Modern Eavesdropping: Its Easier and Cheaper Than Ever To Spy On Someone

McCann Investigations
1018 Preston St.
Houston
TX 77002

Table of Content

Common Eavesdropping Devices

General principles of eavesdropping technology

Eavesdrop is originally a noun pointing to the water dripping off the eaves of a building and the space between the wall and the dripping. By the early 1600s, to eavesdrop actually meant to stand in the eavesdrop of a **house with the intent to hear** conversations within and was criminalised. This is the first time the term "eavesdropping"[1] was legally acknowledged.

However, historical accounts of spies and espionage conspiracies in critical or crisis circumstances appear in some of world's earliest records, from Egyptian hieroglyphs to ancient Rome and Asian military. Over 2500 years ago, General Sun Tzu of the ancient Chinese army explains the importance of espionage in warfare in his famous work "The Art of War"[2]: espionage should be used to obtain information regarding the strength and location of the enemy's forces, terrain and the loyalties of local populations and counter espionage should be used to deny this same information to the enemy.

Two and a half millennia later, spies have continued to be key-factors, influencing the outcome of wars[3] and social movements[4]. Eavesdropping has become **state of the art surveillance**, deploying **impressive technology** and resources to acquire sensitive information. A well placed **microphone bug** was much more efficient than a person eavesdropping next door.

Classic eavesdropping systems were generally comprised of **three essential elements[5]**: a pick-up device, a transmission link and a listening post. A microphone or video-camera picks up a signal and converts it to electric impulses, which are then transmitted **off-site by radio frequency** or by **wire to a processing post.** This kind of devices, once suspected, were easily detected and shut down. The devices themselves began being more and **more discreet,** while losing some of the physical elements: hardwired became wireless and hardware became software.

Software tools are now the most **recent link** in the evolution of surveillance technology. They are **easily deployed**, **amazingly efficient** at acquiring information and require almost no human intervention to operate. Just like hardware devices, software bugs are installed either without your knowledge or by tricking you. This is where espionage starts developing on two different paths.

On one hand, anyone interested can aim at a specific target for acquiring information of interest. This type of targeted espionage and is most similar to **conventional technical surveillance**, only bugs are software rather than hardware. It represents most of the cases of economic cyber-espionage[6], where competitors are

[1] Source: http://www.wordorigins.org/index.php/eavesdrop/

[2] Source: http://www.ancientmilitary.com/Sun-Tzu-The-Art-of-War.htm

[3] Source: http://www.theguardian.com/culture/gallery/2013/apr/13/10-best-real-life-spies

[4] Source: http://listverse.com/2007/08/24/top-10-famous-spies/

[5] Source: http://www.wright.edu/rsp/Security/V3bugs/Methods.htm

[6] Source: http://www.justice.gov/opa/pr/us-charges-five-chinese-military-hackers-cyber-espionage-against-us-corporations-and-labor

targeted to **acquire competitive advantage**. This cases are more frequent and more complex by the year, up to government levels.

The second type of cyber espionage aims at **mass targets or opportunistic targets**, infecting individual devices in order to access **valuable information** on them. This type of bugs are commonly installed unknowingly[7] by the user himself. This kind of attacks are fast profit and volume oriented. Surveillance cyber bugs[8] are most commonly used to **gather information** that can be used for **identity theft**, ever more dangerous with the growing online banking trend.

Software bugs can secretly move **huge amounts of information** to anywhere in the world. They can even do some of the data analysis tasks, searching for specific words or codes, not to mention overriding other functions of the target devices and transform them in ever more efficient spying tools. **Cyber surveillance** has come a long way from the eavesdropping in medieval times.

Avoiding Detection

Evading detection has been one of the main concerns in the technical espionage world. Finding methods to **conceal the device or make it undetectable** by common means has been the main driver for innovation in this field. For hardware devices, eliminating the need for unessential pieces such as a power source or a transmitter lead to **passive devices** that were harder to detect.

For instance, one of the most efficient passive listening device ever used for spying is a **resonant cavity microphone**[9] commonly known as The Thing and used by the Soviets to spy on the US Ambassador from 1945 to 1952.

It uses **passive techniques** to transmit an audio signal, being **energised and activated by electromagnetic energy** from an outside source. There were no wires, no batteries, no waves giving up the bug and the device was only accidentally discovered.

Perhaps the most **common types** of eavesdropping device in use today is the **wireless transmitter**, which picks up sound via a small hidden microphone and then broadcasts it using radio frequencies. This is used to be easily detected by conducting a radio frequency detector sweep but has become more **difficult to pinpoint** with the overcrowding of the airwaves. The RF environment is now very complex and at the same time very dynamic and signals emitted by covert surveillance devices can be lost in the noise or get overshadowed by the multitude of other signals. Masking the **transmitting signal to blend** in in a certain environment can prove to be an efficient way[10] to evade detection and has already arouse the interest of professional TSCM service providers.

---

[7] Source: http://www.computerhope.com/issues/ch001045.htm

[8] Source: http://usa.kaspersky.com/internet-security-center/threats/spyware

[9] Source: http://www.academia.edu/7275923/Lev_Termens_Great_Seal_bug_analyzed

[10] Source: http://www.counterespionage.com/assets/tektronix-rsa6114a-case-history.pdf

However, technological advance has also led to eavesdropping devices that are more and **more difficult to detect**, for example, devices that **do not constantly emit radio waves**. One way of avoiding detection but still use radio frequency to send information is the "burst transmission" device. This kind of device digitises the sound and compresses the resulting record. Then it is transmitted at **predetermined or random intervals** or on command, as a short burst of modulated RF.

This means they could transmit **hours of content in seconds** and remain **virtually passive** to the radio waves landscape in your location for the rest of the time. Other devices simply require inside help to manually download and transmit information[11]. Finding these bursts with traditional spectrum analysers can be very challenging.

Some more sophisticated devices used for cover surveillance do not even require being placed in a sensitive location. **Shotgun microphones, optical devices or parabolic reflectors** can be used to listen to conversations in remote locations. To get an idea of just how broad surveillance technology can be, imagine someone could project a **laser beam[12]** onto the window of your office to record vibrations caused by sound waves and then use optical devices to convert these light pulses back to audio signals. This kind of systems are very expensive and easily detected if specifically targeted. Nevertheless, this goes a long way from the classic telephone wire tapping.

There is a huge amount of information available to describe surveillance devices[13] and their modus operandi, for the concerned reader. **Physical surveillance devices** can prove to be **very elusive**, but are still confined to an actual device that can be pinpointed at one time or another.

Software surveillance tools and technologies are much more flexible as they **blend** in into the devices they are targeting. Just a few examples of measures used to evade detection of a software surveillance tool:

- passing as an established well-known trusted program[14] or service is the most common way of disguising spyware. Governments are believed to have used this on large scales, but smaller, more **targeted pieces of software can be masked** using the same method.

- as to conservation methods after being installed, a good example is **polymorphic spyware** that has the ability to constantly change its filename and location to avoid detection by anti-spyware programs

- sometimes, a **spyware can continuously backup** itself, by injecting a copy into a process that is running on a device, as a security measure. If the main spyware program is deleted, the active copy spawns another copy of itself

[11] Source: http://www.wright.edu/rsp/Security/V3bugs/Methods.htm

[12] Source: http://techlinkcenter.org/summaries/high-sensitivity-laser-microphone

[13] Source: http://www.uscrow.org/downloads/Survival%20Public%20Domain/Understanding%20Surveillance%20Technologies%20Spy%20Devices%20Their%20Origins%20and%20Applications.pdf

[14] Source: http://www.infosecurity-magazine.com/news/wikileaks-releases-finfisher/

- other **spyware run in the background[15],** doing no damage itself, but generating another program that does the actual damage. Anti-spyware detects the active program but not the silent spyware

- some other pieces of surveillance software try to avoid detection by **hiding their real extensions[16]** and showing up a seemingly secure .txt or .doc extension

These are just a few examples of how deeply can a spyware disguise itself to look unobtrusive when targeting a device.

Common eavesdropping devices

Example of Physical equipment for privacy invasion[17]

- **Recorders**, which use a micro SD card as recording medium and can record up to 500 hours of conversation. Recorders can be used as planted devices or as body bugs. These can be placed in key-places or be used only when needed (e.g. during meetings)
- **GSM bugs** which turn mobile telephones into bugging devices and cand transmit conversation to anywhere in the world
- **Hardwire bugs** – considered one of the most reliable and efficient surveillance systems. They can be hidden in walls and ceilings and since these kinds of eavesdropping devices do not emit radio frequencies they are generally very difficult to detect . For examples, telephones are not a risk only when in use. Small electrical modification can leave the microphone on and ensure high quality audio surveillance of the whole room, with no radio waves activity.
- **Radio frequency transmitter** which is at the lower end of the scale, inexpensive and easy to use. They are very popular with private investigators and individuals and though easily detected when targeted, they can be very efficient when placed in a non-suspicious environment.

[15] Source: http://ptgmedia.pearsoncmg.com/images/9780789735539/samplechapter/0789735539_CH03.pdf

[16] Source: http://www.infosecurity-magazine.com/news/mac-spyware-hides-file-extensions-to-evade/

[17] Source: http://www.eyetek.co.uk/blog/types-of-bugs


MCCANN INVESTIGATIONS
EST. 1984
TOTAL SECURITY SOLUTIONS