

Laser Beam Eavesdropping – Si-Fi Bugs?

by Kevin D. Murray, CPP, CISM, CFE

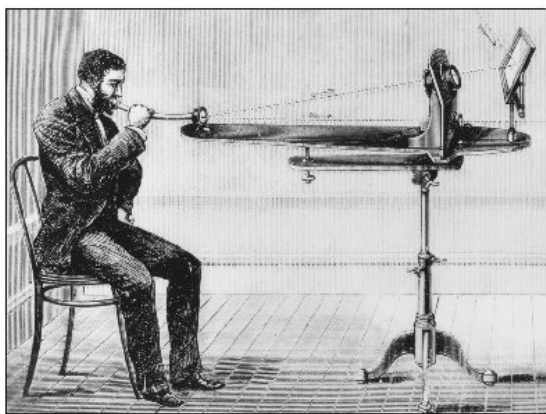


In 1988, newspaper reports about laser beam eavesdropping swept the country. Our clients were scared. To learn exactly how scared they should be, we built a laser beam eavesdropping system and conducted a series of experiments. The following report to clients is the result of those experiments.

---- • ----

Eavesdrop from afar, merely by pointing at a window. The idea is alluring to some, horrific to others.

News media reports of just such a bugging device, based on laser beam technology, have been circulating for some time now. A litany of claims "...can hear from miles away," and compound-claims "...through closed windows," culminates with the coda "No one is safe."



Like the X-Ray vision glasses of comic book fame, laser beam eavesdropping claims tend to be exaggerated. But, like the concept of X-Ray vision, laser listening can be accomplished with the right equipment and conditions.

Over a Century Old Invention.

April 26th, 1880 – Alexander Graham Bell & Sumner Tainter announce their invention - the Photophone. Sound is transmitted on reflected light-rays a distance of 213 meters. They also claim, "it can transmit songs with great purity of tone." This is the forerunner of CDs, DVDs, fiber optic telephone transmission ...*and* remote eavesdropping.

Laser Beam Physics 101 (simplified)

Sound is transmitted by vibration. When you speak, you vibrate the air. The air, in turn, vibrates everything it contacts. Certain objects, eg. windows and mirrors, pick up vibrations very easily. When a laser light beam hits such an object, it *vibrates* also as it reflects and continues its trip. The reflected, *vibrating* beam can be received; electronically processed; and then listened to. Under controlled conditions, very high quality audio can be recovered.

Laser Beam Physics 202

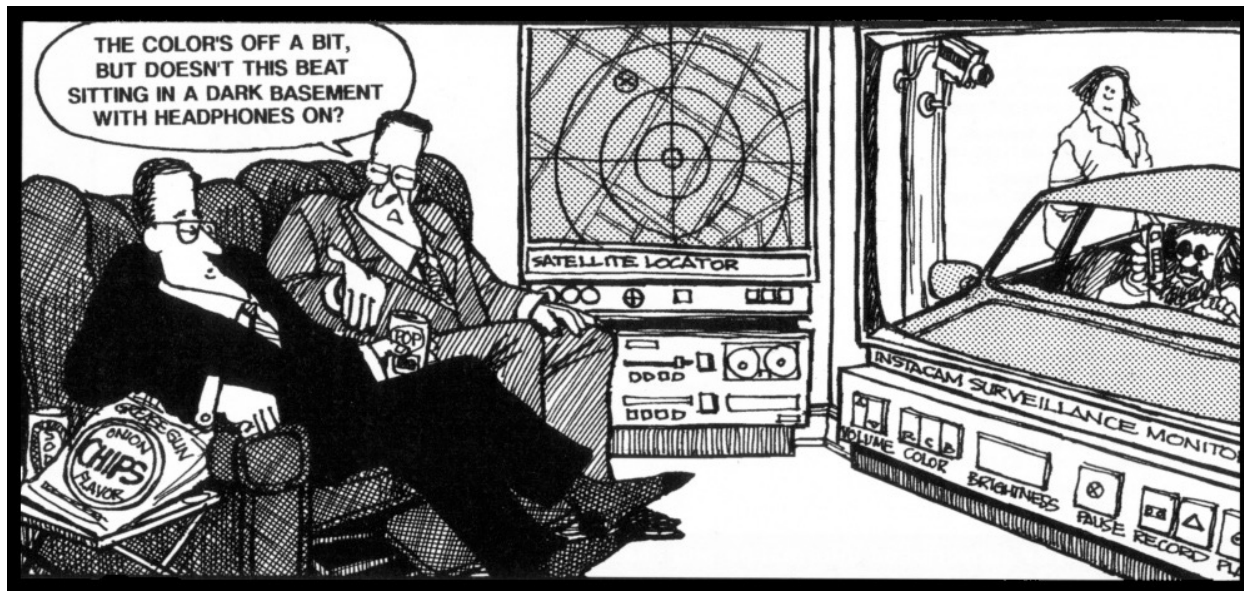
(real world, real problems)

Bouncing an invisible laser beam off a window, and attempting to catch the reflection, is a little like playing 3-D billiards – blindfolded. The fun increases exponentially with distance from the target. As if this doesn't make reception difficult enough... the greater the angle of incidence, the greater the distortion of the received sound.

All sound will vibrate a window. This includes interior conversations as well as exterior noises (cars, trucks, birds, etc.). Audio laboratory

Laser Beam Eavesdropping – Si-Fi Bugs?

by Kevin D. Murray, CPP, CISM, CFE



processing equipment can attenuate this effect, to a degree. We found, if the outside noise is as loud as the conversation indoors audio processing techniques are of marginal assistance.

Reflecting a beam from interior room objects helps reduce external sound, however, the beam loses power with each pane of glass it passes through. This reduces effective working distances and increases the number of reflected beams with which one must cope. Thick glass and thermo-pane glass, as used in office buildings, does not conduct sound vibrations as well as thin residential plate glass.

Air thermals, dust, wind, fog and rain disrupt laser beams. The greater the beam length, the greater the disruption. Wind blowing through a laser beam, we found, generates noise similar to the cacophony of airplane engines.

A laser beam (one powerful enough for professional eavesdropping) is the Neutron Bomb equivalent of a sharp stick in the eye. Both can blind you, but the laser leaves the eye standing. Blinding the subject of a surveillance is not the best way of assuring a continued stream of information while remaining unnoticed. We used safety goggles during our tests.

Update

Advancements in signal processing have been made since 1988, however, the physics problems mentioned above remain.

Consider trying to use laser eavesdropping in a business environment. Thick, double pane windows (which don't open). Loud street noises. Few opportunities to face a target window at a right angle. There must be better ways to eavesdrop and spy," I hear you say. There are.

Laser Beam Eavesdropping – Si-Fi Bugs?

by Kevin D. Murray, CPP, CISM, CFE



The laser beam is not your worst (or only) enemy. When it comes to your privacy and information security keep your outlook holistic. Don't overlook age-old espionage techniques – like burglary, sex and blackmail.



The Future of Remote Eavesdropping

Eavesdropping-from-afar technologies such as: laser beam,

microwave, ultra-wideband, ultra-sound and Tempest attacks will get better with age. We don't discount them. Our clients know this topic has our serious attention and we will continue to keep them informed of new developments – with a realistic perspective.

What will the future bring?

Interception of brainwaves comes to mind... or, was that something you were thinking just now?

Beat the Beam

If you **still** suspect a laser beam eavesdropping attempt is being made against you, fight back...

- Hold confidential conversations in a room without windows.
- Place a radio against the window and close the drapes, or
- Install a white noise generator on the window pane.

Of course, do not discuss your suspicions within the target area. Contact a [professional Information Security Consultant](#) for additional assistance. Your problems are more extensive than you think.

Laser Beam Eavesdropping - Today

It is time to update our views on laser beam eavesdropping. While not entirely practical yet as an everyday amateur or business-level spy tool, advancements are being made.

Researchers from Bar-Ilan University (Ramat-Gan, Israel) and the Universitat de València (Burjassot, Spain) developed a new way to sense sound remotely using a laser beam.

Their research paper is titled: "[Simultaneous remote extraction of multiple speech sources and heart](#)

[beats from secondary speckles pattern](#)" and the authors are: Zeev Zalevsky, Yevgeny Beiderman, Israel Margalit, Shimshon Gingold, Mina Teicher, Vicente Mico, and Javier Garcia.

Unlike classic laser beam eavesdropping, the new method does not rely on interferometer or a reflecting diaphragm, like a window. A single laser beam is aimed at the object to be monitored (a person and a cell phone were used in these tests).



Laser Beam Eavesdropping – Si-Fi Bugs?

by Kevin D. Murray, CPP, CISM, CFE



The speckles that appear in an out-of-focus image of the object are then tracked. This produces data from which a spectrogram or sound signal can be constructed.

The setup is basic.

The laser illuminates a small area on the object and an ordinary digital camera captures the



scene. The camera's lens is de-focused. This produces a pattern that does not randomly change when the object moves. The camera image is processed, calculating the shift of the pattern from frame to frame.

Kevin D. Murray CPP, CISM, CFE is a professional Information Security Consultant, specializing in Technical Surveillance Countermeasures (TSCM), with over four decades of experience.

[Murray Associates](#) is an independent security consulting firm, providing eavesdropping detection and counterespionage services to business, government and at-risk individuals.

Headquartered in the New York metropolitan area, a Murray Associates team can assist you quickly, anywhere in the United States, and internationally.

v.190104

Laser beam audio samples...



- [Cell phone at 60m.](#)
- [Neck of person at 30m.](#)
- [Face at 100m.](#)
- [Heartbeat at 60m.](#)

Note: Audio is labeled as listed in the research paper. However, it sounds like the neck and face audio clips may have been reversed.

