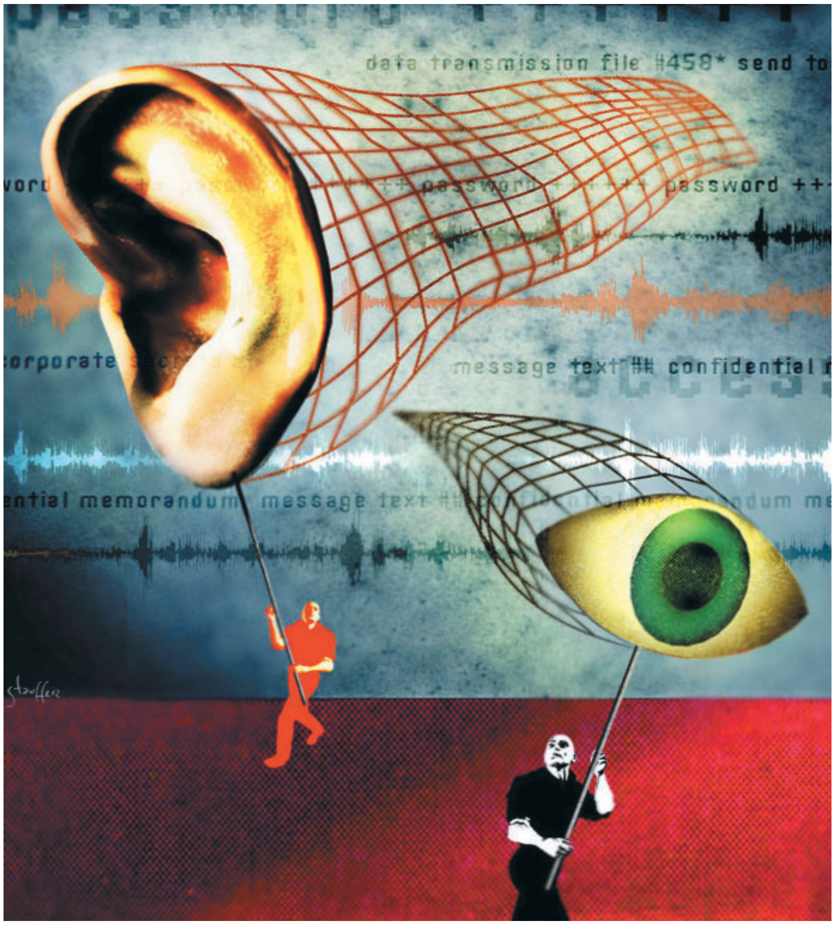
The Undefended Airwaves

Can our cell phones, laptops and pagers ever really be secure? Or are our phone calls, the data on our hard drives, and the messages that we receive inevitably going to be an open book for any suitably motivated government spy—or teenaged hacker?

Certainly, nothing can ever be 100 percent protected. Sadly, though, the makers of portable computing devices and wireless communications systems have led us down a false path by failing to make security a top priority. For more than a decade, cryptographers have possessed strong encryption techniques that could virtually guarantee that data falling into the wrong hands—through a stolen laptop, say, or an intercepted radio signal—would be impossible to decode. Unfortunately, these techniques have not made it from the lab into the mainstream.

As a culture, we have little experience with secure communications—and a lot of experience with communications security gone sour. Time and again, wireless equipment vendors and providers have been shamed by the security failings of their products. The analog cellular telephone systems of the early 1980s lacked any protection at all; a $200 scanner from Radio Shack would let you listen in on anybody's cell-phone conversation.

Rather than endow their products with strong encryption, the wireless companies turned to Washington for help. The result was the 1986 Electronic Communications Privacy Act, which effectively made it illegal to listen in on cellular-phone calls. But the legislation didn't stop snooping: after the law's enactment, House Speaker Newt Gingrich, Virginia governor Douglas Wilder and even Prince Charles all had their wireless communications intercepted.


data transmission file #458* send to
word
++ password ++
password ++
corporate secr
message text ## confidential
ntial memorandum message text ##
dum me
Stauffer

BRIAN STAUFFER

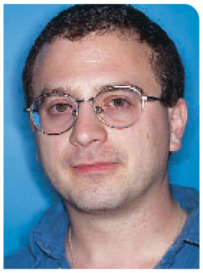
The cellular industry paid dearly for its decision to seek security from Congress rather than cryptographers; just as phone calls were sent through the airwaves without encryption, so were the account numbers used for billing. The 1990s saw an explosive rise in the incidence of cellular fraud, with thieves sniffing account information in order to "clone" phones—that is, have one phone bill to another phone's account. According to industry estimates, phone cloning was costing the industry several hundred million dollars each year by 1997.

Unfortunately, many decision-makers have learned the wrong lesson from these chronic failings: instead of resolving to deliver more secure systems, many seem to have concluded security and privacy are elusive at best—and that scarce resources are better spent on other goals. This spells real danger as wireless devices become a greater part of our economy. All of the large-scale wireless paging and data networks deployed in the 1980s and '90s repeated the cell-phone industry's mistake and eschewed encryption. Today these networks are the basis for popular wireless products like pagers and the Palm VII personal digital assistant. Messages sent using these systems can be—and are—intercepted with ease.

What's worse, it can be nearly impossible for a consumer to make an informed decision about a product's security. Consider the Palm: all Palm-OS-based computers let you make certain records "private," meaning that they shouldn't be visible unless a password is entered. This password could be enforced with encryption, but it isn't: last September, the Cambridge, MA, computer security firm @Stake announced that anyone with physical possession of a person's Palm could reverse-engineer the password.

There are a few signs of enlightenment. The digital telephone services offered by Sprint PCS and VoiceStream use encryption to protect both billing information and the content of calls. The BlackBerry two-way communicator encrypts each message before transmitting it. But security all too often remains an empty promise. AT&T's wireless telephones allegedly offer encryption, but when I turned on the feature, my telephone stopped working. I called AT&T and was told "voice privacy isn't supported." When I was a Metricom customer and enabled the advertised encryption feature, my connections routinely got dropped. The company's advice: if I wanted more reliable service, I should turn the encryption off.

The wireless industry has dropped the ball on communications security, giving up on encryption and leaving us vulnerable to snooping.



Industry officials say that one reason they don't spend the extra money on encryption is because wireless users don't care much about it. Whatever validity that viewpoint once had is fading, though, as more and more of our activities depend on wireless networks. Consider those high-speed wireless local-area networks now being deployed by many homes and businesses. Earlier this year, a friend of mine in Boston installed a wireless network card and found that he could tap into an office across the street. My friend now "borrows" the firm's high-speed Internet connection at night after the people in the office go home. That's a pretty benign imposition, but the security hole allows him far greater access; he could, if he chose, browse the company's files and read its employees' e-mail. And this problem is widespread: earlier this year, Silicon Valley computer consultant Peter Shipley made headlines for driving around town with a laptop in his car and mapping all the wireless networks that he could sniff.

For years, the vendors of wireless local-area networks have advertised their equipment as being secure. The systems use spread-spectrum technologies—a technique that is supposed to make the radio signals incredibly difficult to intercept. The systems also have a form of password protection. Finally, equipment makers say, most wireless local-area networks support some kind of over-the-air encryption.

Don't believe these assurances. Spread-spectrum broadcasts are easy to pick up with a wireless network card specifically designed for such transmissions. Similarly, the password systems offer little security: many wireless network cards let you set the password to "ANY," which tells the card to connect to any network it finds. You can also use a "site monitor" program that comes with many cards to display the passwords of every local network that it hears. And it is so difficult to set up encryption on these systems that most users simply don't go through the trouble.

Why weren't these problems anticipated and corrected when the wireless local-area network standards were being developed? One big reason is that the engineers on the standards committees never sought out advice from cryptography experts.

Cryptographers, as a whole, haven't done much to inspire confidence. Throughout much of the 1990s, many were locked in a battle with the U.S. government. The government was pressuring computer companies to put weak cryptography into their products, arguing that strong encryption would undermine the country's intelligence-gathering and crime-fighting capabilities. Many cryptographers spent their days breaking these weak systems to show just how vulnerable they were. Unfortunately, this experience has left a curious legacy: many engineers now believe that with computers getting faster and faster, it is only a matter of time before cryptographers will be able to crack *any* cryptographic system.

This attitude is nonsense. For years, cryptographers have known how to make algorithms that are so strong that it is inconceivable they will be cracked for a very long time—as in, not before the sun engulfs the earth. That's because the difficulty of cracking a key goes up exponentially with the size of the key. A small network of Pentium computers that can search a billion keys a second can crack a 40-bit encryption key in 18 minutes. Double the key length to 80 bits and that network would have to gnaw away at it for quite a while longer—about 38 million years. With 128-bit encryption (technology that has been available for more than a decade), it would take a billion of these networks roughly 10 trillion years. That's about as absolute a guarantee of security as anyone is likely to need to guard his or her cell-phone conversations.

If the wireless industry understands this, it is doing an odd job of showing it. The current plan for many Bluetooth wireless devices is to base security on a four-digit PIN code—the equivalent of a 14-bit encryption key. Although the standard allows longer PINs, equipment vendors don't want to make their first-generation Bluetooth systems too difficult to use.

As long as people believe that even the most advanced privacy-protecting technologies can be readily compromised, they won't demand better security—after all, why bother? But it is folly to let pursuit of the perfect become the enemy of the nearly perfect. Before we give up on strong encryption and excellent security, we should at least give it a try.