hakin9 +CD ON CD: *hakin9.live* full of security tools
Adrian Pastor's Book *Windows Insecurity Penetrated*

hakin9 live

hakin9

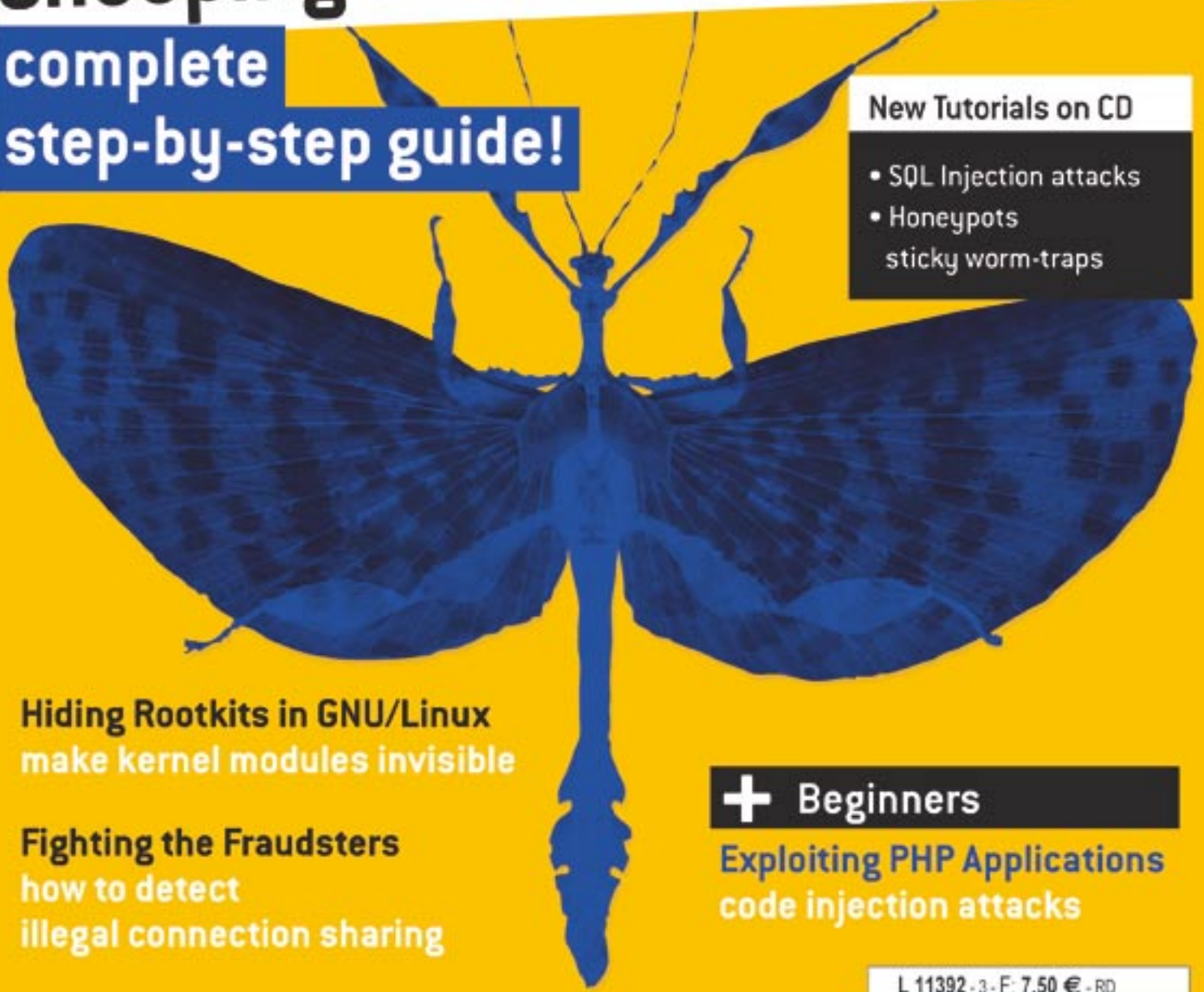
boot • practise • understand
live training center

practical protection

Hard Core IT Security Magazine Issue 3/2005 (3) Price 7,5€ / $9 May/June Bimonthly ISSN 1733-7186

Snooping on Monitor Displays
complete step-by-step guide!

New Tutorials on CD
- SQL Injection attacks
- Honeypots sticky worm-traps



Hiding Rootkits in GNU/Linux
make kernel modules invisible

Fighting the Fraudsters
how to detect illegal connection sharing

Honeypots Versus Worms
Honeyd – bait and cure for malicious code

+ Beginners

Exploiting PHP Applications
code injection attacks

Compromising Emission • Hiding Linux Rootkits • Illegal Connection Sharing • Input Validation Attacks • Honeypots Versus Worms

hakin9 3/2005 (3)

L 11392 - 3 - F: 7,50 € - RD

Europe : 7,50 € CH : 11,50 FS DOM : 7,50 €
TOM : 850 XPF MAR : 60 MAD CAN : 9,95 $CAD A : 7,50 €

TEMPEST – Compromising Emanations

Robin Lobel

TEMPEST, also known as Van Eck Phreaking, is the art of turning involuntary emissions into compromising data. This mainly concerns electromagnetic waves, but it can also be applied to any kind of unwanted emanations induced by the inner workings of a device. The most common TEMPEST phenomena relate to CRT monitors.

The first studies concerning the phenomenon of compromising electromagnetic waves occurred in the 1950s. Through spying on encrypted Russian message transmissions, the NSA discovered weak parasitic rattlings in the carrying tone, which were emanated by the electricity of the encoding machine. By building an appropriate device, it was possible to rebuild the plain text without having to decrypt the transmissions. This phenomenon successively takes the names *NAG1A*, then *FS222* in the 1960s, *NACSIM5100* in the 70s and finally *TEMPEST* (an acronym for *Transient Electromagnetic Pulse Emanation Standard*, although such a name is also said to be untrue), beginning in the 1980s.

In 1985 a Dutch scientist, Wim van Eck, published a report on the experiences that he had had since January 1983 in this field. The report shows that such a system is creatable with little means – however, it gives very little detail. In 1986 and 1988, complementary reports were published. In 1998, John Young – an American citizen – requested the NSA to publish declassified information concerning the *TEMPEST* system. Seeing his request rejected, he ap-

What you will learn...

- you will gain enough knowledge to start building your own *TEMPEST* system.

What you should know...

- you have to have some intermediate experience with practical electronics,
- you should have at least basic knowledge of electromagnetic physics.

About the Author

Robin Lobel has conducted several IT research projects for years, including audio compression, realtime image analysis, realtime 3D engines, etc. He studied the *TEMPEST (Transient Electromagnetic Pulse Emanation Standard)* system thoroughly in 2003 and was lucky enough to be able to use a full laboratory to conduct these experiments and succeed. He also enjoys composing music and doing some 2D/3D artwork. He is currently studying cinema arts in Paris. His web site: *http://www.divideconcept.net*.

Figure 1. *Red, green and blue mix together to synthesise any colour*

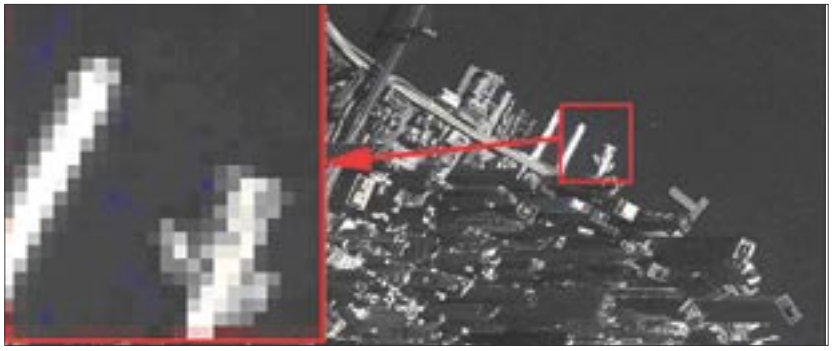


Figure 2. *A grid of pixels form a picture – the sharpness of the picture depends on the pixel's density*

pealed and finally, in 1999, obtained some documents which were largely censored. Very little information is available on this system; the majority of the documents contain nothing but superficial information without giving any details of a practical kind.

So what is it?

The principle of *TEMPEST* and its derivatives is to reconstruct original data from ghost information. A ghost is a trace left by an object in its environment. A definition of a ghost? A footprint, heat, the smell of cooked food and even your own shadow. Such information is valuable to detectives because this is the only basis they have to reconstruct what actually happened. There are three kinds of ghosts in the computer domain which could help us retrieve data: electromagnetic, optical and acoustic.

Electromagnetic emanations

The most discreet and informative trace. Given that every computer uses electricity and that any electric potential induces an electromagnetic field proportional to the potential, we can then deduce back the inner electric activity. This can be applied to CRT display devices and any unprotected cables or wires.

Optical ghosts

Though being an electromagnetic wave, light doesn't have the same rules offering the same possibilities. Contrary to electromagnetic emanations, the lights in a computer system have specific roles, and are intentionally set to inform the user about the system status. If you take a closer look at LEDs, they respond to electric potentials too, so any minimal fluctuations in the system has an effect on LEDs and thus can be perceived with optical sensors. However, this can only be helpful for specific events and in particular conditions. What is more, the acquired information might not be of great value.

Acoustic information

Basically, the same possibilities as with optic emissions. However, the possibilities are less, because most of a computer system is silent and only the mechanical parts are subject to acoustic production. There are quite a few applications for this kind of emission. A hardware keylogger based on acoustic events may be a good example.

A particular study: CRT monitor emanations

One of the most interesting emissions in a computer comes from the display device, because its inner activity clearly deals with important information. Moreover, this device emits strong electromagnetic waves that are relatively easy to capture and treat.

The way monitors work

All colours can be broken down into three fundamental colours: red, green and blue (see Figure 1). It is possible – through the combination of these three colours – to recreate any colour, by varying these fundamental proportions. An image is considered a complex assembly of colours through the use of a pattern of pixels (see Figure 2). A pixel is a point composed of the three colours: red, green and blue. It is possible to recreate accurate images by increasing the density of pixels in a single area. The resolution of an image is represented by x*y, with x being the number of pix-

On the Net

- *http://upe.acm.jhu.edu/websites/Jon_Grover/page2.htm* – a handful of basics on *van Eck phreaking*,
- *http://www.eskimo.com/~joelm/tempest.html* – the complete but unofficial *TEMPEST* information page,
- *http://www.noradcorp.com/2tutor.htm* – NoRad company's CRT Monitors as a Source of Electromagnetic Waves page,
- *http://xtronics.com/kits/rcode.htm* – resistor colour codes,
- *http://web.telia.com/~u85920178/begin/opamp00.htm* – operational amplifier explanation,
- *http://www.hut.fi/Misc/Electronics/circuits/vga2tv/vga2palntsc.html* – Tomi Engdahl's synchronisation signal converter.

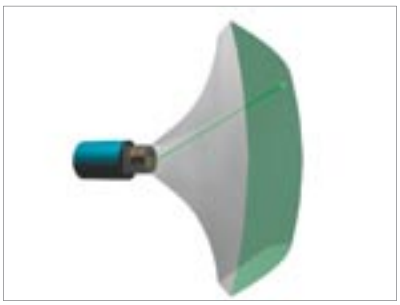


Figure 3. *A beam of electrons produce the actual picture on the screen, by exciting a phosphorescent layer from left to right and top to bottom*

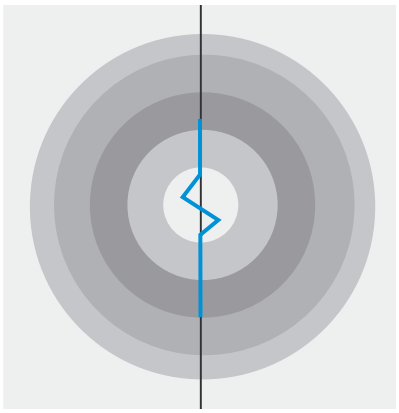


Figure 4. *A difference of potential in a conductive cable generates an electromagnetic wave*

els horizontally and y the number of pixels vertically (examples: 640*480, 800*600, 1024*768, etc.)

A monitor screen is composed of several modules. The first one, the cathode tube, is what reproduces the actual image. An electron beam scans a fluorescent layer at an extremely high speed thereby creating the image. The scanning goes across the entire screen from left to right and from top to bottom at a frequency of 50–100 Hz; as the electrons pass through the fluorescent layer, it emits a light. This layer also becomes phosphorescent in that it continues to emit a light after its initial stimulation for approximately 10 to 20 ms. Its brightness is determined by the debit of electrons, which is regulated by a *Wehnelt* (electronic component). The beam then passes through two bobbins (one to determine the vertical deviation, the other for the horizontal deviation, using electromagnetic forces) to direct its trajectory, so that it scans the whole screen and can reconstruct a complete picture (see Figure 3).

The video signal passes through several channels (6 channels for the video signal itself). Meaning, the Red, Green and Blue channels as well as their respective masses; 2 synchronisation channels for the horizontal and vertical scanning and the communal mass of synchronisation signals.

The synchronisation signals, which indicate the passage to the following line or the return of the beam to the beginning of the screen, are simple differences of potentials of a few volts. They take place (for a screen of a resolution of 800*600 pixels with 70 Hz refresh) 70 times a second for the vertical synchronisation signals, and 600*70=42,000 times a second for the horizontal synchronisation signals.

Video signals are at a voltage of 0 V to 0.7 V, which defines the brightness (the higher the voltage, the brighter the pixel) at the point where the scanning takes place (this voltage is thus able to vary for each new pixel of a different colour; for a screen having a resolution of 800*600 with a refresh rate of 70 Hz, the changes of voltage can reach a frequency of 800*600*70=34 MHz, that is to say 34,000,000 times a second).

Inductance phenomena

Any difference of potential (that is, when an amount of electrical tension gets higher or lower) in an electrically conductive material produces an electromagnetic wave proportional to the potential: this is called *inductance phenomena* (see Figure 4). This process involves Maxwell equations, which describe electromagnetic waves' behaviour. However, it's not necessary to understand all the mathematical and physical rules behind this in order to exploit the phenomena.

The invert phenomena is also true: any electromagnetic wave meeting an electrically conductive material will produce a difference of potential proportional to the strength of the wave. This is basically how LW radio receptors works: the stronger the wave, the stronger the signal received.

For an electromagnetic field to be created, there must be differences of potentials: a constant voltage won't produce any radio waves. In the same way, no signal can be received if the magnetic field is static (that's why dynamos need to be constantly in motion to produce electricity).

Application to CRT monitors

Before being projected in the form of an electron beam, the video signal is amplified to a high voltage. This amplification generates strong

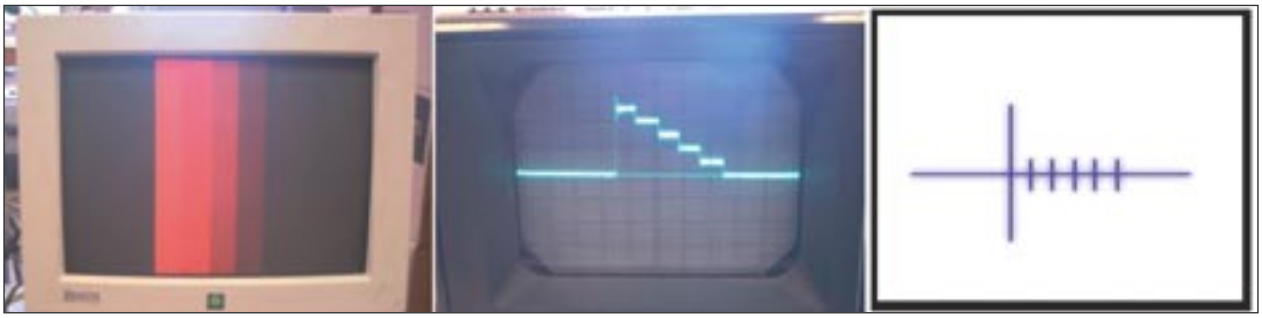


Figure 5. *Example screen and its corresponding electrical coding and electromagnetic inducement*

Figure 6. *A model of a parabolic antenna*

electromagnetic waves, which, if the monitor is not protected enough electromagnetically, can be captured without any physical contact using an antenna from up to a distance of a hundred metres. The strength of the wave is proportional to the contrast between two consecutive pixels. Of course, as the three colour components are treated simultaneously and only one global electromagnetic wave is emitted (to be more specific, electromagnetic waves mix into one when being emitted), we cannot separate retrieving colour information.

Setting up a TEMPEST system

An example screen and its corresponding electrical coding and electromagnetic inducement can be found in Figure 5. On the left, one can see a gradient scale displayed on a monitor screen. The central picture shows the same video signal as analysed by an oscilloscope. Finally, the right picture shows the corresponding electrical emanations (proportional to the differences of potentials). A vertical pattern has been used for clarity (all lines are coded in the same way). This pattern is meant to make us understand what kind of signal we're about to handle. Now, let's start the practical part of our detective game.

The antenna

An antenna can be a simple conductive cable; this will be enough if we want to experiment with the system just two or three metres away from the monitor. For larger distances, one should use a parabolic antenna (Figure 6), which should be pointed towards the display device; it's highly sensitive and directional; that is, it can capture even very low emissions from a specific point in space.

The antenna will capture a highly parasitised signal. This noise is due to the electromagnetic pollution of the environment (miscellaneous radio emissions). Fortunately, monitors emit in a restricted band of high frequencies, which permits us to recover the signal using a filter.

Filtering

To recover the signal, we need to filter all frequencies inferior to the frequency of a single pixel (this also eliminates the wave generated by the synchronisation signal, which makes it hard to recover the beginning of a line). Actually, to acquire better results, it's a good idea to leave a margin and set the filtering frequency slightly inferior to the frequency of a single pixel.

For a screen of resolution 800*600 with a refresh rate of 70 Hz, the critical frequency would be 800*600*70=33.6 MHz.

A high pass filter is composed of a resistor and a capacitor, assembled as in Figure 7:

- *C1* – the capacitor,
- *R1* – the resistor,
- *Ue, Us* – input and output respectively,
- *Y1* stands for the resulting signal.

The critical frequency of this system is determined by $fc=1/(2*\pi*R*C)$, with *fc* for critical frequency (frequency below which the filter will cut any signal), *R* for the resistance's value and *C* for the capacitor's value.

We could set the system to, let's say, a frequency of 1.6 MHz (so that all frequencies inferior to 1.6 MHz are eliminated), which leads us to $1.6*10^6=1/(2*\pi*R*C)$. This results in $R*C=1/(2*\pi*1.6*10^6)=10^{-7}$.

This frequency has been chosen because it left a good margin, and capacitors and resistors for this frequency are easy to find. To achieve this product, we could choose a capacitor of 1 nF (1 nano Farad, which is equivalent to 10^{-9} Farad) and a resistor of 100 Ω (100 Ohms).

This leads us to $10^{-9}*10^2=10^{-7}$, so we got our product, and the system is set to a critical frequency of 1.6 MHz. Of course, you can use any other combination of resistors and capacitors – the main thing is to keep the product constant.

Amplification

The filtered signal has a very low potential (a few mV). In order to exploit the signal, we have to amplify it (that is multiplying the voltage by a constant factor) to an acceptable level. As seen before, video signals are comprised between 0 V and 0.7 V. To achieve this, we'll use an *operational amplifier* (OA, see also Frame *On the Web*), which is an electronic component that can be bought for around 10 Euros. Since we're treating high frequencies (MHz), we should carefully choose this operational amplifier: common OAs cannot handle such frequencies. So, when at the shop, one should ask for a *video operational amplifier*. Model AD844AN is an example but, however, it may not be available in every country. We should look in the catalogues of different electronic manufacturers.

An OA has many applications, but we just want it to amplify our signal for now. To do so, let's refer to the circuit shown in Figure 8. It is comprised of an OA and 2 resistors:

- *R2*, *R3* – resistors,
- *OA* – operational amplifier,
- *V+*, *V-* – OA powering,
- *Ue*, *Us* – input and output,
- *Y1* – resulting signal.

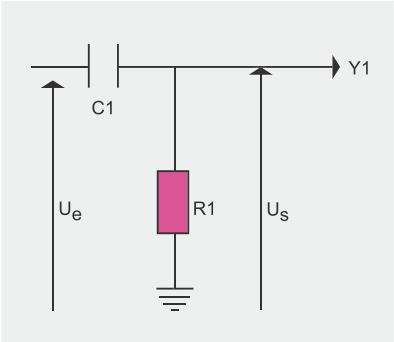


Figure 7. *A High Pass Filter scheme*

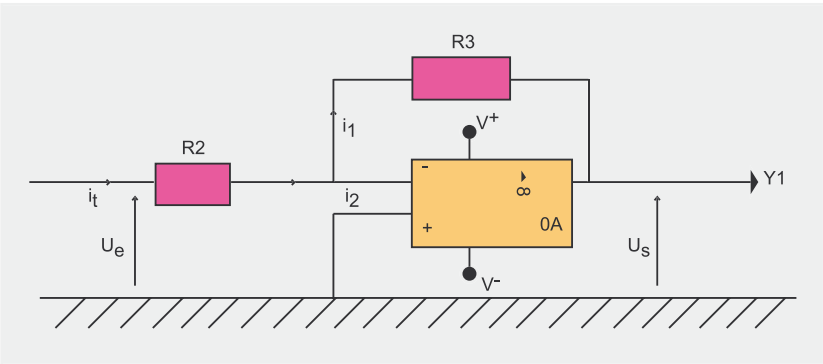


Figure 8. *Operational Amplifier: an inverter assembly*

It is called an *inverter* and is one of the simplest amplifier circuits to build (but see also the Frame *Things to Remember When Amplifying the Signal*). The value of the two resistors will determine the amplification coefficient by using the following formula: $k = -R3/R2$. To amplify a hundred times, we can, for example, choose R2=1 Ω and R3=100 Ω.

Cutting negative components

This is the easiest part: it just consists of adding a diode in order to cut the negative potential of our signal (because your display device will have some difficulties reproducing negative colours). The scheme is shown in Figure 9.

Restoring the display

There are two more things to get the system working – solving these problems depends on the hardware used. The final step includes synchronisation signals and the display device we should use.

Synchronisation signals

These signals can be generated using frequency generators. The main thing is to generate a pulse of a few volts for vertical synchronisation (all screens), and another for horizontal synchronisation (all lines). That is, for a screen of resolution 800*600 with a refresh rate of 70 Hz, 70 impulses per second should be generated for the first channel, and 600*70=42,000 impulses per second should be generated for the second channel.

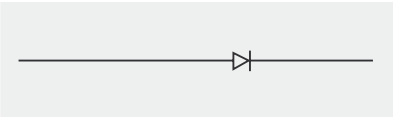


Figure 9. *A diode, as represented in electronic circuits*

If we don't have any frequency generators, then we can use a simple trick: deriving synchronisation channels from the video-out port of a computer (see Figure 10). One only has to set this computer to the desired resolution and the refresh rate as before (in our example, one would set it to 800*600, 70 Hz). To connect the test screen to this video-out port, we can hack an old video cable or buy a SUB-D 15/HD 15 connector (also known as a *VGA 15-pin connector*).

Let's take a look at the picture and corresponding signals:

- *1* – red,
- *2* – green,
- *3* – blue,
- *6* – red mass,
- *7* – green mass,
- *8* – blue mass,
- *11* – mass,
- *13* – horizontal sync,
- *14* – vertical sync.

Remember: we should be very vigilant while working on the video-out port. Any errors could be fatal to the video card.

Display device

For displaying the compromised data we can use either a TV or a computer screen, although a computer screen is preferred. Television devices just won't support all resolutions, where-as computers will (to certain extents, of course).

For computer screen connectivity, this refers to the scheme of the SUB-D HD connector (Figure 10). For TV screens, this refers to the scheme for connectivity (SCART) as shown in Figure 11:

- *5* – blue mass,
- *7* – blue,
- *9* – green mass,
- *11* – green,
- *13* – red mass,
- *15* – red.

However, converting synchronisation signals is pretty difficult. Fortunately, in 1996, Tomi Engdahl designed a circuit which converts the VGA standard to TV standards. His concept is reproduced here in Figure 12.

As can be seen, it's slightly easier if we have a computer screen. But we must remember to still be vigilant! These machines are extremely sensitive. Also, having an oscilloscope to control while manipulating is a plus.

That's almost all (see Frame *Assembling the System* for details on construction).

Things to Remember When Amplifying the Signal

We should bear a few things in mind. At first, it is a good idea to choose a variable resistor R3, so that we can choose the coefficient even when the circuit is assembled. What's more important, the OA needs to be powered! This is something to look carefully at when choosing an OA, as they don't have the same needs in terms of power. Generally, it's around 12 V or 15 V. One also has to be sure to know how to connect an OA before assembly. Different documents are available on the Internet on this subject (see Frame *On the Net*). And last, but not least, this circuit is called an *inverter* because it inverts the output (that's why *k* is negative). With electromagnetic waves this is not a problem, since each signal possesses a negative and a positive part.

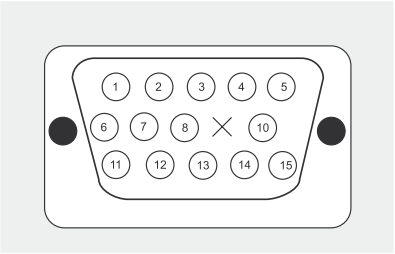


Figure 10. *SUB-D HD Connector*

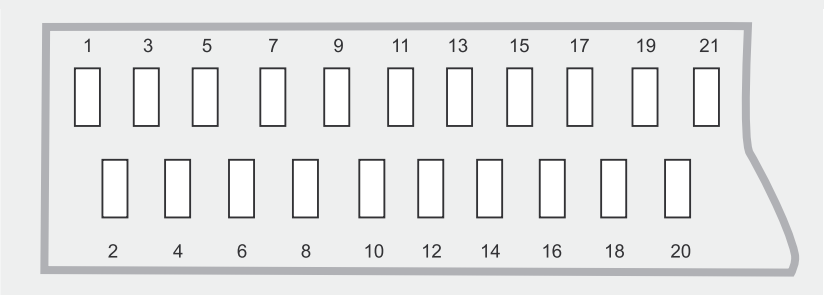


Figure 11. *SCART – Peritel connectivity scheme*

To summarize, the whole home-brew *TEMPEST* system can be seen in Figure 14. To make it clearer:

- A – antenna,
- C1 – capacitor,
- R1,R2,R3 – resistors,
- OA – operational amplifier,
- V+/V- – OA powering,
- 1,2,3 – colours channels,
- 4,5 – synchronisation channels,
- Sync – synchronisation impulses generators.

Well, but does it work?

We have learned how to build a *TEMPEST* system – one should be able to start constructing one's own EM waves intercepting device. However, let's not expect it

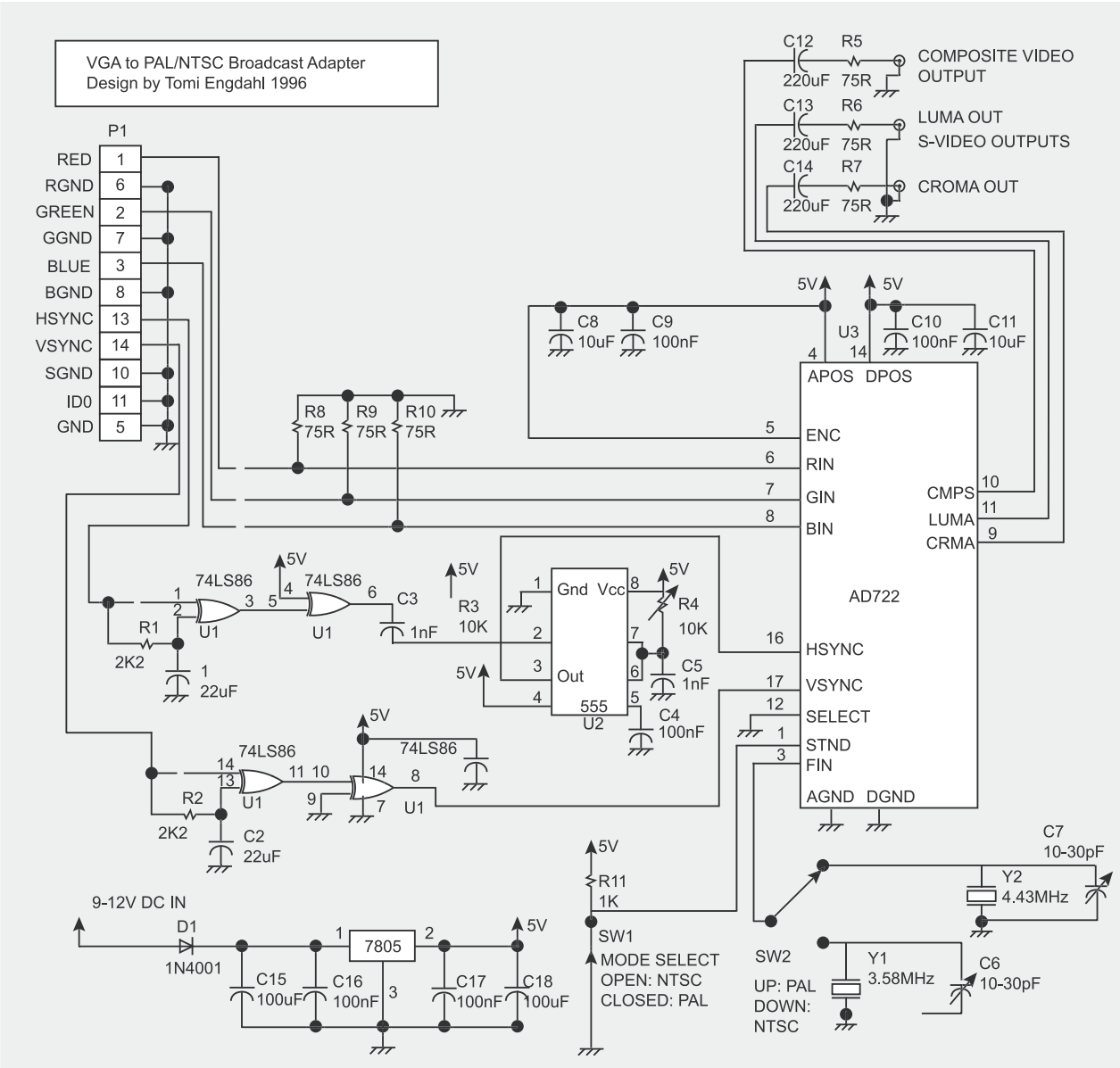


Figure 12. *Tomi Engdahl's synchronisation convertor circuit*

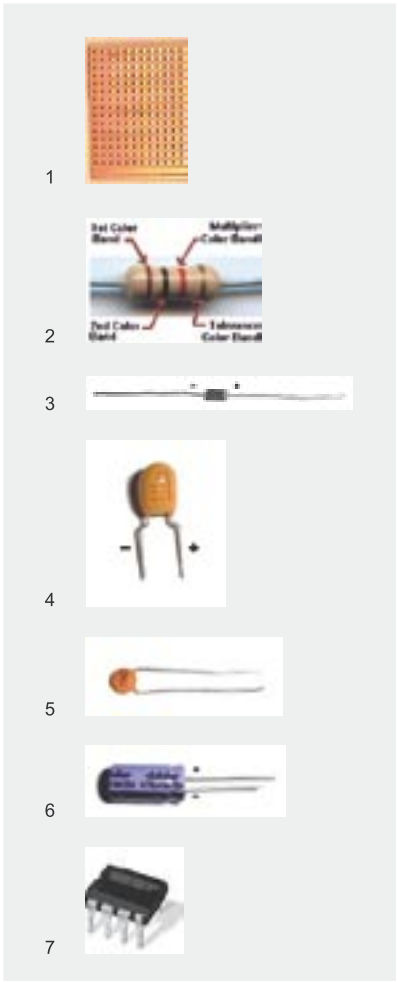


Figure 13. *Parts used in TEMPEST circuit assembly: 1 – a veroboard; 2 – a resistor; 3 – a diode; 4, 5, 6 – capacitors; 7 – operational amplifier*

to work the first time when we test it. This is a very delicate system that needs to be finely tuned in order to function properly; it would be very useful to have an oscilloscope during the tests. Also, this is highly dependant on the environment and the way you use it. CRT monitors' electromagnetic emanations vary from one screen to another, so even with a tuned system results will vary too. Our solution results in a really home-brew device – relatively cheap and rather simplistic. Factory made *TEMPEST* systems are very expensive and really difficult to purchase, not to mention the fact that this kind of information was classified for a long time. ■

Assembling the System

Our electronic circuit is composed of 4 stages (see also Figure 14):

- an antenna (A) which will receive the signal,
- a high pass filter (C1,R1) to cut frequencies below the critical frequency we defined,
- an amplifier (OA,R2,R3,V+/V-) that amplifies the filtered signal so that it can be seen on a standard CRT display,
- a diode to cut negative parts (that cannot be used by a standard screen) and finally output to get the video signal on the screen.

In parallel, there are incoming synchronisation signals. They can be generated by two low frequency generators or directly from a video card.

To get the output onto a standard TV screen, Tomi Engdahl's synchronisation signal converter circuit can be used. It is shown in Figure 12. Since we don't really need this device, an optional description is available at *http://www.hut.fi/Misc/Electronics/circuits/vga2tv/vga2palntsc.html*.

The Components

Practically, you can use a veroboard (Figure 13; 1) to build the circuit. It is a board with a grid of holes linked by copper tracks on every row; that way you don't need to build your own printed circuit – it's all ready-made. This kind of board is available in any electronic shop.

A resistor and a diode are shown in Figure 13 (2, 3 respectively). As for capacitors, there are several kinds available, but one shouldn't worry – they all work the same way (Figure 13; 4, 5, 6). Finally, the operational amplifier (Figure 13; 7) is necessary – right now we don't need to explain any further about it, but you can refer to Harry Lythall's webpage for details (*http://web.telia.com/~u85920178/begin/opamp00.htm*). All these components are available for a few Euros each.

The Assembly

To assemble the whole circuit, you'll need a soldering iron (even a cheap one will be okay) and a tin of lead wire to solder the electronic components to the veroboard.

Insert each electronic component from the back of the veroboard (that is, the side with no copper tracks) so that the pins appear on the other side. Then, apply the tin on the copper track with the soldering iron – a drop of tin should weld the pin to the copper track.

Use the copper tracks as you feel, the main thing is to respect the connections as shown on the TEMPEST's circuit scheme (Figure 14). You can link two copper tracks by welding a short electric cable from one copper track to another.

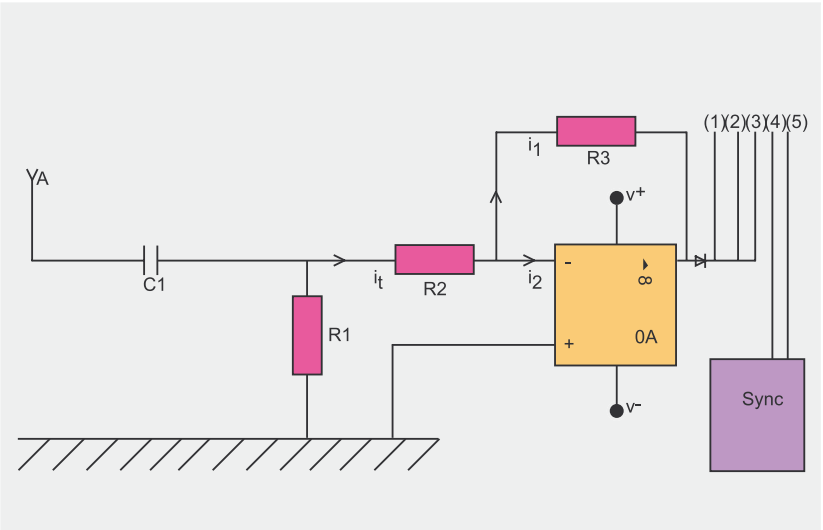


Figure 14. *Robin Lobel's TEMPEST system*