Los filtros Tempest: centros de datos más seguros

Artículo cedido por Cemdal

CEMDAL

www.cemdal.com

Autor: Francesc Daura Luna, Ingeniero Industrial. Director de la Consultoría CEMDAL, Representante de Austria Mikro Sisteme (ams AG) para España y Portugal.
www.cemdal.com
fdaura@cemdal.com

El espionaje ha existido durante siglos. Los espías ya eran conocidos en la época egipcia y sus actividades siguen hoy en día. Acontecimientos recientes, destacados en la prensa, han demostrado que sus actividades son numerosas. Últimamente las actividades de la americana NSA han salido mucho en toda la prensa. Debemos tener en cuenta que tan pronto como se pulsan las teclas de un ordenador, éste envía emisiones electromagnéticas que pueden ser detectadas y decodificadas.

Emisiones conducidas y radiadas

Las fugas de emisiones electromagnéticas de alta frecuencia provenientes de los ordenadores pueden ser radiadas o conducidas. Las emisiones radiadas pueden provenir de su interior directamente o de los cables de datos o de red. Las emisiones conducidas a través de los cables también pueden ser convertidas en emisiones radiadas, si los cables de alimentación de la red eléctrica (220 o 380 V) se comportan como antenas, si no están apantallados o filtrados. Normalmente los cables de red no están apantallados en toda su longitud y por ello es aconsejable filtrarlos adecuadamente.

Estas fugas en forma de emisiones electromagnéticas no son importantes en ordenadores familiares o en las oficinas de una empresa mediana. Pero sobre todo para los militares, o también para las grandes empresas o bancos, que trabajan en campos altamente competitivos con datos muy confidenciales, podrían ser desastrosas. Por lo tanto, es vital que estas fugas de emisiones sean detenidas, o al menos atenuadas, para que la detección sea prácticamente imposible.

Figura 1: Filtro de red TEMPEST de EMIKON

En los ordenadores o en los equipos digitales, las señales con bajas frecuencias no se irradian de manera eficaz, ya que tienen pocos elementos metálicos suficientemente grandes como para comportarse como una buena antena. Pero a partir de los 30 MHz, los únicos elementos metálicos que se pueden comportar como antenas radiantes eficaces son los cables. En los centros de procesado de datos, las dimensiones de los armarios no se convierten en una antena a tener en cuenta hasta alrededor de los 75 MHz ($\lambda = 4$ metros, $\lambda/4 = 1$ m, λ: longitud de onda).

En cambio, las señales con altas frecuencias no se conducen bien, debido a la inductancia de los cables, por lo que las emisiones conducidas son en gran medida un problema de baja frecuencia. Las emisiones conducidas de baja frecuencia tienden a dominar por debajo de los 30 MHz. Las emanaciones electromagnéticas a menudo tienen una componente conducida. Por ejemplo, las señales de alta frecuencia emitidas por un ordenador pueden ser recogidas por los circuitos de alimentación de red y ser llevadas a través del propio edificio y de otros edificios vecinos.

Sin duda puede haber problemas de emisiones radiadas por debajo de los 30 MHz y problemas de emisiones conducidas mayores a los 30 MHz. Por ello, las normas militares requieren pruebas con una considerable superposición de frecuencias.

Un poco de historia

Desde el siglo XIX, los ingenieros saben que las fugas de señales de alta frecuencia en todas partes necesitan medidas protectoras para evitar que causen problemas. Estas fugas ya se explotaron para fines militares en 1914. La técnica usada para "pescar" señales eléctricas o electromagnéticas y así poder "robar" la información a nivel físico se llama en inglés "eavesdropping". Típicamente se usa para detectar las señales electromagnéticas que viajan por los cables telefónicos o de datos, aunque también lo pueden hacer por los cables de red. El gobierno de EEUU desarrolló la normativa TEMPEST desde los años 50. TEMPEST consiste en una serie de normas para limitar las radiaciones electromagnéticas de los equipos electrónicos como equipos de procesado de datos, cables de datos, cables de red o monitores, con la finalidad de evitar el robo de datos confidenciales a través de las radiaciones electromagnéticas que el hardware emite. En 1995 estas normas fueron parcialmente desclasificadas, pudiéndose usar también a nivel civil.

Desde hace años hay preocupación en los gobiernos, las fuerzas armadas, las autoridades autonómicas y municipales y en las empresas y bancos por el hecho de que los aparatos electrónicos emanan emisiones electromagnéticas no deseadas que pueden ser detectadas y reconstruidas como datos inteligibles por organismos externos. Las fugas de información pueden ser suprimidas en gran medida con un diseño cuidadoso de las fuentes de alimentación y los cables de datos adecuados, suprimiéndolas con filtros y blindajes. Esto constituye una parte significativa de la diferencia de coste entre la electrónica militar y la civil.

Los servicios de inteligencia comenzaron a explotar pronto los efectos de las fugas electromagnéticas. En 1960, el primer ministro británico ordenó la vigilancia de la embajada francesa en el curso de las negociaciones de su unión a la Comunidad Económica Europea. Los científicos de la agencia inglesa de inteligencia, MI5, se dieron cuenta de que el tráfico cifrado de datos de la embajada llevaba una señal secundaria

débil y construyeron un equipo para recuperarla. Resultó ser el texto plano (abierto sin encriptar), que de alguna manera llegaba a través de la máquina de cifrado, seguramente debido a un acoplo por diafonía entre cables. Esto es más común de lo que se podría suponer. Ha habido más de un caso de máquinas de cifrado transmitiendo abiertamente en texto plano en las frecuencias de radio, aunque a menudo ha habido razones para sospechar que el gobierno proveedor de la información era consciente de ello y lo usaba para "despistar".

Durante la década de los 70, la seguridad de las emisiones se convirtió en un tema altamente clasificado y desapareció de la literatura abierta. Volvió a la atención pública en 1985 cuando Wim van Eck, publicó un artículo describiendo cómo se las había arreglado para reconstruir la imagen en una pantalla de visualización a distancia. La captación de las fugas electromagnéticas con un equipo relativamente asequible preocupó mucho a la industria de seguridad informática. La publicación de las investigaciones en temas de seguridad y emisiones relacionadas despegó en la segunda mitad de la década de 1990. A finales de los 90 se demostró que muchas de las emanaciones comprometedoras de un PC se podían captar usando los medios técnicos apropiados. En el año 2000, también se mostró que las claves criptográficas utilizadas en las tarjetas inteligentes podían ser recuperadas gracias al procesamiento apropiado de las mediciones precisas de la corriente consumida por la tarjeta, poniendo pequeños sensores de campo electromagnético cerca de la superficie de la tarjeta.

La evidencia en el siglo XXI es que las contramedidas usando la normativa TEMPEST se están volviendo importantes para la seguridad de la información, tanto en el mundo civil como en el ámbito militar.

Emisiones de Wim Van Eck

Las emisiones usadas por Wim Van Eck se utilizan para espiar el contenido de una pantalla de ordenador mediante la detección de las emisiones electromagnéticas del monitor y su cableado. También puede espiarse a través de las emisiones en los cables de red eléctrica. La información que se exhibe en una pantalla del monitor (LCD o CRT) se compone de señales eléctricas de alta frecuencia. Esas señales eléctricas crean emisiones de radiación electromagnética que tienen correlación con la imagen que se muestra en la pantalla. Por lo tanto, en principio, esas emisiones pueden utilizarse para reconstruir la imagen desplegada en el monitor. Este efecto lo descubrió el holandés Wim Van Eck en 1985 usando pantallas CRT. Investigadores de la Universidad de Cambridge descubrieron que las pantallas planas de LCD y los monitores de los ordenadores portátiles también son vulnerables a las emisiones de Win Van Eck. El equipo necesario para realizar este espionaje fue construido en un laboratorio universitario por menos de 2000 €.

EMSEC

La seguridad de emisiones (EMSEC - "EMission SECurity" en inglés) es la aplicación de las técnicas destinadas a evitar la emanación electromagnética de señales que podrían transmitir información sensible. Las señales pueden ser captadas a propósito, por dispositivos de escucha especializados, o sin querer, a través de sistemas wifi u otros dispositivos radioeléctricos. En la gestión de la seguridad de la información (ISMS: "Information Security Management System"), las fugas de información debido a las emisiones electromagnéticas desde dispositivos electrónicos se tratan como un problema de seguridad física. Las especificaciones requieren una evaluación de riesgos de seguridad y sus contramedidas. EMSEC tiene muchos aspectos. En las organizaciones militares se refiere en gran medida a las normas TEMPEST, que previenen las fugas electromagnéticas. Un sistema de apantallamiento EMSEC bloquea la emisión de señales que puede revelar el contenido de la pantalla de un ordenador fuera de la oficina o centro de datos.

Las organizaciones militares del mundo gastan tanto en EMSEC como en criptografía desde hace unos 30 años. Se ha detectado ataques de espionaje electromagnético contra sistemas comerciales, incluyendo cajeros automáticos. También ha habido mucha especulación sobre ataques electromagnéticos activos. Por ejemplo, se podría utilizar una fuente de microondas de muy alta energía para destruir las computadoras de una organización, sin matar a su gente. Las medidas EMSEC activas y pasivas están estrechamente relacionadas con la prevención de la interrupción aleatoria del funcionamiento del sistema.

Seguridad física

La seguridad física en los sistemas informáticos consiste en la aplicación de barreras físicas y procedimientos de control como medidas de prevención y contramedidas contra las amenazas externas a la información confidencial. Más claramente, y particularizando para el caso de grandes equipos Unix y sus centros de operación, por "seguridad física" podemos entender todos aquellos mecanismos, generalmente de prevención y detección, destinados a proteger físicamente cualquier recurso del sistema. Estos recursos son desde un simple teclado hasta los discos de seguridad de datos con toda la información que hay en el sistema, pasando por los propios procesadores del equipo.

Desgraciadamente, la seguridad física (hardware) es un aspecto olvidado con demasiada frecuencia a nivel de seguridad informática en general. En grandes organizaciones se suelen tomar medidas para prevenir o detectar accesos no autorizados o negaciones de servicio a nivel lógico (software), pero rara vez para prevenir la acción de un atacante que intenta acceder físicamente a la sala de operaciones o al lugar donde se depositan los datos del sistema a través del uso de las ondas electromagnéticas. Esto motiva que en determinadas situaciones, un atacante se incline por aprovechar las vulnerabilidades físicas en lugar de las lógicas, ya que posiblemente le sea más fácil robar datos del sistema que intentar acceder a él mediante fallos en el software. Debemos ser conscientes de que la seguridad física es demasiado importante como

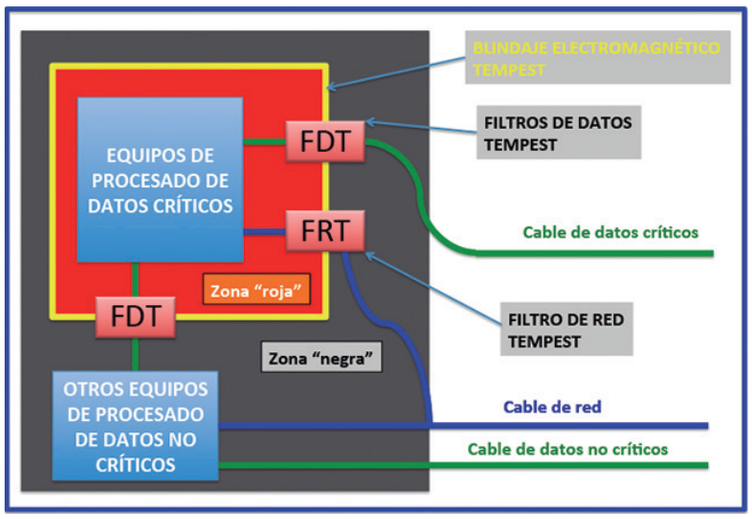

Figura 2: Separación de las zonas "roja" y "negra" con blindajes y filtros TEMPEST.

para ignorarla: un ladrón que roba un ordenador para venderlo, un incendio o un pirata que accede sin problemas a la sala de operaciones nos pueden hacer mucho más daño que un intruso que intenta conectar remotamente con nuestro equipo de forma no autorizada. No importa que utilicemos los más avanzados medios de cifrado para conectar con nuestros servidores, ni que hayamos definido una política de "firewall" muy restrictiva: si no tenemos en cuenta los factores físicos, estos esfuerzos para proteger nuestra información no van a servir de nada. Además, en el caso de organismos con requerimientos de seguridad de nivel medio, unas medidas de seguridad físicas ejercen un efecto disuasorio sobre la mayoría de los piratas.

Si notan a través de medidas físicas que nuestra organización está preocupada por la seguridad probablemente abandonarán el ataque para lanzarlo contra otra red menos protegida.

Para proteger las salas de procesado de datos y las salas de reuniones contra la transmisión de señales de radiofrecuencia emitidas por dispositivos de escucha inalámbricos y teléfonos móviles, se pueden blindar.

Para una solución de relativo bajo coste, el material estándar que se puede usar para crear espacios blindados contra las emisiones electromagnéticas es una tela especial de poliamida metalizada que proporciona una eficacia de blindaje de 100 dB a frecuencias de hasta 1 GHz. Se trata de un material flexible que se ajusta a la estructura en las paredes, techos y suelo de la sala. Además de las paredes, techo, y suelo, hay que proteger también las puertas y ventanas con juntas electromagnéticas ("gaskets") en los marcos. A través de la red eléctrica pueden captarse emisiones radiadas provenientes de las emisiones conducidas. Por ello se debe añadir filtros de red TEMPEST en los cables de red. También se debe filtrar adecuadamente los cables de datos. La figura 1 muestra un filtro TEMPEST.

La normativa TEMPEST

Los grandes equipos de procesado de datos con información confidencial y secreta, sean militares o civiles, requieren una protección especial contra el uso de personal no autorizado. Para este propósito existe la normativa TEMPEST ("Transient ElectroMagnetic Pulse Emanation Standard") publicada por el gobierno de EE.UU.

La fecha exacta de inicio de TEMPEST no se conoce exactamente, pero fue en algún momento de 1950, cuando el gobierno de EEUU se empezó a preocupar por el problema de seguridad de las emisiones para hacer frente al creciente peligro de espionaje. La Directiva 4 del "National Communications Security Committee" de EEUU establece las normas TEMPEST. Los requisitos se presentan en el documento NACSIM 5100A y su norma equivalente AMSG 720B de la OTAN, que son secretas. La certificación TEMPEST para el uso en el sector privado es cara y, como resultado, se ha llevado a una nueva norma, llamada ZONE, que es más rentable, aunque algo menos segura. Los dispositivos TEMPEST aprobados se clasifican en 3 categorías. El tipo 1 es extremadamente seguro y disponible sólo para el gobierno de EEUU y los contratistas aprobados.

El cumplimiento de las normas internacionales para la seguridad TEMPEST se consigue con la aplicación de normas como la OTAN SDIP-27 al Nivel A, B o C, lo que equivale a US NSTISSAM / 1-92 a Nivel I, II o III.

En 2004 la UIT ("Union Internationale des Télécommunications") publicó la norma SGSI X.1051 de las telecomunicaciones. En 2005, fue publicada una información de carácter general del sistema de gestión de la seguridad en forma conjunta como la norma ISO / IEC 27001 y la norma 27002 de la "International Organization for Standardization" (ISO) y la "International Electrotechnical Comisión" (IEC).

Para maximizar la seguridad de la información, las contramedidas TEMPEST están dirigidas a la prevención del espionaje. Los enemigos bien equipados no necesitan utilizar una furgoneta detectora estacionada en la calle con el equipo receptor, o un barco pesquero lleno de antenas como ocurría durante la guerra fría.

Así, por ejemplo, una señal clasificada proveniente de un ordenador portátil puede ser recogida por una línea telefónica o de datos sin protección al poner una sonda electromagnética a su alrededor a muchos metros de distancia. También son críticos los cables entrantes en la fuente de alimentación, que pueden ser controlados a largas distancias. Incluso las inmunes líneas de fibra óptica, que llevan datos a muy alta velocidad pueden llegar a un armario de distribución en el que se puede tener acceso fácilmente con medios ópticos. En consecuencia, el peligro es "claro y presente".

La protección TEMPEST se consigue de dos maneras. En primer lugar, se usan blindajes para evitar la radiación directa desde el equipo de las señales que pueden ser captadas. En segundo lugar, se requiere un

filtro TEMPEST en todos los cables eléctricos que salen de la zona blindada para eliminar las señales inteligibles que se pueden superponer sobre los cables, de modo que las señales no puedan salir fuera de la zona protegida. Los filtros TEMPEST se aplican en los cables de datos y en los cables de red de alimentación.

Separación de zonas "roja" y "negra"

Para mejorar la seguridad contra la captación externa y fraudulenta de datos, un buen método es separar físicamente los equipos en dos zonas: una zona "roja" y una zona "negra". Los equipos de procesado y redes de datos en la zona "roja" (los más sensibles o críticos) deben ser aislados con filtros y blindajes de los equipos en la zona "negra" (equipos que pueden enviar señales directamente al mundo exterior). En la figura 2 se puede ver en detalle esta separación. En ella destacan los filtros TEMPEST de datos y de red y el blindaje TEMPEST entre la zona "roja" y la zona "negra". En los equipos donde existen ambas conexiones "rojas" y "negras", como las máquinas de cifrado, es particularmente difícil hacer bien la separación.

En lo que se refiere a la terminología, los datos sensibles - o dispositivos que contienen o procesan datos sensibles - se clasifican generalmente como "rojos". Esto no implica ninguna clasificación en particular; simplemente significa que no se desea que los datos se escapen. Por el contrario, los datos y los equipos no sensibles se llaman "negros".

Los datos sensibles que se cifran también se consideran como "negros". El procesado de un dato de color "rojo" de dispositivos que todavía no incorporan la protección adecuada para contener las emisiones puede ser "negro" también. Un cable que transporta datos "negros" que pasa cerca de un equipo "rojo", y por lo tanto tiene el potencial para recoger los datos de color "rojo", se puede considerar "rojo" también. Una solución es crear alrededor de las instalaciones informáticas de riesgo una zona reforzada "roja" como zona de seguridad con una de jaula de Faraday forrada de acero, aluminio o cobre, respaldada por la supresión de cualquier emanación conducida que pueda contener información inteligible mediante el filtrado TEMPEST adecuado.

Otra solución es situar la instalación lejos de su vallado perimetral, dado que las señales radiadas se degradan fuertemente con la distancia. Por esta razón, por ejemplo, los centros de mando y control militares permanentes se sitúan generalmente a cientos de metros de las vallas de seguridad alrededor de su recinto. Cuando un cable tiene que pasar a través de una barrera "roja" / "negra", se inserta un filtro TEMPEST como contramedida prevista para filtrar todas las frecuencias excepto la señal deseada.

Normalmente es un filtro de paso bajo que bloquea todo por encima de una frecuencia dada, sobre la base de que es probable que cualquier señal "roja" sea de alta frecuencia.

Esta solución tiene limitaciones obvias, ya que cualquier interferencia dentro de la banda de paso todavía puede conseguir pasar. No se puede utilizar un filtro de paso bajo si la señal deseada es la propia de alta frecuencia. Un filtro TEMPEST evita así que una señal "roja" irradiada se cuele en el lado "negro". Los filtros de red TEMPEST solo deben dejar pasar los 50 Hz de la red aunque su margen de frecuencias suele empezar en los 10 kHz.

Para realizar esta separación se usan salas TEMPEST. Son unas habitaciones construidas con materiales especiales indicados para obtener un buen apantallado. Atenúan los campos electromagnéticos emanados por los aparatos y se vuelven impermeables a las interferencias exteriores. La certificación TEMPEST se consigue cuando la reducción de las emisiones sobrepasa los 110 decibelios (dB); por debajo son medidas Soft TEMPEST. A más dB, mayor protección, pero el coste se dispara. Una atenuación de 40 dB representa sólo una efectividad del 99,9%. A pesar de esta alta cifra, es poco segura; alcanzar los 110 dB exige atenuaciones del 99,999999% : unas milésimas muy caras y difíciles de conseguir. Un diminuto poro en los paneles echa todo a perder.

Ejército, bancos y empresas

El Ejército español, empresas privadas importantes y bancos usan la tecnología TEMPEST para blindar sus ordenadores para evitar la fuga de datos y así evitar que un espía capte las emanaciones de campos electromagnéticos que generan las máquinas. El Ejército español está protegiendo sus ordenadores y sistemas de comunicaciones que manejan información clasificada para evitar su posible robo o destrucción a través de las emanaciones electromagnéticas.

La protección se basa en introducir los equipos críticos de los cuarteles y bases en salas blindadas especiales cumpliendo la normativa TEMPEST. Los equipos electrónicos

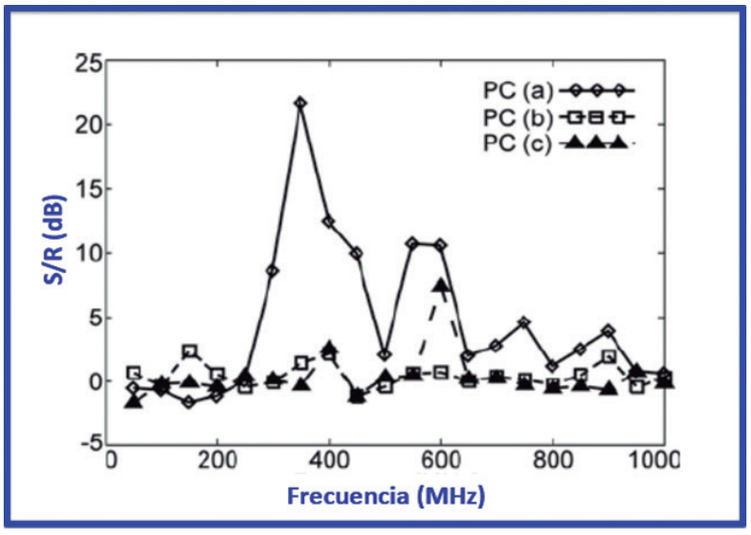

Figura 3: resultados de las pruebas de medición de las emisiones conducidas en el cable de red en tres distintos ordenadores.

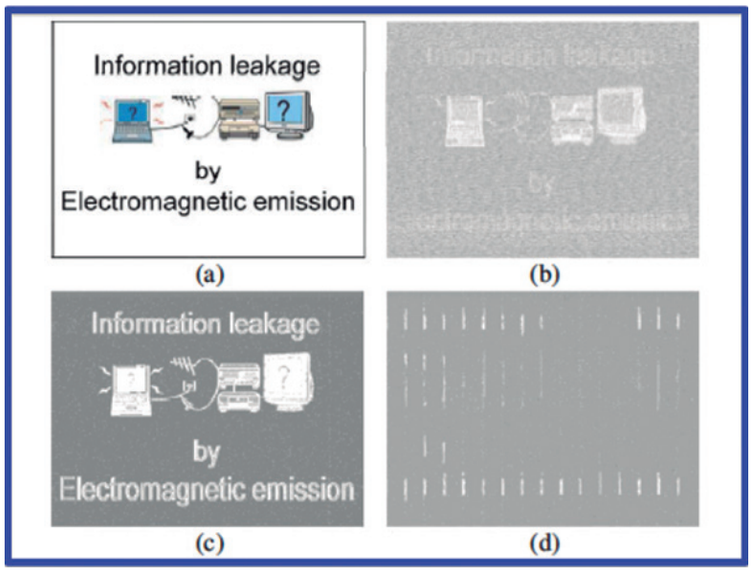

Figura 4: (a) Imagen inicial de prueba en pantalla, (b) imagen a 300 MHz, (c) imagen a 350 MHz, (d) imagen a 700 MHz.

actuales, aunque deben cumplir normativas de compatibilidad electromagnética, no son suficientemente seguros. Por ejemplo, un disco duro emana distintas señales cuando lee un "0", o cuando lee un "1". Un espía, cómodamente instalado a cientos de metros, podría captar las ondas electromagnéticas y reconstruir la información pertrechado con aparatos adecuados muy sensibles.

Los consumidores civiles pueden respirar tranquilos: el vecino espía lo tiene difícil porque acceder a este tipo de equipos es caro, y su manejo, es solo para expertos. Pero los datos confidenciales de las bases militares, de las grandes empresas y de los bancos pueden justificar tener este tipo de equipos sensibles para poder obtenerlos.

Imágenes reconstruidas

Para ver como funciona la recuperación de las imágenes de un monitor usando las emisiones de Wim Van Eck, veamos como ejemplo la figura 3 donde se muestran los resultados de las pruebas de medición de tres distintos ordenadores portátiles fabricados por diferentes marcas. La frecuencia de recepción de la medición del receptor es de 50 MHz a 1000 MHz con pasos de 50 MHz. Los ejes horizontal y vertical indican la frecuencia de recepción y el nivel de señal teniendo en cuenta la relación señal-ruido. La línea continua con diamantes blancos, la línea corta el tablero con rectángulos blancos, y la línea de tiempo el tablero, triángulos negros muestran los resultados de medición para los ordenadores PC (a), (b) y (c), respectivamente. Como se muestra en la figura, el nivel de señal relevante para el PC (a) varía en gran medida de acuerdo con la frecuencia de recepción, siendo la diferencia unos 20 dB en la frecuencia de recepción de 350 MHz. El nivel de la señal relevante para el PC (b) es más débil que para el PC (a), aunque el pico está en la frecuencia de recepción de 600 MHz.

En comparación, el nivel de señal relevante para el PC (c) es casi plano. Dado que el nivel de señal correspondiente depende de la frecuencia de recepción y del PC utilizado, la diferencia se puede utilizar en la evaluación de la fuga de información de la imagen de la pantalla debido a la emisión conducida. El sistema de medición puede evaluar cuantitativamente la fuga debido a la emisión conducida en los cables de alimentación del PC. Para solucionar el problema se podría usar un filtro de eliminación de banda o de paso bajo montado en los conductores de alimentación.

A partir de estas fugas electromagnéticas de la imagen en la pantalla del ordenador se puede reconstruir la imagen usando la emisión conducida en sus cables de alimentación de red. Las imágenes reconstruidas se pueden obtener a partir de la señal relevante debida a la conmutación de las señales de video RGB (rojo-verde-azul) del monitor. La calidad de la imagen reconstruida depende de la frecuencia receptora. Dado que la imagen de la pantalla puede contener información como texto confidencial, la evaluación de la calidad de la imagen reconstruida es muy importante. Es posible medir la señal relevante en la emisión conducida en la red de alimentación en un margen de frecuencias entre 50 y 1000 MHz. En general, la fuga radiante y por conducción desde un PC se emite en un amplio rango de frecuencias debidas principalmente a la conmutación de las señales digitales, tales como los relojes y los buses de datos. Las señales radiadas pueden acoplarse electromagnéticamente con las emisiones de líneas cercanas, como líneas eléctricas y líneas de datos.

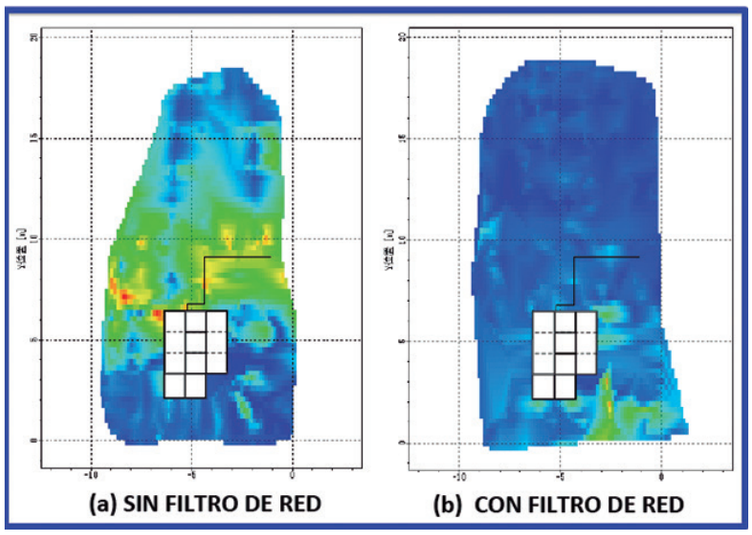

Figura 5: simulación de la intensidad de campo radiado desde la línea de red con y sin filtro de red

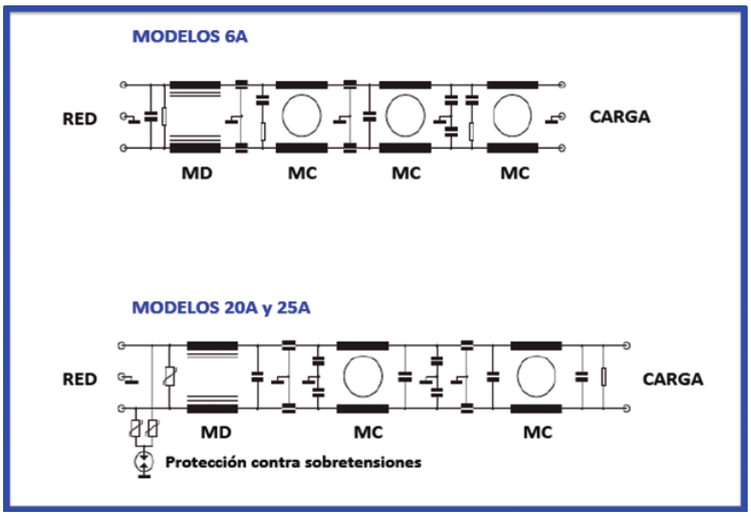

Figura 6: Esquemas básicos de filtros TEMPEST (6, 20 y 25 amperios). MD: modo diferencial. MC: modo común

Así, la señal relevante emitida por la conmutación en las señales RGB puede estar contenida en la emisión radiada. Por otra parte, la señal relevante en las líneas RGB también puede combinarse con las señales en las líneas eléctricas de alimentación.

Es decir, las señales en las líneas pueden acoplarse de forma no deseada por diafonía capacitiva y por diafonía inductiva, o por conducción en los circuitos. Por lo tanto la señal relevante puede también estar contenida en la emisión conducida en los cables de alimentación de red. Por lo tanto, la imagen de la pantalla se puede reconstruir mediante la recepción de la emisión conducida que asimismo podría ser radiada de nuevo al actuar el cable como antena.

Se puede reconstruir una imagen de muestra en un PC a partir de la captación de la emisión conducida en los cables de alimentación utilizando un software de procesado de imágenes. Como ejemplo, la figura 4 (a) muestra una imagen mixta de texto y fotografía visualizada en el monitor del PC (a) (el que tiene más fugas según la figura anterior). Las figuras 4 (b), (c) y (d) muestran las imágenes reconstruidas al recibir las frecuencias de 300, 350, y 750 MHz, respectivamente. La imagen reconstruida fue procesada promediando 256 veces. Las figuras sugieren que la imagen en pantalla puede ser reconstruida con éxito mediante la recepción de la emisión conducida en los cables de alimentación del PC (a). La calidad también depende de la frecuencia de recepción. El texto y la imagen se puede ver vagamente a la frecuencia de recepción de 300 MHz (Figura 4(b)), puede ser claramente reconocida a una frecuencia de recepción de 350 MHz (Figura 4(c)) y es irreconocible a la frecuencia de 700 MHz (Figura 4(d)). La calidad de la imagen reconstruida depende también del nivel de la señal relevante en la emisión conducida. En consecuencia, la visibilidad o legibilidad de una imagen reconstruida, es decir, su calidad, depende de la intensidad de la emisión y de su frecuencia.

Configuración de los filtros TEMPEST

Se ha demostrado que las comprometedoras emanaciones espurias generadas por dispositivos electrónicos puede dar lugar a la fuga de información sensible. La simulación de la intensidad de campo radiado debido a las emisiones conducidas en el cable de alimentación se muestra gráficamente en la figura 5(a) sin el uso de un filtro de red y en la figura 5(b) usando un filtro de red. Es evidente la eficacia del filtro de red en la reducción de las fugas electromagnéticas. Con el fin de mejorar la seguridad de las infraestructuras críticas, como bases militares, centros de procesado de datos de bancos y de grandes empresas se debe usar blindajes y filtros de red además de filtros específicos de datos.

En el caso del filtro de red, su rendimiento se consigue gracias a su buena conexión a tierra. Sin embargo, en situaciones prácticas la buena conexión a tierra es proporcionada por la toma de tierra de protección, que generalmente se encuentra en un solo punto en el armario de distribución de energía. Las pérdidas de inserción de los filtros están directamente relacionadas con las impedancias de entrada y de carga de salida en el filtro. Estas impedancias dependen de la instalación del cable de alimentación, su topología y la conexión de las diversas cargas eléctricas.

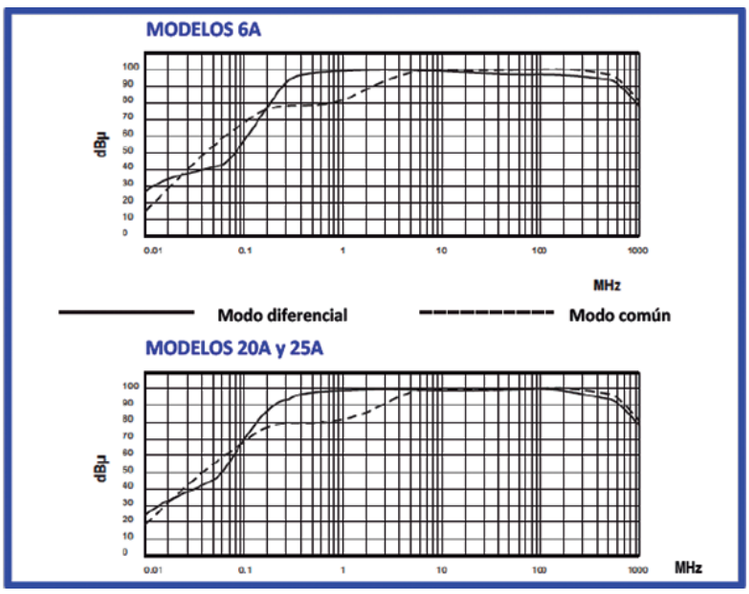

Figura 7: Atenuación de los filtros TEMPEST (6, 20 y 25 amperios) (EMIKON) .

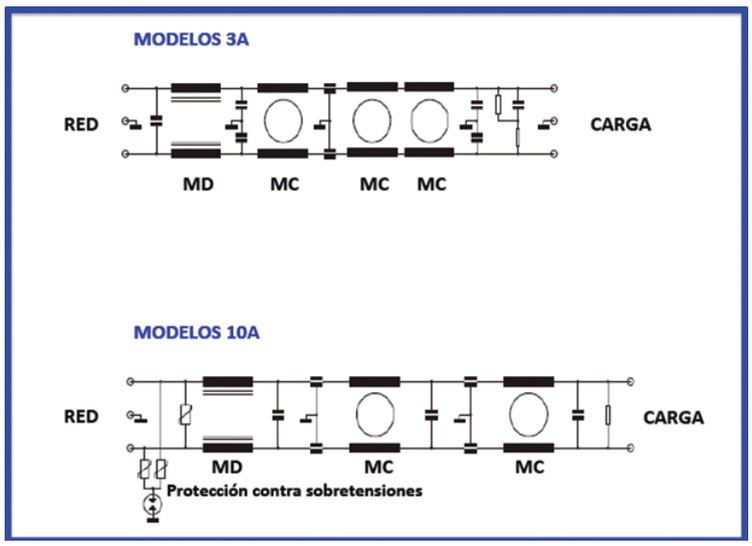

Figura 8: Esquemas básicos de filtros TEMPEST (3 y 10 amperios). MD: modo diferencial. MC: modo común

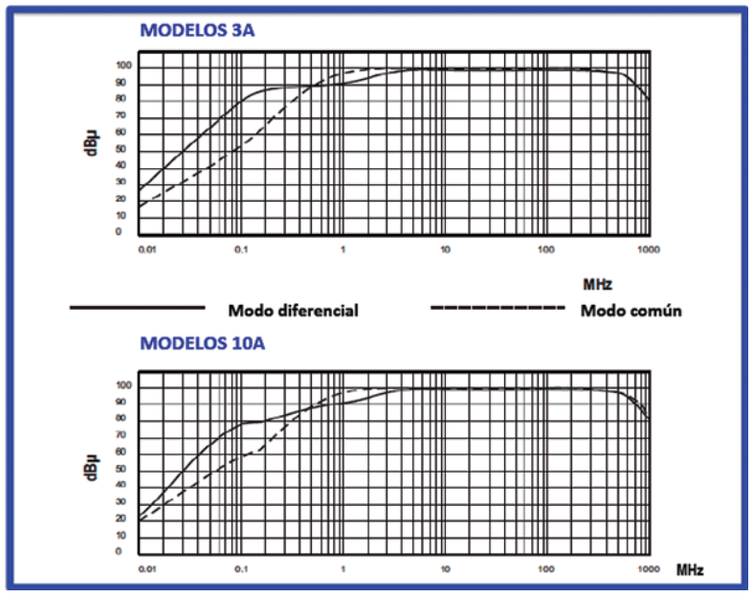

Figura 9: Atenuación de los filtros TEMPEST (3 y 10 amperios) (EMIKON)

Existen considerables diferencias entre los filtros convencionales y los filtros TEMPEST. Las especificaciones TEMPEST son confidenciales y los factores de atenuación requeridos varían de un dispositivo a otro. Las figuras 6 a 9 aportan como ejemplo los esquemas y las gráficas de atenuación de varios filtros TEMPEST del fabricante EMIKON. Estas especificaciones se consiguen mediante filtros diseñados para un amplio rango de frecuencias. El rango de frecuencias abarca desde los 10 KHz hasta 1 GHz para el modo común y también para el modo diferencial. Las señales que exceden este rango de frecuencias son principalmente emisiones radiadas. El filtrado por debajo de 10 KHz es normalmente innecesario. Un filtro de red debe dejar pasar los 50 Hz de la red eléctrica. Las especificaciones de funcionamiento indicadas se logran mediante un circuito multi-etapa y apantallado para conseguir los valores de atenuación en la conmutación de fuentes de alimentación según el nivel B de las normas de emisiones conducidas. Los filtros están herméticamente sellados dentro de sus cajas metálicas y se han fabricado de acuerdo con las especificaciones UL. Cada etapa del filtro se apantalla internamente para reducir el acoplamiento capacitivo entre etapas. Además de los filtros estándar presentados, en caso necesario también se pueden fabricar a medida. La atenuación de los filtros de red convencionales es menor y no abarca un margen de frecuencias tan ancho como lo hacen los filtros TEMPEST.

Conclusiones

Se ha presentado una visión general del problema de las fugas electromagnéticas de equipos críticos, por las que se puede llegar a reconstruir la imagen en la pantalla de un ordenador usando los medios adecuados. Para evitar el robo de datos confidenciales se pueden aplicar varias soluciones siguiendo la normativa TEMPEST. En los centros de procesado de datos que se desea proteger es conveniente aplicar blindajes y filtros de red y datos según normativa TEMPEST entre la zona crítica "roja" y no crítica "negra".

REFERENCIAS

- *Información técnica de los filtros TEMPEST del fabricante EMIKON.*
- *Ross Anderson, "Security Engineering", Wiley, 2010*
- *H. Sekiguchi and S. Seto, "measurement of computer rgb signals in conducted emission on power leads", Progress In Electromagnetics Research C, Vol. 7, 51–64, 2009*
- *MIL-HDBK-232 - Red/Black Engineering-Installation Guidelines*
- *MIL-HDBK-1195 - Radio Frequency Shielded Enclosures*
- *Webs: www.sst.ws/tempest_standards.php y www.jammed.com/~jwa/tempest.html*