

TEMPEST, Conspiracy Theories and Tinfoil Dreams

del.icio.us

Discuss in Forums {mos_smf_discuss:Gates}

By Chris Gates, CISSP, CPTS, CEH

Ok prepare to strap that tinfoil hat on two notches below excruciating, we're going to talk about TEMPEST. What is TEMPEST? It's defined in NSTISSI-7000 as:

Electronic and electromechanical information-processing equipment can produce unintentional intelligence-bearing emanations, commonly known as TEMPEST. If intercepted and analyzed, these emanations may disclose information transmitted, received, handled, or otherwise processed by the equipment. (1)

and in NSTISSI 7003 (TEMPEST GLOSSARY) as:

"A short name referring to investigations and studies of compromising emanations. It is often used synonymously for the term "compromising emanations"; e.g., TEMPEST tests, TEMPEST inspections." (2)

Compromising Emanations (CE) are defined as:

"Unintentional intelligence-bearing signals, which, if intercepted and analyzed, disclose the national security information transmitted, received, handled or otherwise processed by any information-processing equipment." (3)

Clear as mud? What this means is that your computer, your computer monitor, your CAT5 cable going into your router from your computer, your coax cable into your cable modem, and even your power cord going into the wall can carry electronic and electromechanical signals distances away from your computer and could possibly be intercepted either off the wires or through the air. Ok, maybe one more notch on that hat.

What is TEMPEST?

TEMPEST is said to stand for "Telecommunications Electronics Material Protected From Emanating Spurious Transmissions" but I also found; "Transient Emanations Protected From Emanating Spurious Transmissions", "Transient Electromagnetic Pulse Emanation Standard", "Telecommunications Emission Security Standards", and several similar variations on the theme but there is no official meaning for TEMPEST it is more the name of the phenomenon rather than an acronym.

How do these "intelligence-bearing emanations" occur? Basic electromagnetic theory tells us that electromagnetic fields occur as current flows through a conductor. A conductor can be anything metal (your power cord, your CAT5 cable, your phone cord, etc). How does your CAT5 cable pass data? In a simple explanation, current is pushed along the wire and the data goes with it; the more current pushed down the wire and the longer the wire the greater potential for these "emanations" because of growing electromagnetic fields.

Image 1: Electromagnetic Field Composition. Image from NACSIM 5000 (4)

4)

NACISM 5000: (TEMPEST Fundamentals) says that there are three types of TEMPEST Signals; Red Baseband Signals, Modulated Spurious Carriers, and Impulsive Emanations.

From NACCIM 5000 (5), here are the definitions for those three types:

RED Baseband Signals: "The most easily recognized CE is the RED baseband signal in attenuated but otherwise unaltered form, since it is essentially identical to the RED baseband signal itself. This emanation can be introduced into electrical conductors connected to circuits (within an EUT) which have an impedance or a power source in common with circuits processing RED baseband signals. It can be introduced into an escape medium by capacitive or inductive coupling, and especially by radiation with RED baseband signals of higher frequencies or data rates."

Modulated Spurious Carriers: "This type of CE is generated as the modulation of a carrier by RED data. The carrier may be a parasitic oscillation generated in the equipment, i.e., the chopper frequency of a power supply, etc. The carrier is usually amplitude or angle-modulated by the basic RED data signal. Or a signal related to the basic RED data signal, which is then radiated into space or coupled into EUT external conductors."

Impulsive Emanations: "Impulsive emanations are quite common in EUT's processing digital signal, and are caused by very fast mark-to-space and space-to-mark transitions of digital signals. Impulsive emanations can be radiated into space or coupled into EUT external conductors."

EUT=Equipment Under Test

Those definitions didn't mean that much to me (there are some pictures in the 5000 that may help you out though), so I had to ask a person smarter than me what they meant. Here is what they told me for examples of the three.

Red Baseband Signals is basically reading a computer monitor remotely. Here is an example from a Japanese site (6):

Image 2: Red Baseband Signals example

Modulated Spurious Carrier means that a signal changes either the amplitude or frequency of another signal.

Image 3: Modulated Spurious Carrier example. Changing the amplitude of a signal. Picture from NACISM 5000

Impulsive Emanations means that something you are doing on the computer is can be seen on a line or thru the air (like typing on the keyboard). The Japanese site had an example of this one too. (7)

Image 4: Impulsive Emanations example

How do they collect these "emanations"?

From: <http://www2.nict.go.jp/y/y213/english/e-tempest.html>

Image 5: A monitor emitting EM radiation

Image 6: Collecting the signal

Image 7: TEMPEST collection (Van Eck Phreaking) set up from the 80's (8)

Image 8: Data Processing

Image 9: Displaying the TEMPEST information

How do these signals get out?

Here's an example of how TEMPEST information gets out:

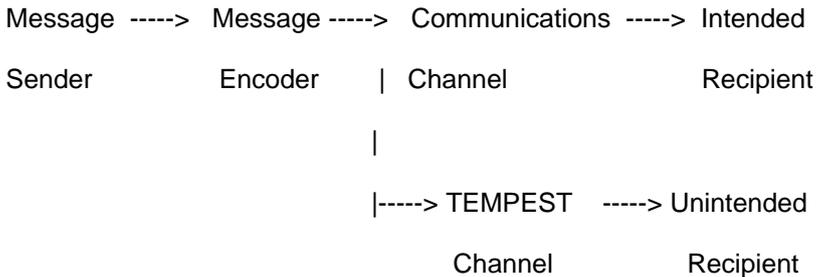


Image 10: Example TEMPEST Information Flow

TEMPEST signals can escape in four ways. They are: Electromagnetic Radiation, Line Conduction, modulation of an intended signal (Fortuitous Conduction), and Acoustics. A brief explanation of each follows.

Electromagnetic Radiation: Whenever a RED signal is generated or processed in equipment, an electric, magnetic or electromagnetic field is generated. If this electromagnetic field is permitted to exist outside of an equipment, a twofold problem is created; first the electromagnetic field may be detected outside the Controlled Space (CS); second the electromagnetic field may couple onto BLACK lines connected to or located near the equipments, which exit the CS of the installation.

Line Conduction: Line Conduction is defined as the emanations produced on any external or interface line of equipment, which, in any way, alters the signal on the external or interface lines. The external lines include signal lines, control and indicator lines, and a.c. and d.c. power lines.

Fortuitous Conduction: Emanations in the form of signals propagated along any unintended conductor such as pipes, beams, wires, cables, conduits, ducts, etc.

Acoustics: Characteristically, plaintext processing systems are primarily electrical in function. However, other sources of CE exist where mechanical operations occur and sound is produced. Keyboards, printers, relays -- these produce sound. and consequently can be sources of compromise.

Explanations from NACSIM 5000 (9)

How to protect and contain Compromising Emanations (CE)

If you read NACSIM 5000 there are numerous methods for reducing and containing CE, the most prevalent methods seem to be following RED/BLACK separation, Shielding the facility or equipment, Filtering signals before they leave the facility, using proper Grounding techniques, and using Isolators on signal lines.

“The RED/BLACK concept is the basis for the development of the facility criteria presented herein. The RED/BLACK concept dictates that electrical and electronic circuits, components, equipments, systems, etc., which handle national security plain language information in electrical signal form (RED) be separated from those which handle encrypted or unclassified information (BLACK).” (10)

All the RED/BLACK information you can handle can be found here: <http://cryptome.org/tempest-2-95.htm>. But a simple explanation of RED/BLACK separation seems to be that if you keep RED machines a certain distance away from BLACK machines you can reduce the possibilities of Compromising Emanations jumping on TEMPEST Channels and getting away from your area of control or Inspectable Space (IS). 2-95 also covers Shielding, Filtering, and Grounding in decent depth. Shielding keeps your signals inside an area, whether is be your computer case or your room or your building.

Filtering takes a set of signals in and usually on lets one (or one type) of signal out. For example, a low pass filter allows low frequency signals to pass but blocks high frequencies. Grounding, or proper grounding, means that the path of least resistance for a conductor is to ground (earth or building ground) and not along the conductor away from your inspectable space (IS).

Now What?

Before you go out and wrap your computer room with aluminum foil and chicken wire a few things to remember. First, your whole security posture can be broken down into four parts; Personnel Security, Operational Security, Physical Security, and Information Security. TEMPEST is just a piece of information security. It is a very costly and technical attack and has to be launched by a determined or very lucky attacker.

A much more feasible scenario is to have someone steal whatever information the attacker wants by stealing documents or just telling the attacker (rival company perhaps) about it. This would be attacking your Personnel Security because you hired an untrustworthy person.

An Operational Security attack would be if you let it known to the public via blog, email, internet postings, or simply having someone overhear a conversation talking about whatever information you were trying to keep secret and taking that information to another person or rival company.

A Physical Security attack would be an attack walking in and stealing or breaking in an stealing whatever data you were trying to keep secret. This is a much more realistic scenario than someone point an antenna at your house or office. I wait until you leave, I break in, and I take what I want. Not an elegant solution but gets the job done cheaply and quickly.

Information Security covers all your Information Assurance issues like cryptography, patching your systems, maintaining a strong defense network perimeter, and enacting your TEMPEST countermeasures. A good information security posture should help keep people from hacking/cracking their way into your network and stealing the information.

Looks like the whole defense in depth mantra takes on new meaning with you take TEMPEST into consideration.

Author's Note

I am not a TEMPEST researcher or expert, I don't do TEMPEST for a living or even as a hobby. I remember taking a TEMPEST question on my CISSP exam, became interested, and did some research. All the materials I used are publicly available and documented throughout the article. Since I am not a TEMPEST expert, if you find any factual inaccuracies let me know and I'll make the update to the article.

References and Extra Reading Materials

Dutch Voting Machine TEMPEST Video

<http://www.youtube.com/watch?v=B05wPomCjEY>

TEMPEST for Eliza **Supposed to play mp3s through your monitor that you can receive on an AM radio.

<http://www.eriky.de/tempest/>

EckBox **Van Eck Phreaking device

<http://eckbox.sourceforge.net/>

Cryptome TEMPEST documents

<http://cryptome.org/nsa-tempest.htm>

Unofficial TEMPEST Timeline

<http://cryptome.org/tempest-time.htm>

The Complete Unofficial TEMPEST Information Page

<http://www.eskimo.com/~joelm/tempest.html>

All You Ever Wanted To Know About TEMPEST

<http://libarynth.org/cgi-bin/view/Libarynth/AllYouEverWantedToKnowAboutTempest>

TEMPEST 101

<http://www.tscm.com/TSCM101tempest.html>

TEMPEST Wiki

<http://en.wikipedia.org/wiki/TEMPEST>

NSA TEMPEST Endorsement Program

<http://www.nsa.gov/ia/industry/tempest.cfm>

TEMPEST article on forbes.com

<http://www.forbes.com/2000/08/10/mu9.html>

TEMPEST Leak article

<http://cryptome.org/tempest-leak.htm>

There's more...Google is your friend. Checking out the original Van Eck articles may be a good place to start.

Image at top of document with Rory Culkin, Mel Gibson and Abigail Breslin from the movie Signs (2002). © Touchstone Pictures. All rights reserved.