Government Levels of Security Enhanced with TERA® Cabling System

It's no news flash that IT security issues are a hot topic. While security has always been in the back of the IT manager's mind, the recent flood of information, regulation and product pertaining to network security is fairly new in the private sector. Not so in government and military networks. These critical networks have long put security at the top of the list and this focus has resulted in extremely robust security parameters and processes.

In the private sector, information security typically relies on such measures as firewalls, passwords, biometrics and access cards. Government information, which may include department of defense information, health and human services data or municipality infrastructure information, is often protected by similar systems. The levels of security are dictated by the nature of the data, and in more secure/classified government networks, the physical layer cabling plant is included in security measures

Information system security can be divided into Personnel, Physical, Operational, Information, and Electromagnetic categories. Personnel represent the most vulnerable level, as paying workers for access or information is the least costly, least risky, and fastest method of exploitation. Lack of Physical protection allows an adversary to obtain facility, system, cabling, and information access directly, but with moderate risk. Good Operational security will minimize errors in configuration and operation of systems and limit ways that sensitive information can leak out. Information security will prevent outside access to information through encryption, firewalls, and other bitstream protection measures. Electromagnetic security serves to prevent the reception of signal emanations from equipment and cabling that would allow an adversary some distance away to intercept and decode communications signals.

Cabling security measures fall into multiple categories. Physical security must be implemented to prevent outside uncontrolled access to the cabling and equipment. The government uses Protected Distribution Systems (PDS) (glued conduit, pipe, alarms, video monitoring, etc.) to physically protect cabling, which runs through uncontrolled areas.

Operational measures to document and label the cabling and equipment infrastructure are needed to minimize the possibility of mistakenly allowing sensitive/classified information to be transmitted out on uncontrolled media or allowing untrusted personnel access to sensitive cabling and equipment. Distribution labeling will allow inspection and access control to detect unauthorized cable connections. All cable termination points should be labeled and controlled, and it is important to understand every point of ingress and egress on a network. Documentation and periodic inspection serve to address potential network breach points and actual breaches. Physical layer documentation can be achieved via intelligent patching, modifications to drawings or databases, entry of new labels on termination points, or a combination of these. Such steps are easily employed by the private sector and are increasingly a part of network management in non-governmental enterprise.

Beyond limiting physical accessibility, the cabling plant's radiated signals must be controlled. The control of all compromising emanations to within controlled spaces is critical for Government communications that require a high level of security, such as homeland security. This falls under what the government terms EMSEC (Emissions Security), INFOSEC (Information Security), and TEMPEST. These programs/ratings work to assure that the normally radiated signals are shielded in some way from unscrupulous listeners that would use this captured information for unauthorized means.

Radiated signals or emissions occur in every piece of computer equipment and in all copper cabling. In the US, the FCC controls the amount of allowable emissions and international counterparts exist (IEC CISPR documents). The unwanted variety of signal emissions are known as compromising emanations. Compromising emanations can be transmitted through power lines, data and telephone cabling, or simply radiated through the air. When a compromising emission is received or intercepted, secure information can be compromised where the signals can be reconstituted into the original sensitive information. Microchips, diodes transistors and other non-linear electronic components in data processing equipment are a potential source of compromising emanations. Signals on copper cables especially data signals where sharp transitions produce significant higher frequency signals, can create compromising emanations.

TEMPEST is a US. government code word which defines the counter-intelligence standards developed to protect secure data transmissions from electronic espionage. Although actual requirements are classified, it is widely known that TEMPEST sets out strict limits on signal radiation from data handling electronic equipment. While the scope of published TEMPEST information focuses on physical equipment such as monitors, printers and devices containing microchips, the term is commonly used to describe efforts throughout the field of Emissions Security (EMSEC). EMSEC is defined as 'the protection resulting from all measures designed to deny unauthorized persons information that might be derived from intercept and analysis of compromising emanations from other than crypto-equipment and telecommunications systems," according to the ATIS Committee TIAI.

TEMPEST began many years ago when it was determined that transmissions could be detected through the open air from a significant distance through listening to the emissions from a cable. In 1918, Herbert Yardley and his staff of the Black Chamber were engaged by the US Army to develop methods to detect, intercept and exploit combat telephones and covert radio transmitters. However the code-word TEMPEST was not used until the 60's and 70's. There are several definitions for the acronym including "Telecommunications Electronics Material Protected From Emanating Spurious Transmissions" and Transient Electromagnetic Pulse Emanation Standard," However, these acronyms are somewhat speculative, as the official title, along with its requirements, are classified. In short, TEMPEST is the means to protect transmissions and covers media, communications devices and other protective measures.

Although the transmission, reception and testing of signal emanations is called TEMPEST, the implementation criteria designed to minimize this is called RED/BLACK. RED commonly refers to clear text sensitive information, and BLACK would be the encrypted or unclassified signals. Basic RED/BLACK requirements and

criteria were declassified in 1995 as NSTISSAM TEMPEST/2-95 (FOUO). Actual emission limits and test parameters remain classified. Even without more complete parameters, it is known that TEMPEST served as a model for many other governments' equivalent programs. The NATO equivalent is AMSG 720B. In Germany, even the names of the standards supplied by the government remain classified, but it is known that the National Telecom Board administers their equivalent to the TEMPEST rating program. In the UK, Government Communications Headquarters (GCHO), the equivalent of the NSA (National Security Administration), administers their program.

While there is only one U.S. TEMPEST standard, there are three U.S. levels of NSA encryption level approval. Type 1 is acceptable for use in classified or controlled cryptographic equipment and may refer to assemblies, components or other items endorsed by the NSA for securing telecommunications and automated systems for the protection of classified or sensitive U.S. Government information. This equipment is subject to restrictions in accordance with the international Traffic in Arms Regulations. Type 2 approval is for equipment, assemblies and components used in the transmission of non-classified but sensitive information. Type 3 implements an unclassified algorithm registered to the National Institute of Standards and Technology (NIST) for use in protecting unclassified sensitive or commercial information.

U.S. TEMPEST certification can apply to both equipment and to complete systems in a network environment. There are separate TEMPEST testing procedures for equipment in a laboratory and for systems in the field. Both field and laboratory TEMPEST tests include all system components, with field tests including the cabling plant as part of the TEMPEST test. Changing one single component can compromise the security of the entire system. In secure communications, the medium used to transmit the data (i.e. the cabling) is part of the TEMPEST or EMSEC system. TEMPEST emission control standards for equipment and cabling, combined with data encryption and other security systems, allow for INFOSEC (Information Security). Because of these stringent requirements, the government historically, has had few options for physical layer (cabling) security.

One effective TEMPEST cabling option is the use of fiber optic networks. This provides added protection due to the fact that the fiber does not radiate /emit signals and would have to be physically compromised in order to access the communications. Fiber network equipment, however, is more costly than the equivalent copper components resulting in higher maintenance costs as they are based on original purchase pricing and requires more maintenance than copper.

Copper networks are commonly used, but require very specific installation practices, such as NSTISSAM TEMPEST/2-95 RED/BLACK separation guidelines. In RED/BLACK, the RED cabling and equipment is separated and/or shielded from the BLACK cabling and equipment to prevent coupling. The RED equipment and cabling are restricted from external access as well as proximity to other potential signal radiators. Other equipment that could listen to or carry or propagate emanations such as cell phones and radios are forbidden in RED areas.

Most federal agencies dealing with classified information have trained Certified TEMPEST Technical Authorities (CTTAs) to advise on and approve classified system installations. CTTAs have significant TEMPEST training and background to enable them to balance RED/BLACK security criteria against the threat to the system to provide an optimum cost benefit TEMPEST security solution. There is less of a need for TEMPEST security in certain situations such as those where there is a large controlled or inspectable space around the secure system, and more of a need for TEMPEST security where the controlled or inspectable space is minimal. Only a Certified TEMPEST Technical Authority can determine inspectable space and protection criteria IAW NSTISSI 7000.

Shielded copper cable provides an additional layer of security by significantly limiting emissions. While this would in theory allow reduced RED/BLACK separation distances, the TEMPEST installation practices may not allow this reduction in practice. Shielded cable is required depending upon security level, inspectable space, and threat. The use of shielded cable can reduce cable separations, eliminate or reduce the need for signal isolation and filtering, is usually required for use with TEMPEST approved equipment, and reduce or eliminate the need for additional cable or other shielding. Shielded cable can also be used for BLACK signaling to reduce the possibilities of these cables picking up other emanated signals.

F/UTP or foil shielded UTP cable has one overall foil shield surrounding four unshielded-twisted pairs and is traditionally used when shielded cable is specified, although this may not be sufficient in some situations. Additional signal isolation can be provided through braided shields, tighter braids, foil with braid, or individual pair shields with an overall foil shield. Metallic distribution systems and the facility itself can also provide signal isolation. A cable and configuration must be selected that will limit any emanated signals to within the controlled or inspectable space.

Recent testing sheds additional light on the standards and copper options for connections to TEMPEST and other secure processing equipment. Siemon's TERA®, a Category 7/ Class F copper system has passed TEMPEST emissions testing by an independent, NSA certified lab, Dayton T. Brown Inc. in a specific configuration. This indicates that TERA cabling should meet all TEMPEST shielded cabling requirements in even the most demanding situations. Although cabling in general cannot be TEMPEST approved, as the signals and configuration will vary, the TERA shielded cabling configuration will provide the best TEMPEST protection commonly available.

While the majority of the test parameters are classified, it is understood that the combination of TERA connectivity and cable suitably minimized/eliminated emissions as part of an overall system. TERA utilizes S/FTP cable and fully shielded connectivity. In S/FTP cable, each pair is individually shielded and an overall braid shield surrounds all conductors. Additional shielding is integrated into the outlets and plugs, eliminating another potential emission source. It is important to note that a 6A F/UTP system did not pass the same testing when a single foil shielded cable was used with RJ45 jacks.

For the TEMPEST test, a four-connector, 100 meter TERA channel was deployed in a shielded anechoic chamber. The channel was energized with full duplex Gigabit

Ethernet (1000 Mb/s) traffic using a Spirent Smarbits multiport analysis system. Emissions from the cabling system were then monitored and compared to the TEMPEST requirements, with the TERA cable emissions not exceeding the TEMPEST requirements. The TERA cable systems emissions did not exceed the TEMPEST emission requirements and outperformed the same configuration using a single foil shielded cable with RJ 45 (which had emanations exceeding the limits allowed).

According to the independent test report, TERA cable is suitable for applications, such as TEMPEST, where radiated and compromising emissions are a concern. The remainder of the test report is classified. TERA cable should be used with TEMPEST equipment, as it provides the greatest assurance of limiting cable emanations to those of the TEMPEST equipment. TERA cable can also be used for other types of signals (analog, synchronous data, video, other speed network, etc.), and in place of additional conduit, building, or other shielding, where high quality TEMPEST and other emanation reduction or elimination is needed.