# TEMPEST

**http://www.fas.org/irp/program/security/tempest.htm**
**Maintained by Steven Aftergood**
**Created by John Pike**
**Updated Friday, February 11, 2000 6:01:37 AM**

TEMPEST is an unclassified short name referring to investigations and studies of compromising emanations. (Though it is not really an acronym, TEMPEST is sometimes said to stand for Transient Electromagnetic Pulse Surveillance Technology.) Compromising emanations are unintentional intelligence-bearing signals that, if intercepted and analyzed, will disclose classified information when they are transmitted, received, handled, or otherwise processed by any information processing equipment. Because the details of many TEMPEST issues are classified and controlled under strict conditions of need-to-know, unclassified discussions must be somewhat general.

Computers and other electronic equipment release interference to their surrounding environment. You may observe this by placing two video monitors close together. The pictures will behave erratically until you space them apart. Any electrical/electronic circuit that carries a time-varying current will emanate electromagnetic signals with the strength of the emission proportional to the current amplitude and its time rate of change, These signals propagate outward from the source as free space waves and as guided waves along conductors connected to or close to the radiator. If time variations of the source currents are related in any way to the information content of the signals (which will almost certainly be the case on a data line), then the emanation will also bear some relationship to the data. It may, therefore, be possible to reconstruct the original intelligence by analysis of these

unintentional emissions.
TEMPEST equipment can essentially remotely mirror what is being done on a remote device. TEMPEST monitoring technology has gotten to the point that it is possible for an intruder to park in a van on the street and observe on their receiver exactly what a user is doing on an unprotected personal computer. Emissions from a video monitor normally exist at around 55-245 Mhz, and can be picked up as far as one kilometer away. The cost of Tempest eavesdropping equipment can vary from $5000 to $250,000, and the costs of protection against these devices varies according to the sophistication of the eavesdropper.

If the source information is classified, interception and analysis of the emanations by unauthorized personnel will compromise national security. The aim of the TEMPEST discipline is to control stray emissions in a manner that prevents such disclosures. TEMPEST countermeasures are applied in proportion to the threat of exploitation and the resulting damage to the national security, should the information be obtained by a foreign intelligence organization. Typical security measures include screens attached to individual machines or screened rooms in which all sensitive equipment is placed.

Communication security (COMSEC) is the term used to denote steps taken to prevent disclosure of national security information to unauthorized recipients during the communication process. The information to be guarded includes plain text of classified messages, as well as cryptographic technology and materials. Cryptographic information is especially sensitive, not as an end in itself, but because it is used to protect other classified data. If the integrity of an encryption system is breached at any point, all classified information protected by that coding may be compromised.

COMSEC consists of four main parts: physical security--all

physical meas:1res to sat eguard materials from unauthorized access ; emissions security control of emanations from equipments processing classified data; transmission security--protection of transmissions from traffic analysis, imitative deception, and disruption; and cryptographic security--the use of technically sound cryptosystems.

A RED equipment or circuit is one that handles plain text information with national security value. Equipment processing signals that are unclassified, either because of content of the text or because the intelligence is obscured by encryption, is denoted in BLACK. The unintentional emission characteristics of RED systems and equipments are categorized according to strength and nature of their emanations. The reason for the strength element is clear: high-level signals can be intercepted at magnitudes that permit analysis with greater physical separations between the source and the eavesdropper. The second factor relates to the correlation between waveform of the emitted signal and the information to be protected.

Concerns about electromagnetic surveillance have been intensified by advances in state-of-the-art equipment design and signal processing techniques. While a few technologies such as fiber optics and multiplexing have made interception and analysis more difficult, the overall effect has been to open new opportunities for eavesdroppers. Projections into the immediate future indicate that this trend will continue. The only safe approach is a reasonable worst-case evaluation. It must be assumed that the opposition has the proper equipment to monitor all signals of significant amplitude in areas where access is uncontrolled.

Encryption is the method used to guard against disclosure of classified information when long-distance telecommunications are monitored. However, it does not prevent possible compromise through interceptions and analyses of unintentional emanations

from RED equipments.

Many approaches are available to equipment and facility designers to avoid disclosures through potentially compromising emanations. All of these techniques reduce the stray signal strength at locations where access is uncontrolled, so that the intelligence content is lost in the background electrical noise.
Examples of preventive measures include the following:

- Physical separation--excluding unauthorized individuals from areas near the source where the emanations are larger in amplitude than the ambient noise.
- Electromagnetic separation--the use of shielding, filtering, and other methods of EM isolation to attenuate the unintentional emissions.
- Signal level minimization--design and operation of circuits at lowest feasible power levels to minimize the strength of unintentional emissions.

These methods can be employed in an infinite variety of combinations to achieve the desired goals.

Facilities that require TEMPEST protection in accordance with NSA 73-2A are specified for 50-decibel (nominal) TEMPEST shielding and penetration protection. There are no fundamental differences in the principles and technical approach between 100-decibel (nominal) shielding and penetration protection and the 50-decibel (nominal) isolation subsystem; only the required performance and implementation practice change. It is still necessary to not only provide an electromagnetic shield on a closed topological surface around the RED equipment area, but also to protect each penetration properly. Special cases, if any, must be identified and treated; RED/BLACK isolation practices must be followed within the shielded volume. Because the required effectiveness in linear (not decibel) units is lower by a factor of

about 300, less expensive components and assembly techniques can be used. Communication security interests will be best served and the most cost-effective TEMPEST design will be achieved by limiting the extent of the shielded volume to the minimum size needed for protection of the RED equipment.

The cost of the shielding and penetration protection subsystem can be most strongly influenced during the layout of the facility floor plan. The RED equipment to be shielded should be concentrated into a single, minimum-size area consistent with system growth requirements. BLACK equipment should be placed in a physically separate location rather than intermixed with the RED hardware. This layout will enhance TEMPEST performance by minimizing the potential for cross-coupling of classified data into BLACK circuits.

For high-level 100-decibel (nominal) attenuation of radiated electromagnetic fields, a continuously welded 10-gauge steel liner integrated into the facility structural design is the preferred approach. For installations that require only 50-decibel (nominal) TEMPEST isolation, however, less expensive shielding techniques are available for consideration. When very large volumes must be shielded, it becomes cost-effective to integrate the shield into the overall design for the floors, walls, and ceilings. In these cases, the shield can be constructed using either thin (22- to 26-gauge) galvanized steel or copper sheets, or copper or stainless steel foils. A design solution is, in fact, a combination of these methods--galvanized steel sheets for the floor shield and copper or stainless steel foils for the walls and ceilings.

Modular shielded enclosures in sizes up to about 93 square meters of floor area are commercially available from the standard product lines of numerous shielding suppliers. Prices for these enclosures vary with the dimensions of the room and the number and type of penetration panels.

## Sources and Methods

- Engineering and Design - Electromagnetic Pulse (EMP) and Tempest Protection for Facilities
- Eavesdropping On the Electromagnetic Emanations of Digital Equipment: The Laws of Canada, England and the United States

**http://www.fas.org/irp/program/security/tempest.htm**
**Maintained by Steven Aftergood**
**Created by John Pike**
**Updated Friday, February 11, 2000 6:01:37 AM**