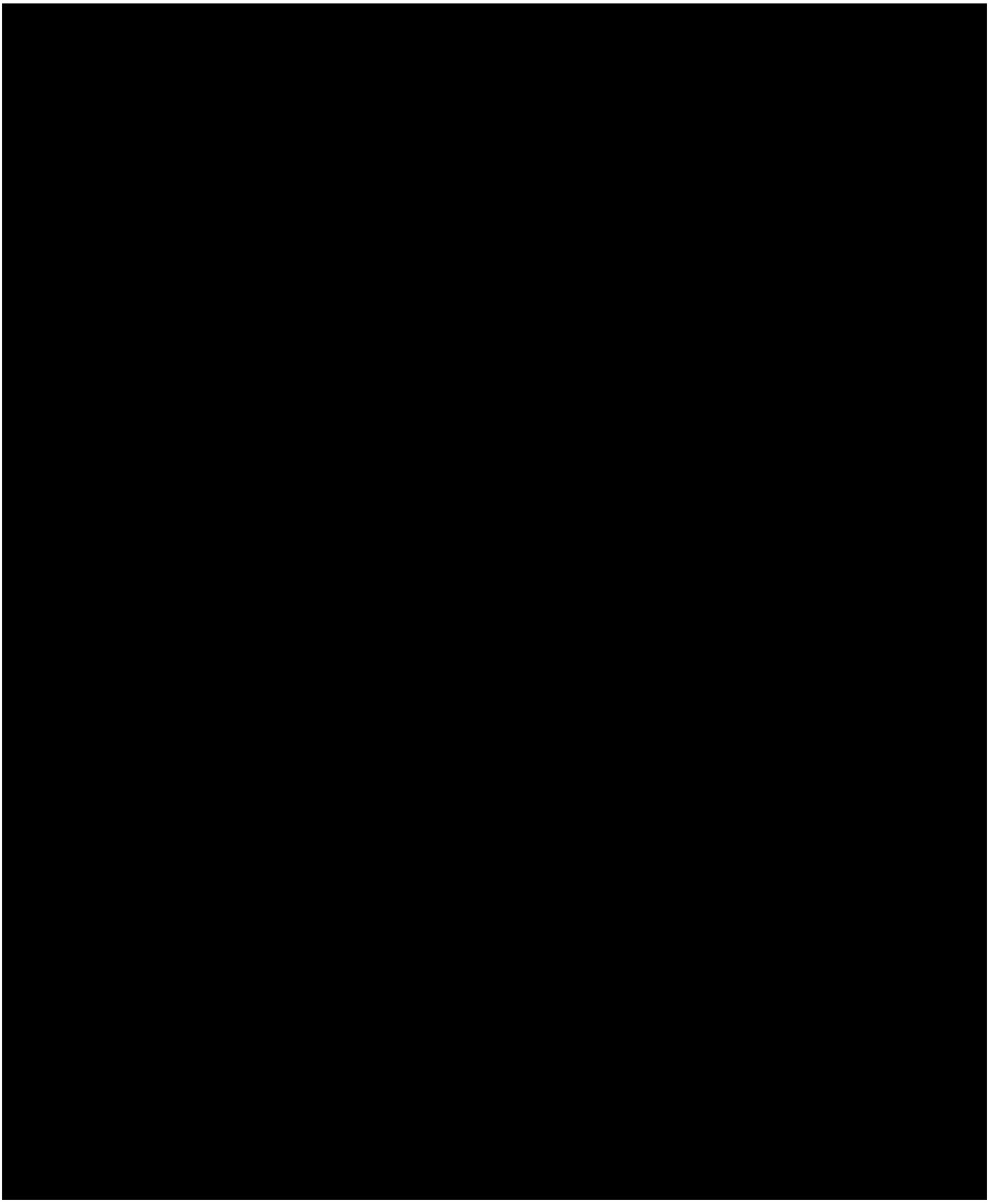

By Aviel D. Rubin, Guest Editor

WIRELESS NETWORKING SECURITY

In the time span of just a few years, wireless local area networking went from being a novelty to revolutionizing the way many organizations connect their computers. Visit any major department store, hospital, or office building, and you will encounter 802.11 cards in all of the PCs and access points hanging from the ceiling. The speed with which wireless networking has caught on is not surprising, as 802.11b offers up to 11Mbps of bandwidth, and a range of several hundred feet. Newer standards, such as 802.11g, promise five times the speed. Multiple wireless access points can be easily installed on the same network to increase the coverage area, so that an entire building can be easily connected. Conversely, wiring buildings with Ethernet is expensive and limits the locations from which networked computers can be used.

ILLUSTRATION BY PAUL WILEY

AS INCREASING NUMBERS OF ORGANIZATIONS ADOPT THE TECHNOLOGY, WE ARE LEARNING HOW TO SECURE COMMUNICATIONS AT DIFFERENT LAYERS IN THE NETWORK STACK, AND FUTURE STANDARDS FOR WIRELESS PROTOCOLS APPEAR TO HAVE BETTER DESIGNS FOR SECURITY.

Most new laptops purchased today are outfitted with built-in 802.11 networking capabilities, and configuring a home or office wireless network out of the box can take less than 10 minutes. Furthermore, PC cards are rapidly coming down in price and increasing in power. The economic forces influencing wireless networking are matched only by the convenience to users. Wide-scale adoption of 802.11 was inevitable, and the general expectation is that it will only increase. Eventually, it is likely that most public areas will offer some sort of wireless connectivity; there are initiatives to extend coverage to airplanes and trains, as well as shopping malls and airports.

The advent of wireless networking has raised some very unique and compelling issues. The first issue is security. Given the open nature of wireless networks, what threats do they introduce? Other issues are legal and social. Is it right for someone to share with their neighbors the bandwidth for which they are paying an ISP? Do service providers have a right to insist on payment from anyone who obtains connectivity? Is it appropriate for a coffee shop to resell Internet service to wireless users?

This special section was developed to address some of these issues. The first article discusses security architectures. The fact that it is trivial for anyone on a network to plug in an access point and turn the network into a wireless one changes the way network architecture should be developed, especially from a security standpoint. While traditional networks used firewalls to partition networks into different trust zones, the possibility of an internal network being accessed by an off-site user changes the way networks should be designed.

One of the ways to deal with the security problems of wireless networking is to build security, using cryptography, right into the wireless standard. Unfortunately, it has been a rocky road for the standards bodies specifying wireless networking. The second article in this section deals with the cryptographic issues involved in wireless networking: some of the mistakes that have been made are discussed and a variety of solutions are proposed.

The third article in this special section is included to show just how open wireless networks are. With minimal off-the-shelf equipment, it is possible to access thousands of networks in a very limited geographical area. The authors discuss some of their experiences mapping access points in the spirit of the so-called war-driving phenomenon where people drive around with 802.11 devices and inexpensive antennas, yielding many open networks not using encryption that are willing to hand out IP addresses to any device that requests one.

While the discussion in the third article deals with the unauthorized use of organizations' wireless networks, an amazing subculture of free wireless networking providers has emerged all over the world. The final article discusses open networks and the sharing of bandwidth in public places. The ease of deployment and configuration and the movement toward built-in wireless connectivity present an opportunity for ubiquitous networking from anywhere on any device. This final article was developed as an educational essay rather than a technical article, to round out the section.

Wireless local area networking has taken the world by storm. As is often the case, proper security was not built in at the beginning, and the act of retrofitting it has not been without difficulty. Nonetheless, as increasing numbers of organizations adopt the technology, we are learning how to secure communications at different layers in the network stack, and future standards for wireless protocols appear to have better designs for security. The articles in this section focus attention on these security technologies as well as on some of the social issues we will all encounter and have to address in some manner soon. Given the rapid pace of development, it is beneficial to begin considering these issues now. C

AVIEL D. RUBIN (rubin@cs.jhu.edu) is an associate professor of computer science and the technical director of the Information Security Institute at Johns Hopkins University in Baltimore, MD.