Several compromising-emanations based interception techniques and their implications

Paul Shotbolt, June 2003

psho010@ec.auckland.ac.nz

Abstract

Security models of computer systems have traditionally had little focus on some of the more unusual outputs associated with electronic equipment, such as electromagnetic emanations, and physical vibrations. In many cases these emanations may be detected and analysed and important data intercepted by a motivated attacker; yet only high-level government agencies and large corporations appear to be actively considering this problem.

Historically, for a typical computer user with only moderately important data, these 'compromising emanations' appear to have been little problem. Government and industry entities are at a greater risk, and a small proportion have become aware of these threats and taken steps to neutralise them. However, the field of emission security (EMSEC) is growing and new types of attacks are being suggested, and the feasibility of mounting these attacks is changing also. If the cost to facilitate these attacks drops in future, they present a far more pressing threat, and this may necessitate the introduction of countermeasures even for low- to mid-end security systems.

Introduction

We live in an era where large numbers of people have become increasingly dependent on computers for myriad tasks, and consequently computers are being entrusted with increasing amounts of confidential data[1]. With the trends in recent years of powerful encryption [Pgp03] becoming more readily available to the public, attackers attempting to intercept this data are forced to explore new side-attacks[2] because of the infeasibility of succeeding in a conventional attack against these ciphers.

[1] Sebastiani [Seb98] makes this observation in his conclusions in his paper on TEMPEST. While it does not seem to relate greatly to the rest of his paper, it is, nonetheless, a valid point.

[2] Schneier uses the term to describe unconventional attacks which bypass traditional security measures. In the June-15 '98 issue of Crypto-gram he suggests that "TEMPEST is another side channel that can be very effective [in cryptanalysis]".

Some of the more interesting types of side-attacks are based on the detection and analysis of 'Compromising Emanations' (CE). Emanations are considered compromising if they are not an expected avenue for distributing information and are, according to Loughry [LU02], "…intelligence bearing signals that, if intercepted and analysed, disclose the information transmi[tted], received, handled or otherwise processed by any information processing equipment[3]". In these CE attacks, a device outputs some form of emanation (e.g. light emitted) which intentionally or unintentionally carries information correlating to the data in that device. A properly equipped attacker may be capable of receiving the emanation and reconstructing the data in question, violating the privacy of the legitimate owners of that data.

Here, several types of emanation-interception based attacks are compared and discussed, and their implications for current security systems, from low to high-end[4], are examined. Finally, some possible future directions for emission security (EMSEC) are discussed. During this report I hope to investigate the current and future implications of these little-known threats for interested parties, from an average citizen to a company dealing with highly confidential data. I also wish to observe the varying scope of these threats and their relative difficulty of implementation.

Emission Security Model

To begin with, I would like to develop a model within which various types of compromising emission may be described. There are inherently many different emissions from any electronic or computer system, and each must be examined to ensure that it is not broadcasting compromising data. Loughry, in his paper [LU02] "Information Leakage from Optical Emanations" introduces a new taxonomy for classifying how compromising an optical signal is, however there appears no reason that this model should apply only to optical emissions, and it is useful in describing compromising signals in general.

His classes are as follows:

[3] The article 'unintentional' was removed from this definition, as strictly speaking, light output by CRT phosphors is generally intended, yet interception of this signal is considered a compromising emanation-based attack. However without this word, Loughry's definition becomes overly general and requires revision.

[4] In this paper, 'high-end' security system refers to systems implemented by governments, corporations and large firms dealing with highly confidential and desirable data. The terms 'low-level' and 'mid-level' refer to the systems protecting a citizen's personal computer at home or average small firm, respectively, where the interception of the data is likely to provide only moderate benefits.

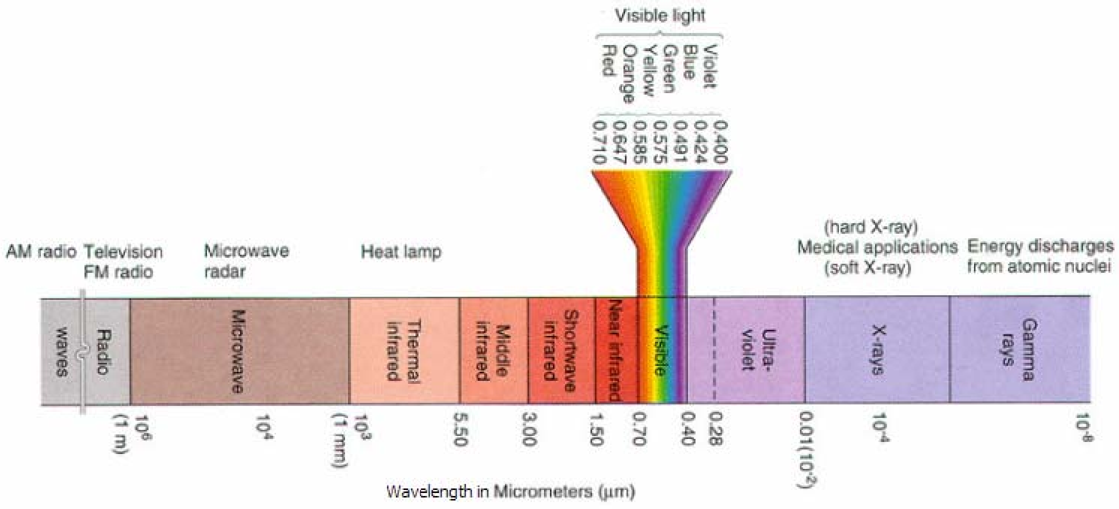
Class I: The compromising signal relates only to the 'state' of the device, Loughry uses the example of a 'power-on' LED on a computer.

Class II: The compromising signal relates to the 'activity-level' of the device, for example, noise from hard-disk-access on a PC. Loughry correctly notes that this allows a *traffic-analysis* attack to be performed.

Class III: The compromising signal is correlated with the data being processed or transmitted by the device. An example might be an LED-tuple which displays each input byte as it is sent through a programmable logic device (PLD). Here the '*content'* of the information in the device is available for interception. This is evidently the most dangerous class, and has subsequently been investigated further than the others.

Additional to this measure of the danger of the signal is the nature of the emission.
I propose that outputs from any given physical system are either physical, electronic, acoustic, thermal, or electromagnetic (EM). Electronic (e.g. network packets) and physical outputs (eg a disk, or printed material) are already considered in most current computer security models. The papers that I examine here are concerned primarily with types of electromagnetic emission (as shown in Fig. 1.) including optical and radio-frequency (RF, also known as TEMPEST[5]) emissions. However, it is apparent that other EM waves have a role to play in computer security, such as an attack described by Kuhn [Kuh98] in which "an attacker who knows the resonant frequency of (say) a PCs keyboard cable can irradiate it with this frequency and then detect keypress codes in the retransmitted signal thanks to the impedance changes they cause". Also, I see no reason why acoustic and thermal emissions should be partially or completely ignored; it is evident that the sound of a photocopier or heat from a facsimile machine could both be considered Class II emissions. Class III background noise in military radio/audio communications could conceivably give information as to the whereabouts of the source.
Lastly, there is the concept of scope; not necessarily all data handled by a system is contained in the compromising emanations. It is therefore important to identify what types of data are at risk with respect to each kind of attack.

[5] TEMPEST is the unclassified military codeword for a program to develop countermeasures to compromising-emanations based attacks [McN03]. Since its declassification, it has been increasingly misused to describe the attacks themselves.



source: Christopherson (2000) *Geosystems*

Fig. 1: The Electromagnetic spectrum, showing classifications of EM waves, some of which may be intercepted in a compromising-emanations based attack.

Physical Intrusion and Projective observation

Observing Class III emanations from a computer monitor by looking directly over someone's shoulder while they view confidential data is certainly nothing new. The practice is likely the most common of those techniques discussed in this paper because of its cheapness and effectiveness.

Historically, it has usually been deterred by placing some physical boundary immediately around the system in question, and preventing access by unauthorized personnel. The attack itself has a limited scope, in that only information present on screen while the attacker is within line-of-sight is vulnerable to interception. A video recording device such as a VCR may greatly expand the scope of this type of attack.

In practice, most security systems, from low-end to high-end appear to have been vigilant about defending against this kind of interception[6]. In a recent paper, [Kuh02], Kuhn briefly examines the underlying physics behind projective observation using a telescope, and concludes that with commonly available telescopes, information can be read off computer screens at a distance of up to 60 meters with standard telescope apertures of less than 60°. This telescopic version of the attack may not have been quite so effectively

[6] A quick Internet search reveals that the practice of facing computers away from windows and doors is explicitly described in several dozen security policies, including some from government agencies (USAID) and some from private corporations.

combated, but common sense would dictate that most security professionals would have considered and neutralised the well known threat of line-of-sight interception.

Optical attack (Kuhn, 2002)

In a paper in 2002 [Kuh02], Kuhn describes a new class of optical attack, where Class III optical EM emanations from CRT monitors are captured and the resulting image can be reconstructed at up to 50m distance. Interestingly, even ‘diffuse reflection from a wall’ from a CRT display in a low-lit room is still able to be recovered at significant distance, which raises implications for the common ‘air-conditioned glass house’ approach to computer placement [LU02].

Kuhn notes during the paper that the equipment is somewhat easier to acquire compared with the RF-monitoring tools needed for van Eck interception today.

This optical attack involves using a high-speed photo-sensor to receive information about the average light-intensity of an area around the CRT monitor being attack. Using periodic averaging and a form of deconvolution (with an filter depicting the inverse of the phosphor-decay) Kuhn was able to reconstruct the data being displayed. The scope of Kuhn’s optical attack is limited by many of the same constraints as projective observation, in that only information that is displayed on-screen may be intercepted. This attack has immediate implications for the high-end security systems of governments and corporations, as their existing security systems and policies might not cater against this new type of threat. As for medium and low-end security systems and their users, Bruce Schneier [Sch02] offered a pragmatic angle on Kuhn’s optical attack:

> *“Several reporters have asked me how big a deal I thought [Kuhn’s optical attack] is. Short answer: not very.*
> *I have no way of defending myself against attackers this well motivated and this well funded. They can already park a van outside my house and eavesdrop [through Van Eck phreaking or otherwise] on my computer. They can already break into my house when I'm away and install dozens of listening devices … now they have another way they can eavesdrop on me. I still can't do anything about any of them. At least, not without spending a WHOLE lot of money.”*

Van Eck Phreaking (~1960s)

In December 1985, Dutch researcher van Eck brought a type of emission-based attack into public attention. His paper, [vEc85] and subsequent appearance on a BBC documentary [Hig88] in which he collected information from a van parked outside New Scotland Yard, received a large amount of media attention. The attack he described related to capturing Class III radio-frequency (RF) based EM-emanations from video display units (VDUs), and reconstructing the video signal via externally generating and mimicking the video-synchronization signal. The scope of this kind of attack is again limited by what information is displayed by the user. It is worth noting that in practice, all confidential data must be received by some party at some point for consumption, and in most cases this is consumption is visual, and therefore the data could be a candidate for being sent to a VDU.

The ease at which van Eck's attack appeared to have been mounted, and the relatively small price of only several hundred dollars [vEc85] of his interception equipment initially gave rise to fears that thousands of enthusiasts would soon be building their own interception equipment [Hig88]. Thankfully, this possible scenario never materialized, and Kuhn notes [Kuh02-2] that as there have still been no recorded cases of criminal convictions for this type of attack,[7] either these attacks are not occurring, or are conducted so well that no perpetrator has ever been caught.

Due to developments in the nature of colour-CRT monitors, the price of mounting this kind of attack appears to have climbed considerably: Kuhn describes the Hewlett Packard Signals Analysis System, costing around $100 000 US [Kuh99], which is enormous compared with van Eck's original $200 US [vEc85]. This huge cost appears to have been sufficient to deter these attacks in most situations. However, it is still a possible threat, and proprietors of highly confidential data, such as the US military or corporations dealing with particularly sensitive material still must take precautions against these attacks. Indeed, many sources, including Joel McNamara [McN03], indicate that the military was aware of compromising emanations decades before van Eck's paper. McNamara also notes that in the US, over $1 billion dollars is spent per year on TEMPEST security, which includes countermeasures against van Eck phreaking. While there is little available information on the identities of the purchasers of this equipment,

[7] McNamara notes that an Israeli citizen, Shalom Shaphyr, was arrested mid-1999 for illegally attempting to export van Eck monitoring equipment from the U.S. The agreed price for the equipment was $30 000 USD. However, his conviction was for attempting to (illegally) acquire the equipment, rather than for conducting an attack as such.

CE countermeasures only appear to be implemented by a minority of large corporations. On the private level, Schneier's quote (above) on Kuhn's optical attack indicates that due to the costs and difficulty of implementation, the average user does not and cannot [at this point] consider implementing any countermeasures this type of attack.

RS-232 Cables (Smulders 1990)

A paper by Peter Smulders in 1990 described another form of attack in which the Class III RF-electromagnetic signal generated by RS-232 serial cables may be intercepted with only household equipment (including an AM/FM capable walkman) from ranges of around 7 meters. The lack of open literature on compromising emanations [You03] means that it is difficult to surmise how much additional range could be achieved if Smulder's experiments were repeated with higher quality, more specialised equipment. Smulders also carefully notes that, by nature, more confidential data (e.g. a password) is sent down RS-232 cables than is displayed openly on VDUs, making the scope of this attack significantly larger than van Eck phreaking. The costs to mount this kind of attack are almost completely insignificant, and additionally, relatively small expertise is needed to recover the data (compared with van Eck phreaking). The implications of this attack are evident for high-end security systems for governments, and corporations such as banks. One source notes that these cables are often used inside ATM machines and carry bank-card details and PIN numbers in plaintext form [Kuh98]. Because of the low cost of this kind of attack, this has implications for low to mid-end security systems also. Smulders notes that it is feasible to monitor a neighboring firm's modem connections from an adjacent building. Additionally, other sources [Mol88] have noted that 'shell waves' on cables, and similar currents on other surfaces responsive to induction from those cables may also create a form of compromising emanation. Moller notes that these 'shell waves' often allow higher quality signals to reconstructed than standard RF emanations.

Generalized EM- phreaking (~1960s)

Van Eck's and Smulder's eavesdropping techniques focused entirely on RF emanation from VDUs and cables, however the attack can be generalised. Listening to RF emissions of any component in the computer system may be possible (although some signals carry no useful information, and some are infeasible to recover). Periodic signals, such as the EM emanation from screen-buffer output are the traditional targets of this type of attack, however, it is interesting that the NSA website on TEMPEST (EMSEC) endorsed-products[8] [NSA03] lists such diverse components as disk-drives, computers, scanners, printers, cabinets, routers and hubs. This implies that these types of components are at risk from, or associated with, compromising emanations of some form. Indeed, Kuhn briefly discusses keyboards, disk drives and DRAM refreshing as potential attack avenues [Kuh98]. Open literature regarding standard van Eck phreaking is difficult to find; the many government restrictions, mentioned by H.J. Highland, [Hig88-2] make it difficult to find any specific information on reading data from screen buffers or many other non-VDU components. It is generally agreed that, in practice, of the compromising emanations from a computer system, the amplified video signal is by far the easiest to recover (as it is at 'several hundred volts' compared to normal TTL voltages) [vEc85]. Because of this, only entities that would consider van Eck phreaking to be a real threat should consider countermeasures to this more general form of the attack. The costs to implement generalised EM phreaking will mirror the increases in difficulty from standard van Eck phreaking[9]. High-end security systems should include this type of attack in their threat model, whereas at this stage, an average citizen is unlikely to be the target for this type of attack.

However, Kuhn mentions [Kuh98] that over the next few years, 'software-radio' equipment is likely to be available for PCs. This gives the ability to anyone with such a device to replicate a RF monitor using appropriate software. With organisations such as the 'Cult of the Dead Cow' offering tutorials such as "The Tao of Buffer Overflow," [Cdc03] it seems likely that the software for performing RF-interception techniques, (van Eck or otherwise) will be quickly produced by the hacker community after these devices are released.

LED-based Optical attack (Loughry)

In 2002, J. Loughry and D. Umphress described a series of experiments examining common devices (such as routers, modems, and hardware encryption devices) for Class

[8] These NSA-endorsed products are officially designated as being of TEMPEST standard, indicating that they are sufficiently safe from compromising-emanations based attacks. Interestingly these products are generally around double the price of similar non-TEMPEST equipment.

[9] Detecting emanations from TTL Logic is more difficult in part due to the lower voltages involved, and in general, these signals are non-periodic, which prevents the attacker using periodic averaging to improve their results. To achieve the same quality data, more specialised, higher quality equipment would be needed.

III emanations from Light emitting diodes, or LEDs [LU02]. The results were surprising in that 38% of the devices tested broadcast Class III optical signals, and some or all of the information passing through these devices could be gleaned from observation. The cost to implement this type of attack appears to be moderately small, and additionally Loughry notes: "It requires little apparatus, can be done at considerable distance, and is completely undetectable." A fast photosensor, the skill to write an analysis tool and enough motivation appear to be all that is required to mount the attack. Obviously this LED based attack does not apply to all security systems, but the authors' results would seem to indicate a significant portion of current systems might be vulnerable to this attack. Considering the wide variety of devices that Loughry examined and the wide variety of data being handled by these devices, the scope of this attack appears to be quite large. Fortunately low and mid-end security systems are less likely to include components that employ many LEDs, so the probability of this attack affecting an average citizen's PC at home is minimal.

Larger corporations and governments will have to take note of this risk; however it is still too soon to make observations about how the security industry is responding to Loughry's research.

Auxiliary Tools

Two papers [LU02 and Kuh98] describe auxiliary software that can be used to alongside CE-attacks. Loughry's LED altering program (inspired by the behaviour of a character in a critically acclaimed novel [Ste99]) broadcasts information to an attacker through the manipulating the Caps-Lock, Scroll-Lock and Num-Lock LEDs. Kuhn and Anderson describe a program that enters the system as either a virus or Trojan horse, searches the system for confidential information, and then broadcasts it to the waiting attacker using a special dithering technique which makes van Eck interception significantly easier. They also suggest alternative broadcasting using only the VDU cable as an alternative antenna. Tools such as these effectively broaden the scope of any type of emanation based attack, exposing any and all data available to the Trojan process to interception by the attacker. The increase in scope that these tools bring to an attack can make these respective interception techniques far more dangerous when they occur. Fortunately, there seem to be few scenarios where it is feasible to place one of these tools on a system without the possibility of using a traditional network back-door approach to perform the interception, so attacks using these auxiliary tools have limited application in the real world.

Some comparisons and trends

The interception methods discussed have several major similarities.

An expected trend is that the proficiency and financial cost associated with each kind of attack would be the largest factors in determining how probable the attack is; yet despite there being a number of feasible attacks, there have been no recorded instances in open literature. A possibility is that at present, there is little market for an interception device that shows only the severely restricted amount of data moving through some device at one time; attackers are more concerned with gaining random access to any information they choose, regardless of the increased risks of capture associated with more conventional methods. If corporate espionage is concerned with obtaining specific, as opposed to general, information, then most CE based attacks would be of little use. A more simple possible explanation for the lack of recorded attacks might be that popular social engineering and Trojan horse attacks are so overwhelmingly effective already that there is little need for an alternative interception technique.

Another common trend is that these EMSEC threats seem to apply primarily to high-end security systems, rather than home and small business users; and this seems to be related to the high cost of mounting the attacks described. It is surprising, however, that Smulder's cable phreaking method appears to be alarmingly cheap to conduct, yet this attack is not widely considered in threat models.

Regarding optical and RF-based CE-interception techniques, Schneier (quoted in full, above), [Sch98] discounts the problem as one that he is unable to do anything about, which fits well with his view of security as risk-management. The obvious danger with this view is that the implications of this kind of attack are still present and should be considered in the development of any computer security threat-model, regardless of whether the appropriate countermeasures are feasible. It is important to note that the risk from these attacks is not static, but highly dependent on market forces; nearly all the sources in this paper agree that for most of these attacks, high-expertise is unnecessary, and the apparent lack of motivation for CE interception attacks may dissolve at any time, if the alternative attacks become less convenient.

Future Trends

The various techniques described above constitute only a small part of the possible avenues into interception through compromising emanations, however they encompass almost the entire set of CE-based attacks described in open literature.

The cost to mount a van Eck -phreaking attack is out of range of the great majority, yet this trend can only last so long. There are several unpleasant possibilities to consider if these costs do drop, as speculated by Kuhn [Kuh98]. If the costs of effective countermeasures remain very high, personal computer use involving confidential information would have to be reduced drastically. It would be impossible to continue with the current level of private transactions enjoyed today, in the case where any hoodlum with a laptop and a software-radio had access to the displays of any computer within a hundred yards.

It should be expected that more types of compromising emanation attack will be discovered over the next decade, although the implications of these are more difficult to predict. A hypothetical attack might involve keyboards being read acoustically, combined with profiling data (either giving the identity of the typist, or at the extreme, some information correlating to the content typed). Developments in machine learning techniques and increases in processing power over recent years make this increasingly feasible. Eventually, such attacks exploiting Class II emanations, through some form of traffic analysis will inevitably be developed.

Another likely development in the EMSEC industry is the development of a more general version of Kuhn's and Loughry's 'Tempest Trojans'. At the moment these malicious programs are restricted to using the CRT, video cable or keyboard LEDs in order to transmit data to an attacker. In future, tempest Trojans may make use of many different kinds of emitters, including: cables to other devices, optical mice LEDs, and the plethora of palmtops, digital cameras, wireless peripheral connections and Bluetooth enabled cellphone equipment that are appearing in our increasingly-wired world.

Conclusions

In conclusion, there are a number of CE based attacks known at this time, operating over a range of different emanations from devices, and exhibiting varying scopes of interception.

Currently, EMSEC is something only high-end security systems must consider, as the CE-attacks require too much in the way of resources. Under rudimentary analysis, effort appears to be the main barrier to attackers utilizing CE-based attacks; van Eck phreaking simply requires more effort compared to the straightforward, and often cheaper alternatives of spoofing an identity, appearing on-site, and intercepting the target information through social engineering. The field of compromising emanations certainly benefit from this analysis of their scope; in the past the information available to van Eck phreaking was well understood, but discoveries in the last 5 years have done much to expand the scope of these attacks.

The field of EMSEC is potentially volatile, with new attacks being discovered every few years, and CE-interception equipment varying in cost wildly throughout the last decade and a half. Due to this volatility, constant vigilance is necessary to ensure that these attacks do not become feasible in the near future or that if so, the general public is made aware of it quickly.

With the increasing inter-connectedness of devices that is occurring, it would be prudent to remember that each additional component in a computer system brings potentially another avenue of attack for the motivated adversary.

References

[Cdc03] ‘Dildog’. [no date given] Cult of the Dead Cow Website *The Tao of Buffer Overflow* [tutorial online] Available from: http://www.cultdeadcow.com/cDc_files/cDc-351/ Accessed 2003 May. 31.

[Hig88] Highland, H. J. 1988. The Tempest over Leaking Computers *Abacus*, Vol. 5. No. 2. pp. 10-18.

[Hig88-2] Highland, H. J. 1988. Electromagnetic Eavesdropping Machines for Christmas? *Computers and Security,* Vol. 7. No. 4.

[Kuh98] Kuhn, M. G. and Anderson, R. J. 1998. *Soft tempest: hidden data transmission using electromagnetic emanations* Information Hiding Second International Workshop. Springer-Verlag, Berlin, Germany. pp.124-142

[Kuh99] Kuhn, M. G. and Anderson, R. J. 1999. *Soft Tempest: An Opportunity for NATO* Protecting NATO Information Systems in the 21st Century Washington DC, USA. [article online] Available from: http://www.ftp.cl.cam.ac.uk/ftp/users/rja14/nato-tempest.pdf Accessed 2003 May. 29.

[Kuh02] Kuhn, M. G. 2002. *Optical time-domain eavesdropping risks of CRT displays* IEEE Symposium on Security and Privacy. Los Alamitos, CA, USA. pp.3-18.

[Kuh02-2] Kuhn, M. G. 2002. *Optical Emission Security – Frequently Asked Questions* [article online] Available from: http://www.cl.cam.ac.uk/~mgk25/emsec/optical-faq.html Accessed 2003 May. 31.

[LU02] Loughry, J. and Umphress, D. 2002. *Information leakage from optical emanations* ACM Transactions on Information & Systems Security, vol.5, no.3. pp.262-89.

[McN03] McNamara, J. 2003. *The Complete, Unofficial TEMPEST Information Page* [resource online] Available from: http://www.eskimo.com/~joelm/tempest.html Accessed 2003 May. 31.

[Mol93] Moller, E. 1993. Protective Measures Against Compromising Electro Magnetic Radiation Emitted by Video Display Terminals *Phrack* magazine, Issue 44, Article 10. [online magazine] Available from: http://www.phrack.org/show.php?p=44&a=1 Accessed 2003 May. 31.

[NSA03] U.S. National Security Agency. 2003. *Endorsed Tempest Products List* [resource online] Available from: http://www.nsa.gov/isso/bao/tempest1/endorsed.htm Accessed 2003 May. 31.

[Pgp03] Various Authors. 2003 *The International PGP Home Page*
[encryption software] Available from:
http://www.pgpi.com
Accessed 2003 June. 1.

[Sch98] Schneier, B. 1998. Side Channel Cryptanalysis
Crypto-Gram Newsletter Issue June 15
[newsletter online] Available from:
http://www.counterpane.com/crypto-gram.html
Accessed 2003 June. 1.

[Sch02] Schneier, B. 2002. News Section
Crypto-Gram Newsletter Issue March 15
[newsletter online] Available from:
http://www.counterpane.com/crypto-gram.html
Accessed 2003 June. 1.

[Seb98] Sebastiani, S. 1998. *Characterization to a TEMPEST testing laboratory and methodology for control to compromising emanation* [sic]
IEEE EMC Symposium. International Symposium on Electromagnetic Compatibility. Part .1. vol.1. Piscataway, NJ, USA. pp.165-70.

[Smu90] Smulders, P. 1990. *The Threat of Information Theft by Reception of Electromagnetic Radiation from RS-232 Cables*
Eindhoven University of Technology, Dept. of Electrical Engineering, the Netherlands.

[Ste99] Stephenson, N. 1999. *Cryptonomicon*
New York: Avon Books.

[vEc85] van Eck, W. 1985. Electromagnetic Radiation from Video Display Units: An Eavesdropping Risk?
Computers & Security vol 4, no. 4, pp. 269-286.

[You03] Young, J. *Cryptome – NSA TEMPEST documents*
[resource online] Available from:
http://cryptome.org/nsa-tempest.htm
Accessed 2003 May 31.

The electromagnetic spectrum diagram was found at
http://geography.uoregon.edu/shinker/geog101/lectures/lec01/lec01_figs/electromagnetic-spectrum-fig2-6.gif