The Complete, Unofficial TEMPEST Information Page

formerly at: www.eskimo.com/~joelm/tempest.html

Over seven years of public disclosure, and one-stop shopping for TEMPEST info...

Across the darkened street, a windowless van is parked. Inside, an antenna is pointed out through a fiberglass panel. It's aimed at an office window on the third floor. As the CEO works on a word processing document, outlining his strategy for a hostile take-over of a competitor, he never knows what appears on his monitor is being captured, displayed, and recorded in the van below.

This page is about surveillance technology. If a search engine mistakenly led you here, try **Shakespeare, Pontiacs,** or **Arcade Games.** (The graphic on the right is the logo for the US Army Blacktail Canyon TEMPEST Test Facility.)

THIS PAGE IS NO LONGER BEING UPDATED AND IS LEFT UP FOR ARCHIVAL PURPOSES.

News & Updates

skip the news and go to the introduction

March 29, 2004 - Markus Kuhn has released what is the definitive (non-classified, available to the general public) research document on TEMPEST and emanation monitoring: Compromising emanations: eavesdropping risks of computer displays. This is Kuhn's doctoral thesis and is a must read for anyone who has a serious interest in this topic.

September 10, 2003 - There always seems to be some argument over whether TEMPEST is an acronym with deeper meaning, or simply a random codeword that doesn't relate to anything. A reader who wishes to remain anonymous, with a lengthy career doing TEMPEST testing for the Air Force and later in the private sector, sent in this story on the "real" PG-13 origins of term:

"One day when I was stationed at Lackland AFB (before we moved to Brooks), I answered the phone and a man on the other end told me that his major was looking through the phone book, and wanted to know what TEMPEST stood for. Being the wet behind the ears two striper that I was, I asked my NCOIC what I should tell the caller. He took the phone, puffed out his chest and told the man that TEMPEST stood for "Tremendously Endowed Men Performing Exciting Sexual Techniques" and hung up. Needless

to say, our major got a call from his major very shortly afterwards."

April 15, 2003 - Many thanks to "Agent Hammer" and Dan Robey for their independent English translations of Robin Lobel's French TEMPEST research mentioned a few days ago (click on the above links to get the translations). The U.S. Air Force produced a TEMPEST security training video called "So You Think You're Secure." The video was declassified in 1991 and "Shows measures used to prevent compromising of classified information during its handling by electronic equipment and explains purpose and application of Air Force Security Service's TEMPEST program." The video is available in the National Archives (ARC Identifier: 64336).

April 8, 2003 - Robin Lobel has been doing some TEMPEST research over the past year and has published his results. The TEMPEST documents from the Turkish National Institute of of Electronics and Cryptology mentioned in the last update seem to have a vanished. Thanks to an astute reader who archived them, they're both available zipped together here (if you can spare some bandwidth, I'd appreciate someone volunteering a mirror). John Young's Cryptome has a couple of TEMPEST-related nuggets including an Air Force document on TEMPEST Protection for Facilities, a TEMPEST glossary, and an extensive collection of background information (including court documents) on Frank "Spy King" Jones; who once was hawking "TEMPEST intercept" surveillance gear. I haven't been doing a great job keeping up with TEMPEST-related job submissions. Here's a promise to improve, with a recent "wanted" ad submitted in March finally posted.

January 26, 2003 - It's been awhile since I've updated the site. I've been writing a book called "Secrets of Computer Espionage: Tactics and Countermeasures" which has been seriously consuming a large amount of my time. The book will be published by Wiley in June, and has a section on TEMPEST along with a number of other interesting tidbits (sketchy details on it, which will be updated soon, are available here). Look for an update to this site in the coming months when I finish the book. In the meantime, here's some recent TEMPEST-related links that have crossed my desk. Two great TEMPEST research papers from the Turkish National Institute of of Electronics and Cryptology (TÜB•TAK UEKAE), including: Information Extraction from the Radiation of VDUs by Pattern Recognition Methods and Signal Processing Applications for Information Extraction from the Radiation of VDUs. Noted TEMPEST expert Bruce Gabrielson now offers a completely unclassified TEMPEST design course and is selling CD-ROM versions of his book, "Hardwire and Cable Design in Secure Communications." Check his site for more info.

March 22, 2002 - Slashdot has interesting links and commentary on conductive concrete being used as electromagnetic shielding for buildings.

March 5, 2002 - Joe Loughry has authored and released a fascinating paper on what he calls "**Optical TEMPEST**." To quote the introduction, "*A previously unknown form of compromising emanations has been discovered. LED status indicators on data communication equipment, under certain conditions, are*

shown to carry a modulated optical signal that is significantly correlated with information being processed by the device. Physical access is not required; the attacker gains access to all data going through the device, including plaintext in the case of data encryption systems. Experiments show that it is possible to intercept data under realistic conditions at a considerable distance. Many different sorts of devices, including modems and Internet Protocol routers, were found to be vulnerable." At least the black, electrician's tape is a cheap countermeasure. Later in the day, Markus Kuhn released a paper entitled **Optical Time-Domain Eavesdropping Risks of CRT Displays**. To quote from the conclusion, "*The information displayed on a modern cathode-ray tube computer monitor can be reconstructed by an eavesdropper from its distorted or even diffusely reflected light using easily available components such as a photo-multiplier tube and a computer with suitably fast analog-to-digital converter*." Kudos to you both gentlemen. Excellent research.

February 25, 2002 - The **Complete, Unofficial TEMPEST Information Page** is back. I took the site down around the first of the year and had John Young archive it at cryptome.org. However due to popular demand and some time freeing up, I've decided to continue with updates. - **A new Help Wanted section** has been added for companies, agencies, and recruiters looking for folks with TEMPEST/RFI/EMI experience. If you're trying to find an engineer, send me your requirements and I'll post them. No guarantees on successful leads, but this site does generate a fair amount of traffic, and for now the service is free. - A couple of years ago **Frank Jones**, AKA "Spy King" was hyping supposed TEMPEST surveillance products. You may be interested in his conviction and probation papers. - **TinFoil Hat Linux** is a single floppy-based distro with a variety of privacy features, including some unique "anti-Tempest" features. Review here, download Web site here.

December 30, 2001 - From an anonymous UK source: "*1. GCHQ in the UK is the #1 monitoring place for TEMPEST, they HAVE NOT scaled down any business to do with TEMPEST and now even use their techniques for corporate applications. They are STILL the first port of call of the Ministry of Defence for any queries. 2. The GCHQ standard (BTR) is the bible for the UK Military with regard to installations that may negate TEMPEST emissions, mainly due to good practices and safe areas around antenna and cryptographic equipment, also JSP440 is a watered down version of the standard that also covers computer security which is available to all CIDA's (Installation Design Authorities) within the Ministry. CIDA is one of the main 'businesses' within the MoD. Stories... these I have 'heard' from people in the know and witnessed myself:*

Whitehall, London
A Ford Transit van was converted to carry an entire Tempest test kit including antennas and terminals. This was parked on the road outside the building. The antennas were able to pick up the Telephone emissions from all areas of the building, including 'Shielded' areas due to the pre-1970 external telephone wiring, and as all conversations are routed to the local telephone exchange before encoding, this posed a major security threat. Also, static CRT images were reformed on the terminals within the van. (I have also witnessed this whilst attending a TEMPEST course at GCHQ.)

Gibraltar

An old 'story'. There is one main transmission site on Gibraltar where all of the signals to the passing allied fleets are sent (also submarine signals). These are coded within the building then transmitted via antenna and satellite. However a number of 'unfriendly' vessels (mainly Russian registered trawlers) were hovering near to the shore by the chain link fence. The comms officer got curios and asked for a TEMPEST check to see if they were picking up any signals. A test proved that the fence was picking up uncoded signals that were emanating from the large capacitors used in th encoding process. The fence then acted as an antenna and the unfriendlies were receiving uncoded signals. The station was closed down immediately.

Interference and Non-intentionally Interception.
Modern digital mobile phones are the current enemy of the UK teams. Mainly as the signal can act as a carrier wave for any radiated signal. Also, it has been noted, that people making Mobile calls at the end of the runway at RNAS Yeovilton can eavesdrop on the tower and pilot conversations. Another 'story' tells how a British Telecom engineer was testing a mast when his laptop screen started to fill up as if the computer was typing. What had actually happened was that the voice recognition software on his laptop had detected the radiated signal from the mast during decoding and regeneration and displayed it on the screen as plain text.

August 3, 2001 - TEMPEST mentioned in James Bamford's "Body of Secrets" book (NSA tell-all, follow-up to The Puzzle Palace). Specifically, ship implemented eavesdropping on Cuba. Ross Anderson also has a lengthy section on emissions security in his new book "Security Engineering." (I recommend Anderson's work to anyone interested in security systems - from ATMs to art galleries to EMSEC to crypto. This book is destined to become a classic.) NSA's online TEMPEST Endorsement Program has recently been updated. SANS Institute (the security folks) have a nice, concise TEMPEST FAQ (my only complaint is the reference to Codex Data Systems). Some good info on BEMA's TEMPEST shielded tents (lots of interest in these at the recent Special Operations Command Show and Conference). National Security Telecommunications Information Systems Security Committee Maintenance and Disposition of TEMPEST Equipment (PDF format dated December 2000). And finally the Nicodemo Scarfo trial is underway, and the outcome will definitely have an impact on the future of legal electronic surveillance. Stay tuned...

January 14, 2001 - John Young has released a FOIA version of NACSEM 5112, NONSTOP Evaluation Techniques. This is the first public document to come to light on NONSTOP surveillance techniques. The document has been heavily redacted. We do know NONSTOP testing is very similar to TEMPEST testing. In Side Channel Cryptanalysis of Product Ciphers (Postscript format), John Kelsey, Bruce Schneier, David Wagner, and Chris Hall speculate that NONSTOP and HIJACK refer to the compromise of cryptographic devices through nearby radio transmitters (such as a cell phone, handheld radio, intercom). One of the more interesting things about the document is toward the end. "*It is further noted that UNCLASSIFIED information concerning NONSTOP should not be discussed or made available to persons without a need-to-know. No information related to NONSTOP should be released for public consumption through the press, advertising, radio-TV or other public media.*" The original document came out in 1975, and has gone through several updates.

January 1, 2001 - John Young has received eight more TEMPEST-related documents from his October 1999 NSA FOIA appeal. The printing in the documents is in pretty poor shape, so text is being hand-typed. Currently available documents include: NSTISSAM TEMPEST/2-95, 12 December 1995 - "Red/Black Installation Guidance", Specification NSA No. 94-106, 24 October 1994 - Specification for Shielded Enclosures, NACSIM 5000, 1 February 1982 - TEMPEST Fundamentals, and NSTISSI 7000, 29 November 1993 - "TEMPEST Countermeasures for Facilities." (This last document is especially interesting in that it reveals the U.S. Government keeps a list of countries it views as having the ability and motivation to conduct TEMPEST attacks on U.S. interests. Censors did a bad job of blacking out the text in this 1995 document, and 12 of the 25 countries are identifiable. Including: Singapore, Norway, Hungary, Netherlands, Taiwan and some big industrial states that are known to dabble in economic espionage.) The remaining documents will be added as John has them transcribed.

December 10, 2000 - French SCSSI TEMPEST site, TEMPEST history, Ft. Huachuca Blacktail Canyon logo, fixed www.dtic.mil links (an astute reader pointed out that the "dead" DoD dtic sites on the TEMPEST Sources page could be revived by changing the domain - thanks Rob!).

December 6, 2000 - Over the past four years a tremendous amount of information has come to light on TEMPEST and related topics. So much that even though the page had no graphics, it was taking a couple of minutes to load on slow, dial-up connections. To celebrate the site's four year birthday, I've split it into four pages so it will load a bit faster. - CNET News reports on the Feds using a bugged keyboard to snag a Philadelphia mobster who was using PGP. I've been telling clients for years that this is a significant risk. In most cases it's much easier to do a "black bag" job on a target and install key monitoring software or hardware (or even hide a wireless CCD camera positioned to transmit what's being typed on the keyboard or appearing on the screen), than deal with strong encryption. Although the risk of discovery is obviously higher than a TEMPEST intercept, the lower cost and fewer required technical skills make this a much more likely attack option.

Introduction to this Site

If you're even vaguely familiar with intelligence, computer security, or privacy issues, you've no doubt heard about TEMPEST. Probably something similar to the above storyline. The general principle is that computer monitors and other devices give off electromagnetic radiation. With the right antenna and receiver, these emanations can be intercepted from a remote location, and then be redisplayed (in the case of a monitor screen) or recorded and replayed (such as with a printer or keyboard).

TEMPEST is a code word that relates to specific standards used to reduce electromagnetic emanations. In the civilian world, you'll often hear about TEMPEST devices (a receiver and antenna used to monitor emanations) or TEMPEST attacks (using an emanation monitor to eavesdrop on someone). While not

quite to government naming specs, the concept is still the same.

TEMPEST has been shrouded in secrecy. A lot of the mystery really isn't warranted though. While significant technical details remain classified, there is a large body of open source information, that when put together forms a pretty good idea of what this dark secret is all about. That's the purpose of this page.

The following is a collection of resources for better understanding what TEMPEST is. And no, I seriously don't think national security is being jeopardized because of this information. I feel to a certain extent, the "security through obscurity" that surrounds TEMPEST may actually be increasing the vulnerability of U.S. business interests to economic espionage. Remember, all of this is publicly available. A fair amount has come from unclassified, government sites. Up to this point, no one has spent the time to do the research and put it all together in a single location.

References marked with an (**X**), are good primary sources. If you just read these, you'll end up with an excellent overview on TEMPEST-related topics.

References marked with an (**O**) are reported dead links. These pages may be temporarily or permanently unavailable. Dead links are left for reference sake (you may want to check the main domain name or do further searching with AltaVista, etc.). It's interesting to note the number of military sites that now report 404 - Not Found or Forbidden Request errors for certain documents.

The site content is listed below. There are three pages in addition to this one. Introduction provides detailed background info on TEMPEST. Sources provides links to hardware manufacturers, software vendors, and specific government documents. Miscellaneous is comments from readers and other things that don't fit in the other pages.

Note: As you start viewing TEMPEST info, you likely will run into vague or confusing acronyms. A great Net resource is the Acronym Finder site.

Happy reading!

Joel McNamara - joelm @ eskimo dot com (spam filter)
Original page - December 17, 1996 - Last update March, 2004

Site Contents

Non-TEMPEST computer surveillance
Change log

Disclaimer: I've never been involved with the TEMPEST community, had a security clearance for TEMPEST, or have access to classified material relating to TEMPEST. The information on these pages is completely derived from publicly available, unclassified sources.

Last changed March 29, 2004

The Complete, Unofficial TEMPEST Information Page

This page is about surveillance technology. If a search engine mistakenly led you here, try **Shakespeare**, **Pontiacs**, or **Arcade Games**.

THIS PAGE IS NO LONGER BEING UPDATED AND IS LEFT UP FOR ARCHIVAL PURPOSES.

Introduction to TEMPEST

What is TEMPEST?

TEMPEST is a U.S. government code word that identifies a classified set of standards for limiting electric or electromagnetic radiation emanations from electronic equipment. Microchips, monitors, printers, and all electronic devices 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 your TV screen is emanation caused interference. (If you want to learn more about this phenomena, a company called NoRad has an excellent discussion (**X**) of electromagnetic radiation and computer monitors (and Chomerics has a good electromagnetic interference 101 page), that you don't need to be an electrical engineer to understand. Also, while not TEMPEST-specific, a journal called Compliance Engineering (**O**), typically has good technical articles relating to electromagnetic interference. There's also the Electromagnetic Compliance FAQ.)

During the 1950's, the government became concerned that emanations could be captured and then reconstructed. Obviously, 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. Research showed it was possible to capture emanations from a distance, and as a response, the TEMPEST program was started. (For some interesting perspectives on the history of TEMPEST, see this timeline and do a text search for TEMPEST at this UK list archive.)

The purpose of the program was to introduce standards that would reduce the chances of "leakage" from devices used to process, transmit, or store sensitive information. TEMPEST computers and peripherals (printers, scanners, tape drives, mice, etc.) are used by government agencies and contractors to protect data from emanations monitoring. This is typically done by shielding the device (or sometimes a room or entire building) with copper or other conductive materials. (There are also active measures for "jamming" electromagnetic signals. Refer to some of the patents listed below.)

Bruce Gabrielson, who has been in the TEMPEST biz for ages, has a nice unclassified general description of TEMPEST that was presented at an Air Force security seminar in 1987.

In the United States, TEMPEST consulting, testing, and manufacturing is a big business, estimated at over one billion dollars a year. (Economics has caught up TEMPEST though. Purchasing TEMPEST standard hardware is not cheap, and because of this, a lesser standard called ZONE (**O**) has been implemented. This does not offer the level of protection of TEMPEST hardware, but it quite a bit cheaper, and is used in less sensitive applications.)

Emanation standards aren't just confined to the United States. NATO has a similar standard called the AMSG 720B Compromising Emanations Laboratory Test Standard. In Germany, the TEMPEST program is administered by the National Telecom Board. In the UK, Government Communications Headquarters (GCHQ), the equivalent of the NSA, has their own program.

TEMPEST History

The original 1950s emanations standard was called NAG1A. During the 1960s it was revised and reissued as FS222 and later FS222A.

In 1970 the standard was significantly revised and published as National Communications Security Information Memorandum 5100 (Directive on TEMPEST Security), also known as NACSIM 5100. This was again revised in 1974.

Current national TEMPEST policy is set in National Communications Security Committee Directive 4, dated January 16, 1981. It instructs federal agencies to protect classified information against compromising emanations. This document is known as NACSIM 5100A and is classified.

The National Communications Security Instruction (NACSI) 5004 (classified Secret), published in January 1984, provides procedures for departments and agencies to use in determining the safeguards needed for equipment and facilities which process national security information in the United States. National Security Decision Directive 145, dated September 17, 1984, designates the National Security Agency (NSA) as the focal point and national manager for the security of government telecommunications and Automated Information Systems (AISs). NSA is authorized to review and approve all standards, techniques, systems and equipment for AIS security, including TEMPEST. In this role, NSA makes recommendations to the National Telecommunications and Information Systems Security Committee for changes in TEMPEST polices and guidance.

Just how prevalent is emanation monitoring?

There are no public records that give an idea of how much emanation monitoring is actually taking place. There are isolated anecdotal accounts of monitoring being used for industrial espionage (see Information Warfare, by Winn Schwartau), but that's about it. (However, see a very interesting paper written by Ian Murphy called Who's Listening that has some Cold War TEMPEST spy stories.) Unfortunately, there's not an emanation monitoring category in the FBI Uniform Crime Reports. (While not TEMPEST-specific, the San Jose Mercury News printed a November 11, 1998 article(**O**) on how much money American businesses are losing to economic espionage. Considering some of the countries involved, hi-tech spying techniques are likely being used in some cases.)

Threat?

There are a few data points that lead one to believe there is a real threat though, at least from foreign intelligence services. First of all, the TEMPEST industry is over a billion dollar a year business. This indicates there's a viable threat to justify all of this protective hardware (or it's one big scam that's making a number of people quite wealthy).

This scope of the threat is backed up with a quote from a Navy manual that discusses "compromising emanations" or CE. "Foreign governments continually engage in attacks against U.S. secure communications and information processing facilities for the sole purpose of exploiting CE." I'm sure those with appropriate security clearances have access to all sorts of interesting cases of covert monitoring.

Or not?

In 1994, the Joint Security Commission issued a report to the Secretary of Defense and the Director of Central Intelligence called "Redefining Security." It's worthwhile to quote the entire section that deals with TEMPEST.

TEMPEST (an acronym for Transient Electromagnetic Pulse Emanation Standard) is both a specification for equipment and a term used to describe the process for preventing compromising emanations. The fact that electronic equipment such as computers, printers, and electronic typewriters give off electromagnetic emanations has long been a concern of the US Government. An attacker using off-the-shelf equipment can monitor and retrieve classified or sensitive information as it is being processed without the user being aware that a loss is occurring. To counter this vulnerability, the US Government has long required that electronic equipment used for classified processing be shielded or designed to reduce or eliminate transient emanations. An alternative is to shield the area in which the information is processed so as to contain electromagnetic emanations or to specify control of certain distances or zones beyond which the emanations cannot be detected. The first solution is extremely expensive, with TEMPEST computers normally costing double the usual price. Protecting and shielding the area can also be expensive. While some agencies have applied TEMPEST standards rigorously, others have sought waivers or 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 was installed with no thought given either to cost or actual threat.

A general manager of a major aerospace company reports that, during building renovations, two SAPs required not only complete separation between their program areas but also TEMPEST protection. This pushed renovation costs from $1.5 million to $3 million just to ensure two US programs could not detect each other's TEMPEST emanations.

In 1991, a CIA Inspector General report called for an Intelligence Community review of domestic TEMPEST requirements based on threat. The outcome suggested that hundreds of millions of dollars have been spent on protecting a vulnerability that had a very low probability of exploitation. This report galvanized the Intelligence Community to review and reduce domestic TEMPEST requirements.

Currently, many agencies are waiving TEMPEST countermeasures within the United States. The rationale is that a foreign government would not be likely to risk a TEMPEST collection operation in an environment not under their control. Moreover, such attacks require a high level of expertise, proximity to the target, and considerable collection time. Some agencies are using alternative technical countermeasures that are considerably less costly. Others continue to use TEMPEST domestically, believing that TEMPEST procedures discourage collection attempts. They also contend that technical advances will raise future vulnerabilities. The Commission recognizes the need for an active overseas TEMPEST program but believes the domestic threat is minimal.

Contractors and government security officials interviewed by the Commission commend the easing of TEMPEST standards within the last two years. However, even with the release of a new national TEMPEST policy, implementation procedures may continue to vary. The new policy requires each

Certified TEMPEST Technical Authority (CTTA), keep a record of TEMPEST applications but sets no standard against which a facility can be measured. The Commission is concerned that this will lead to inconsistent applications and continued expense.

Given the absence of a domestic threat, any use of TEMPEST countermeasures within the US should require strong justification. Whenever TEMPEST is applied, it should be reported to the security executive committee who would be charged with producing an annual national report to highlight inconsistencies in implementation and identify actual TEMPEST costs.

Domestic implementation of strict TEMPEST countermeasures is a prime example of a security excess because costly countermeasures were implemented independent of documented threat or of a site's total security system. While it is prudent to continue spot checks and consider TEMPEST in the risk management review of any facility storing specially protected information, its implementation within the United States should not normally be required.

The Commission recommends that domestic TEMPEST countermeasures not be employed except in response to specific threat data and then only in cases authorized by the most senior department or agency head.

It's also interesting to note that the National Reconnaissance Office (NRO) eliminated the need for domestic TEMPEST requirements in 1992.

Maybe

The main difficulty in tracking instances of emanation monitoring is because it's passive and conducted at a distance from the target, it's hard to discover unless you catch the perpetrator red-handed (a bad Cold War pun). Even if a spy was 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, you really need to weigh the costs and benefits. Is it cheaper and more efficient to have a spy pass himself off as a janitor to obtain information, or to launch a fairly technical and sophisticated monitoring attack to get the same data? 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.

TEMPEST Urban Folklore

Because of the general lack of knowledge regarding TEMPEST topics, there is a fair amount of urban

folklore associated with it. Here's some common myths. And if you can provide a primary source to prove me wrong, let me know (no friends of friends please).

- *It's illegal to shield your PC from emanation monitoring*. Seline's paper suggests this, but there are no laws that I've found that even come close to substantiating. Export of TEMPEST-type shielded devices is restricted under ITAR, and most manufacturers will only sell to government authorized users, but there are no laws banning domestic use of shielded PCs.

- *Emanation monitoring was used to snare CIA spy Aldrich Ames and also during the Waco incident*. Winn Schwartau appears to have started the speculation on these two events. While conventional electronic surveillance techniques were used, there's no published evidence to support a "TEMPEST attack."

- *You can put together a emanation monitoring device for under $100 worth of Radio Shack and surplus parts.* Perhaps for a dumb video display terminal (VDT), but certainly not for a VGA or SVGA monitor. And definitely not for doing serious remote monitoring. There have been anecdotal accounts of television sets with rabbit ears displaying fragments of a nearby computer screen. Beyond that, effective, cheap, easy-to-build devices don't seem to exist. If they did, the plans would be available on the Net at just about every hacker site.

- *LCD displays on laptops eliminate the risks of TEMPEST attacks.* Maybe, maybe not. The technology behind LCD monitors versus typical CRT monitors may somewhat reduce the risk, but I wouldn't bet my life on it. There have been anecdotal accounts of noisy laptop screens being partially displayed on TVs. If laptops were emanation proof, I seriously doubt there would be TEMPEST standard portables on the market.

- *TEMPEST is an acronym*. Maybe. There have been a variety of attempts to turn TEMPEST into a meaningful acronym (such as Transient ElectroMagnetic Pulse Emanation STandard) by government and non-government sources. The official government line denies this, and states TEMPEST was a code word originally given to the standards, and didn't have any particular meaning.

- *There's virtually no information about TEMPEST on the Net because it's so secret*. Nonsense. The world does not revolve around AltaVista. You just need to dig a little deeper. (*Boy, does mention of AltaVista date when I first wrote this.*)

General TEMPEST Information

Online Sources

- *August 11, 2000* - The Wall Street Journal published an article on TEMPEST on August 7, 2000. I did several e-mail interviews with the reporter, and was pretty disappointed to see the final result. A whole lot of good information on TEMPEST went by the wayside, in favor of a lot of fairly sensational column inches. On August 10, the folks at Forbes questioned the credibility of the WSJ article. See their response (which I completely agree with) here. I'm always willing to help journalists with questions about TEMPEST. But figure it out folks. Every time your article totally blows it, your source isn't going to want to play with you or your fellow journalists again. I know a whole bunch of intelligent, well-informed people who have sworn off dealing with the media because of misquoted information or general cluelessness when an article is finally published (and for those reporters in the house, please don't whine and blame your editors). Unfortunately, the ranks of decent and willing sources will continue to thin as long as this behavior continues...
- Ross Anderson and Markus Kuhn (from Cambridge, UK) have written a new paper that I consider one of the most definitive sources of contemporary research on TEMPEST. Soft Tempest: Hidden Data Transmission Using Electromagnetic Emanations (**X**), looks at the software side of the topic, including TEMPEST viruses that can enhance interceptions. The most startling aspect, and the issue that has a lot of spook's knickers in a knot, is the use of special fonts to defeat monitoring. This .PDF file is a must read. You can now also download the anti-TEMPEST fonts. Demcom, makers of the excellent Steganos security suite have released a freeware Windows text editor (called Zero Emission Pad) that incorporates anti-TEMPEST font technology.

- One of the most distributed sources of TEMPEST information on the Net is a paper by Christopher Seline called "Eavesdropping On the Electromagnetic Emanations of Digital Equipment: The Laws of Canada, England and the United States." It deals with laws relating to eavesdropping on the electromagnetic emanations of digital equipment. Seline postulates that it is illegal for a U.S. citizen to shield their hardware against emanation eavesdropping. There are no laws to support this contention. Other information in the Seline paper has been questioned by informed sources, however, there is good source material contained in it.

- The other widely distributed source is Grady Ward's "TEMPEST in a teapot" (**X**) post to the Cypherpunks list that discusses practical countermeasures based on techniques radio operators use to reduce electromagnetic interference. Good technical source material.

- "Electromagnetic Radiation from Video Display Units: An Eavesdropping Risk?" (**X**) by Wim van Eck, Computers & Security, 1985 Vol. 4. This is the paper that brought emanation monitoring to the public's attention. Van Eck was a research engineer at the Dr. Neher Laboratories of The Netherlands' Post, Telegraph, and Telephone (PTT) Service. His paper was purposely incomplete on several points, and modifications were required to actually build a working device based on his plans. (.PDF format)

- "Electromagnetic Eavesdropping Machines for Christmas?" (**X**) Computers & Security, Vol. 7, No. 4 [1988] A follow-up article to the van Eck paper. Excellent source material regarding why (and what) certain details weren't included in the original. .PDF and HTML formats.

- "The Threat of Information Theft by Reception of Electromagnetic Radiation from RS-232 Cables", Peter Smulders, Dept of Electrical Engineering, Eindhoven University of Technology, 1990. Many people just think their computer monitors are vulnerable to emanation monitoring. This paper clearly shows that cabling is equally at risk. (.PDF format)

- "Protective Measures Against Compromising Electromagnetic Radiation Emitted by Video Display Terminals" (**X**) by Professor Erhart Moller, Aachen University, Germany, 1990. A good introduction. Reprinted in Phrack 44.

- "Data Security by Design" was written by George R. Wilson and appeared in Progressive Architecture, March 1995. It offers some interesting facts on shielding structures from emanation leakage.

- PC Week, March 10, 1987 v4 p35(2) has an article by Vin McLellan (**O**) about emanation monitoring and TEMPEST.

- TEMPEST Industry and People Grapple with Changing Perspectives is a 1991 paper by Dr. Bruce C. Gabrielson (a very respected name in the TEMPEST community) that discusses some of the economic challenges of the industry. Good background. Gabrielson also has a variety of EMC and INFOSEC papers online.

- Winn "Mr. Information Warfare" Schwartau gave a presentation at DefCon II (the annual Vegas hacker get together) in 1994. Real Media audio links: Winn Schwartau: Overview of Tempest and VanEck shielding and radiation and somewhat related, Winn Schwartau - HERF Guns, EMP Bombs and Weapons of Mass Disruption (Unclassified) - parts 1, 2.

- TEMPEST MONITORING: A MAJOR THREAT TO SECURITY appears to be a university student paper. Decently written and fairly comprehensive.

- Truthnet, Issue 2 (an e-zine) has a short, general layman's article on TEMPEST.

- COMPUTERWOCHE, August 8, 1986, #34 Lauschangriff auf unbekannte Schwachstelle is a German article regarding TEMPEST shielded terminals. Thanks to Ulf Möller for the following summary:

  The article says that authorities had long known about compromising radiation, but the

information had leaked to business only recently. It was usually neglected by commercial computing centers and completely unknown to users. Experts estimate that screen contents can be received over a distance of 1 km, and of 300 m using amateur equipment. SCS GmbH gave recommendations on low-radiation screens determined in experiments. Room protection with Faraday cages is explained. Radiation-free computers, typically implemented by a Faraday cage inside the box, existed but were not available to the market. Beginning March 1 that year, authorities processing sensitive data were required by order of the ministry of interior to use only Tempest-protected devices approved by the ZfCH (= central office for encipherment, the predecessor of the BSI). The producers of those devices are obliged to secrecy and may deliver to authorities only. Ericsson was the market leader for security screens with a special version of the S41 terminal with an annual turnover of 10,000,000 DM. They would have liked to sell more of them, but were not allowed to deliver them to private companies.

- Illegal Communications Interception Equipment Was Destined for Vietnam (from iPartnership)

7/9/99
iDEFENSE
By Bill Pietrucha

Vietnam was the intended final shipping point for restricted U.S. communications intercept
equipment, iPARTNERSHIP has learned. Shalom Shaphyr, arrested earlier this week for allegedly possessing and selling Tempest computer intercept equipment, planned to first falsify the nature of the equipment in export papers, ship it to a U.S. NATO ally, then to Israel, and finally to Vietnam.

The Tempest computer intercept equipment, also known as a video intercept receiver, is considered a defense article under the International Traffic in Arms Regulations (ITAR), and cannot be shipped to Vietnam without an export license.

In the U.S. District Court in the Eastern District Virginia late yesterday, Shaphyr, an Israeli citizen living in the U.S. under a business visa, requested his detention hearing be postponed until July 20, to give his lawyers "time to review the charges against me."

Shaphyr will continue to be held in the City of Alexandria, Va. detention center until the July 20 detention hearing date.

In papers filed with the court, FBI Special Agent Christian Zajac testified Shaphyr was "looking for a Tempest monitoring system" capable of remotely capturing computer emanations. The reason for the equipment, Shaphyr had said, was to view what was on a computer monitor from a distance of "a few tens of feet maybe to a few hundred feet"

away.

Zajac, an FBI Special Agent for the past two years, told the court Shaphyr indicated the equipment would be used by the Vietnamese government "in a joint venture." Along with the equipment, Zajac told the court, Shaphyr also asked for a syllabus outlining the training that would be provided on the Tempest equipment, indicating the trainees would be Vietnamese.

Shaphyr, iPARTNERSHIP learned, operates a business with offices in Vietnam and England, and is an FAA certified pilot, flight engineer and navigator listing his address in Ho Chi Minh City, Viet Nam.

Zajac said the joint FBI-U.S. Customs Service investigation, which began in November 1998, led to Shaphyr's arrest this past Wednesday after Shaphyr paid an FBI undercover agent $2,000 in U.S. currency to export the Tempest equipment to Israel without a license. The total price Shaphyr allegedly agreed to pay for the Tempest equipment was $30,000, Zajac testified.

Zajac said the investigation did not end with Shaphyr's arrest, and is continuing.

- Slashdot has a short thread on TEMPEST (7/19/99) with some interesting personal accounts of ex-military types.

- Berke Durak has some interesting test results as well as source code that demonstrates how easy a CPU can transmit data in the FM band.

- Some general notes on a presentation and workshop given by Professor Mueller (Moller?) during the 1997 HIP conference. Some interesting technical notes.

- Tempest - een beeldige opsporingsmethode - 1997 Dutch article by Bert-Jaap Koops. Quick summary by an anonymous reader:

  In the article Drs. B.J. Koops -- a researcher at the Katholieke Universiteit Brabant and the Technische Universiteit Tilburg (Catholic University Brabant and Technical University Tilburg, both in the Netherlands) gives a short introduction to what TEMPEST is, what it can be used for.

  He notes that there are three ways of tapping info: wires (electrical), direct radiation and radiation emitted by screen-to-PC cable.

He continues talking about wether or not it is legal for individuals and the police to use TEMPEST monitoring. It turns out that it is illegal for individuals (due to some amendments to wiretapping laws), and it is illegal for police (since they need explicit permission to do so, and TEMPEST nor radiation monitoring is mentioned in Dutch law).

He ends the article proposing a discussion in the parliament on wether or not PC-tapping would be allowed in the Netherlands, since that is a political decision.

- c't interview (4/94) with surveillance expert Hans-Georg Wolf on industrial espionage. Some interesting TEMPEST tidbits. There's also another general article in the same issue with some eavesdropped monitor photos.

- November 13, 1999 - Issue 21 of the hacking magazine SET (think of a Spanish Phrack), has a lengthy text file on TEMPEST with some interesting schematics. Check out the Spanish version here, or cut and paste interesting bits into Babelfish for translation here (any readers more fluent in Spanish than I are encouraged to submit a decent translation).

- November 8, 1999 - New Scientist has a short TEMPEST article, where Markus Kuhn predicts intercept devices for under £1000 within the next five years (and although not TEMPEST specific, an interview with Ross Anderson included). Slashdot also has a thread going regarding the article.

Patents

A quick search of IBM's patent server service revealed several interesting patents:

- Patent number 4965606 - Antenna shroud tempest armor (1989)
- Patent number 5165098 - System for protecting digital equipment against remote access (1992)
- Patent number 4932057 - Parallel transmission to mask data radiation (1990)
- Patent number 5297201 - System for preventing remote detection of computer data from tempest signal emissions (1994)
- Patent number 5341423 - Masked data transmission system (1994)

A note about patent 5297201. It references patent 2476337 that was issued July 1, 1949. Unfortunately, the details aren't available online, but the reference may be telling as to just how long emanation monitoring has been taking place.

Paper Sources

- "Cabinets for Electromagnetic Interference/Radio-Frequency Interference and TEMPEST

Shielding" by Kenneth F. Gazarek, Data Processing & Communications Security, Volume 9, No. 6 [1985].

- Information Warfare, Winn Schwartau, Thunder's Moth Press, New York, 1996 (second edition)

  Chapter 7, The World of Mr. van Eck, is devoted to TEMPEST-related topics. There's some good information, but it's painted pretty broadly, and really doesn't get into technical details (the second edition does present much more material on HERF guns and other topics, but nothing has been added to the van Eck chapter). Still, a good read, also some additional sources not mentioned on this page in the Footnotes section.

- Computer Security Basics, (**X**) Deborah Russell and G. T. Gangemi Sr., O'Reilly & Associates, Sebastpol, CA, 1991. Chapter 10, TEMPEST, provides an excellent overview of the risks of emanations as well as the government TEMPEST program. This is a must read.

- I don't have a citation, but in 1997 the German computer magazine c't apparently published an article that described a home-built TEMPEST monitor. It consisted of an old Russian television (because it wasn't limited to receiving certain channels - stepless frequency tuning) and a piece of copper for the antenna. The testers couldn't target individual computers though, and received images from a variety of screens when cruising through a neighborhood. Anyone that has access to an original copy of the article, please contact me.

EMSEC Those in the know no longer generically use the term TEMPEST to refer to emanations security. The current buzzword d'jour is EMSEC, or Emissions Security. If you read between the lines, the change to the term EMSEC is interesting. A quote from an Air Force site(**O**):

> "Emission Security (EMSEC) better known as TEMPEST has taken a drastic change over the past few years. These changes have necessitated a complete revision of rules and regulations, causing the need for new publications. While these new publications have been drafted and are in the coordination stages, we must continue to keep informed and up-to-date on EMSEC policy and procedures."

Hmmm. Just what drastic changes are we talking about? Idle speculation might include:

- Budget cuts and directives have cut back on TEMPEST use forcing new policies.
- Other types of emissions have been discovered that pose a security threat.

From the same site comes this quote:

> "WHAT IS COMPROMISING EMISSIONS (sic)? Compromising emissions are unintentional intelligence-bearing signals which, if intercepted and analyzed, disclose the classified information transmitted, received, handled, or otherwise processed by any information processing equipment."

It's curious that the term "electromagnetic radiation" isn't used in the definition. So, there are other monitoring vulnerabilities besides TEMPEST. Which leads us to HIJACK and NONSTOP.

HIJACK and NONSTOP

In my quest for open-source material regarding TEMPEST, I've started to run into two new codewords, HIJACK and NONSTOP. At first there was only some sketchy information:

- References to NONSTOP and HIJACK testing is starting to appear in outlines for TEMPEST training courses (with a reference to NACSEM 5112). Secret clearances are required for attending the classes. A Department of Defense course description reads, "The course will train students in the operation of the Honeywell and HLDS test detection systems and in the fundamental requirements of NONSTOP/HIJACK testing."
- An Air Force training glossary(**O**) lists the definitions of HIJACK and NONSTOP as classified.
- Countermeasures are apparently being used against NONSTOP, with a reference to NSTISSI 7001.
- NONSTOP has been around for awhile, NACSEM-5112 (RP-4) 1, 2, 3 & 4 NONSTOP Evaluation Techniques (SECRET) dates back to April 1975.

Then, thanks to publicly available documents I found on the Net, we now know a little bit more. Although the documents had classified information excised, there were still enough tidbits to put together a speculative guess regarding what HIJACK and NONSTOP related to.

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

HIJACK is a classified codeword that apparently 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 (these can be wire or wireless). The adversary uses antennas, receivers, a display device, a recording device, and one additional piece of equipment (a special detection system

that is supposedly very sensitive and very expensive; and there are not very many of them in existence - sorry, I don't have any other details). Also, the technician using this special equipment will supposedly require a great deal of training and experience.

Remember, the above is speculation. And whether the guesses are accurate or not, at this point you'd need to have a security clearance to know for sure.

Monitoring Devices

John Williams (Consumertronics, P.O. Box 23097, Albuquerque, NM 87192) sells the Williams Van Eck System, an off the shelf emanation monitoring device. He also has a demonstration video and and a book called "Beyond Van Eck Phreaking." The updated Consumertronics Web site has a variety of interesting products (the $3 paper catalog is a good read too). In past written correspondence with Mr. Williams, he has provided a considerable amount of technical details about his products.

Ian Murphy, CEO of IAM/Secure Data System wrote a very interesting paper on TEMPEST, including a Radio Shack parts list for building a receiver.

Legal News - November 15, 1999 - I just received an e-mail from a Terrance L. Kawles, Esq. who is representing Frank Jones of Codex and DataScan fame. Mr. Kawles takes exception to a note I recently added to this page that states some people question Mr. Jones' credibility. Mr. Kawles feels there is some type of smear campaign going on against his client by persons unknown, and is in the process of filing an action against various parties. In the note I suggested that interested readers check USENET archives and decide for themselves about Mr. Jones (over the years there has been a lively discussion on Mr. Jones, both pro and con). Mr. Kawles feels this note is defamatory, and offers me two options: "***... either remove the Note, or remove your references and links to the Mr. Jones and Codex.***"

I'm going to indulge Mr. Kawles and remove all links and information regarding Mr. Jones and his TEMPEST products from this section. Not because I'm caving in to the demands of some lawyer (my legal counsel states I have not published any defamatory statements regarding Mr. Jones). But mostly because anyone that resorts to these kinds of tactics on the Net, really doesn't deserve to be mentioned in this site, which is devoted to public disclosure.

And Mr. Kawles, in regard to your statement, "*As I understand, Mr. Jones was instrumental in providing information when you began your studies of TEMPEST, yet you reward him with this unnecessary editorial comment.*" Ha! I'd love to see you substantiate that by providing any logs of communications between Mr. Jones and myself.

Update - See an interesting Forbes online article that appeared August 10, 2000. Also see Mr. Jones'

conviction and probation papers which surfaced in December 2001.

Do It Yourself Shielding Sources

After you've read Grady's paper...

If you're handy with a soldering iron, Nelson Publishing produces something called the EMI/RFI Buyers' Guide. This is a comprehensive list of sources for shielding material, ferrites, and other radio frequency interference and electromagnetic interference type products. There's even listings for TEMPEST products and consultants. Unfortunately, most of the sources don't have links. But company names, addresses, and phone/FAX numbers are supplied.

A more general electronics manufacturer data base is electroBase. They have over 7,800 manufacturers of all types listed.

There's an interesting product called Datastop Security Glass, that's advertised as the only clear EMF/RFI protection glass on the market. It's free of metal mesh, so has excellent optical clarity. This is the same stuff the FAA uses in air traffic control towers. Contact TEMPEST SECURITY SYSTEMS INC. for more details.

Just remember, effective emanation security begins with the physical environment. Unless you can shield the wiring (telephone lines, electrical wiring, network cables, etc.), all of the copper around your PC and in the walls isn't going to stop emanations from leaking to the outside world. In shielding, also remember that emanations can pass from one set of wires to another.

---

last changed February 22, 2002

back to main TEMPEST

The Complete, Unofficial TEMPEST Information Page

This page is about surveillance technology. If a search engine mistakenly led you here, try **Shakespeare**, **Pontiacs**, or **Arcade Games**.

THIS PAGE IS NO LONGER BEING UPDATED AND IS LEFT UP FOR ARCHIVAL PURPOSES.

TEMPEST Sources

TEMPEST Hardware & Consulting

Here's some of the players in the billion dollar plus a year TEMPEST industry (this is by no means a complete list):

ADI Limited(**O**) is a big Australian defense contractor that does some TEMPEST testing.

AFC (Antennas for Communications) manufacturers TEMPEST shielding enclosures for antennas.

Advanced Technology System Corporation sells TEMPEST equipment and provides consulting services.

Aerovox manufactures a variety of EMI filters. Nice downloadable catalog (Windows help format) with photos.

Allied Signal Aerospace performs Canadian TEMPEST testing.

Austest Laboratories is a down-under company that provides TEMPEST testing.

DEMCOM provides Soft-TEMPEST fonts in their Steganos II security suite.

Cabrac makes TEMPEST enclosures (nice picture).

Candes Systems Incorporated (**X**) produces TEMPEST products, including monitors, printers, and laptops. Nice photos and specs.

COS provides TEMPEST design and consulting services.

BEMA Inc. produces shielding products including a slick portable TEMPEST tent.

Braden produces shielded room components.

Computer Security Solutions is a women owned business in Virginia specializing in TEMPEST products.

Compucat (**O**) is an Australian company that provides a variety of TEMPEST products and services.

Compunetix(**O**) produces various TEMPEST rated product.

Conductive Coatings, a division of the Chromium Corporation, produces a variety of shielding solutions.

Corcom makes a variety of shielded jacks (RJ type) in its Signal Sentry line.

Corton Inc. manufactures TEMPEST keyboards.

Cryptek(**O**) sells TEMPEST photocopiers and communication products.

Cycomm sells TEMPEST workstations, terminals, printers, and more to folks like the State Department. Recently merged with Hetra.

D2D/Celestica(**O**) is a British TEMPEST testing, design, and manufacturing firm.

Dina distributes Emcon TEMPEST products.

Dynamic Sciences (**O**) is another TEMPEST-oriented company. Among other things, they produce a piece of hardware called the DSI-110, for surveillance and testing purposes.

Einhorn Yaffee Prescott is an architecture and engineering firm that has built TEMPEST buildings for defense contractors.

Elfinco SA(**O**) is a British company that produces shielding products. Most notable is electromagnetic shielded concrete.

Equiptco Electronics (**O**) sells a variety of general electronic equipment and supplies, some TEMPEST standard (but you need to dig through their catalog to find it).

EMC Technologies is an Australian company that provides TEMPEST testing.

Emcon Emanation Control Limited, in Onatrio, Canada, has been providing TEMPEST equipment to NATO governments for the past 12 years.

EMP-tronic is a Swedish company specializing in shielded rooms.

ERS is a recruiting service that finds jobs for TEMPEST engineers (and others).

Filter Networks produces inline TEMPEST line filters.

Framatome Connectors International manufactures TEMPEST cables and connectors in the UK, especially suited for marine use.

GEC-Marconi Hazeltine(**O**) produces COMSEC products as well as TEMPEST design and test facilities.

Glenair is a multi-national company that produces some shielding products.

Greco Systems manufactures factory tools and ruggedized TEMPEST computers.

GSCG. Formerly GRiD Government Systems. Tempest laptops, desktops, and printers.

GTE, the phone people, make a TEMPEST version of their Easy Fax (**O**) product, complete with a STU-III (encrypted phone) gateway.

HAL Communications Corp. provides TEMPEST shielded modems and radio equipment to the government.

Hetra Secure Solutions (**X**) sells lots of TEMPEST goodies.

Hewitt Refractories Limited produces Manta, a ceramic material that can be used for shielding.

Hyfral is a French company that specializes in room shielding.

IAM Secure Data Systems (**O**) offers Tempest consulting services.

ILEX Systems sells TEMPEST fax machines and other goodies.

JMK makes a variety of filters (including those of the TEMPEST variety).

Kern Engineering makes TEMPEST backshells for connectors.

Kontron Elektronic is a German company that offers a slick little shielded portable.(**O**)

LCR Electronics makes Tempest filters.

Lindgren-Rayproof is a British company specializing in shielding.

Logical Solutions builds and sells Tempest cables.

Lynwood is a UK supplier of TEMPEST and ruggedized PCs.

Motorola SSTG EMC/TEMPEST Laboratory(**O**) - Arizona testing facility.

NAI Technologies (**X**)(**O**) produces a variety of TEMPEST standard workstations and peripherals.

Nisshinbo is a Japanese company that provides quite a bit of detail on its TEMPEST shielding products.

The DENGY-RITE 20 wideband grid ferrite absorber panels is especially interesting.

P & E Security Analysis - TEMPEST and security consulting. Some good links to government pubs.

Panashield manufactures a variety of shielding enclosures.

Profilon makes a TEMPEST laminate that can be installed over glass.

Pulse Engineering manufactures shielded COMSEC and INFOSEC hardware.

Racal Communications does TEMPEST evaluations.

Radiation Sciences Inc. is a TEMPEST consulting and training firm in Pennsylvania.

Raytheon Systems Company provides TEMPEST testing services (not much detail).

SCI Consulting has done TEMPEST work for clients like the Department of Energy.

Schaffner EMC supplies EMC filtering and testing devices.

Secure Systems Group (SSG) has been around since 1986, providing a variety of TEMPEST computer products.

Security Engineering Services Inc. is a consulting firm that offers TEMPEST courses and other services. The courses are only offered to students who have a security clearance. The interesting thing is the course books appear to be orderable by any U.S. citizen. TEMPEST Hardware Engineering and Design and TEMPEST Program Management and Systems Engineering, with over 800 pages of total material are available for $200.

Seimens makes TEMPEST versions of HP LaserJets and other product.

Shadow Chaser Investigations is a private investigation firm that supposedly does TEMPEST work.

Solar Electronics sells a variety of EMI filters, including TEMPEST specific.

Southwest Research Institute(**O**) (SwRI) performs TEMPEST and other testing.

SystemWare Incorporated is another consulting company that offers TEMPEST consulting. Not much information at this site.

TRW Specialized Services offers TEMPEST testing, both in the lab and field. This site has a nice Acrobat brochure that describes their services.

TSCM Consultant supposedly offers TEMPEST security consulting (page was under construction).

Tecknit is one of the leaders in shielding products. They specialize in architectural shielding (copper coated doors, panels, etc.) and smaller gaskets and screens for electronic devices. A very informative site, with downloadable Acrobat catalogs.

Tempest Inc. has been around for 13 years and produces TEMPEST standard hardware for the government and approved NATO countries. Their catalog isn't online, but as an example they offer an interesting Secure Voice Switching Unit that's used in USG executive aircraft. Not much technical information here.

Turtle Mountain Communications makes a TEMPEST fax device and other communications equipment.

TUV is a British firm that does TEMPEST testing.

Tempest Security Systems - Vendor of Pilkington architectural glass that reduces emanations.

Wang Federal Systems (**O**) also sells TEMPEST rated hardware as well as performs testing. This site contains their product and services catalog. Some good information.

Windermere Group performs government TEMPEST testing.

Veda Inc. (**O**) is a defense contractor who landed a 5.6 million dollar Navy contract for TEMPEST and COMSEC services.

XL Computing is a Florida company with a large catalog of TEMPEST hardware.

ZipperTubing manufactures EMI cable shielding.

There's an interesting EMC-related site that has lots of job listings, many having to deal with TEMPEST. This is a good intelligence source.

A truth in advertising note: Just because a piece of hardware is advertised as "designed to meet NACSIM 5100A" or "designed to meet TEMPEST standards" doesn't mean the device has gone through the rigorous TEMPEST certification process. "Real" TEMPEST hardware will clearly state it has been certified or endorsed.

US Government Information Sources

"The National TEMPEST School (at Lackland Air Force Base - here's a map(**O**)) is responsible for providing training on TEMPEST criteria for installing, designing and testing electronic information processing systems for all U.S. Government departments and agencies, selected non-government agencies, and approved personnel from allied nations." Check out their course listings and schedules (archived here(**O**)). Gee, wonder if I can enroll in a class or two?

Department of Energy (DOE)

The Department of Energy is an extremely security conscious agency. A variety of their documents provide revealing glimpses of TEMPEST procedures.

While not TEMPEST-specific, the DOE's Computer Incident Advisory Capability (CIAC) has an interesting document called CIAC-2304 Vulnerabilities of Facsimile Machines and Digital Copiers (PDF format). In it, TEMPEST threats to FAX machines and copiers are briefly discussed. There are several papers referenced, including:

- DOE 5639.6A, Classified Automated Information System Security Program, July 15, 1994
- DOE M 5639.6A-1, Manual of Security Requirements for the Classified Automated Information System Security Program, July 15, 1994
- DOE 5300.2D, Telecommunications: Emission Security (TEMPEST), August 30, 1993(**O**)

The DOE's Safeguards and Security Central Training Academy also has some relevant classified training courses.

The DOE apparently uses a company called DynCorp(**O**) to perform internal TEMPEST assessments.

Department of Justice

Ricoh supplies TEMPEST shielded FAX machines to the FBI, DEA, and U.S. Marshals Service.

Geological Survey (USGS)

Even the map making folks get involved with TEMPEST. Check out the National Security Information Automated Information Systems section of their manual.

National Institute of Standards and Technology (NIST)

In the 1989 Annual Report of the National Computer System Security and Privacy Advisory Board(**O**), NIST stated that "TEMPEST is of lower priority in the private sector than other INFOSEC issues." It's fairly well known that NIST is influenced by the NSA, so this quote needs to be taken with a grain of salt.

NIST has a list of accredited laboratories) that perform MIL-STD-462 (electromagnetic interference) testing. Some of these also do TEMPEST testing.

While a bit dated (1986), A GUIDELINE ON OFFICE AUTOMATION SECURITY has a few references to TEMPEST, as well as other computer security nuggets.

Brief mention of the Industrial TEMPEST program as well as contacts (may be dated).

National Security Agency (NSA)

The NSA publishes something called the Information Systems Security Products and Services Catalogue (**X**). It contains a list of TEMPEST compliant hardware (as well as other approved security products). The cost of the catalog is $15 for a single copy or $34 for a yearly subscription (four issues). Requests for this document should be addressed directly to:

- The Superintendent of Documents
  U.S. Government Printing Office
  Washington, D.C. 20402

NSA Endorsed TEMPEST Product List part of the NSA's TEMPEST Endorsement Program.

Unfortunately, several of the following classified documents can't be ordered:

- "Tempest Fundamentals", NSA-82-89, NACSIM 5000, National Security Agency, February 1, 1982 (Classified).
- "Guidelines for Facility Design and RED/BLACK Installation, NSA-82-90, NACSIM 5203, National Security Agency, June 30, 1982 (Classified).
- "R.F. Shielded Enclosures for Communications Equipment: General Specification", Specification NSA No. 65-6, National Security Agency Specification, October 30, 1964.
- "Tempest Countermeasures for Facilities Within the United States", National COMSEC Instruction, NACSI 5004, January 1984 (Secret).
- "Tempest Countermeasures for Facilities Outside the United States", National COMSEC Instruction, NACSI 5005, January 1985 (Secret).
- National Security Telecommunications and Information Systems Security Advisory

Memorandum (NSTISSAM) TEMPEST/2-95, RED/BLACK Installation Guidance; 12 December 1995
- NCSC 3 - TEMPEST Glossary (title UNCLASSIFIED; document SECRET)
- NACSEM 5009 - Technical Rational: Basis for Electromagnetic Compromising Emanations limits (title UNCLASSIFIED; document CONFIDENTIAL)
- NTISSI 4002 - Classification Guide for COMSEC Information (title UNCLASSIFIED; document SECRET)
- NACSEM 5904 - Shielded Enclosures (title UNCLASSIFIED; document CONFIDENTIAL)
- NSTISSAM TEMPEST/2-91 - Compromising Emanations Analysis Handbook (title UNCLASSIFIED; document CONFIDENTIAL)
- NACSEM 5108 - Receiver and Amplifier Characteristics Measurement Procedures (title UNCLASSIFIED; document FOR OFFICIAL USE ONLY)

October 25, 1999 - John Young filed a Freedom of Information Act request for TEMPEST-related material on May 18, 1998. The US government denied access to 22 of the 24 requested documents on grounds of secrecy. Parts of the two released documents (NSTISSAM TEMPEST/1-92 - Compromising Emanations Laboratory Test Requirements, Electromagnetics - Appendix A , Table of Contents, Sections 1 - 5, and Sections 6 - 12, Appendix A, Appendices B-M, Distribution List and NSA/CSS Regulation 90-5, Technical Security Program) are now available for review. John has filed an appeal in an attempt to get additional material disclosed.

November 30, 1999 - John Young has acquired more NSA TEMPEST documents. His growing collection now includes NSA Endorsed TEMPEST Products Program, NSA Endorsed TEMPEST Test Services Procedures, and NSA Zoned Equipment Program.

One interesting tidbit in all of this is the use of the codeword TEAPOT - "A short name referring to the investigation, study, and control of intentional compromising emanations (i.e., those that are hostilely induced or provoked) from telecommunications and automated information systems equipment." Who says the NSA doesn't have a sense of humor. TEMPEST, TEAPOT, ha, ha...

Note: John's release was mentioned over at Wired News and Slashdot, so be sure to check for insightful (or amusing) comments there.

State Department

While it's not hard to guess, the State Department uses TEMPEST equipment in foreign embassies. There's a position called a Foreign Service Information Management Technical Specialist - Digital(**O**), that pays between $30,000 to $38,000 a year. The ideal candidate should have a knowledge of TEMPEST standards as well as the ability to repair crypto hardware.

Along with cryptography, the export of TEMPEST standard hardware or devices for suppressing

emanations is restricted by the International Traffic in Arms Regulations (ITAR). However, there is an exception in that: "This definition is not intended to include equipment designed to meet Federal Communications Commission (FCC) commercial electro-magnetic interference standards or equipment designed for health and safety."

Treasury Department

The Treasury Department's Office of Security is mandated with handling TEMPEST and emissions security.

US Military Information Sources

Part of the government's mandate to reduce costs is to make information available online. While the average user doesn't have access to Milnet or Intelink, there are a variety of unclassified, military sources on the Internet that directly or indirectly relate to TEMPEST standards.

Jargon alert. You'll sometimes see references to RED/BLACK systems. A red system is any device that stores or transfers classified data. Black systems store/transfer unclassified data. Gee, with all of the black projects and helicopters around these days, I would have thought it would be the other way around.

U.S. Navy

The Navy seems to be a further ahead then the other services in putting content online, including:

Chapter 16 of the Navy's AUTOMATED INFORMATION SYSTEMS SECURITY GUIDELINES manual is devoted to emanations security (**X**). Probably the most interesting section in this chapter deals with conducting a TEMPEST Vulnerability Assessment Request (TVAR). Completing the TVAR questionnaire provides some common sense clues as to how electronic security could be compromised. (The Navy seems to have pulled this. Try this alternate link.(**O**))

Chapter 21 of the same manual deals with microcomputer security. Section 21.8 Emanations Security, reads: "TEMPEST accreditation must be granted for all microcomputers which will process classified data, prior to actually processing the data. Your security staff should be aware of this and submit the TEMPEST Vulnerability Assessment Request (TVAR) to COMNISCOM. Microcomputers may be able to comply with TEMPEST requirements as a result of a TEMPEST telephone consultation, as permitted by COMNISCOM. Contact the Naval Electronic Security Engineering Center (NESSEC) for further information to arrange a TEMPEST telephone consultation. Use of a secure phone may be required and your request will be followed with written guidance." This leads one to believe that certain PC systems

may not be as susceptible as others to emanations monitoring.

C5293-05 TEMPEST Control Officer Guidebook - "Provides guidance to the individual assigned responsibility for TEMPEST implementation at a major activity." Unfortunately, not online, and likely classified.

NISE East Information Warfare-Protect Systems Engineering Division(Information Warfare-Protect Systems Engineering Division - Code 72) puts on a couple of TEMPEST related training courses, (**O**) including "Tempest Criteria for System/Facility Installation" and "Tempest Fundamentals." These are targeted toward Department of Defense personnel and civilian contractors who must comply with TEMPEST standards as part of their business.

"The Reduction of Radio Noise Emanating from Personal Computers" (**O**) is a thesis topic at the Department of Electrical Engineering, Naval Postgraduate School.

Electromagnetic Environmental Effects. While not security-related, some good background information.

Check out Grumman Aerospace's spiffy TEMPEST building, where they do development work for the Navy on the EA-6B aircraft.

The Navy's INFOSEC site has lots of interesting information. There's even a TEMPEST related services link. Information Warfare (IW) Protect Systems Engineering Division (Code 72) appears to be the key TEMPEST players.

U.S. Air Force

The Air Force Emission Security Program instruction manual (AF Instruction 33-203) has a remarkable amount of information about TEMPEST. My guess is this site won't remain available to the public for very long.

Even though the DoD started shutting down Web sites back in September for security reasons, there is still a tremendous amount of material being made to the general public. Examples that came from Offut Air Force Base these:

- AIR FORCE EMISSION SECURITY PROGRAM (AFI 33-203) (**X**)(**O**) or here(**O**) in case it is pulled
- EMISSION SECURITY ASSESSMENTS (AFSSI 7010) (**X**)(**O**) or here(**O**) in case it is pulled
- EMISSION SECURITY COUNTERMEASURE REVIEWS (AFSSI 7011) (**X**) or here(**O**) in case it is pulled

I really doubt these will be available very long. There is a remarkable amount of detail in these documents.

The Air Force's Rome Laboratory has produced a variety of interesting defense related systems. Some developments likely related to TEMPEST include:

- In 1961 the Electromagnetic Vulnerability Laboratory was established.
- In terms of emanation monitoring, circa 1965 - 70, a Wullenweber antenna(**O**) (called the "elephant's cage") is reputed to have done an excellent job of retrieving stray signals. While hardly a portable device, it does suggest the military was actively pursuing emanation monitoring during this period.
- In 1964, Rome developed the AN/MSM-63 Electromagnetic Measurement Van (no information as to whether it just served a testing function, or could be used for surveillance).
- In June of 1965, RADC a lightweight (350-pound) electromagnetic surveillance antenna was developed that was operationally equivalent or better than systems that were up to ten times larger and heavier. During that same year considerable progress was made in the area of reducing vulnerability to electromagnetic interference. Mr Woodrow W. Everett, Jr. was among personnel recognized for technological improvements in wave guides, electronic tube components, and greater electronic compatibility.

The Air Force is currently engaged in research and development for building TEMPEST shielded vans and command shelters using lightweight composite components.

Other Air Force documents:

- "Ground-based Systems EMP Design Handbook", AFWL-NTYCC-TN-82-2, Air Force Weapons Laboratory, February 1982.
- "Systems Engineering Specification 77-4, 1842 EEG SES 77-4", Air Force Communications Command, January 1980.

Lately the Air Force has developed a program called SATE (Security Awareness Training & Education) that integrates COMSEC, COMPUSEC and EMSEC disciplines.

The 497th Intelligence Group (497 IG), out of Bolling Air Force Base, Washington DC, manages TEMPEST related issues for the Air Force.

U.S. Army

The U.S. Army Information Systems Engineering Command(**O**) is headquartered at Fort Huachuca, Arizona (here's the new link for ISEC, with access password protected). The Fort engages in a variety of spook-related activities. One of the classified documents that is referenced is:

- AR 380-19-1, Control of Compromising Emanations; 4 September 1990

The Army Corps of Engineers released a publication called "Electromagnetic Pulse (EMP) and TEMPEST Protection for Facilities" (**X**) EP1110-3-2, in December 1990 (unclassified). This is a treasure trove of information related to shielding buildings. (Thanks to John Young for digitizing parts of this massive document. It's also available in sections, PDF format, from an Army site.)

The Army Corps of Engineers, Construction Engineering Research Laboratories, has also been experimenting with low cost TEMPEST shielding technologies. Low Cost EMP EMI Tempest Shielding Technology (**O**) fact sheet link doesn't work anymore, but you can get a summary here(**O**).

The Army's White Sands Missile Range has a Test Support Division(**O**) that does TEMPEST testing as well as other things. An interesting photo of the inside and outside of a test truck is shown.

The Army's Blacktail Canyon (**X**) EMI/TEMPEST facility at Ft. Huachuca (spook-related location in Arizona), recently put up a Web page, with lots of interesting info. Also check the main Electronic Proving Ground site (why it is a .com instead of .mil or .gov site I have no idea).

The Army's Protective Design Center in Omaha specializes in structure designs to resist blasts as well as TEMPEST attacks.

Cute, full color illustration of a military TEMPEST secure room.

U.S. Coast Guard

The Coast Guard has a TEMPEST security program(**O**) in their Security Policy and Management Division (G-WKS-5)

Department of Defense

The Department of Defense's Defense Technical Information Center has information regarding the Collaborative Computing Tools Working Group (representatives from private sector and the intelligence and defense communities). The CWG put together some TEMPEST recommendations for video-conferencing products.

From a post to the Cypherpunks list in April of 1994, by Steve Blasingame:

- An overview of TEMPEST can be found in DCA (Defense Communications Agency) Circular 300-95-1, available from your nearest Federal Documents Depository / Government Library. The

section of interest in is Volume 2, DCS Site and Building Information, sections SB4 & SB5, (Grounding,Shielding,HEMP). SB5 though not directly covering RFI/RF Emanation is devoted to shielding for high altitude electromagnetic pulse radiation (HEMP). The documents discuss Earth Electrode Systems, Fault Protection Systems, Lightning Protection Systems, Signal Reference Systems, and RFI containment, they also briefly discusses radio signal containment (TEMPEST) as well. This is a must-read for anyone wishing to keep their bits to themselves. Discussions of testing and validation methods are not discussed in the unclassified documents. I have included the references to the Secret/Classified documents for the sake of completeness. It is possible that some of them are by now de-classified, or may be requested through FOIA.

DA Pamphlet 73-1, Part One, 16 Oct 1992 (DRAFT) (**X**)(**O**) is an obscure document that discusses survivability and mission performance of military systems. The interesting thing in this pamphlet is a fairly detailed description of the military's Blacktail Canyon facility.

Other Defense Department documents:

- MIL-STD-188-124, "Grounding, Bonding, and Shielding for Common Long Haul/Tactical Communication Systems", U.S. Dept. of Defense, June 14, 1978.
- MIL-HDBK-419, "Grounding, Bonding, and Shielding for Electronic Equipments and Facilities", U.S. Dept. of Defense, July 1, 1981.
- "Physical Security Standards for Sensitive Compartmented Information Facilities (SCIF), Manual No. 50-3 Defense Intelligence Agency (For Official Use Only), May 2, 1980.
- "Design Practices for High Altitude Electromagnetic Pulse (HEMP) Protection", Defense Communications Agency, June 1981.
- "EMP Engineering Practices Handbook", NATO File No. 1460-2, October 1977

Some interesting FOIA Star Wars program computer security requirements, including a TEMPEST separation table.

December 4, 1999 - John Young has found an excellent source for non-classified, military TEMPEST information. The Defense Automated Printing Service has a searchable Web database devoted to military specifications and standards (from nukes to nylons). John reports some of the handbooks and standards contain information the NSA removed from documents that were recently released to him under the FOIA. Here are some of the TEMPEST-related gems. Just enter a title and submit.

MIL-HDBK-232 - Red/Black Engineering-Installation Guidelines
MIL-HDBK-411A - Long Haul Communications (DCS), Power and Environmental Control for Physical Plant, MIL-HDBK-419 - Grounding, Bonding, and Shielding for Electronic Equipments and Facilities
MIL-HDBK-1195 - Radio Frequency Shielded Enclosures
MIL-STD-188-124 - Grounding, Bonding, and Shielding for Common Long Haul/Tactical Communications Systems
MIL-STD-285 - Attenuation Measurement for Enclosures, Electromagnetic Shielding, for Electronic

Test Purposes, Method of
MIL-STD-461E - (Replaces previous 461 and 462) Electromagnetic Interference Characteristics

Warning: These are huge PDF files, so have lots of bandwidth available. Also, if you're interested in these documents, you might want to get them now. There's no telling if and when the DoD might decide to shut down this open source site.

Other Countries

The US isn't the only one playing the TEMPEST game. Here's some additional sources from various countries.

Australia

A brief defense document on emanation security.

Canada

COMMUNICATIONS SECURITY ESTABLISHMENT PUBLICATIONS

- COMSEC Installation Planning (TEMPEST Guidance and Criteria) (CID/09/7A), 1983, (English only)(Confidential)
- Criteria for the Design, Fabrication, Supply, Installation and Acceptance Testing of Walk- In Radio Frequency Shielded Enclosures (CID/09/12A)(Unclassified)

European Commission

I love it when governments can't keep their acronyms/codewords straight. There is an official TEMPEST testing lab, but TEMPEST stands for Thermal, Electromagnetic & Physical Equipment Stress Testing and deals with devices used in animal tagging. Sheesh...

France

The French information security service (SCSSI) has a large amount of information devoted to TEMPEST. Have BabelFish or your favorite translator ready.

UK

The British Central Computer and Telecommunications Agency(**O**) publishes a variety of computer

security titles including:

- TEMPEST: The Risk (Restricted) CCTA Library 0 946683 22 0 1989

Last changed December 25, 2001

back to main TEMPEST

The Complete, Unofficial TEMPEST Information Page

This page is about surveillance technology. If a search engine mistakenly led you here, try **Shakespeare**, **Pontiacs**, or **Arcade Games**.

THIS PAGE IS NO LONGER BEING UPDATED AND IS LEFT UP FOR ARCHIVAL PURPOSES.

~~TEMPEST/RF/EMI Help Wanted Ads~~

~~Are you a company, agency, or recruiter looking for an engineer with TEMPEST/RFI/EMI experience? I get requests every now and then for such folks, and decided to add this section to the site. A few ground rules:~~

- ~~Ads should be **no longer than a paragraph**, please include **contact information**.~~
- ~~If you **fill a position**, let me know so I can remove the ad.~~
- ~~**Engineers** - If you contact a recruiter or HR person about an ad, let he or she know **you saw it here**.~~
- ~~I take **no** responsibility for the legitimacy or accuracy of the ads.~~
- ~~This service is **free**. (However if it becomes wildly successful, I reserve the right to figure out some type of compensation for helping place people.)~~

EMI/Tempest Engineer Needed - February 22, 2002

We are an executive recruiting and placement firm and have a client that needs an EMI/Tempest engineer. This busy and growing company is in the aerospace industry and manufactures various enclosures that are constructed under EMI/Tempest requirements. The company needs an engineer that is familiar with designing and testing structures under the EMI/Tempest guidelines. The candidate must have at least a BS in electrical engineering or physics and 5 to 10 years involved with EM/Tempest and 5 years in the aerospace industry is preferred. Please contact John Canaan if you are qualified and interested in this position. MR of Stones River, phone 615-494-1333/ FAX 615-494-1372, john@mristonesriver.com.

Senior RF Engineer - April 5, 2003

A worldwide leader in Information Technology, Intelligence services, Engineering and Logistics, Modeling and Simulation and Network Solutions, is currently seeking talented RF Engineers to join our team in Northern Virginia.

Responsibilities include supporting our customer in the development of RF Signal Intelligence (SIGINT) systems including the design, evaluation, development, integration, testing and fielding of SIGINT sensors and systems; evaluation of COTS products for incorporation into SIGINT systems platforms and applications; and, the development of special purpose RF devices e.g. RF front ends, amplifiers, preamps, and antennas.

Positions may require some CONUS and OCONUS travel.

Requirements include a relevant technical degree (or the equivalent work experience), and a minimum of 5 years demonstrated work experience. A current Top Secret ISSA Poly security clearance is essential.

If this is of interest, please email your full resume to me in
Word format, and give me a call.

Lynn Rodens
MRI of BWI
lynn@recruitergurus.com
410-712-0770

Last changed April 5, 2003

back to main TEMPEST

The Complete, Unofficial TEMPEST Information Page

This page is about surveillance technology. If a search engine mistakenly led you here, try **Shakespeare**, **Pontiacs**, or **Arcade Games**.

THIS PAGE IS NO LONGER BEING UPDATED AND IS LEFT UP FOR ARCHIVAL PURPOSES.

Miscellaneous TEMPEST

Used TEMPEST

TEMPEST shielded computer equipment sometimes leaks out into the public in the form of surplus and scrap sales. This section is devoted to descriptions.

One informant used to work at a Defense Reutilization and Marketing Office (DRMOs are the DoD's version of a garage sale). In the past, TEMPEST equipment was de-miled (crushed), now due to miscoding and classification downgrades, TEMPEST equipment is literally a dime a dozen. Computer surplus goodies go for about 12 cents a pound.

Through a contractual association with a major defense company, Fluid Forming Technologies has been assigned to dispose of a TEMPEST level "secured working environment." Modular construction, 160' x 20' x 10', can probably be segmented into smaller units. Available as of January 1, 1998. E-mail fftllc@eci.com for additional details or snail mail:

> Fluid Forming Technologies LLC,
> 9 Brush Hill Rd, Suite 318
> New Fairfield, CT 06812

JC describes two shielded IBM PC cases he picked up from a scrap dealer for $35 each (unfortunately

they had already sold the printers and monitors). The cases were labeled EMR XT SYSTEM UNIT (on the front), with a model number of 4455 1 (on the back). The cases are similar to a standard IBM XT case, except deeper toward the back, so a filter bank and power supply baffle could be installed. The top is bolted down, requiring an allen wrench to remove. The top part of the case has a gasket groove for the brass colored RF gasket, and the mating surface is a finished in anodized aluminum. The top appears to be a cast aluminum plate. Each of the ports in the rear has a filter, unused ports have a metal blocking cover that mates to the case and make a good eletrical contact.

W.J. Ford Surplus Enterprises(**O**) had the following printer for sale in December 1996:

LASER PRINTER Make:MITEK Model:100T 300 X 300 DPI LASER PRINTER WITH LETTER SIZE PAPER TRAY, 8 PPM, MEETS NACSIM TEMPEST SPECS, C.W. OWNER'S MANUAL (TONER CARTRIDGE NOT INCL.) Dimensions: 19.00"w x 16.00"h x 16.50"d 1.00 on hand, No Graphic on file, Item No.:1208 RAMP Price: $ 250.00

As of February 8, 1997, Dark Tangent (of DEFCON fame) has a whole collection of TEMPEST shielded equipment for sale. Check out his page (**X**) for complete info and photos. Lots of great details and specs. Also a related Slashdot thread.

As of June 15, 1998, Hugh Sebra had fifty TEMPEST-shielded Fibercom 7197 DPT Dual Path Fiberoptic Transceivers for sale.

While not for sale, H. Layer has a photo of a circa 1986 Tempest Macintosh as his cool Mind Museum page.

Note: I personally don't own or have access to any surplus TEMPEST equipment. However, if you've encountered such hardware, let me know about it.

Tales of the TEMPEST

Recent publicity about this page has resulted in some interesting personal accounts dealing with TEMPEST-related topics. This section lists excerpts from various correspondence. In most cases, the names have been removed to protect the innocent.

C writes:

> Interesting page of TEMPEST-related stuff. One additional information source you may want to include for those attempting to proof themselves against an EME-type attack

might be the ARRL (Amateur Radio Relay League) Handbook for the Radio Amateur. It has a very complete chapter on preventing radio interference caused by ham radio gear, much of which could be adapted for use with a computer. The book is updated yearly, so the information is usually top-notch. Most libraries have it.

BTW, for those on the other side of the question (or who wish to be) there's probably enough info in the book to help them put together a TEMPEST monitoring outfit if they're handy with a soldering iron.

F writes:

I have an early SVGA 15" Gateway CrystalScan monitor (the ones that are purported to be part of a class-action lawsuit), which, when attached to a Mac, will display *exact* and *readable* text on TVs within a reasonable distance--a measured 60-plus feet for sure, through walls and floors, and quite possibly more, I didn't have the inclination to drag a TV out into the lot on an extension cord to find out how far I could go.

Though it is only readable during the 'dark' between commercials on certain channels, it was a pretty frightening revelation, as I accept and produce some pretty sensitive materials. The scarier part for me was that I had used it for weeks before I finally turned on a TV at the same time that the monitor was not in screen-saver mode (a password-protected mode I generally drop into anytime I leave the desk, alone in the building or not). Anyone in my building, including unassociated neighbors, or anyone within whatever the ultimate range might have been could have seen a bunch of stuff that could have caused serious damage to my firm. If anyone did see anything, they haven't bit me with it--yet.

In addition to displaying readable text, you can also discern images to a limited degree, and I imagine with some simple tweaks of the color guns, some enterprising cracker could get some pretty good imaging.

The monitor has some other more obvious side effects, such as emitting such EMF levels as to *seriously* distort any monitor within about a foot of its left side, and about two feet of its right side. It also gave me frequent eye strain if I used it too long (even though the picture was incredibly sharp for its class).

Since I'm a MacHead and use multiple monitors (three to seven screens, depending on where I am), this situation was unacceptable all by itself, but I was using the monitor ($15 at a local thrift store) as a temporary display while my prime screen was off in warranty land (I never did get that one back).

It will also emit such a frequency as to produce varied-intensity scrolling vertical and

horizontal lines on a TV with either rabbit ears or hooked up via 75 Ohm cable to an attic antennae, depending on what channel you are tuned to. I can't recall the exact per-channel results, but (if memory serves) it was minor (but annoying) lines and rolls on the lower VHF, and major interference and ghosting with the readable text on the UHF.

The funny thing is, other people in the building couldn't watch TV without all the serious distortion any time the monitor was not in screen saver mode (just having the monitor powered at all would produce a limited interference), and never noted any readable text, because they avoided the badly affected channels. When they would ask me to look at the TV situation and prescribe a fix (I'm the boss and building owner) , I never saw it, because (of course) I put the monitor to sleep before I would venture out for an inspection. Talk about Keystone Kops! They would joke that the TV was afraid to not be working properly when the boss was present, and we just wrote it off to rogue cell phone or CB users, because our portable phones and computer speakers would frequently pick up passing car/ truck audio signals from such devices.

(Yet another bonus was that the staff wasn't prone to hang out in the break room and watch TV anytime I was working)

I'd have never discovered the source of the whole thing, save for a Sunday when I came into get some computer backups and volume house-cleaning done, and I dragged in a little B&W TV to also "watch" the football game. I was going mad trying to get any decent reception at all that close to the damn thing, not noting for at least a couple of events that it cleared up substantially when the screen went into an idle screen saver mode on its own. I finally gave up and settled for just audio, and only noted the relation hours later when I powered off the monitor to rearrange my desk. A couple of on-off clicks later, I started laughing, finally finding the source of all the problems for the whole building--that is until a commercial pause came on, and I saw the contents of my open-folder list displayed on the screen.

I goofed around for the next sixty minutes, trying desperately to discern what I could see in that momentary darkness between commercials, and in those brief moments, I found that I could *easily* read my email, word docs, spreadsheets, database, etc., and I could repeat the ability on every TV screen in every room on every floor to which I had access--Eeek!

Anyway, this note got a lot longer than I wanted, but I still have the monitor, if it holds any interest to you as a "primary source" of the fact that an SVGA can most definitely be a victim of low-cost TEMPEST (albeit an admittedly and likely rare event on only one monitor I can name).

M writes:

"LCD displays on laptops eliminate the risks of TEMPEST attack."

No way. I get a few channels in my apartment via rabbit-ear and UHF loop antenna reception - they're pretty weak, but on a good day and in the absence of major interference, I can watch Ally McBeal. I'm also a longtime notebook computer user, mostly Apple Powerbooks. The TFT LCD screen specifically interferes with the lower-numbered VHF channels on my TV, which also happen to be more poorly propagated at my location. The CPU and motherboard also interfere, but the screen is by far the worst and can't be within twenty feet and/or two interior walls of the antennae without substantial, patterned interference. And this is a low-power laptop with a relatively small 10" screen (800x600, 60Hz refresh), using under seven watts including the 180MHz CPU. Shutting off the screen independently of the rest of the machine greatly reduces the interference.

That doesn't mean that there's intelligible information in all that noise, of course, but given that I can change the appearance of the interference by changing the onscreen display, I'd be willing to bet that there is. It's also worthwhile to note that conventionally (greyscale) anti-aliased fonts look horrible on crisp LCD screens because there's none of the natural inaccuracy and softening that a CRT produces (in other situations this is a good thing and reduces eyestrain, the main reason I don't use CRTs any more). This includes the filtered ones your page links to (I'm looking at them now). There is a different mode of anti-aliasing that makes use of the slight RGB offset on an LCD display (one of the few real innovations to come out of Microsoft, of all places), which might be applied to this purpose. Unfortunately one has to use different fonts depending on whether the screen elements are arranged RGB or BGR (both exist at the moment, in approximately equal proportion).

S writes:

In a (government) security briefing, I did witness a legitimate Tempest intercept of an IBM Selectric typewriter. However, the typewriter had been modified to produce unusually high levels of signals, the distance over which the intercept occurred was fairly short, and the conductors of the demo insisted all other potential sources of emanations be powered down in the area where the demo was conducted.

While my time with the government (Secret Service and Naval Intelligence) did not deal directly with Tempest intercept or screening, the general consensus, even in the most sensitive circles, was that there were far easier, effective and more efficient methods of gathering information. At one time the threat was taken seriously, but not anymore.

Just think, in an average office or even modern home environment, how many sources of radiation there are, and how difficult it would be to target one and one only. Remember

the strength of a field decreases with the square of the distance. Your wristwatch at close range produces a stronger signal than a large CRT the other side of the room.

In the early days, before every cigarette lighter and toaster over contained a microprocessor, and CRT technology was not refined, there may have been a threat. Anymore, CRTs operate at much lower levels and the RF/EMI environment is much busier. Remember when we were young and televisions came with warnings about sitting too close? Do you see those anymore, even on large color screens? Far less energy now is needed to excite the extremely efficient phosphors in the CRT. In the early days, it was done with brute force.

It's fun to talk about, but from a practical level I believe there no longer is a threat.

I have never seen a real world demo of a genuine Tempest/Van Eck intercept, and I have been around some. The alleged construction articles leave themselves an out, like saying a lot of experimenting is needed to fine tune or whatever. Sort of like the chemical formulas with a line buried deep "then a miracle occurs".

V writes:

I read your web page on TEMPEST with quite some interest. I've always wondered about the truth in all the stuff we hear about the US military over here in Australia. i found your web site very interesting and informative.

Once upon a time, I owned an Apple][c and a matching hi-res "green-screen". ow the cable for this monitor was a bit shorter than I wanted it to be, particularly, I wanted to be able to sit the computer/keyboard on my lap while I typed or played Star Blazer (I still do, although it's now a $250 Wang keyboard). I found that with a pair of very primitive antennas, I could easily make the computer communicate wirelessly with the monitor. Text was quite readable in 80-column mode. This led me to experiment further, and I soon had a wireless link to the TV, using the Apple][RF modulator with no antenna, and a loop of ribbon cable attached to my TV. The picture came through in full colour.

Somewhat later, I began to become interested in intercepting data signals. I found that with a fairly high-tech receiver, I could intercept RS232 transmissions, as long as it was only a half-duplex link. If both parties transmitted at once, the data got garbled. This was done with a very sensitive antenna and radio receiver, and a lot of signal processing circuitry. It also only worked over a range of about 1.5m.

That was the only one of my interception experiments that succeeded. however, I wonder if there aren't other busses that can have their data intercepted more easily, now. USB and FireWire are both serial busses. Perhaps if I tried, I could capture data from these busses

and record it for later replay. And what about Ethernet? 100baseT would be and ideal standard for clean emission of data. i wonder if anyone has tried to pick up packets? I doubt it would be difficult. It's just a fancy multimaster serial bus.

Once upon a time, all microprocessor-based devices from the USA bore the following notice, or something similar. It varied from device to device (copied from an Apple 400k floppy drive c. 1986):

Certified to comply with the limits
for a Class B computing device pur-
suant to Subpart J of part 15 of FCC
Rules. See instructions if interfer-
ence to radio reception is suspected.

Several years ago, the notice was changed to the following (copied from a Texas Instruments TI-82 graphing calculator, c. 1991):

THIS DEVICE COMPLIES WITH PART 15 OF THE FCC RULES.
OPERATION IS SUBJECT TO THE FOLLOWING TWO CONDITIONS:
(1) THIS DEVICE MAY NOT CAUSE HARMFUL INTERFERENCE, AND
(2) THIS DEVICE MUST ACCEPT ANY INTERFERENCE RECEIVED,
INCLUDING INTERFERENCE THAT MAY CAUSE UNDESIRED
OPERATION.

This new notice is the same on every device I've seen. No variations. Why this change? The original notice seemed sensible enough, it basically says the device has to be well-behaved and not cause too much interference to any other devices. The second seems to be a license for the US government to remote control your computer or whatever else.

Here in Australia, we now have this C-tick certification scheme. For an electronic device to be sold in Australia, it has to meet ridiculously stringent emission and interference standards. They place it in an EM-shielded room, and blast it with radiation from every part of the RF spectrum, and if it misses a beat, then it fails the test. Then they measure its own emissions. They have to be very low to pass. A lot of manufacturers are opposed to these strict regulations. However, it strikes me that it's probably very hard to do a TEMPEST or NONSTOP attack on a device that meets C-tick standards.

D writes:

I used to be a "Robot Killer" (high tech military scrap) and we used to keep funny named gear around for humor and one of our favorates was a 19" rack mount "Vortex Tempest Generator" with a small crt for lidiuios(sic) paterns and minute time delay, sweep, and odd

controls. Always wondered what it was and now, thanks to your amazing page I think that it isn't for testing the airflows off of wingtips, I never did, it came with some of the finest Mil-Spec electronics I ever disasembled, and was elegantly manufactured and the batch it came with was transmission/radio/rtty/ stuff. we would also see many super shielded Computers and P/C s (Many Zieniths!) and other compleatly mysterious and sometimes untouched techno-dukey. I could (and sometimes do) go on about all the strange gear that floated thru the shop.

Non-TEMPEST computer surveillance

In researching TEMPEST topics, sometimes I run into little-known tidbits that relate to possible computer surveillance techniques.

Infrared Ports

The Department of Energy Information Systems Security Plan has an interesting section titled, 8.5 Wireless Communications (Infrared Ports). It states:

"The use of wireless communications (infrared) ports found on most PPCs to interface with printers and other peripheral devices is strictly forbidden when processing classified information. These ports must be disabled on all accredited PPCs and peripherals by covering the window with a numbered security seal or physically removing the infrared transmitter."

Change Log

12/17/96 - original document
12/18/96 - added link to van Eck follow-up article, shielding comments
12/21/96 - reorganization and additional comments about Rome Lab, ZONE, DOE, non-TEMPEST
12/22/96 - added Smulders paper
01/02/97 - added Compliance Engineering, additional NIST, Navy, Canada, Used, and paper sources
01/08/97 - added UK, patents
01/11/97 - added DA Pamphlet 73-1/Blacktail test facility, Army, COMPUTERWOCHE, EMC, HAL, Austest, Racal, Compucat, Nisshinbo
02/02/97 - added Naval Postgraduate School, EMC FAQ, DynCorp, Conductive Coatings, GEC Marconi, CorCom, AFC, Corps of Engineers, Ford Surplus, GTE, ECM job list, White Sands, Cortron, SwRI, Veda, Emcon
02/14/97 - added DEFCON goodies to Used
02/18/97 - added Redefining Security report, Lynwood

03/10/97 - added Datastop glass to shielding section
03/21/97 - added Moller paper (from Phrack 44)
03/26/97 - added Army Corps of Engineers pub, Elfinco, recommended Xs
04/12/97 - added Computerwoche translation
06/09/97 - added Blacktail page, Framatome Connectors International
07/02/97 - added JMK
12/15/97 - added LCR, Logical Solutions, IAM, GSGC, Tempest Mac
02/08/98 - added Anderson & Kuhn paper, FFTLLC, dead link check
03/03/98 - added Army EMP, Compunetix, XL Computing
03/30/98 - added USGS, Motorola, Tempest Security Systems
11/14/98 - added EMP-tronic, SSG, Filter Networks, Australia section, Braden, Hewitt, TUV, Windermere, ERS, ADI, ZipperTubing, Army EPG, Glenair, Allied Signal, D2D, Truthnet, EC, Hyfral, Navy E3 and other, BEMA, Raytheon, Shadow Chaser, Dina, ATSC, Profilon, EYP, CSS, ILEX, DOE 5300, Cycomm, Murphy paper, Cryptek, Greco, Lindgren-Rayproof, Turtle Mt., Kern, Cabrac, Solar Electronics, National TEMPEST school, Air Force 33-203, HIJACK/NONSTOP
11/17/98 - added Gabrielson papers, SJM News article, Pulse Eng, US Coast Guard, DRMO, c't article, Chomerics, JY FOIA
11/19/98 - Air Force van, EMSEC, Air Force sec mems, new HIJACK & NONSTOP info
11/25/98 - anti-TEMPEST fonts link, alt Air Force links, Schwartau .WAV speech
7/3/99 - Computer Security Solutions, TSCM consultant, student paper, Seimens, P&E, SATE, dead links
7/11/99 -iDefense TEMPEST bust, Acronym Finder
7/19/99 - Hetra, updated DefCon page, Slashdot article
8/19/99 - Gabrielson piece, DEMCOM
8/21/99 - Durak CPU, Mueller HIP
10/10/99 - ISEC update, 497 IG, Treasury, NRO, Star Wars, Navy Code 72, COS, Koops, Army PDC, c't articles
10/24/99- John Young FOIA news
10/25/99 - more JYA FOIA, added new NSA docs referenced in FOIA, DOJ, patent, slashdot/wired
11/7/99 - Final JYA, Jones, Koops summary, Tales, Web tracking
11/8/99 - New Scientist
11/13/99 - SET21
11/15/99 - Jones stuff
11/30/99 - More JYA
12/4/99 - DoD DB
8/2/00 - JYA news, Consumertronics address change, general organizational stuff
8/11/00 - WSJ/Forbes, JYA update, search engine links to other TEMPEST stuff
10/2/00 - Uncategorized stuff at the top
11/30/00 - More Uncategorized stuff at the top
12/6/00 - Site reorganization, CNet Fed tap
12/10/00 - JYA timeline, SCSSI, revised dtic links, Blacktail logo
12/30/00 - JYA NSA FOIA docs
1/1/01 - More JYA FOIA
1/14/01-JYA NONSTOP

12/25/01 - final update (missed listing some during the course of the year)
2/22/02 - site is back, Help Wanted section, SpyKing
2/25/02 - TinFoil Hat Linux

Special thanks to John Young for his relentless pursuit of information and archival prowess - see his Cryptome site for additional crypto/government/privacy/security/etc. information.

Last changed February 25, 2002

back to main TEMPEST

"Agent Hammer's" English Translation of Robin Lobel's TEMPEST paper

Note from the translator: "I just don't have a mastery of the English words and don't know this stuff well enough to make them up. I think you will be able to decipher my crazed translation though. It doesn't look like they got all that they wanted out of their experiment...rather they weren't able to finish it. I get the impression they had to turn in their report before they were done. Its clear to me that these were students in a professional technical high school/ community college type setting."

Introduction:

1. Definition and basic information

When an electronic device is used, it sends out electronic waves that can stretch several meters out into the surrounding environment. When these waves are captured, they can be used to reproduce the information contained within them. These waves are called “jeopardizing waves” because they put the information that is contained within them into jeopardy. This is true for all kinds of electronic devices. These waves can theoretically be captured and allow us to read even the most secretive information. Nevertheless, the amplitude of the waves diminish quickly, making it difficult to capture them for more than a few centimeters from the initial signal, thus it is difficult to capture signals from most devices. Computer screens, however, send out signals 500 times stronger than the initial image the video card sends out, thereby sending out waves at a an amplitude strong enough to easily capture them.

2. Proof that the phenomenon exists

If a computer screen is plugged into a central unit with a non-reinforced cable, an echo effect will take place as well as a delayed reproduction of the original image on the computer screen. The cord acts as a receiving antenna, capturing the waves from the antenna and transforms them into electronic waves sent to the screen.

3. Objective

The objective of this report is to prove that the phenomenon of “jeopardy” exists, and to attempt to understand under what conditions and at what cost it is possible to reproduce images on a computer screen

I. History of TEMPEST

A historical summary of TEMPEST is presented. They summarize how and when Tempest began, previous names of what is currently called TEMPEST and discuss attempts to get declassified information about TEMPEST. Most attempts have failed to produce satisfactory results. The latest attempt in 1999 produced severely censored documents about TEMPEST. There is very little detailed information available about this system.

II. Theory of Screens

1. Deconstruction of an image

All colors can be broken down into three fundamental colors: red, green and blue. Using variations of intensities in the combinations of these colors, any other color can be created. An image is considered a complex assembly of colors through the use of a pattern of “pixels”. A pixel is a point composed of three colors, red, green and blue. By increasing the density of pixels in a single area, it is possible to recreate accurate images. The resolution of an image is represented by the formula X*Y with X being the number of horizontal pixels and Y being the number of vertical pixels (ex: 640*800, 800*600, 1024*768…)

2. Reproduction of an image on a screen

A screen is composed of several modules. The cathode tube is what reproduces the actual image. An electron beam scans a fluorescent layer at an extremely high speed, 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 sends out a light. This layer also becomes phosphorescent in that it continues to send out a light after its initial stimulation for approximately 10-20 ms. Its brightness is determined by the debit in the electrons, which is regulated by a “wehlnet”. The beam then passes through two bobbins that determine its trajectory through electromagnetic forces, and an image is then scanned onto the screen.

3. Coding of the video signal

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 synchronization channels for the horizontal and vertical scanning and the communal mass of synchronization signals. The synchro signals are simply the difference in a few voltage potentials. They take place 70 times per second for vertical synch (for a 800*600 resolution screen cooling at 70 Hz) and 70*600=42000 times per second for horizontal synch.

Video signals are at a voltage of 0 V to .7 V, which defines the brightness at the point where the scanning takes place (this voltage tends to change depending on each new pixel color. For an 800*600 res screen with a cooling of 70 Hz, the changes in voltage can go all the way to a frequency of 800*600*70= 34MHz, or 34 000 000 times per second).

III. Theoretical Expansion on Circuits

1. Circuit Demands

Earlier, we learned about the nature of the electrical signals that, through amplification, drive an image toward a screen. As a result of this amplification, the“jeopardy waves” that we are attempting to capture, are created.

For every difference in potential that is created at the exit of the amp circuit, an electromagnetic wave of proportional amplitude is emitted. The amplitude of this wave diminishes as the electromagnetic energy spreads across the front of the spherical wave.

(graph)

An oscilloscope shows us that the image on the right is deformed by the absorption of the wave linked to the horizontal synchronization signal (center); note that the signal oscillates on the y-axis because of disturbances in the supply. We want to capture the video signal at left.

Based upon what we have demonstrated earlier, this image is not directly exploitable on a screen because we need a positive signal whose voltage is between 0 V and .7 V.

The solution must allow us to cancel out the signal created by the synchronization signal and the supply while amplifying the signal.

2. Signal filtering

In an effort to eliminate parasitic signals, we create an open (???) circuit between the receiving antenna and the screen. There are two types of circuits, high band and low band, which will allow high and low frequencies through them. In our case, we need a high band circuit because the video signals (several 10’s of MHz) are higher than the synchronization signals (several 10’s of KHz for horizontal synchronizations).

Drawing

The drawing, through the use of a condenser and resistance, creates a high band filter.

Essentially, all signals can be considered as the sum of the sinusoidal signals. Consequently, the high band filter can “suppress” the components whose frequencies are less than the frequency of the breaker (??).

When the high band filter is exposed to a sinusoidal voltage (tension), the condenser takes a charge. Then, when the sinusoid changes variation and direction (??), the condenser discharges. However, if the voltage period is superior to the charging period, the condenser will react like a circuit breaker and impedes the signal’s passage. One can vary the frequency of the breaker by adjusting the values of “C” and “R”. Suppose $\tau=RC$. If τ increases, the charging period on the condenser increases and therefore the frequency of the breaker diminishes.

On can deduct from this that the frequency of the breaker f_c is inversely proportional to τ=RC. We then have:

$$f_c = 1/2\pi RC$$

One can then deduct how the voltage will appear as it exits the device relative to the voltage as it enters the device.

If the frequency at entry f_e is higher than the frequency of the breaker, the condenser takes a positive charge then a negative charge. On can thus write the equation of the voltage at the circuit terminals RC:

$$U_s = \sin(f_e t).(1-e^{-t/\tau})$$

On can therefore trace the voltage at the circuit terminals RC relative to the frequency of the voltage at entry.

(Graph)

As such, if the voltage at entry is the sum of two (or more) signals, one of which is higher in frequency than the breaker and the other of which is lower than the breaker frequency, all that will emerge will be the frequency signals that are higher than those of the breaker:

Graph

One notes that the exiting signal (yellow) is "almost" the same as the frequency signals that are higher than the breaker signal (blue). It is slightly deformed. In green, the entry signal – the sum of two different frequency signals

3. Amplification

To have an exploitable signal, we need a signal that is between 0V and .7V. It must therefore be amplified, but the proportion of the difference between signals must be preserved. To do this, we must therefore multiply the voltage exiting from the RC circuit by a factor of k. For this, we chose to use a circuit based on an Operational Amplifier (O.A.), referred to as an "inverser".

Drawing

An inverser circuit that amplifies the entry voltage by a factor of k

In such a circuit, we see that Ohm's Law applies to the resistance R_2. This then reduces the voltage entering the operational amplifier; the voltage U_r is therefore less than Voltage U_e. The Voltage U_s is therefore proportional to the value of the resistance R_2. The resistance R_3 is in diversion with the OA; the more its value increases, the less current will cross it and therefore more current will cross the OA, knowing that $i_1 < i_2$. On deducts from this that the exit voltage is proportional to the value of R_3's resistance.

One notices that the set up is reversed (entry on the negative terminal and grounding on the positive terminal). The exit signal is therefore multiplied by a negative coefficient, hence one can deduct that:

$$K = - R_3 / R_2$$

By regulating the values of R_2 and R_3, we are able to vary the voltage at the terminals of entry on the Operational Amplifier. The OA will then multiply the voltage of the entry signal (through stable feeding from the V+ and V- terminals).

4. Synchronizing of Signals

The recuperated signals are de-synchronized. The screen cannot therefore recreate coherent images. We must then, send artificial synchronization to the screen. To do so, we can use two methods:

- Generate a signal with the use of two GBF (one for the horizontal synchro, the other for the vertical)

- Capture signals emitted by the graphic card in a functioning computer

The first option appears to be most appropriate because it allows for changes in order to adapt the synchro signals to the received signals.

5. Expected Results

Because of the fact that a wave is only emitted for each different voltage in the screen, the obtained image cannot be an exact replica of the first image. But it will allow access to the information posted on the original screen. In theory, one would obtain an image something like this:

Picture

IV. Experiment

1. Choice of values for the high band:

As we saw earlier, we would like to eliminate the effects of the synchro signals. These signals repeat themselves at a frequency of around 70*600 = 42KHz (for a screen of 800*600*70Hz, taking into account the horizontal synchronization). We choose a slightly higher value for the breaker frequency of f_c to assure a margin of safety and eliminate a maximum number of parasites. One therefore chooses a neighboring breaker frequency of 160 KHz:

$$f_c = 1/2\pi RC$$

$$RC = 1/2\pi f_c$$

$$RC = 1/2\pi.160000$$

$$RC = 10^{-6} \text{ s}$$

We must therefore choose an RC relationship around 10^{-6}s. At this point, the condensers represent their maximum values in micro Farad (μF). The resistance employed must therefore be represented by a kilo Ohm (kΩ).

2. Choices for amplification values

    a. Choice of Operational Amplifier models:

For our experiment, we need an operational amplifier capable of supporting significant frequencies nearing 50MHz. To be safe, we have chosen an OA that can handle closer to 60 MHz. We are therefore in the realm of OA's that are uniquely created for video production. The model we selected is the AD844AN. This model needs a stable feeding of 5V and a maximum voltage entry of 5 μV.

    b. Choice of resistance values

Our Operational Amplifier choice necessitates strong resistance values such that the entry voltage can be 5 μV. To obtain such a large resistance value, we assert the following:

A voltage is a difference in electrical states, or the difference between two potentials. The weaker the gap, the weaker the voltage!

Drawing

Our goal is to choose a resistance that allows us to have a voltage between 3 and 5μV. The wire on the positive terminal is connected to the ground. Its potential is therefore zero. We will therefore need a potential of 5μV from the wire on the negative terminal. This value is extremely weak near an entry potential (about .1V). When adding a large resistance, we obtain a strong voltage at the resistance terminal (Ohm's law) and therefore a weak potential at the lesser terminal. We will therefore choose a resistance variable, R_2, of 1 Ω (Ohm).

We witnessed the amplification relationship earlier. Knowing that we want to amplify in a block of 1 to 100, we will need a resistance, R_3, somewhere between 10 and 100 Ω.

Photo

The original signal (green, -3V) and after amplification (+5V).

V. Results

At the point of writing this thesis, our experiment has not yet been completed (although we do have all the necessary components to make it happen).

Our most encouraging results that we have obtains thus far are below:

2 Photo

The original image is on the left. At right the 2 central pics, captured electro magnetically, correspond to the beginning and end of the white band.

The signal on the right was obtained thanks to a high frequency filter, which demonstrates its effectiveness. We now have simply to amplify this signal and transmit it to a second screen that we will synchronize with the help of 2 GBF's to create a ghost image, similar to the original image.

We had several problems with the operational amplifier (most notably the resistance) but these were eventually resolved (as is evidenced by the image on the previous page.

back