Tempest

Article URL
Tempest

Author
SecurityHome.eu

Published: 12 September 2006

Last updated on 29 May 2012.

Â

All electric machines send out unwanted electric radiation. Especially with computers and other data processing units, this radiation carries essential data which can be monitored and recorded by third parties. TEMPEST is the name the American government gives to a few standards to limit this radiation.

Since the 1950's, governments discovered that unwanted radiation(emanations) can be monitored and reconstructed. From then on the governments spend heavily in prevention and in capturing of these signals from enemy computers.
Famous is the example from Peter Wright in the book Spycatcher, where he describes how the MI5 (British secret intelligent) used the Tempest technology to pass the France diplomatic code. They couldn't break the code and they really wanted to know how De Gaulle thought about England entering EEG. The coded signal appeared to contain a very weak interfering component, that contained the original message in clear language.

From that day government use expensive metal sealing equipment to protect computers, rooms and even entire buildings. Even within these sealed environments they use the "red/black"-principal. The "red" are sensitive machines, like computer terminals, and black parts are parts that are connected to the outside world, like modems.

Especially computer screens send out radiation, so anyone with a little knowhow can see what's on your screen.
But also the signals from a RS-232 wire (modem wire) can be monitored. Signals can also be transferred (unwanted) from one cable to another (telephone, power, ...).
But one of the most noisy parts of a computer is the keyboard. In particular the keyboard cable and the keyboard controller (a little chip inside the keyboard).

So how much of a thread is this ?

It looks like a big thread to anyone who want's to keep there privacy. Specialists say the government agency's can capture and reconstruct signals up to a distance of 1 km. And some handy amateur with some cash, up to

300 m.
With tempest they don't need to break in, leave tracks and they can stay well out of sight.

Lucky it's not all that easy, Tempest-receivers are very expensive and do not always work. Because of the secrecy around tempest, there is no real data.

Why should we consider tempest as a thread?

* The tempest-protection industry makes in the USA a turnover of more then a billion dollars in 1999. This is standard for most government institutions.

* Several military institutions report that they suffer from tempest-attacks to gain information.

* For companies its also recommended to use tempest-proof machines to counters extraction of data.

But there is also:

* Tempest-receivers are very sensitive, in difficult (weather-)situations they don't always function.

* These receivers are very expensive, you need skilled people and time to get results. This is no "Plug and Play".

* Isn't it cheaper and faster to bribe someone? Are there other ways to gain this information?

How can you protect yourself?

You can of course build a *cage of faraday*

(A closed room of metal). But this is very expensive and hard to build (modems-, and power-lines need to get out.)
But there are some cheap tricks to make it harder to capture these signals.

* Use tempest-proof fonts. These fonts are a bit flew on screen, but are extremely hard to reconstruct by tempest-receivers.

* Also use a good up-to-date virus scanner.
Why ? There are tempest-viruses out there. They put a easy recognizable code on your screen. The user can hardly see this code on his screen but for tempest-receivers it's a lot easier to reconstruct the images.
But this can not only be used for the screen. It can also manipulate your harddisk, processor, ...

* Leave the metal-cage of your computer intact. Close any open slots with metal plates.

* Use good quality cables to connect your computer with your printer, screen, ... Keep these cables as short as possible.
Try not to place them parallel with telephone, network or power-lines.

* Remove infrared ports or seal them with proved sealing stuff.

* There are also Tempest-proof tents, very expensive but stops all radiation between 10 Khz and 2 Ghz.
More info : http://cryptome.org/bema-se.htm

* If you want to write or read important data, be mobile. Tempest receiver are somewhat large and take time to configure. So take your laptop, palmtop and go to a restaurant or some public place.

If you want more security, you should know that it cost more and more for less extra security.

* Get filters to block ElectroMagnetic Interference (EMI) in the power-cables.
Especially for the computer and the monitor. (printer and others are not that important).

* If you can get also a EMI-filter for telephone lines.

* You can also turn your cables around a core of ferrites. This "absorbs" the unwanted radiation.
Don't forget the cable of the keyboard, mouse and telephone.

Warning

LCD-screens are NOT tempest save. The technology reduces the risk a bit but not much. Especially the cable that connects the monitor with the graphics card, send out much radiation. Some laptops are very "noisy" because there are a lot of cables in a small box without any metal sealing. Some color LCD-screens are even easier to "monitor". This because every transistor (pixel) is directed separately, so tempest-receivers have less synchronization-problems.
I still recommend that you buy LCD-screen cause they are better for your eyes, are smaller and use up to 80% less energy than normal screens.

There are also some good books
Spycatcher by Peter Wright