GIAC
CERTIFICATIONS

Global Information Assurance Certification Paper

Copyright SANS Institute
Author Retains Full Rights

This paper is taken from the GIAC directory of certified professionals. Reposting is not permited without express written permission.

Interested in learning more?

Check out the list of upcoming events offering
"Security Essentials (Security 401)"
at http://www.giac.org/registration/gsec

An Introduction to TEMPEST

For many years, TEMPEST was shrouded in secrecy. Government documents concerned with this were classified, which obviously gave rise to many speculative theories.

During the 1950s, the U.S. government became concerned that "compromising emanations" from computers could be captured and then reconstructed. Compromising emanations are defined as unintentional intelligence-bearing signals which, if intercepted and analyzed, disclose the classified information transmitted. Research showed that it was possible to capture emanations from a distance, and as a response, the TEMPEST program was started.

In his 1986 book, Spycatcher, Peter Wright (ex-MI5) revealed how he had spied on messages sent by the French during Britain's negotiations to join the European Economic Community. In 1960, Britain was negotiating to join the EEC, and the Prime Minister was worried that De Gaulle would block Britain's entry. He therefore asked the intelligence community to determine the French negotiating position. They tried to break the French diplomatic cipher and failed. However, Wright and his assistant noticed that the enciphered traffic carried a faint secondary signal, and constructed equipment to recover it. It turned out to be plaintext, which somehow leaked through the cipher machine.

So what is TEMPEST?

TEMPEST is the name of a technology involving the monitoring (and shielding) of devices that emit electromagnetic radiation (EMR) in a manner that can be used to reconstruct intelligible data. The term's origin is believed to simply be a code word used by the U.S. government in the late 1960s, but at a later stage it apparently became an acronym for Telecommunications Electronics Material Protected from Emanating Spurious Transmissions. Some sources insist that it is an acronym for Transient Electromagnetic Pulse Emanation STandard.

National Communications Security Committee Directive 4 sets U.S. TEMPEST standards. The requirements are set out in document NACSIM 5100A, which is classified. TEMPEST certification for private sector usage is extremely expensive and, as a result, it has led to a newer standard, called ZONE, which is more cost effective, though somewhat less secure. Approved TEMPEST-shielded devices are classed into 3 categories. Type 1 is extremely secure and available only to the U.S. government and approved contractors, who must undergo strict vetting. Type 2 is somewhat less secure, but still requires government approval to use. Type 3 is for general commercial use. For more information on TEMPEST certification, see the NSA TEMPEST Endorsement Program.

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 is also sometimes referred to an 'Van Eck Phreaking' after the Dutch Scientist Wim van Eck who in 1985 demonstrated that he could easily pick up nearby computer monitor emissions and display them on a TV monitor. His research paper entitled Electromagnetic Radiation from Video Display Units: An Eavesdropping Risk? described the TEMPEST problem like this:

> It is well known that electronic equipment produces electromagnetic fields, which may cause interference to radio and television reception. However, interference is not the only problem caused by electromagnetic radiation. It is possible in some cases to obtain information on the signals used inside the equipment when the radiation is picked up and the received signals are decoded. Especially in the case of digital equipment this possibility constitutes a problem, because remote reconstruction of signals inside the equipment may enable reconstruction of the data that the equipment is processing.

Some of his conclusions caused quite a stir:

> A normal TV receiver made suitable for this purpose will in some cases be able to restore the information displayed on a video display unit or terminal on its own screen, when this field is picked up. Depending on the type of video display unit or terminal, this reconstruction may under optimum conditions be feasible from distances of up to 1 km.

People were alarmed at the apparent ease with which data could be captured by relatively simple means. Although van Eck was deliberately vague/misleading on the technical details of the experiments, there were quite a few attempts to reproduce the results, with varying degrees of success.

How does TEMPEST work?

Every electronic, electro-optical or electromechanical device, whether or not it was designed as a transmitter, gives off some type of electromagnetic signals, or "emanations." An electric shaver, for example, may radiate strongly enough to interfere with nearby radio or television reception. Transistor radios are banned from airlines because their unintentional signals can interfere with navigational equipment. Equipment may also give off unwanted signals in the form of sound.

Proper design minimizes the unintentional signals given off by a device, but some unintentional signals will always be present. When a device processes information such as printed text or voice, it may "leak" that information through unintentional signals. A common example is "crosstalk" on telephone lines. Signals "leak" from one line to another, and someone else's voice intrudes on your phone call.

TEMPEST eavesdropping technology works by capturing and reconstructing the Electromagnetic Radiation given off by digital equipment. Computer monitors display information through the use of an electron gun to manipulate pixels on the screen. The electron gun shoots out pulses of electrons, which sweep across the screen striking pixels, left to right and up and down many times a second. The voltage level pushing the electrons out, rises and falls depending on whether the pixel is to be made light or dark. This process generates Electromagnetic Pulses, which in turn emit Electromagnetic Radio Waves or Electromagnetic Radiation, which emanates outward for a great distance. Hard disks are another source because data is stored in binary code, and is processed as 1s and 0s, ONs and OFFs; again causing pulses and EMR. These radio waves are as distinct as fingerprints, even in computers of the same make and model, due to minute differences in the manufacturing of the components.

Computer cables, phone lines and poorly grounded electrical systems can act as both a receiver and transmitter for EMR, thus allowing the waves to be travel even further afield. These radio waves can then be captured with an Active Directional Antenna, fed into a monitor and be zeroed in on and deciphered by using a horizontal and vertical sync generator.

Monitors, microchips and devices such as printers and PCs all emit EMR into space or into some conductive medium (such as power lines, communications wires or even water pipes). The EMR that is emitted contains the information that the device is displaying, creating, storing or transmitting. With the correct equipment and techniques, it is possible to reconstruct all or a substantial portion of that data.

TEMPEST equipment

TEMPEST monitoring equipment include various kinds of sensitive receivers, which can monitor a wide range of frequencies, and a combination of hardware and software that is capable of processing the received signals into the original data. The data that is picked up is often corrupted by things such as external EMR interference, signal

weakness over distances and partial transmission. Advanced algorithms can help provide a more complete picture of the original data.

Codex Data Systems markets a TEMPEST-type scanner called D.I.R.T. (Data Interception by Remote Transmission. Their website describes it like this:

> Data Interception by Remote Transmission is a powerful remote control monitoring tool that allows stealth monitoring of all activity on one or more target computers simultaneously from a remote command center. No physical access is necessary. Application also allows agents to remotely seize and secure digital evidence prior to physically entering suspect premises.

Although the sale of TEMPEST monitoring devices to the general public is prohibited by the U.S. government, it is of course possible that non-approved organizations and individuals can acquire the technology, or even build it themselves as the designs and equipment are relatively easy to acquire. For example, see the paper Who's Listening? for a list of components for a "Radio Shack" Reader.

How can you protect yourself against TEMPEST eavesdropping?

Shielding of devices from EMR is achieved by a number of methods. The most sophisticated devices use advanced micro-components that have been designed from scratch to minimize TEMPEST emanations. Generally, shielding involves encompassing the device in a Faraday cage that does not permit stray emanations, along with special modifications to the power source. This usually involves a heavy metal case around an object. TEMPEST shielding also involves such issues as the design of a room and placement of equipment within it, to ensure that no information can escape. Going to such lengths is obviously a very expensive business, and usually limited to government and diplomatic agencies. As with all things, the potential risk has to be weighed up against the cost.

Companies and individuals can purchase TEMPEST-certified computers but the high cost of such a secure system may be prohibitive to most consumers. For individuals who wish to be more secure against TEMPEST but cannot invest in this level of equipment, there are a few simple steps to take to reduce compromising emanations. Purchase computer equipment that meets modern standards for emission. Use only shielded cable for all system interconnections, and keep cable between components as short as possible. Block radiation from the power cords into the building wiring. To prevent your phone, fax or modem line from acting as an antenna, install a telephone line filter.

On the software side, it is also advisable to encrypt any data that you send from your computer systems so that even if the emanations were captured, they won't be easily reconstructed into anything meaningful.

For much more detailed information on ways of minimizing risk associated with compromising emanations, have a look at the Emission Security Information Guide issued by Andrews Air Force Base.

"Soft" TEMPEST

Two scientists from the University of Cambridge, Ross Anderson and Markus Kuhn, published a paper in 1998 discussing the techniques that enable the software on a computer to control the electromagnetic radiation it transmits. This software can be used for both attack and defense. To attack a system, malicious code can encode stolen information in the machine's radio frequency emissions and optimize them for some combination of reception range, receiver cost and covertness. To defend a system, a trusted screen driver can display sensitive information using fonts which minimize the energy of these emissions. Using text fonts with softened edges, they say, will limit high frequency emissions – radiation which beams farthest afield from the computer. For more information, see the

full text of Soft Tempest: Hidden Data Transmission Using Electromagnetic Emanations.

Threat or Hoax?

Seen by some as a definite threat, or as Big Brother watching, others dismiss TEMPEST monitoring as somewhat of a hoax.

James Atkinson, a telecommunications engineer specializing in the field of technical surveillance countermeasures (TSCM), and president of Granite Island Group (a company specializing in doing communications security work for government and defense contractors) has worked with TEMPEST for 20 years. TEMPEST is not a spying technology, he says, and anyone who says otherwise is either lying or misinformed. He says that the reason today's PCs are shielded is not to prevent their emanations from being intercepted, but to keep their electronic "noise" from leaking out and interfering with other electronic devices, such as radios and TVs. While sneaking a peak at what's on someone's computer screen from a distance is theoretically possible, Atkinson says, it is very difficult to do, extremely costly and impractical.

Others like Wayne Madsen from the Electronic Privacy Information Center agrees that most people do not need to concern themselves with TEMPEST. The following comes from an interview with him by Smart Computing Magazine:

> "TEMPEST is the study of vulnerabilities of compromising emanations from communications and other electrical equipment that contain data. A radio receiver can be placed near an emanating machine and pick up the signals, usually harmonic frequencies, emitted by the equipment. However, today's computer equipment, unlike the type of cathode-ray tubes used in monitors more than a decade ago, has become more 'ruggedized', and is heavily shielded so that these emissions are not so easily picked up by a radio receiver."
>
> TEMPEST is not as big a problem as it once was. However, the TEMPEST engineers don't like to admit this, and they still hype the problem."

However, many people disagree with these views, and insist that TEMPEST monitoring can and does occur.

John Young is a New York architect who says he often designs TEMPEST security features into building for clients, such as law firms and banks. He has an active interest in TEMPEST technology and has filed several Freedom of Information requests with the U.S. government to declassify NSA documents dealing with TEMPEST. These are available for public scrutiny on his website.

In a paper entitled "Who's listening?", Ian Murphy, the President of IAM / Secure Data System Inc. gives some (dated) examples of espionage attempts using low-tech equipment, as well as many examples and explanations of electronic signals, interference and interception. He ends off with details on how to construct readers/receivers using equipment readily available from electronics stores. According to Murphy, "…. the capability of these units is well within the range of any person with the intent... The equipment is nothing of major technical wonderment, just a few simple block circuits put together, so that they work together to do the final requested product."

Joel McNamara, who operates The Complete Unofficial TEMPEST Information Page, has spent a lot of time to bring together an impressive number of information sources. He believes that the "security through obscurity" that surrounds TEMPEST may actually be increasing the vulnerability of U.S. business interests to economic espionage.

Closing comments

The term TEMPEST has fallen out of use, and this branch of security is now generally referred to as EMSEC. EMSEC (Emission Security) is the protection resulting from all measures taken to deny unauthorized persons information of value which might be derived from intercept and analysis of compromising emanations from cryptographic-equipment, automated information systems (AIS), and telecommunications systems.

Two other terms, which you might come across when researching TEMPEST, are NONSTOP & HIJACK.

NONSTOP is a classified code word that apparently relates to a form of compromising emanations, but involves the transmittal of signals from radio frequency devices -- handheld radios, cellular phones, pagers, alarm systems, cordless phones, wireless networks -- in proximity to a device containing secure information. There are specific guidelines for either tuning the RF device off, or keeping it a certain distance away from the secure device (PC, printer, modem etc.).

HIJACK is a classified code word that apparently relates to a form of compromising emanations, but involves digital vs. 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 is being compromised. It does apparently require access to communications lines though.

References:

Joel McNamara – The Complete, Unofficial TEMPEST Information Page
http://www.eskimo.com/~joelm/tempest.html

Prof. Erhart Moller – Protective Measures Against Compromising Electro Magnetic Radiation Emitted by Video Display Terminals.
http://www.fc.net/phrack/files/p44/p44-10.html

Markus G. Kuhn and Ross J. Anderson – Soft Tempest: Hidden Data Transmission Using Electromagnetic Emanations.
http://www.cl.cam.ac.uk/~mgk25/ih98-tempest.pdf

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

Grady Ward -- TEMPEST in a teapot
http://www.eff.org/pub/Privacy/Security/tempest_monitoring.article

ANDREWS AFB Emission Security (EMSEC) Information Guide
http://www.andrews.af.mil/89cg/89cs/scbsi/emsecguide.doc

Arik Hesseldahl, Forbes.com, The Tempest SurroundingTempest
http://www.forbes.com/2000/08/10/mu9.html

Is Tempest A Threat Or Hoax? "Transient Electromagnetic Pulse Emanation Standard" Supposedly Reads PC Screens From A Distance; Smart Computing Magazine, April 2000• Vol.8 Issue 4
http://www.smartcomputing.com/editorial/article.asp?article=articles%2Farchive%2Fg0804%2F23g04%2F23g04%2Easp

New-wave spies -- Electronic eavesdropping is becoming mere child's play; New Scientist Magazine, 6 November 1999
http://www.newscientist.com/ns/19991106/newsstory6.html

WHO'S LISTENING ? Ian A Murphy, President CEO IAM / Secure Data System Inc.
http://www.ravenswoodinc.com/captwhos.htm