Master Thesis
Computer Science
Thesis no: MCS-2003:13
June 2003

TEMPEST Attacks

- Using a simple radio receiver

Jonas Karlsson

Department of
Software Engineering and Computer Science
Blekinge Institute of Technology
Box 520
SE – 372 25 Ronneby
Sweden

This thesis is submitted to the Department of Software Engineering and Computer Science at Blekinge Institute of Technology in partial fulfillment of the requirements for the degree of Master of Science in Computer Science. The thesis is equivalent to 10 weeks of full time studies.

Contact Information:
Author: Jonas Karlsson
Address: Folkparksvägen 21, 372 38 Ronneby
E-mail: it99jca@student.bth.se

University advisor: Rune Gustavsson
Department of Software Engineering and Computer Science

Department of
Software Engineering and Computer Science
Blekinge Institute of Technology
Box 520
SE – 372 25 Ronneby
Sweden

Internet : www.bth.se/ipd
Phone : +46 457 38 50 00
Fax : + 46 457 271 25

ABSTRACT

There are no public records that give an idea of how much *emanation monitoring* is actually taking place. However, there are a few data points that lead us to believe there is a real threat. One of these is that *TEMPEST* industry is over a billion dollars a year business.

Reports like the ”Redefining Security” by Joint Security Commission stated that electronic equipment such as computers, printers, and electronic typewriters give off electromagnetic emanations and that this has long been a concern for various industries. An attacker using the latest and most efficient equipment can monitor and retrieve classified or sensitive information as it is being processed without the user being aware that a loss is occurring. But new information states that the attacker doesn’t need to have access to the latest equipment.

This master thesis is based on the three statements below:

- It exists a cheap and simple *TEMPEST* technique that is a security risk.
- A downloadable *TEMPEST virus* is a powerful tool when conducting *TEMPEST* attacks.
- It does not exist a cheap and simple solution that protects common users from *TEMPEST* attacks.

In the experiment I use a program called Tempest_for_eliza and a simple Philips radio receiver.

In this thesis I prove that it exist a *TEMPEST* technique, that is cheap and relatively simple and still is a security risk. I prove this with facts from literature studies and an experiment. Today there is only one way to protect yourself against *TEMPEST* attacks and that is by metal shielding. This is expensive and home users have the option but not often the resources to finance this type of protection.

Keywords: TEMPEST, electromagnetic emanation, security, metal shielding

CONTENTS

1 INTRODUCTION

The aim of this master thesis is to find out if it is possible to pick up information from a computer using a *TEMPEST virus* and a simple radio receiver. I will do this by explaining what *emanation monitoring* is and by conducting an experiment. I will also look into, if there are ways to minimize the risk of these types of attacks.

Is it possible to pick up information from a computer using a *TEMPEST virus* and a simple radio receiver? This is the main question that I have and from this main question I have made three statements that I will answer. The three statements are:

- It exists a cheap and simple *TEMPEST* technique that is a security risk.
- A downloadable *TEMPEST virus* is a powerful tool when conducting *TEMPEST* attacks.
- It does not exist a cheap and simple solution that protects common users from *TEMPEST* attacks.

It has been known to military organizations since at least the early 1960s that computers generate *electromagnetic radiation*, which not only interferes with radio reception, but also leaks information about the data being processed [6]. This is known as compromising emanations or *TEMPEST* radiation. *TEMPEST* is an United States government code word that identifies a classified set of standards for limiting electric or *electromagnetic radiation* emanations from electronic equipment. *TEMPEST* is an acronym for Transient Electromagnetic Pulse Emanation Standard.

All electronic devises like microchips, monitors, printers, emit radiation through the air or through conductors (such as wiring or water pipes). An example is using a kitchen appliance while watching television. The static on the TV screen is emanation caused interference. The emanations from a blender aren't important, but emanations from an electric encryption device would be. If the emanations were recorded, interpreted, and then played back on a similar device, it would be extremely easy to reveal the content of an encrypted message.

TEMPEST computers and peripherals (printers, scanners, tape drives, mice etc.), are used by government agencies and companies to protect data from emanations monitoring. Shielding the device with copper or other conductive materials typically does this. In the United States, *TEMPEST* consulting, testing, and manufacturing is a big business, estimated at over one billion dollars a year [6].

My interest about this subject began after reading Ross Anderson’s book ”Security Engineering”[7]. In his book he states that you can use a *TEMPEST virus* and a simple radio receiver to pick up data from a target computer.

This thesis will proceed as follows: In section 2 I will explain what *emanation monitoring* and *electromagnetic radiation* is and security issues regarding them. Section 3 provides information about different types of *TEMPEST* attacks, such as the low-cost *TEMPEST* technique. In section 4 I describe the experiment and present the result. Section 5 provides information about how to prevent *TEMPEST* attacks by

metal shielding. In section 6 I provide a discussion about *TEMPEST* attacks and what can be expected in the future regarding *TEMPEST* attacks. All my conclusions are presented in section 7. The words that are in italics can be found in the dictionary presented in section 8. Section 9 provides information about all the references I have used during my work with this thesis.

2 EMANATION MONITORING

An electric current can be understood as a flux of electrically charged particles, for example electrons. Electric tension can be defined as spatial concentration of electric charges. Electric charges create electric fields around them, whose intensity increases with increased tension.

Moving charges create magnetic fields. When a charge is accelerated (when it's velocity changes) the magnetic field changes. The greater the velocity, the greater the magnetic field. Magnetic and electric fields propagate in space, at precisely the speed of light. Their combination is called an electromagnetic field. When either component of the electromagnetic field changes, this change also propagates in space, forming an electromagnetic (EM) wave. Various characteristics of EM waves are their shape (planar, spherical), frequency, phase relationships between their magnetic and electric parts and direction/shape of polarization. EM waves might be reflected, absorbed, transmitted, conducted and otherwise affected by matter. The more conductive the matter, the more it is likely to affect EM waves. Magnetic and electric fields are tied together. For further details see "electricity and electronics" by Dale R. Patrick and Stephen W. Fardo[2].

There are no public records that give an idea of how frequent *emanation monitoring* is actually taking place. There are only isolated anecdotal accounts of monitoring being used for industrial espionage.

In 1960, Britain was negotiating to join the European Economic Community, and the Prime Minister was worried that French president De Gaulle would block Britain's entry. He therefore asked the intelligence community to determine the French negotiating position. They tried to break the French diplomatic cipher but failed. However, they noticed that the enciphered traffic carried a faint secondary signal, and constructed equipment to recover it. It turned out to be the plaintext, which somehow leaked through the cipher machine.

However, there are a few data points that lead us to believe there is a real threat to the common user. The *TEMPEST* industry is over a billion dollar a year business [6]. This indicates that there is a viable threat to justify all of this protective hardware. This threat is backed up with a quote from a Navy manual that discusses "compromising emanations"(CE). "*Foreign governments continually engage in attacks against U.S. secure communications and information processing facilities for the sole purpose of exploiting CE* [6]."

Reports like the Joint Security Commission issued called "Redefining Security" in 1994 also need to be considered. It states that electronic equipment such as computers, printers, and electronic typewriters give off electromagnetic emanations and that this has long been a concern for various industries.

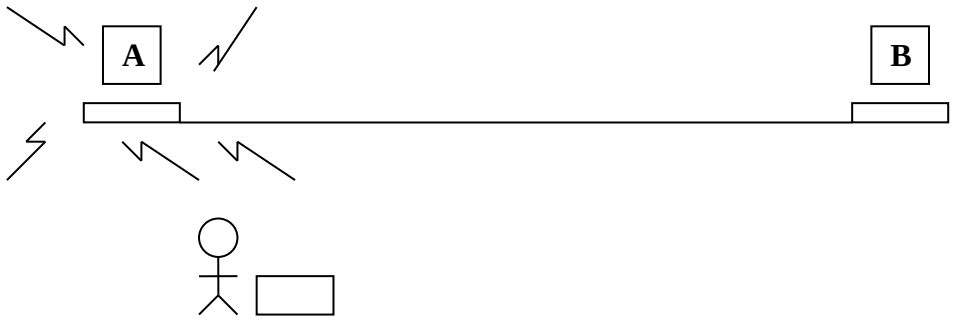
2.1 Radiation and security

Electromagnetic radiation as a computer security risk was mentioned in the open literature as early as 1967. One of the first more detailed public descriptions of the *TEMPEST* threat appears to have been a 1983 report in Swedish, but the problem was brought to general attention by a 1985 paper in which van Eck demonstrated that the screen content of a video display unit could be reconstructed at a distance.

Smulders later showed that even shielded cables can often be eavesdropped at a distance. Compromising emanations are not only caused directly by signal lines acting as antennas. Power and ground connections can also leak high frequency information.

Laptop owners frequently hear radio interference on nearby FM-radio receivers, especially during operations such as window scrolling that cause bursts of system bus activity. A *TEMPEST virus* can use this effect to broadcast data.

When writing a computer virus to infiltrate a target computer, to obtain key material and broadcast it to the attacker over an improvised radio channel, then an important design criterion is the cost of the receiver. While intelligence services may already possess sophisticated antennas and software radios, such equipment is not yet available for common people. The equipment used is more likely to be just a radio receiver connected to an audiocassette recorder. In figure 2.1 you can see the attacker with the radio placed near the target computer. The attacker has planted a *TEMPEST virus* in computer A using techniques like the Trojan horse. The attacker can now pick up the signals from computer A for example from the company's parkinglot. Interesting things for the attacker would for example be passwords, account numbers etc.



The attacker with a simple radio receiver

Figure 2.1

In order to get a computer monitor to produce audible tones on the attackers radio, the attacker design a screen image that causes the monitor beam current to approximate a FM/AM radio signal broadcast.

The timing of a digital video display system is first of all characterized by the pixel clock frequency f_p, which is the reciprocal of the time in which the electron beam travels from the center of one pixel to the center of it's right neighbor.

The pixel clock is an integer multiple of both the horizontal and vertical deflection frequencies, that is the rate $f_h=f_p=x_t$ with which lines are drawn and the rate $f_v=f_h=y_t$ with which complete frames are built on the screen. Here, x_t and y_t are the total width and height of the pixel field that we would get if the electron beam needed no time to jump back to the start of the line or frame. However, the displayed image on the screen is only x_d pixels wide and y_d pixels high as the time allocated to the remaining $x_ty_t-x_dy_d$ virtual pixels are used to bring the electron beam back to the other side of the screen. See Table 2.2.

f_p	Pixel clock frequency*	**Pixel clock**
f_h	Horizontal deflection frequency**	
f_v	Vertical deflection frequency***	
x_t	Total width of the pixel field****	**VDisplay**
y_t	Total height of the pixel field****	**HDisplay**
x_d	Width of the displayed image on the screen	
y_d	Height of the displayed image on the screen	
$x_ty_t-x_dy_d$	Virtual pixels*****	**HTotal**

* The reciprocal of the time in which the electron beam travels from the center of one pixel to the center of it's right neighbor.
** The rate with which lines are drawn.
*** The rate with which complete frames are built on the screen.
**** The total width and height of the pixel field that we would get if the electron beam needed no time to jump back to the start of the line or frame.
***** The time allocated to the remaining, are used to bring the electron beam back to the other side of the screen.

Table 2.2

The words that are in bold are the parameters the attack software needs see section 4.1. Attack software can read these parameters directly from the video controller chip, or find them in configuration files.

It is not necessary to fill the entire screen with the pattern, but the energy of the transmitted signal is proportional to the number of pixels that display it. The reception range depends largely on how noisy the radio spectrum is near the selected carrier frequency f_c, so this frequency should be selected to avoid nearby broadcast stations.

3 TEMPEST TECHNIQUES

Video display units output their frame buffer content periodically to a monitor. When conducting attacks, the video display units often are targets, especially when the video signal is amplified to several hundred volts. Knowledge of the fonts used with video displays and printers allows maximum likelihood character recognition techniques to give a better signal/noise ratio for whole characters than is possible for individual pixels.

Malicious software implanted by an attacker can also generate periodic or pseudorandom signals that are easy to detect. Similar techniques can be applied when snooping on CPUs that execute known algorithms. Even if signals caused by single instructions are lost in the noise, correlation techniques can be used to spot the execution of a known pattern of instructions.

NONSTOP is a classified codeword that relates to a form of compromising emanations. NONSTOP involves the transmittal of the signals from radio frequency devices (handheld radio, cell phone, pager, alarm system, cordless phone, wireless network) in proximity to a device containing secure information. There are specific guidelines for either turning the device off, or keeping it a certain distance away from the secure device (PC, printer, etc.).

HIJACK is a classified codeword that relates to a form of compromising emanations, but involves digital versus electromagnetic signals. An attack is similar in nature to a *TEMPEST* attack, where the adversary doesn't need to be close to the device that's being compromised (it does require access to communication lines). The adversary uses antennas, receivers, a display device, a recording device and a special detection system. The technician using this special equipment will supposedly require a great deal of training and experience.

3.1 Low-cost TEMPEST technique

In a low-cost attack, the attacker could implant the attack software using standard virus or Trojan techniques and place a radio and cassette recorder near the target. Since the broadcast patterns will be visible, the attack should take place after business hours while avoiding times when the chosen frequency is swamped by ionospheric propagation of interfering stations. Many PCs are not turned off at night, a habit encouraged by the power management features of modern systems. If monitors are also left powered up, then the attack software might monitor network traffic to detect the presence of people in the department. Where monitors are turned off but PCs are not, a serviceable signal can usually be picked up. In these cases, the attack software can broadcast unobtrusively in the evening and early morning hours.

The attack software can use frequency shift keying, with 0 and 1 represented by tone patterns. Fast switches between screen patterns can also be accomplished using the color lookup table. The bit pattern would be encoded first to provide forward error correction before its bits are used to select the sequence of tones transmitted.

The attacker can then take the cassette with the recorded broadcast to his PC and digitize the signal with his sound card. The remaining steps involve symbol detection, synchronization and decoding. Targets include password files, key material and documents selected by text searching of the hard disk.

The main difficulty in tracking instances of *emanation monitoring* is because it's conducted at a distance from the target, and this is hard to discover unless you catch the perpetrator red-handed. Even if a spy were caught, more than likely the event would not be publicized, especially if it was corporate espionage. Both government and private industry have a long history of concealing security breaches from the public.

As with any risk, companies really need to weigh the costs and benefits against each other. While some "hard" targets may justify a technical approach, traditional human intelligence (HUMINT) gathering techniques are without a doubt, used much more often than *emanation monitoring*.

4 EXPERIMENT

4.1 Description of the experiment

The purpose with this experiment is to find out if there is a cheap and simple way to bug computers using a *TEMPEST* technique. To accomplish this I am using a program that is available on the Internet and a simple Philips radio receiver. I want to point out that I have not bugged any other computer then my own.

First of all I looked at the programs that where available on the Internet. At this time, in the beginning of February, there where a few that I where able to download. I looked at each of these programs and the one I decided to use was Tempest_for_eliza-1.0.5. The reason for this was that I thought that the instructions and the technique the program used approved to my theory. The program Tempest_for_eliza-1.0.5 is written by Erik Thiele and is based on TEMPEST-AM-0.9 written by Pekka Riikonen.

The next step I had to take was to gather more information about the program and how to use it. I did this by putting out questions in different discussion groups. I also sent emails to different people, including the authors behind Tempest_for_eliza here either. Last but not least I did an extensive search on hacker- and cracker sites. I did not receive any response from any of these attempts to gather information.

Tempest_for_eliza is written in the programming language C++. Markus G. Kuhn's and Ross J. Anderson's paper; "Soft TEMPEST: Hidden Data Transmission Using Electromagnetic Emanations"[6] was used as a reference when programming Tempest-AM-0.9. Tempest_for_eliza uses an algorithm that makes it possible to send radio waves from the computer monitor. To make this possible there are a number of parameters that you have to enter (see below). I described some of these in section 2.1.

HDisplay
VDisplay
HTotal
Pixel Clock
Radio frequency
Music file

The program runs in full screen and displays pictures on your screen, one for each note in the song.

4.2 Discussion of the experimental result

I started with the installation of Linux Mandrake 9.1 with kernel 2.4.21 because Tempest_for_eliza is designed to run in Linux. Then I installed Tempest_for_eliza. I did this by extracting the files to the directory Tempest_for_eliza. The specific

directory now contained several files. The command I used when I installed Tempest_for_eliza was configure and make.

To make Tempest_for_eliza work you need to have SDL installed. SDL stands for Simple DirectMedia Layer and is a cross-platform library designed to make it easy to write multi-media software, such as games and emulators. I downloaded the SDL package from the Internet and began the installation process.

I installed the SDL package by using the following command in the following order:

./configure --prefix=${prefix}
make
src/libSDL.la: -lpthread
make install-strip

After the installation was completed I started X11. This means that I started a graphic user interface. I use the term X11 cause it is common to use when it comes to Linux. Now I had to find out the different parameter values. I did this by starting the program xvidtune and wrote down the values of the parameters. Xvidtune contains information about the monitor settings.

Hdisplay - 800
Vdisplay - 600
Htotal - 1376
Pixel Clock - 94,5 * 1000000 equals 94500000
Radio frequency - 15000000
Music file – songs/forelise

I had to multiply the pixel clocks value by 1000000 to get the right value. The radio frequency is up to me to decide but it got to contain 8 digits. Last but not least the music file forelise is the specific music file that comes with the program.

When this was done I ran the following command:

./Tempest_for_eliza 94500000 800 600 1376 15000000 songs/forelise

This command starts the program and as I mentioned earlier it runs in full screen. The monitor looked like this:

It all seemed to work so I turned my simple Philips radio on and tried to fetch the signal on the FM. I did hear a signal between 93.5 FM and 94.0 FM, but the signal was bad and I had to held the radio very close to the monitor. I switched over to AM

and found a very strong and clear signal around 1500 kHz. Note that the radio frequency parameter I set was 15000000.

To test if the signal could be fetch from a longer distance I walked out on my balcony about 15 meters and two rooms away. The signal was still strong and clear. I was able to do this with a regular monitor, a simple radio and a program that I downloaded from the web.

4.3 Lessons learned

There where some lessons that I learned working with this experiment. First of all the installation of Linux Mandrake 9.1 caused me problem. This is not the first time and probably not the last. I found out that this Linux version was not compatible with my old monitor, so had to use my new one.

Another problem occurred when I had extracted the files to the directory Tempest_for_eliza. When I ran the command configure it seemed to work, but that was not the case, cause when I after that ran the command make nothing happened. When this problem came up I had no information on what to do. After several hours searching I finally realized that you need to have the SDL installed on the computer. The SDL library is available on the Internet.

The installation guideline that followed the SDL package was poor so I had to search for more information. Finally, I found a Japanese Web page that gave me the full instructions.

5 SHIELDING FOR INCREASED SECURITY

The only protection against *TEMPEST* attacks is to use some type of metal shielding. The metal shielding is to prevent the signals to fall in the "hands" of an attacker. There are several types of solutions, but the main difference between these are the type of metal that are used.

Sensitive government systems today employ expensive metallic shielding of individual devices, rooms and sometimes entire buildings. Even inside these shielded environments, the "red/black" separation principle is often followed. "Red" equipment carrying confidential data (such as computer terminals) has to be isolated by filters and shields from "black" equipment (such as radio modems) that handles or transmits unclassified data. Equipment with both "red" and "black" connections, such as cipher machines and multilevel secure workstations, requires particularly thorough testing.

For example, the US Government has long required that electronic equipment used for classified processing to be shielded or designed to reduce or eliminate transient emanations to counter this vulnerability. An alternative is to shield the area in which the information is processed to contain electromagnetic emanations, or to specify control of certain distances or zones beyond which the emanations cannot be detected.

TEMPEST computers normally costs double the usual price. These *TEMPEST* computers do not offer full protection against *TEMPEST* attacks. Shielding the area is the only way to accomplish full protection against these types of attacks. This can be expensive using special metal. While some agencies have applied *TEMPEST* standards rigorously, others have used various levels of interpretation in applying the standard. In some cases, a redundant combination of two or three types of multi-layered protection is installed with no thought given either to cost or actual threat.

The fact that *TEMPEST* shielded PCs and peripheral are more expensive than standard models, has the effect that it is practically never used outside the diplomatic and defense communities. The only way to accomplish full protection against *TEMPEST* attacks is to shield the equipment and there are no cheap and simple solutions for common users.

Another way to lower the risk of *TEMPEST* attacks is to simply turn off computers and monitors after business hours. It is common that companies have their computers going 24 hours a day, 7 days a week. This makes it possible for an attacker to make his move without being noticed. This is a cheap way when it comes to security measurements, but is obviously not enough if you want total protection against *TEMPEST* attacks.

6 DISCUSSION

When I started to work on this master thesis my knowledge about electromagnetic emanation was very limited. The first four weeks I had to search and study the information I found on the Internet. There aren't very much public literature on this topic, but there are a few technical papers and web sites on the Internet. When I felt that I had found enough information about the subject, I started with the experiment.

Tempest_for_eliza is a tool that is relatively easy to use and fully functional. The experiment proves that it is possible, and most of all cheap and relatively easy, to bug a computer using the Tempest_for_eliza and a simple radio receiver. In this experiment I have shown that it is possible to listen to the song that the program generates, and this means that the possibility to catch classified and more important information exists. There would be more of a value to us if we for example listened to the bus or CPU activity in the search for passwords and other interesting information.

The signal that the monitor sends out is relatively strong. Like I explain in my experiment, I placed the radio receiver several rooms away and still got a strong signal. The monitor and the radio receiver are the most crucial components when it comes to the range of the signal. The better equipment the stronger signal.

The *TEMPEST* attack could be carried through as follows: The attacker plants a *TEMPEST virus* on the target computer using techniques like the Trojan horse. Then the attacker waits until business hours are over and launches his attack. This can only be possible if the computers are still running. The fact is that many companies leave their computers and monitors running 24 hours, 7 days a week. The attacker then places the radio receiver at a distance where he can pick up the signals, for example on the company's parkinglot. He then launches the program and records the transmission on his radio receiver. The attacker has made the intrusion without any knowledge by the employees or management.

I think that the publishing and availability of tools on the Internet, like Tempest_for_eliza, is good. The different *TEMPEST* techniques aren't mentioned and discussed much in media, but maybe thesis like this will open up the eyes for companies, and in that way the security will be improved. This probably will bring the security thinking on to a higher level when it comes to solutions in *TEMPEST* security techniques

Something that companies should consider is if *TEMPEST* emanation is a security area where they need to do investments. They need to be assure that the confidential and important information is safe in their network. As the problem gets more and more acknowledge, the prices on these solutions will drop. This will make it possible for small business and maybe even home users to purchase this type of protection. There are still a long way to go, but I think that it is a matter of time before this will be a fact.

As I mentioned earlier it is hard to get information on the development in this research area. I haven't studied the security solutions that are known and what effect these solutions has to computers and networks. My proposal for further studying includes to study the different solutions and analyze their advantages and disadvantages. This could then lead to a own proposal of which parts that needs to be considered when developing and using the security techniques.

7 CONCLUSIONS

In this thesis I have proved that it exist a *TEMPEST* technique, that is cheap and relatively simple and still is a security risk. I have proven this with facts from literature studies and an experiment.

Emanation radiation is a problem when it comes to some electronic devices. The computer today is a multimedia machine on which you can look at movies, listen to CDs and so on. This means that the computer gives away *electromagnetic radiation*. This radiation can be transformed into radio waves using a program like Tempest_for_eliza. The fact is that *TEMPEST* techniques and *TEMPEST* security risks is not discussed much in media. Antivirus and firewalls are discussed in every security magazine and are often rated on a scale one to ten. But if a attacker uses a *TEMPEST* technique to launch the attack, these security precautions are not much help.

In the experiment I used a *TEMPEST virus* and a simple radio receiver. I planted the virus in my computer and ran it. The virus uses a algorithm that makes it possible to send radio waves from the computer monitor. To make this possible there are a number of parameters that you have to enter. These parameters are important to get right or else the program doesn't work. There was some lessons that I learned during the experiment, but it is relatively easy to launch this type of attack.

This type of *TEMPEST* technique can be used on a ordinary computer or *LAN*. One thing that came up during my work on this thesis was the vulnerability that *WLAN* has. *WLAN* sends data using radio waves. There has been and are still today discussions regarding the *WLAN* security. A know problem is that *WLAN* gives a way *electromagnetic radiation* in form of radio waves. If you have a laptop and a *WLAN* card you can get access to data on a *WLAN*. The only thing you need to do is to get close enough to the specific *WLAN* to pick up the radio waves. The solution to this problem could be shielding the equipment, but this is rarely common. This can be solved by using a method that encrypts the data. But if we can our hands on the data before it is encrypted we can look at it in plaintext. Using a *TEMPEST* technique to for example listen to the bus or CPU activity we may be able to get classified information like usernames and passwords. This area needs to be investigated more.

There is only one way to protect yourself against these types of attacks and that's shielding. There are not any other way known today that can prevent the radio signals from an attacker. The signal need to be shielded. You can shield a specific equipment or an entire building. This is usually done by expensive metal. But the solutions today are expensive and are only used by agencies and big companies. The regular home user has no resources or knowledge about the problem. Being attacked using a *TEMPEST* technique is not common, but it is still a big security. Using a *TEMPEST* technique an attacker can get access to your information without your knowledge.

8 DICTIONARY

Electromagnetic radiation	Radiation from electronic equipment.
Emanation monitoring	Using a TEMPEST technique to fetch data from a target computer or network.
LAN	Local Area Network. A small network with computers where the computers are connected to each other by cables.
TEMPEST	U.S. government code word that identifies a classified set of standards for limiting electric or electromagnetic radiation emanations from electronic equipment. TEMPEST is an acronym for Transient Electromagnetic Pulse Emanation Standard.
TEMPEST virus	A virus that transforms data into radio waves or another electromagnetic signal.
WLAN	Wireless Local Area Network. A small network where the computers are connected to each other using radio waves and not ordinary cables.

9 REFERENCES

1 Christopher Seline, "Eavesdropping On the Electromagnetic Emanations of Digital Equipment: The Laws of Canada, England and the United States" http://www.eff.org/pub/Privacy/Security/TEMPEST_legal.draft 15 Feb

2 Dale R. Patrick and Stephen W. Fardo, 1995: *Electricity and Electronics.* Prentice-Hall

3 Joe Loughry and David A. Umphress." Information Leakage from Optical Emanations" http://applied-math.org/optical_TEMPEST.pdf 15 Feb 2003

4 Joel McNamara. "The Complete, Unofficial TEMPEST Information Page" http://www.eskimo.com/~joelm/TEMPEST.html 5 Feb 2003.

5 Markus G. Kuhn. "Optical Time-Domain Eavesdropping Risks of CRT Displays" http://www.cl.cam.ac.uk/~mgk25/ieee02-optical.pdf 5 Feb 2003

6 Markus G. Kuhn and Ross J. Anderson. "Soft TEMPEST: Hidden Data Transmission Using Electromagnetic Emanations" http://www.cl.cam.ac.uk/~mgk25/ih98-TEMPEST.pdf 5 Feb 2003

7 Ross Anderson, 2001: *Security Engineering.* WILEY

8 Teo Hong Siang. "Security in wireless LAN" http://security.dso.org.sg/publications/wireless/WLAN_security.pdf 28 April 2003

9 Wim van Eck. "Electromagnetic Radiation from Video Display Units: An Eavesdropping Risk?" http://jya.com/emr.pdf 15 Feb