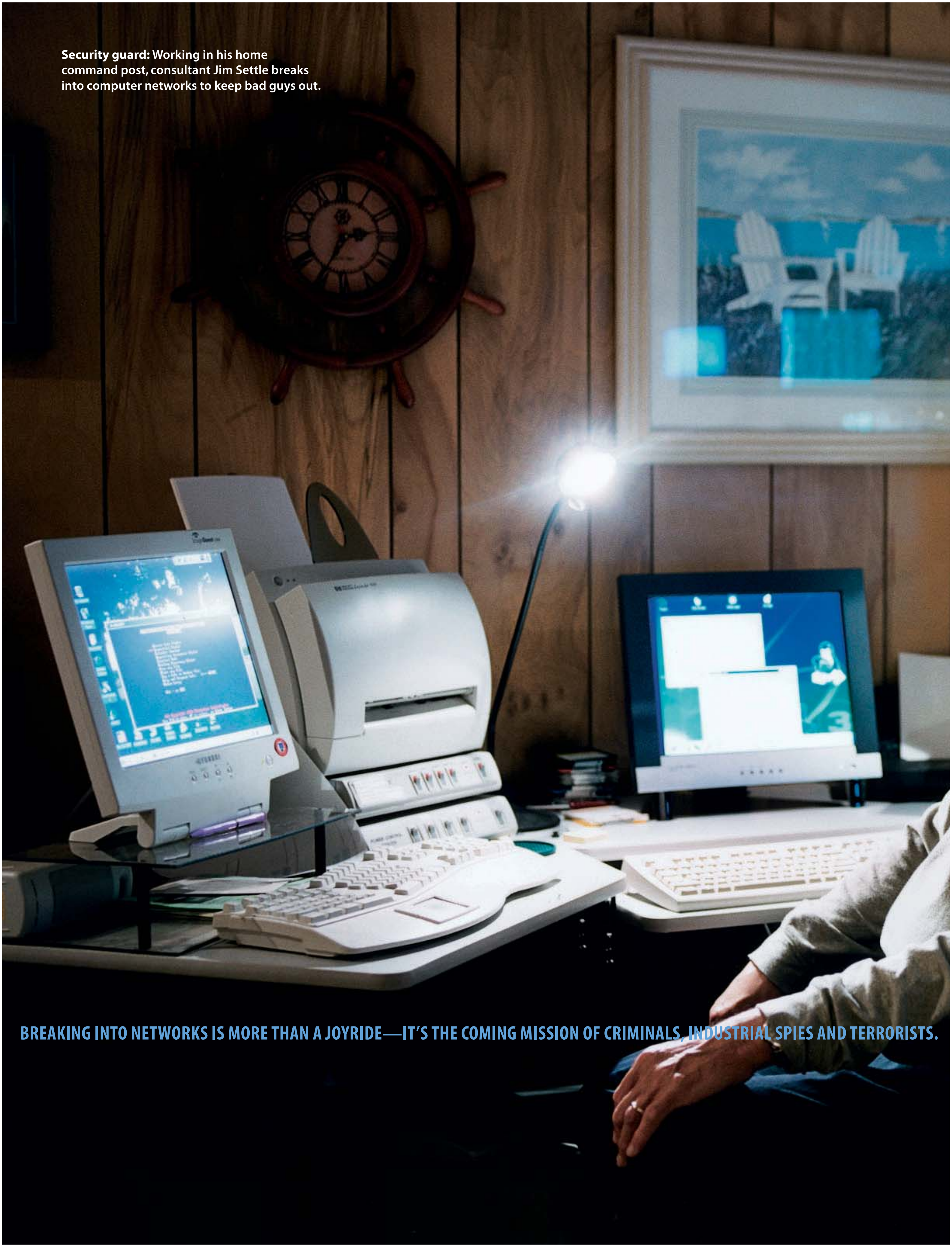
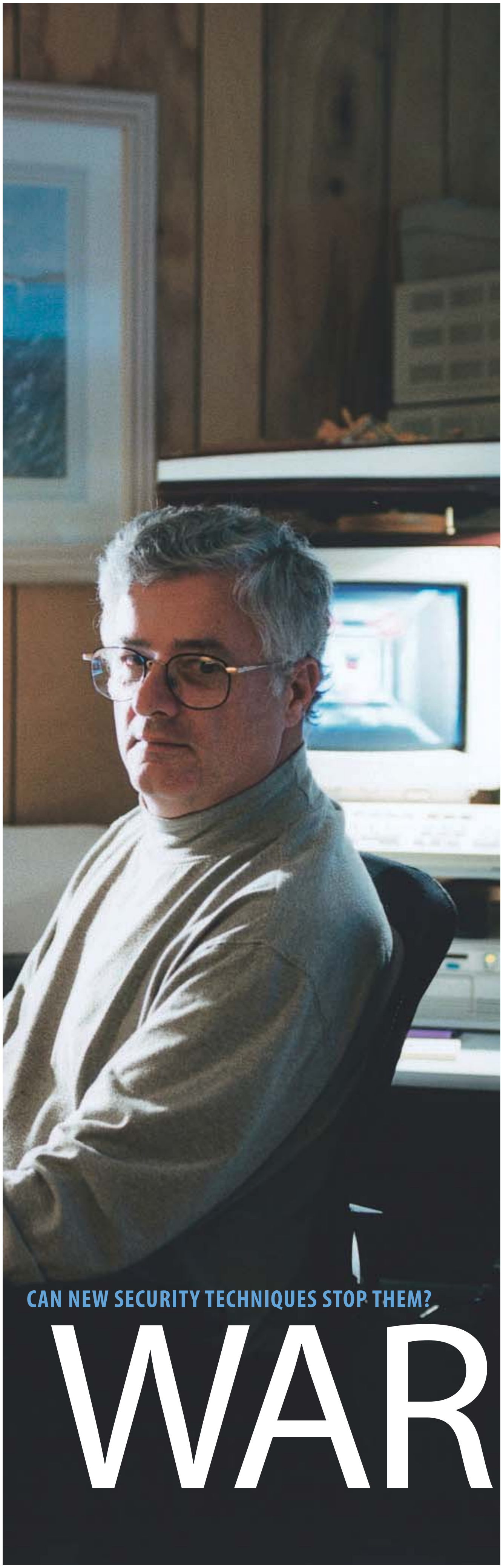


Security guard: Working in his home command post, consultant Jim Settle breaks into computer networks to keep bad guys out.

BREAKING INTO NETWORKS IS MORE THAN A JOYRIDE—IT'S THE COMING MISSION OF CRIMINALS, INDUSTRIAL SPIES AND TERRORISTS.



INFORMATION WARFARE

CAN NEW SECURITY TECHNIQUES STOP THEM?

BY DAVID FREEDMAN
PHOTOGRAPHS BY ETHAN HILL

THE MIDDLE-AGED MAN—CALL HIM JOHN—PEERED AT THE NUMbers rolling across his computer monitor, which provided the only illumination in the cramped basement. One number, 307, caught his eye. Like the others, it designated a port, or gateway, between a certain corporation's computers and the outside world. John had just run a program on his PC that sent electronic probes throughout the corporation's network to find a complete list of these ports. Port 307 was "open"—any data coming through it could be displayed on John's screen. Would the information prove useful?

It did. Port 307 turned out to be where one network server sent bad passwords, along with the usernames of whoever typed them in. Network administrators had taken the trouble to hide legitimate passwords from prying eyes but hadn't worried about rejected passwords. John knew, however, that most failed passwords aren't wild guesses but rather are "fat-fingered," or typos. It was pretty easy to guess what "valentime3" was meant to be. Seconds later, John had logged onto the server. Three minutes after that he discovered a password file that listed one user's password as blank—a shortcut favored by systems administrators out to avoid having to type in a password hundreds of times daily. Now John had "root access," meaning the server recognized him as God. He whooped and called Jim Settle, former head of the FBI's computer crime squad and now CEO of Washington, DC-based security consultancy SST. "I'm in."

Settle congratulated him, hung up and called the chief information officer of the corporation whose network his man had just penetrated. “Guess who just took over your network?” asked Settle. The man was stunned—but grateful. After all, he had quietly retained Settle’s services precisely to learn if his network was vulnerable. Now he knew. Before Settle and his crew finished, they would find dozens of other ways to take control.

Though Settle’s break-in took place with the victim’s blessing, it echoes tens of thousands of malicious invasions. Each year the Computer Security Institute, a San Francisco-based organization of computer security professionals, and the FBI survey computer security managers at large companies and government agencies. In this year’s survey of 538 managers, 85 percent of these organizations suffered security breaches; most suffered financial loss as a result. The average reported loss: about $2 million.

IMAGINE THE COMPUTER-DRIVEN TARGETING DISPLAYS IN BOMBERS MISIDENTIFYING FRIENDLY INSTALLATIONS AS ENEMY POSITIONS,

That probably offers an optimistic view of the problem’s scope. Settle has been hired by more than 60 companies to “red team” their computer systems—that is, to test security by breaking in the way hackers would. Not only did his people gain intimate access to every system, but only one firm even detected a breach. Moreover, the problem’s not just corporate: according to a review by the U.S. General Services Administration, outsiders broke into and temporarily controlled at least 155 computer systems at 32 federal agencies last year.

And that’s not even the bad news. While computer network break-ins have long been almost exclusively the work of joyriding, bored teenagers, security and law-enforcement professionals believe the threat is about to shift from run-of-the-mill hackers toward professional criminals, industrial spies, hostile governments and terrorists. Eventually, say experts, computer attacks are likely to bankrupt companies, compromise U.S. security and perhaps even kill hundreds or thousands of citizens by disrupting computer control of anything from traffic signals to food supply transport. “These threats are real,” says Jack Holleran, former technical director of the National Security Agency’s National Computer Security Center and now an independent computer security consultant. “It’s just a matter of when, and it will be sooner rather than later.”

The rising stakes have touched off an escalating stream of network skirmishes between those determined to break into organizations’ computers and those charged with protecting them. Right now, the bad guys are winning. “Internet security is a big mess,” says Bill Cheswick, a chief scientist at Lumeta, a Somerset, NJ, computer-security software firm spun off from Lucent Technologies. “It gets discouraging sometimes.” That sobering reality has sent Cheswick and other top computer scientists into their labs to come up with new weapons for the intensifying battle.

Electronic Pearl Harbor

THE HAVOC THAT CAN BE WREAKED ONLINE HAS BECOME almost limitless. Unless you’re living deep in the woods on fish you catch, chances are almost every aspect of your life is mediated through computers, from your train ride into work (thanks to computer-controlled track switches) to paying bills to relaxing in front of the television (which gets its juice from a computerized electric power grid). A terrorist organization or hostile nation that wanted to disrupt life in the United States, or a thief who wanted to plunder a company, has an embarrassment of riches to choose from, notes Pat Lincoln, director of the Computer Science Laboratory at nonprofit research institute SRI International. Lincoln, whom U.S. officials have briefed on these concerns, notes that though the details are classified, the government is carefully watching several groups and nations for warnings of computer attacks. “If you’re recruiting people to drive trucks that blow up, maybe next year you’ll get someone to plant an Internet ‘worm,’” says Lincoln.

Possible targets of terrorist or state-sponsored attacks include electric power grids, natural-gas pipelines, water supplies, dams, hospitals and a variety of other critical facilities that could be paralyzed by assaults on the right computers, possibly resulting in widespread suffering and even death. Holleran notes that 80 percent of the food transported by rail in the United States crosses either of two bridges over the Mississippi River; even a moderate computer-driven mishap near one of them could potentially cause shortages and skyrocketing food prices. Phone service could increasingly be at risk, too, thanks to plans to move most voice traffic onto the Internet, which is far less secure than conventional phone networks. Banks, stock exchanges, the U.S. Social Security Administration and the U.S. Postal Service are also vulnerable. An attack on any such crucial network would serve as what security experts call an “electronic Pearl Harbor.”

Access to, or a means to disrupt, military networks would be a special prize in this computer cold war. “A commercial site might be willing to put up with a certain amount of fraudulent traffic” that slows or temporarily halts service, says Robert Anderson, head of the information sciences group at nonprofit think tank the Rand Corporation. “But in a military system you’d be talking about lives being lost.” Imagine, for example, the computer-driven targeting displays in tanks and bombers misidentifying friendly installations as enemy positions, or radio command networks being disrupted, or even inundated with fake commands. Such infiltrations could conceivably influence the outcome of a war. Uncle Sam is widely believed to have developed its own capabilities for attacking enemy computer systems, but because the United States tends to be far more computer dependent than its overseas counterparts, we have more to lose via information warfare, Anderson says.

Computer attacks could even become a force to reckon with in politics, notes AT&T Labs security expert Avi Rubin—at least if some communities follow through on plans to allow voting over the Internet. All a malicious agent would have to do is launch a mild attack that slowed down a vote-processing server enough to prevent a few percent of the ballots from getting through in a couple of districts. “It’s the easiest type of attack one could possibly launch, and it could be enough to disrupt an election,” says Rubin.

On the business side, the attacks are less theoretical. Citibank was ripped off in 1994 to the tune of $10 million by a Russian computer whiz, who transferred the funds to his and his accom-

OR RADIO NETWORKS INUNDATED WITH FAKE COMMANDS. SUCH INFILTRATIONS COULD INFLUENCE THE OUTCOME OF A WAR.

Network cartographer: Lumeta's Bill Cheswick exhaustively maps every point where hackers could attack networks.

plices' accounts. Most of the money was eventually recovered, but experts say there have probably been larger, more successful computer heists at other financial-services companies. Why haven't we heard about them? Because the companies quietly bury the loss in the books as some other type of expense. "If someone breaks into a company's computers and gets $50 million, the company will feel there's nothing to gain by reporting it," says Jon David, a senior editor of the journal *Computers and Security* and a security manager at a large financial-services firm. "It just makes customers and stockholders nervous."

For a growing number of thieves, though, purloined corporate information—not money—is likely to become the currency of choice. R&D data, financial records, personnel files, details of upcoming deals—corporate servers are treasure troves of data that can be sold to competitors, speculators or anyone with a grudge. And of course, a few firms or their employees may stoop to direct computer-based espionage against competitors. Since hijacked information would typically be copied and not altered, companies might never know they've been hit. In a so-far-unique public case of industrial espionage allegedly carried out by computer, Moore Publishing, a Wilmington, DE, investigative firm, filed a $10 million lawsuit against Steptoe and Johnson, a well known Washington, DC, law firm. Settled in July 2000 for an undisclosed sum, the suit claimed that Steptoe and Johnson repeatedly broke into Moore computers, allegedly in revenge for Moore's having bought the rights to the "steptoejohnson.com" domain name (which it subsequently gave up).

Infinite Standoff

THE SECURITY WAR CAN SEEM LIKE AN INFINITE STANDOFF; for every new defense researchers devise, invaders develop countermeasures, leading to counter-countermeasures, and so on. Fortunately, defenders don't have to make it impossible to break into networks; they only have to make getting in so difficult, or so fraught with the risk of being tracked down, that the bad guys think twice.

COMPANIES OFTEN FIND OUT ABOUT VULNERABILITIES WHEN "WORMS" SPREAD THROUGHOUT THEIR NETWORKS. "IF YOUR NETWORK

Consider, for example, the most common means of breaking into a computer system: stealing passwords. Since employees often use a word or proper name as a password, would-be intruders can turn to any of several automated password-guessing programs freely available on the Web (try a search on "LOphtCrack," for example) to run through a dictionary full of guesses. "It just takes one user with a bad password to compromise a system," says Dorothy Denning, a computer scientist at Georgetown University.

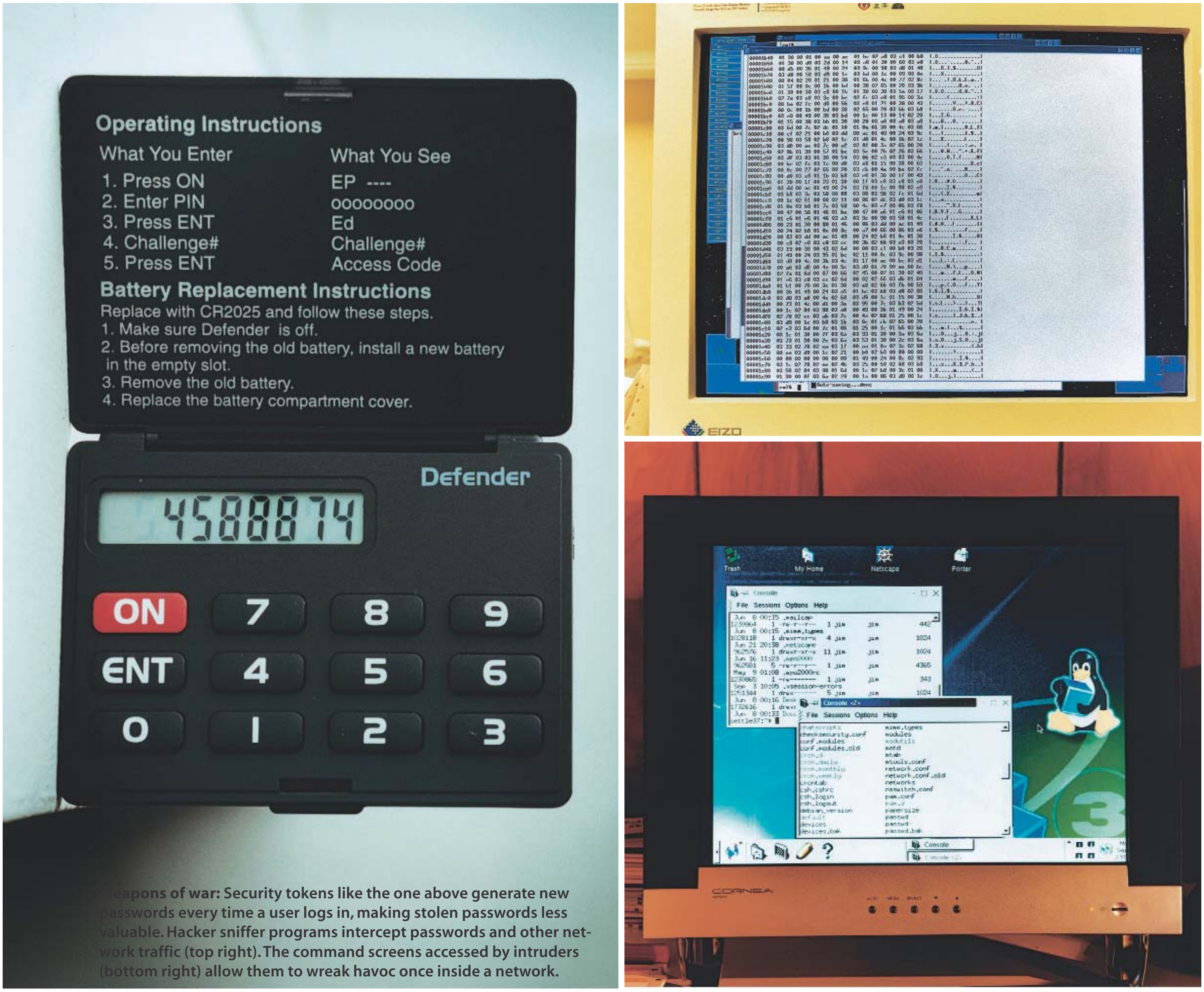
To fight back, organizations can enlist software that automatically rejects passwords based on words or names and forces users to change their passwords regularly to limit potential damage. Even safer are security "tokens"—devices from keychains that plug into computers to small liquid-crystal displays—which make stolen passwords less valuable. Tokens like those made by Symantec and San Jose, CA-based Secure Computing dynamically generate a new password each time a user needs to log in; a version made by RSA Security of Bedford, MA, generates a new password every minute or so in synchronization with servers. But even these precautions won't stop highly motivated malicious agents. They can fast-talk employees out of passwords by posing as systems administrators over the phone or simply walk through the offices, where they can often spot passwords that are written down. And acquiring a token can be as simple as stealing a purse.

A growing number of companies and government agencies are also turning to smart cards to limit illicit entry into their systems. Smart cards have embedded computer chips containing code that identifies the holder. Passed through a reader that can be attached to any computer, the smart card authorizes the holder to use that computer to access the network: the network will reject commands from a computer that hasn't been presented with an authorized smart card. Smart cards can also contain the "keys" required to read or send encrypted data. Unlike encryption keys stored on a PC, keys encoded on a smart card can't be stolen via the network. Even tighter access control can be engineered by combining smart cards with "biometric signatures" like fingerprints or voiceprints. RSA Security, Luxembourg's Gemplus and the Datacard Group in Minnetonka, MN, are among the vendors already selling smart cards; Siemens offers smart cards tied to a fingerprint, and Domain Dynamics of Swindon, England, is prototyping cards encoded with voiceprints.

Of course, smart cards can be stolen, too, and though tamper-resistant, the code on embedded chips can in theory be cracked once a card falls into the wrong hands. One way around this weakness is to build the authorization chips into the innards of the computer itself. This way, bad guys must physically get their hands on an authorized computer to crack a network—a dicey proposition that even if successful isn't likely to go unnoticed for long. IBM, Intel, Hewlett-Packard, Microsoft and Compaq Computer founded the Trusted Computing Platform Alliance, now 170-plus members strong, to push for the development of such chips. The technology could be used in conjunction with smart cards and other security devices. "It puts a hardware barrier in front of a malicious software attack," says David Safford, manager of IBM Research's Global Security Analysis Laboratory. Safford estimates that in three to five years, every computer built will include the chips. IBM Research has also developed a tamperproof device that can be installed in servers, similar to the chips endorsed by the Trusted Computing Platform Alliance.

Eventually, though, the chip has to talk to software, and some security experts peg that as the weak point of the Trusted Computing Platform Alliance's scheme. And once logged into a system, intruders can send commands that might coax the operating system—whether it's Unix, Microsoft Windows or Sun Solaris—into granting them systems administrator privileges. That typically includes the ability to examine server files, gain access to other servers, install "back doors" that allow easy future entry and cover their tracks by altering the system's logs.

Operating systems can be "tightened down" to prevent this sort of manipulation, but most systems administrators aren't familiar with the approximately 300 manual programming routines the procedure requires. Even if they are, malicious parties can exploit newly discovered holes (an average of 10 new



Operating Instructions

What You Enter	What You See
1. Press ON	EP ----
2. Enter PIN	00000000
3. Press ENT	Ed
4. Challenge#	Challenge#
5. Press ENT	Access Code

Battery Replacement Instructions

Replace with CR2025 and follow these steps.

1. Make sure Defender is off.
2. Before removing the old battery, install a new battery in the empty slot.
3. Remove the old battery.
4. Replace the battery compartment cover.

Weapons of war: Security tokens like the one above generate new passwords every time a user logs in, making stolen passwords less valuable. Hacker sniffer programs intercept passwords and other network traffic (top right). The command screens accessed by intruders (bottom right) allow them to wreak havoc once inside a network.

IS TIGHT, YOU SHOULD NEVER SEE ANYTHING LIKE CODE RED INSIDE. BUT IT RAN THROUGH ALL KINDS OF ORGANIZATIONS."

Windows vulnerabilities, for example, circulate around the Web each month) unless systems administrators are unusually diligent about updating security features. "The machines get worse just sitting there," notes Dan Farmer, a security consultant who has worked extensively for Sun Microsystems.

A terrorist or industrial spy doesn't have to be proficient in the nuts and bolts of security hole exploitation to capitalize on these weaknesses. Software penetration "tool kits" that automate the process of invading and taking over a system can be downloaded from thousands of sites on the Web.

To help combat marauders who exploit such server vulnerabilities, systems administrators can employ intrusion detection software, such as Cybercop from Santa Clara, CA-based Network Associates, Cisco Systems' Secure IDS and SRI International's Emerald. These systems monitor network traffic looking for sequences of commands specifically associated with malicious attacks, as well as out-of-the-ordinary command sequences or data traffic. When the software spots something unusual, it notifies the systems administrator, who can then decide whether to shut the questionable traffic down.

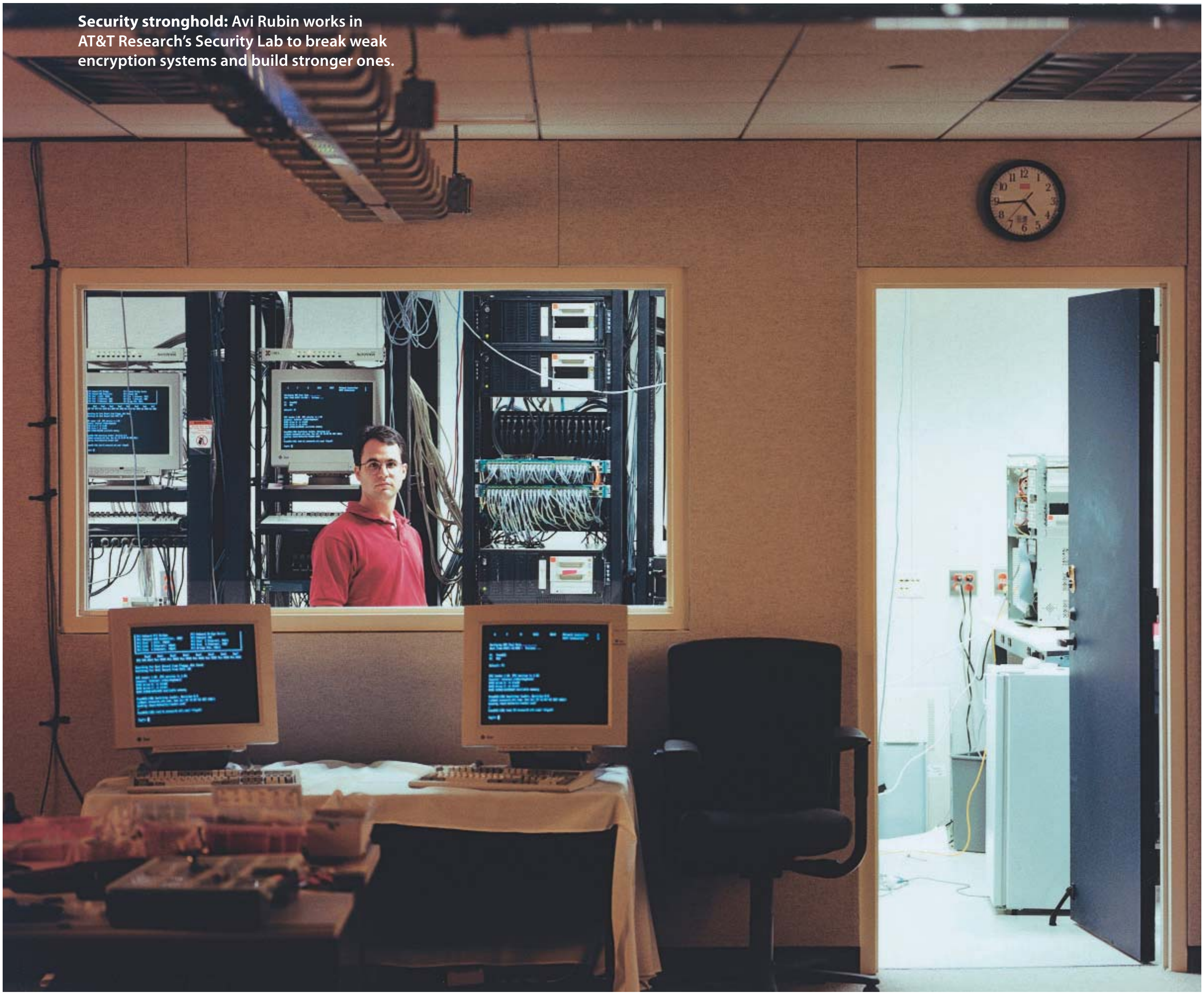
But some attacks will be new and subtle enough to avoid detection. Or more commonly, invasions may be detected but ignored. Routine hackers and even inept legitimate users so frequently trigger current intrusion detection systems that many systems administrators disregard the alarms—or turn them off. Many of the companies Jim Settle's team penetrated were running high-end intrusion detection software costing $100,000 or more but for one reason or another didn't recognize the attack.

To counteract these glitches, researchers at Sandia National Laboratories, Network Associates and Cisco are working on intrusion detection systems that do a better job of differentiating false alarms and amateurish attacks from serious invasions. Some systems under development will even be able to analyze activity across a network to distinguish isolated attacks from the sort of massive, coordinated assaults that tend to be more damaging, says Fred Cohen, a security consultant and Livermore, CA-based Sandia researcher who coined the term "computer virus." Future intrusion detection systems, he notes, will also make the network "self-coordinating": when a particular server is under attack, the network will place similar servers on high alert, or even shut them down, under the assumption that the attacker will attempt to exploit related vulnerabilities. Cohen has been working on ways to allow intrusion detection systems to recognize "slow attacks," an especially subtle and hard-to-spot technique in which an attack is purposely spread out over hours or even days to avoid triggering conventional alarms. "Most organizations have been ignoring that problem, because they have their hands full just recognizing attacks that occur in real time," he says.

Cohen is also among those working on another method to defend servers: so-called deception techniques. These involve setting the network up not merely to resist intruders but also to confuse and mislead them—preventing them from causing damage and making it easier to monitor their activities. For example, an intruder will normally use software to scan a network for open ports, typically resulting in a list of 30 or so gateways that can be explored for vulnerabilities. One deception technique is to have the network automatically reply to a port scan with a list of a million or more ports—far more than even the most motivated agent is likely to sift through looking for weaknesses. Organizations that want to go all out can even set up entire databases of phony information that are made available to anyone trying to improperly access the system.

Cohen notes that some security professionals have shied away from deception techniques out of concern that legitimate users will be fooled or inconvenienced, but he disagrees. "We've been experimenting with the techniques for four years on our networks, and we haven't seen one case where a user wasted time because of them, or as far as we know, one case where an

"IF THE FBI IS WHERE OUR EXPERTISE LIES, WE'RE IN TROUBLE"— THEY'RE ILL EQUIPPED TO DEAL WITH COMPUTER CRIME AND



Security stronghold: Avi Rubin works in AT&T Research's Security Lab to break weak encryption systems and build stronger ones.

attacker got to real data," he says. Cohen currently gives away some deception software on his Web site, and security firm Recourse Technologies of Redwood City, CA, sells a product called ManTrap, probably the most sophisticated deception system available commercially. But Cohen says more advanced systems are generally built in-house because they require a great deal of customization and maintenance.

In an effort to identify network vulnerabilities before invaders exploit them, companies can run software designed to ferret out and flag flaws. For example, Bill Cheswick's group at Lumeta sends a barrage of specially tagged packets of data from inside an organization's network to servers outside the network, and vice versa. The software then points out any network servers that let traffic move through in both directions. Such "leaky" servers represent an easy way in for intruders—and for malicious software like the Code Red worm that infected servers worldwide last summer. "The way companies usually find out about leaky servers is when a worm like Code Red spreads throughout the network," notes Cheswick. "If your network is tight, you should never see anything like Code Red inside. But it ran through all kinds of organizations."

TERRORISM. INVADING HACKERS CAN MORE OR LESS OPERATE WITHOUT FEAR OF BEING TRACKED DOWN, EVEN IF THEY'RE DETECTED.

Cybercrime's Next Frontier

EVEN WHEN SECURITY PROFESSIONALS MANAGE TO DEFEND existing networks, the ever increasing demand for more access by legitimate users creates new vulnerabilities. Take the explosion in wireless data networks, which allow an organization's employees to exchange messages and other data while wandering around with laptops and other devices. These networks provide malicious agents with "the next great frontier" for cybercrime, says Padgett Peterson, a Lockheed Martin security expert. The Internet is lousy with instructions for breaking into cell phones, pagers and personal digital assistants like the Palm. Intruders can also try "war-driving," which involves cruising the roads around corporate or government strongholds with equipment that intercepts wireless data transmissions—no passwords needed.

In an attempt to defeat such drive-by hacking, many wireless networks incorporate the popular Wired Equivalent Privacy protocol, which scrambles all data sent over the network. Unfortunately, AT&T researchers led by Avi Rubin and guided by theoretical work published by researchers at Cisco and the Weizmann Institute in Israel cracked the scheme in August, essentially rendering it useless. Rubin suggests replacing the approach with a technique compatible with the new (and so far impenetrable) Advanced Encryption Standard expected to be adopted by government agencies by year's end. But this won't be much consolation to organizations that have already invested millions of dollars in setting up their wireless networks. "When the new standard comes out, all the wireless PC cards and base stations will have to be replaced," says Rubin.

But no matter how successfully such technologies fend off existing threats, no end to the security wars is in sight. That's because experts can't predict perfectly what tricks criminals, spies and saboteurs will come up with next to turn our reliance on computers against us. "I'm always surprised by what the next threat turns out to be," says Lockheed Martin's Peterson.

To guard against threats that pros haven't even imagined yet, Peterson advocates a different sort of defense: rethinking the basic architecture of organizational networks. Conventional corporate network architecture, he says, affords employees fairly open access to internal databases, while attempting to place generally ineffective restrictions on connections to the outside world. Under that scheme, he says, a malicious agent need only gain access to an employee's computer in order to get into the databases.

Under the plan Peterson supports, users would have relatively open access to the outside world, while databases and other files are placed under severe and closely monitored restrictions. That way, an invader could take over Internet servers and employees' computers but still couldn't gain access to the databases and files—because nobody gets free access. "You have to be willing to reverse your thinking," Peterson says. "Not many people are."

There's another weakness to address: law enforcement's limited ability to respond to computer security threats. Despite increasing security efforts in both the private and public sectors, sophisticated invaders can more or less operate without fear of being tracked down, even if they are detected. "Law enforcement and systems administrators are always behind the curve," says Settle. Experts agree that the FBI, which bears much of the federal responsibility for responding to computer attacks, is woefully ill equipped to deal with computer crime and terrorism. "If that's where our expertise lies, we're in trouble," says *Computers and Security* editor David. That's another reason most companies don't bother to report break-ins when they manage to detect them. In the Computer Security Institute and FBI survey, only 36 percent of the companies that admitted to being hit said they reported the crime to law enforcement.

It may be, says security consultant Farmer, that the only reason we haven't been victimized by a much more intense barrage of computer assaults is that most professional criminals and terrorists still perceive conventional physical attacks like armed robbery and bombings as providing more reliable payoffs. "That will change as we move our critical infrastructures online," he asserts.

In the end, the solution may be to rethink what the Internet is good for, as Lockheed Martin's Peterson suggests. Just as savvy travelers know not to pack irreplaceable possessions in a checked suitcase or walk in an urban park after dark, so organizations and individual users will recognize that highly sensitive data shouldn't be sitting on easily accessed servers. "Security probably won't improve in a technical sense," says Farmer. "Only in a social sense."

As for less sensitive information, well, organizations may need to accept the notion that the advantages of keeping it accessible outweigh the pain of occasionally having it swiped. Consider it a cost of doing business in a wired world—or to put it another way, an acceptable casualty of electronic war.

Join an online discussion of this article at
www.technologyreview.com/forums/info