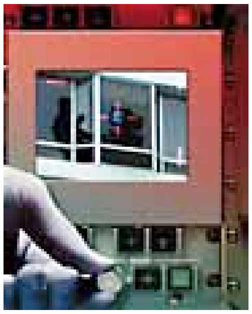
Big Brother
April 2000• Vol.8 Issue 4

Is Tempest A Threat Or Hoax?

"Transient Electromagnetic Pulse Emanation Standard" Supposedly Reads PC Screens From A Distance

Jump to first occurrence of: [SURVEILLANCE]



A large van parks outside a house. Inside the van is a vast array of high-tech equipment: oscilloscopes, demodulators, hidden antennas, wide-band receivers, black-and-white TV monitors. A technician fiddles with dials and buttons until, suddenly, words begin to appear on one of the monitors. The man living in the house is typing the words on his monitor in his house at the precise moment they appear on the **surveillance** monitor. Spies, who have tapped into the electromagnetic radiation emissions given off by the computer's monitor, are stealing the words as they're being typed.

This frightening scenario is often painted on Internet Web sites that warn of the dangers of an electronic eavesdropping method loosely termed "Tempest monitoring." It's also known as the capture of low-level electromagnetic emanations emitted by electronic equipment, such as computer monitors. Another term for the phenomenon is "van Eck phreaking," named after a Dutch research engineer, Wim van Eck, who in the mid-1980s demonstrated that he could easily pick up nearby computer monitor emissions and display them on a TV monitor.

The problem is, James Atkinson says, "there is no such thing as Tempest monitoring. It is an urban legend; one of the biggest hoaxes and snake-oil cons that has been running around for a while." Atkinson is a Tempest engineer certified by the National Security Agency (NSA).

Atkinson is president and senior engineer at Granite Island Group, a Boston company that does communications security work for the federal government and defense contractors, among other clients. He has worked with Tempest for almost 20 years and says that Tempest (an acronym for Transient Electromagnetic Pulse Emanation Standard), refers to the shielding of electromagnetic emanations that come from electronic equipment, not the interception of these emissions.

In Atkinson's view, Tempest concerns have been whipped up by "convicted felons and psychiatric patients" who aim to scare the public, including business owners, into paying for bogus "anti-Tempest interception" devices.

Most sources contacted for this article disagree with Atkinson and believe that Tempest monitoring can and does occur. However, all of our sources say it is rare, and they downplayed its risk to the general public and to small-business people.

Wayne Madsen, senior fellow at the Washington, DC,-based Electronic Privacy Information Center, says most people have no reason to be concerned with Tempest.

"Tempest is the study of vulnerabilities of compromising emanations from communications and other electrical equipment that contain data," he says. "A radio receiver can be placed near an emanating machine and pick up the signals, usually harmonic frequencies, emitted by the equipment.” However, today’s computer equipment, unlike the type of cathode-ray tubes used in monitors more than a decade ago, “has become more ruggedized,” and is heavily shielded so that these emissions are not easily picked up by a radio receiver, Madsen says.

Atkinson notes that the reason today’s consumer PCs are shielded is not to prevent their emanations from being intercepted by spies, but to keep their electronic “noise” from leaking out and interfering with other electronic devices, such as radios and TVs. Government PCs, on the other hand, are often expensively, and heavily, shielded and placed “within rooms within rooms” for security reasons, Atkinson says.

Joel McNamara, who operates the Complete, Unofficial Tempest Information Page (http://www.eskimo.com/~joelm/tempest.html), says Tempest-shielded devices essentially are “the child of government security programs. Shielded devices have never been marketed to consumers outside the government or those industries, such as defense, where Tempest shielding is mandated as a requirement of government contracts.

■ Why Are They Looking At You?

“Tempest-type eavesdropping means you are an interesting enough target to warrant the use of sophisticated equipment and highly trained operators, which cost money,” he says. “The average person or small business really doesn’t fall into this risk category.”

“Tempest is not as big a problem as it once was,” Madsen says. “However, the Tempest engineers don’t like to admit this, and they still hype the problem.”

While the Internet is rife with rumors that you can build a device for $100, using parts bought at a store, such as Radio Shack, that will let you pick up and view data from a nearby computer, Madsen says that this is impossible with today’s computers. In order to capture the emanations from a typical home computer today, Madsen says you would need much more expensive equipment. A surveillance van as described at the beginning of this article would cost $600,000 to $1 million, Madsen says, and it would have to sit close to its target in order to grab the data, making it much more likely to be detected.

“There are much easier ways to get business information,” Madsen says. “Most people would not have to worry about a Tempest threat.”

Similarly, Gary McGraw, Ph.D., who is vice president of corporate technology for Reliable Software Technologies in Dulles, Virginia, says, “Individuals and small-business people have little to worry about regarding Tempest unless they have become a target of spy agencies, who actually do use this stuff.”

“There’s no evidence, as far as I’m aware, of it ever having been used to snoop data from computers belonging to U.S. organizations or individuals within the continental United States of America,” says Ross Anderson, Ph.D., a computer scientist at Cambridge University who has studied and written about Tempest. “It definitely does get used in [U.S.] diplomatic missions overseas, as in this environment the attackers can get up real close, less than 100 yards, and stay there for years.”

Tim Belcher, Chief Technical Officer at RIPTech, an Alexandria, Virginia,-based security consulting firm that employs former military intelligence officers, says that some people have expanded the definition of Tempest to also include the recording of data from emanations in transmission lines, such as Ethernet cables.

Belcher, whose firm counts the government and *Fortune* 100 companies among its clients, says if you use this definition of Tempest, there is a threat, albeit small, to the general public, primarily due to nonsecure home computer networks and small-business networks.

“A lot of home networking and small networking products have emanations problems,” Belcher says. “They will emanate past the borders of your home as much as a block away.”

If somebody wanted to capture data you were transmitting over your network, such as a small Ethernet network in your office, he or she would have to know the specific technology you were using, Belcher says. If the eavesdropper had this information, he or she could pick up your transmission emanations with a device that might cost about $1,000.

🟦 Protect Yourself & Your Data.

If you want to protect your PC against this type of security leak, Belcher advises making sure any data you send from your computer is encrypted, so that even if a person is able to record the emanations, he won't be able to understand what you've written.

However, this type of eavesdropping would pick up only the data that you were transferring between computers. Unlike the traditional Tempest scenario, the eavesdropper could not see what you were typing on your computer monitor, only information that you sent to another computer on your network.

Anderson has predicted that new devices will come on the market in the next few years that can more easily and less expensively intercept computer emissions, making this sort of eavesdropping more of a threat than it is today. He is concerned enough about this incipient threat that he and an associate professor have developed and are attempting to patent several software solutions to the Tempest threat, including a set of fonts he believes would be illegible to Tempest snoops.

Atkinson calls these fonts another hoax that has been around for years.

"The next several years will bring increased horsepower processors at lower prices to make homebrew Tempest intercept devices a reality," McNamara says. "Just as you're seeing hardware and software being developed to crack various encryption schemes, it's a matter of time before someone decides to work on a Tempest project."

McNamara compares the detection of these computer emanations to the situation today with wireless phones, cell phones, and baby monitors, which can be easily intercepted using radio scanners that cost about $100 used. He notes that for a little more money, $600 to $800, he can purchase a scanner with a device that tunes into the cell phone in the car next to him.

"Yes, doing so is illegal, but like a Tempest intercept, it is passive and difficult to detect," he says. "It also requires no technical training, just turn the scanner on and press a couple of buttons."

Yet, despite how easy it is to monitor wireless phone conversations, people continue to make them, McNamara points out. "Does the security risk prevent people from using phones? No," McNamara says. "Informed people may take precautions not to discuss sensitive business or personal topics over a wireless phone, but most people either are unaware of the threat or don't care. When cheap Tempest intercept devices become available, the situation will be the same."

John Young is a New York architect who says he often designs Tempest security features into buildings for clients, such as law firms and banks; he does not work for any government entities. He has become so interested in Tempest that he has filed numerous Freedom of Information Act requests with the government to declassify NSA documents concerning Tempest, which he has posted on his Web site. Young believes as the general public becomes more aware of Tempest, they will begin clamoring for technology and equipment to protect their privacy, just as they requested encryption capabilities in the past.

"I wouldn't be pursuing it if I didn't think it was going to break," he says.

McNamara points out on his Web site that Tempest consulting and manufacturing services currently are a $1 billion business. "This indicates there's a viable threat to justify all of this protective hardware," McNamara says on his site. Either that, or, as he adds in a parenthetical comment, "it's one big scam that's making a number of people quite wealthy." ■

by Lorna Collier

Want more information about a topic you found of interest while reading this article? Type a word or phrase that identifies the topic and click "Search" to find relevant articles from within our editorial database.

Enter A Subject (key words or a phrase):

● Word Search ○ Phrase Search

Search

Return to Previous Page

Copyright & Legal Information Privacy Policy Site Map Contact Us Need Site Help?