How to Steal Secrets w

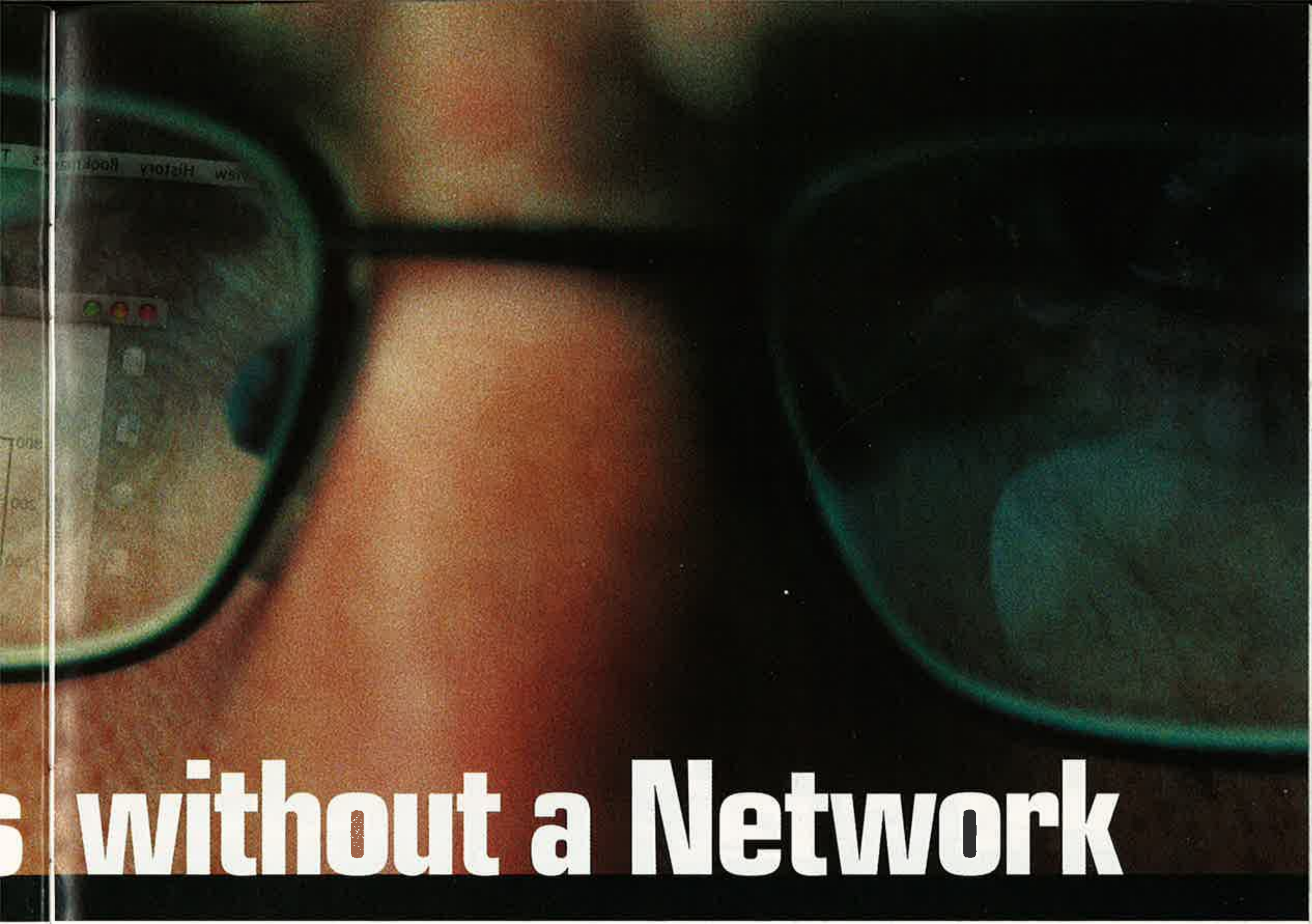
Information thieves can now do an end run around encryption, networks and the operating system > > > BY W. WAYT GIBBS

Through the eyepiece of Michael Backes's small Celestron telescope, the 18-point letters on the laptop screen at the end of the hall look nearly as clear as if the notebook computer were on my lap. I do a double take. Not only is the laptop 10 meters (33 feet) down the corridor, it faces away from the telescope. The image that seems so legible is a reflection off a glass teapot on a nearby table. In experiments here at his laboratory at Saarland University in Germany, Backes has discovered that an alarmingly wide range of objects can bounce secrets right off our screens and into an eavesdropper's camera. Spectacles work just fine, as do coffee cups, plastic bottles, metal jewelry—even, in his most recent work, the eyeballs of the computer user. The mere act of viewing information can give it away.

The reflection of screen images is only one of the many ways in which our computers may leak information through so-called side channels, security holes that bypass the normal encryption and operating-system restrictions we rely on to protect sensitive data. Researchers recently demonstrated five different ways to surreptitiously capture keystrokes, for example, without installing any software on the target computer. Technically sophisticated observers can extract private data by reading the flashing light-emitting diodes (LEDs) on network switches or by scrutinizing the faint radio-frequency waves that every monitor emits. Even certain printers make enough noise to allow for acoustic eavesdropping.

Outside of a few classified military programs, side-channel attacks have been largely ignored by computer security researchers, who

JEN CHRISTIANSEN (*photoillustration of reflection*); DIGITAL VISION/GETTY IMAGES (*man with glasses*)



s without a Network

have instead focused on creating ever more robust encryption schemes and network protocols. Yet that approach can secure only information that is inside the computer or network. Side-channel attacks exploit the unprotected area where the computer meets the real world: near the keyboard, monitor or printer, at a stage before the information is encrypted or after it has been translated into human-readable form. Such attacks also leave no anomalous log entries or corrupted files to signal that a theft has occurred, no traces that would allow security researchers to piece together how frequently they happen. The experts are sure of only one thing: whenever information is vulnerable and has significant monetary or intelligence value, it is only a matter of time until someone tries to steal it.

From Tempest to Teapot

The idea of stealing information through side channels is far older than the personal computer. In World War I the intelligence corps of the warring nations were able to eavesdrop on one another's battle orders because field telephones of the day had just one wire and used the earth to carry the return current. Spies connected rods in the ground to amplifiers and picked up the conversations. In the 1960s American military scientists began studying the radio waves given off by computer monitors and launched a program, code-named "Tempest," to develop shielding techniques that are used to this day in sensitive government and banking computer systems. Without Tempest shielding, the image being scanned line by line onto the screen of a standard cathode-ray tube monitor can be reconstructed from a nearby room—or even an adjacent building—by tuning into the monitor's radio transmissions.

Many people assumed that the growing popularity of flat-panel displays would make Tempest problems obsolete, because flat panels use low voltages and do not scan images one line at a time. But in 2003 Markus G. Kuhn, a computer scientist at the University of Cambridge Computer Laboratory, demonstrated that even flat-

KEY CONCEPTS

- Even with the best network security, your electronic data may not be safe from a determined hacker.
- Researchers have extracted information from nothing more than the reflection of a computer monitor off an eyeball or the sounds emanating from a printer.
- These attacks are difficult to defend against and impossible to trace.

—The Editors

DIGITAL VISION/GETTY IMAG (man with glasses)

Anatomy of a Vulnerable Office

Researchers have figured out how to turn your office against you. Every reflection, every sound, every invisible pulse of electromagnetic radiation has the potential to reveal secret data to a trained eye. Here are a few of the vulnerabilities that have been exposed by academic experts. As for the less forthcoming experts, we can only guess what they have found.

WEBCAM Click on the wrong link in an e-mail or a Web page, and a spy can take over any camera attached to your computer. By joining Webcam data with a new automated system called ClearShot that deciphers keystrokes through video, an eavesdropper could record everything you type.

PRINTER A dot-matrix printer creates sounds that can later be used to reconstruct the individual words that were being printed [*see box on opposite page*]. One group is now attempting to extend the trick to the far more ubiquitous ink-jet printer.

KEYBOARD Each key emits a unique radio-wave signature when it is pressed. Two graduate students recently demonstrated that, based on those waves, they could reconstruct a person's keystrokes using a simple wire antenna located 20 meters away and separated by a wall.

COMPUTER MONITOR Researchers once thought that only old-fashioned cathode-ray tube monitors (such as the ones pictured here) emit enough electromagnetic radiation for a spy to reconstruct the image on a screen. But new research shows that even flat-screen LCD monitors are vulnerable.

JEN CHRISTIANSEN (*photoillustration of printer and cup*); THOMAS NORTHCUT *Digital Vision* (*office scene*)

panel monitors, including those built into laptops, radiate digital signals from their video cables, emissions that can be picked up and decoded from many meters away. The monitor refreshes its image 60 times or more each second; averaging out the common parts of the pattern leaves just the changing pixels—and a readable copy of whatever the target display is showing.

"Thirty years ago only military suppliers had the equipment necessary to do the electromagnetic analysis involved in this attack," Kuhn says. "Today you can find it in any well-equipped electronics lab, although it is still bulky. Sooner or later, however, it will be available as a plug-in card for your laptop."

Similarly, commonplace radio surveillance equipment can pick up keystrokes as they are typed on a keyboard in a different room, according to Martin Vuagnoux and Sylvain Pasini, both graduate students in computer science at the Swiss Federal Institute of Technology in Lausanne. The attack does not depend on fluctuations in the power supply, so it works even on the battery-powered laptops you see by the dozen in any airport terminal.

Vuagnoux and Pasini showed off the feat in an online video recorded last October. They are now preparing a conference paper that describes four distinct ways that keystrokes can be deduced from radio signals captured through walls at distances up to 20 meters. One of the newer methods is 95 percent accurate. "The way the keyboard determines which key is pressed is by polling a matrix of row and column lines," explains Kuhn, who proposed (but never demonstrated) one of these methods a decade ago. "The polling process emits faint radio pulses, and the position of those pulses in time can reveal which key was pressed."

Last May a group led by Giovanni Vigna of the University of California, Santa Barbara, published details of a fifth way to capture typing that does not require a fancy radio receiver; an ordinary webcam and some clever software will do. Vigna's software, called ClearShot, works on video of a victim's fingers typing on a keyboard. The program combines motion-tracking algorithms with sophisticated linguistic models to deduce the most probable words being typed. Vigna reports that ClearShot re-

GLASS REFLECTIONS Curved glass is perfect for snooping, because it captures reflections from a wide area of the room. With computer-based techniques for correcting the image [*see box on next page*], a spy could record images of your computer screen.

WHITEBOARD Images can also be pulled off any other reflective surface—a wall clock, a metal coffee carafe or a whiteboard.

constructs the typed text about as quickly as human volunteers do, but not quite as accurately.

It might seem implausible that someone would allow their own webcam to be used against them in this way. It is not. Gathering video from a webcam can be as simple as tricking the user into clicking on an innocuous-looking link in a Web page, a process known as clickjacking. Last October, Jeremiah Grossman of WhiteHat Security and Robert Hansen of SecTheory revealed details of bugs they discovered in many Web browsers and in Adobe's Flash software that together allow a hostile Web site to collect audio and video from a computer's microphone and webcam. Just a single errant click launches the surveillance.

Eye See You

Still, Backes points out, "almost all these interception methods are accessible only to experts with specialized knowledge and equipment. What distinguishes the attack based on reflections is that almost anyone with a $500 telescope can do it, and it is almost impossible to defend against completely."

Backes, a fellow of the Max Planck Institute for Software Systems in Saarbrücken, Germany, who made a name for himself at IBM's research lab in Zurich before entering academia, spends most of his time working on the mathematics that underlies cryptography. But every year he works on a new project with his students just for fun. This year they wrote computer code that translates an audio recording of a dot-matrix printer—the noisy variety that is still often used by airlines, banks and hospitals—into a picture of the page that was being printed at the time. Based on the success of that work, Backes's group has been performing experiments to determine whether the method could be extended to retrieve text from recordings of ink-jet printers. "Obviously, this is much harder because ink-jets are so quiet," Backes says.

Last year the idea for the annual fun project dawned on Backes as he was walking past the office where his graduate students were furious-

Side-channel leaks offer the easiest way to bypass elaborate network security systems—and they do it without leaving a trail.

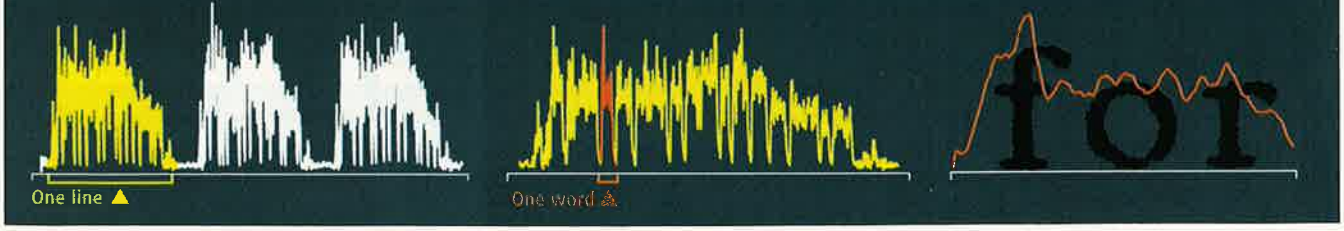
[AUDIO SURVEILLANCE]

HOW TO SPY ON A PRINTER

Inside a dot-matrix printer, a printhead scans a number of tiny pins back and forth against an ink ribbon. Each letter creates a unique sound—for example, tall letters require more pins and thus make a louder noise. Yet the correlation is not perfect, and so researchers put the initial guess of what the printed message is through an additional linguistic analysis that determines the most reasonable letter sequence.

FROM AUDIO TO LETTER FORMS

A plot of volume across time for three lines ⟶ A closer look at one line ⟶ And one word



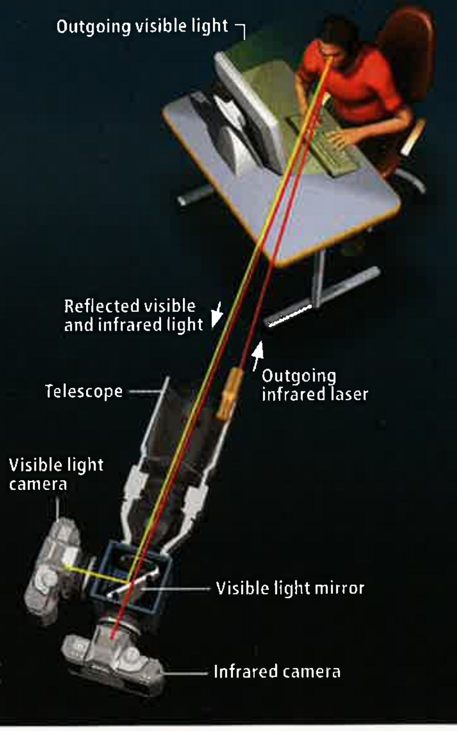
JEN CHRISTIANSEN; SOURCE: MARKUS DUERMUTH

[VIDEO SURVEILLANCE]

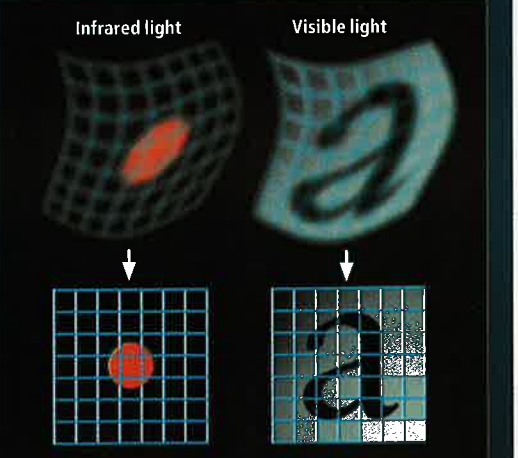
HOW TO READ AN EYEBALL

Although your eyeball reflects your monitor, any potential spy would have to overcome substantial obstacles to record a usable image of the screen contents. Any powerful telescope directed at you will have a wide aperture and thus could bring into focus only a very narrow slice of the world—anything a few millimeters in front of or behind the focus point will appear blurry. In addition, the constant motion of our eyes blurs any exposure lasting over a few hundredths of a second. To correct these problems, the spy could use an adaptive optics system (*diagram*). The system would bounce a laser beam (infrared so as not to be noticed) off the eyeball, then record what the reflected beam looks like in a camera separate from the one that captures the visible image.

SETUP



DECONVOLUTION



▲ The spy would then run the image of the laser beam through a deconvolution process. The reflection of the beam appears smudged, yet the spy knows that the laser beam was originally a perfect circle. A computer program determines how to best manipulate the smudge to return it to its original state, then performs these same operations on the blurry photograph containing the stolen information. End result: the blurry image comes into focus.

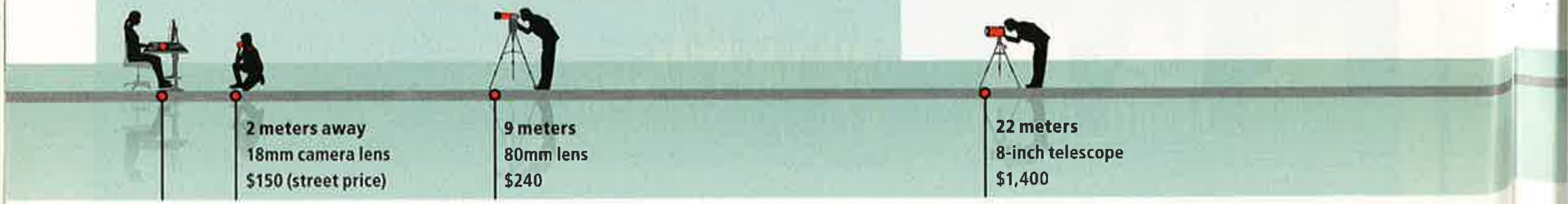
ly typing away. "'What are they working on so hard?' I wondered," Backes says. As he noticed a small blue-white patch in a teapot on one student's desk and realized it was the reflection of the computer screen, the idea struck. "The next day I went to a hobby shop and bought an ordinary backyard telescope [for $435] and a six-megapixel digital camera."

The setup worked surprisingly well. Medium-size type was clearly legible when the telescope was aimed at reflections in a spoon, a wine glass, a wall clock. Nearly any shiny surface worked, but curved surfaces worked best, because they revealed wide swathes of the room, thus eliminating the need for a peeping hacker to find a sweet spot where the reflected screen is visible. Unfortunately, all of us who use computer screens have nearly spherical, highly reflective objects stuck to our faces. Could digital secrets be read off the eyes of their beholders?

Backes knew he would need a bigger telescope and a more sensitive camera to find out. Because eyeballs are rarely still for more than a second or so, the shutter speed on the camera would have to be fast to reduce motion blur. "For eyes, it is the brightness of the reflected image, not its resolution, that limits how far away a spy can be," Backes says.

He bought a $1,500 telescope and borrowed a $6,000 astronomical camera from the Max Planck Institute for Astronomy in Heidelberg, Germany. Now he was able to make out 72-

SIZE VS. DISTANCE: A spy attempting to read a reflection is limited by the aperture (or width) of his telescope. A telescope that is too narrow will diffract the light coming into it, thus obscuring text. Yet larger telescopes are not only more expensive, they are also more difficult to conceal. The diagram below indicates the telescope size a spy would need at a given distance if the aim were to read 14-point type reflected in an 85-millimeter-wide coffee mug. To read features in an eye, the spy would have to be much closer—divide these distances by about a factor of four.



DON FOLEY (*setup*); LUCY READING-IKKANDA (*telescope lineup*); JEN CHRISTIANSEN (*diagram*)

point text in the eye of a target 10 meters away.

He figured he could do even better by borrowing something else from astronomy: a process called deconvolution that removes blur in photographs of distant galaxies. The idea is to measure how a point of light in the original image (such as a star or a reflected status LED on a monitor) smears when captured by the camera. A mathematical function can then reverse the blurring to restore the point, sharpening the rest of the image at the same time [*see box on opposite page*]. The deconvolution software lowered the threshold of legibility to 36-point type at 10 meters for a telescope that could easily be hidden inside a car. A van-size telescope could do even better.

Backes will present his results this month at the IEEE Symposium on Security and Privacy, but he already has ideas for further improvement. "A real attacker could train an invisible laser on the target," he notes. That would enable autofocusing on the eyeball and better deconvolution of the motion blur. Spies could take advantage of software from HeliconSoft that can assemble one clear image of an object by combining many partially blurry images; only those regions that are in focus are retained. They could also exploit software for high dynamic-range imaging that uses similar techniques to create one high-contrast photograph from images shot with a variety of exposures.

A Blind Defense

Protecting ourselves against our overly communicative computers is much harder in some ways than defending against spam, phishing and viruses. There is no convenient software package one can install to dam the side channels. On the other hand, it is not clear that anyone is actively exploiting them. Backes and Kuhn say it is safe to assume that military organizations have used the techniques to gather intelligence, but they can cite no specific examples.

The blinds in Backes's office were drawn as we discussed these possibilities, and curtains are one obvious way of frustrating a reflection thief. But Backes points out that it is naive to expect that people will always remember, or be able, to cover their windows. Although many laptop users apply "privacy filters" to their screens to protect against over-the-shoulder eavesdropping, these filters increase the brightness of the reflection on the viewer's eyes, thus making the hacker's job easier.

Flat-panel displays emit polarized light, so a polarizing film on a window could in principle block reflections from every screen in the room. In practice, however, this fix does not work. Small variations in the polarization angle of displays are common, and the resulting small mismatches let enough light escape that a good telescope can still make out the screen.

Compared with conventional forms of computer espionage, side-channel attacks do have a couple of major limitations, Kuhn notes. "You have to be close to the target, and you must be observing while a user is actively accessing the information. It's much easier if you can instead convince someone to open an e-mail attachment and install malicious software that opens a back door to their entire system. You can do that to millions of people at once."

For that reason, side-channel hacks are unlikely to become as common as spam, malware and other assaults through the network. Instead they will likely be used to infiltrate a few highly lucrative targets, such as the computers of financiers and high-level corporate and government officials. In these cases, side-channel leaks probably offer the easiest way to bypass elaborate network security systems and do it without leaving any trail that a security team could trace after the fact. Anecdotal evidence suggests such surveillance is already taking place. "Some people in investment banks cite cases where information has disappeared, and they are certain it wasn't a traditional attack such as a software hack or the cleaning lady duplicating a hard disk," Kuhn says. "But to my knowledge, no one has ever been caught in the act." ■

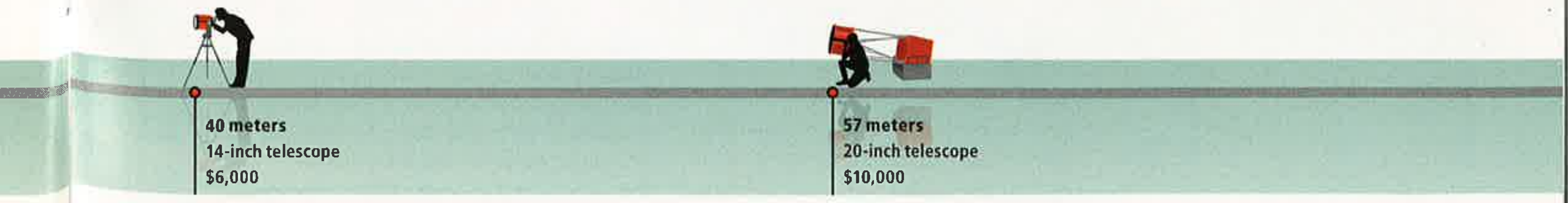
W. Wayt Gibbs, a contributing editor at Scientific American, *is executive editor at Intellectual Ventures in Bellevue, Wash.*

➡ MORE TO EXPLORE

ClearShot: Eavesdropping on Keyboard Input from Video. Davide Balzarotti, Marco Cova and Giovanni Vigna in *Proceedings of the IEEE Symposium on Security and Privacy,* pages 170–183; May 18–22, 2008.

Compromising Reflections, or, How to Read LCD Monitors around the Corner. Michael Backes, Markus Dürmuth and Dominique Unruh in *Proceedings of the IEEE Symposium on Security and Privacy,* pages 158–169; May 18–22, 2008.

Compromising Electromagnetic Emanations of Wired and Wireless Keyboards. Martin Vuagnoux and Sylvain Pasini. Swiss Federal Institute of Technology Web site: **http://lasecwww.epfl.ch/keyboard**



DON FOLEY (setup); LUCY READING-IKKANDA (telescope lineup); JEN CHRISTIANSEN (diagram)