LA AMENAZA «TEMPEST». ESA GRAN DESCONOCIDA

Antonio VALLES CASTRO

Cualquier tecnología suficientemente avanzada es indistinguible de la magia.

Arthur C. Clarke

Antes de empezar

URANTE mi destino como profesor en la Escuela Antonio de Escaño tuve la suerte de que llegara a mis manos un curso de algo que hasta el momento nunca había visto. La palabra «TEMPEST» era algo nuevo para mí. Con el tiempo esa materia formó parte de la asignatura de Compatibilidad Electromagnética que yo impartía.

Es un tema cuyo conocimiento debe ser más extendido en la Armada, y bajo mi punto de vista muy importante. Aunque en principio puedan parecer historias de espías de película, lo cierto es que es una amenaza que está ahí y que puede llegar a ser muy peligrosa.

Introducción

En estos últimos años, con el desarrollo de las Tecnologías de la Información se pone de manifiesto la necesidad, en nuestra sociedad, de un mayor control de la información que se maneja, especialmente de la que podríamos considerar sensible.

En este sentido, se ha producido un desarrollo legal importante y se han puesto los medios, por parte de la Administración, con el fin de proteger la información sensible del ciudadano, no solo en el ámbito de esta, sino también por parte de las empresas que la manejan.

La Armada gestiona una gran cantidad de información clasificada, cuyo conocimiento por parte de personas ajenas podría traer consecuencias graves a

la Seguridad Nacional. Es por ello que se hace un esfuerzo mucho mayor para proteger esta información.

La información clasificada es por definición aquella que puede resultar de interés para un posible adversario. Por lo tanto, nos interesa protegerla con todos los medios necesarios para que no llegue a otras manos. Pero para que sea aprovechable, primero tenemos que generarla, después codificarla y por último transmitirla. De nada nos vale una información que no podemos compartir.

Para realizar estas operaciones utilizamos máquinas, y aparece entonces un problema. Estas utilizan sistemas eléctricos y electrónicos que radian, sistemas mecánicos que suenan, sistemas ópticos que se pueden ver, etc. Además no están aisladas, sino que tienen líneas de alimentación, de datos, de transmisión, que pueden ser camino de fuga de la información.

Si el adversario tiene interés e invierte los recursos adecuados, es posible obtener la información clasificada aprovechando el funcionamiento de aquellos dispositivos que la procesan o transmiten.

Aparece entonces el concepto de «Emisiones Comprometidas», fundamental en el mundo TEMPEST, que se define como: «Señales radiadas no intencionadamente, orientadas a inteligencia, cuyo origen puede ser cualquier equipo o elemento de un sistema de información, las cuales si son interceptadas y analizadas pueden comprometer a la seguridad nacional».

Estas señales consisten en energía eléctrica o acústica emitida no intencionadamente por cualquier fuente dentro de los equipos y sistemas que procesan información sensible. Esta energía puede ser relativa al mensaje o a la información, y cuando se procesa puede conducir a la recuperación del texto original.

Dentro del campo de la Seguridad de la Información, uno de los aspectos menos conocidos es el TEMPEST. El objeto de este artículo es dar una visión general sobre este concepto en aspectos como la amenaza, los medios de protección, la normativa aplicable y su organización en España.

Concepto TEMPEST

Para el manejo y tratamiento de la información clasificada es necesario utilizar máquinas. Con ellas se realizan operaciones de generación, codificación y transmisión de la información. Estas máquinas pueden producir emisiones comprometidas que son susceptibles de ser utilizadas por un adversario para extraer información de interés para él. Estas emisiones pueden ser de diferentes tipos, tales como eléctricas, acústicas o luminosas. Este artículo se centrará en las emisiones eléctricas, ya que son las más vulnerables a un ataque TEMPEST.

Dentro del campo de la Seguridad de la Información existe una materia muy importante, que es la Seguridad de las Emanaciones (EMSEC). Como se comentó anteriormente, las máquinas de tratamiento de la información pueden

producir emisiones o emanaciones, y en el caso de que estas emanaciones afecten a la confidencialidad de la información manejada por esas máquinas entonces estaremos hablando de TEMPEST.

Un poco de historia

El concepto TEMPEST, aunque poco conocido, no es nuevo. En 1970 aparece la primera normativa TEMPEST en Estados Unidos, pero los efectos de este problema se remontan a muchos años antes, a los primeros tiempos de las comunicaciones telefónicas y de radio.

El primer caso documentado sobre emanaciones se produjo en el año 1884. Se detectó que se producía acoplo entre las líneas telefónicas de cable paralelo y se solucionó con el par de cable trenzado.

En el año 1914 se produjeron las primeras emisiones comprometidas en un conflicto. Durante la Primera Guerra Mundial se llegaron a recuperar mensajes a través de filtraciones producidas por las tomas de tierra de los cables telefónicos. Se solucionó alejando las primeras tomas de tierra a 3.000 yardas.

En 1946 se recibió en la embajada de los Estados Unidos en Moscú una réplica del escudo americano como regalo del Gobierno soviético. Hasta 1952 no se enteraron de que en ese escudo había micrófonos.

Un documento clasificado en 1972 y desclasificado en 2007 relata un ataque TEMPEST descubierto en 1962 en la embajada de EE. UU. en Japón. Realizando una revisión rutinaria en las inmediaciones de la delegación, se descubrió que en la ventana de un hospital cercano había un dipolo apuntando al edificio.

En el año 1970 se publicó la primera norma TEMPEST. Fue en los Estados Unidos, la NACSIM 5100.

En 1989 un antiguo agente del MI 5 británico escribe un libro en el que relata que en el año 1960, con motivo de la solicitud de entrada en la Comunidad Económica Europea por parte del Reino Unido, quisieron conocer la postura de Francia al respecto. No fueron capaces de hacer saltar la clave diplomática francesa, pero se dieron cuenta de que en medio del tráfico de mensajes cifrados llegaba una débil señal con información en claro. Diseñaron un equipo para recuperar esa información y lo consiguieron.

Existen muchos más casos que no salen a la luz debido a que los descubiertos son en su mayoría clasificados por los gobiernos.

Amenaza TEMPEST

Se puede definir como «Fenómeno relacionado con la emisión electromagnética no intencionada producida por los equipos eléctricos y electrónicos que, detectada y analizada, puede llevar a la obtención de información».

Cualquier circuito eléctrico/electrónico que lleve una corriente variable en el tiempo, emitirá señales electromagnéticas con una potencia de emisión proporcional a la amplitud de tal corriente y a su variación en el tiempo. Estas señales se propagarán más allá de la fuente como ondas en espacio libre y como ondas guiadas por conductores conectados a/o cercanos a la fuente de radiación.

Si las variaciones de corriente en la fuente son relativas de alguna manera al contenido de la información de dichas señales, entonces puede ser posible la reconstrucción de su mensaje original por análisis de estas emisiones no intencionadas. Las características principales de esta amenaza son las siguientes:

— Es una amenaza real.
— Es una alternativa real al análisis criptológico.
— Es muy difícil de detectar. No deja rastro.
— No es necesario el acceso físico para su explotación.
— Es muy seguro para el atacante.

Estas características la hacen muy peligrosa por su dificultad de detección, por no dejar rastro y porque el atacante no necesita acceder físicamente al lugar donde se encuentra la información. Es por ello que los gobiernos dedican muchos recursos a la protección contra esta amenaza.

Concepto RED/BLACK

Un concepto muy importante en el mundo TEMPEST es el RED/BLACK, «que engloba a circuitos eléctricos y electrónicos, componentes, equipos y sistemas, los cuales manejan texto en claro relativo a la seguridad nacional en forma de señal eléctrica (RED) por contraposición de aquellos que manejan información encriptada o cifrada (BLACK)».

Básicamente se engloban en el concepto RED todas aquellas señales clasificadas no cifradas, las líneas, componentes y equipos que las procesan y aquellas aéreas donde se encuentren.

Serían BLACK aquellas señales no clasificadas o cifradas, las líneas, componentes y equipos que las procesan y aquellas aéreas donde se encuentren.

Mecanismos de propagación

Como se ha señalado anteriormente, cualquier señal que varía en el tiempo genera un campo eléctrico (E) y uno magnético (H), perpendiculares entre sí y proporcionales a su amplitud y a su frecuencia. Estos campos electromagnéticos pueden contener información comprometedora de la señal procesada o de otras próximas. Pueden también alcanzar otras líneas y producir un acoplamiento

de la información radiada. A su vez, la segunda línea puede generar otro campo electromagnético con trazas de la información original.

Básicamente existen dos mecanismos de propagación de las señales TEMPEST:

— *Radiación:* siempre que una señal RED es generada o procesada en un equipo, se origina un campo eléctrico, magnético o electromagnético. Si este campo electromagnético sale fuera del equipo, puede ser detectado por radiación.
— *Conducción:* si además este campo electromagnético se acopla a cualquier tipo de conductor que salga del espacio controlado o a líneas BLACK que escapen de la instalación, puede ser detectado por conducción. Entre este tipo de líneas no solo se consideran las de señal, sino también las de alimentación.

Las distancias de interceptación/propagación y el análisis de tales emisiones están afectadas por una variedad de factores, tales como el diseño, instalación y condiciones del entorno relativas a la seguridad física.

Tipos de señales TEMPEST

Las señales TEMPEST de interés, a las que se deben dedicar recursos para reducir su magnitud, son todas aquellas que proceden del proceso, almacenamiento y transmisión de la información. Por lo tanto, serán señales tanto internas de equipos como procedentes de interfaces de comunicaciones. En función del tipo de proceso y velocidad del mismo, la complejidad para la reconstrucción de la información será mayor o menor. Los tipos de señal más importantes son audio, vídeo, datos serie y datos paralelos.

El equipamiento necesario para poder captar y explotar emisiones comprometidas consta de una antena de alta ganancia, un receptor de banda ancha y un procesador que permita la digitalización, proceso y reconstrucción de la señal captada.

Protección TEMPEST

Hasta ahora, hemos analizado el problema TEMPEST. A continuación veremos cómo protegernos del ataque TEMPEST.

A la hora de buscar los medios más adecuados para la protección TEMPEST tenemos que tener en cuenta en primer lugar la amenaza, con parámetros como el interés en la información, los medios técnicos y la libertad de operación del agresor. Por otra parte deberemos tener en cuenta la vulnerabil-

idad de los equipos y locales, la temporalidad de las instalaciones y la zona de seguridad con la que se cuenta. Todo ello nos debe llevar a un compromiso de optimización entre los objetivos y los recursos utilizados para su consecución.

Evaluación y reducción de las emisiones comprometidas de equipos

Una aproximación maximalista y de sentido común nos llevaría a proteger mediante blindaje todos y cada uno de los equipos de una instalación de proceso de la información en la que se manejaran señales en claro (RED). Esta solución, aunque correcta, no es la óptima debido a su elevado coste, tanto de adquisición como de mantenimiento.

Como todos los equipos radian y es muy costoso reducir las emisiones comprometidas, se realizan perfiles de radiación en Jaula de Faraday y se establece una clasificación de los equipos y sistemas en función del nivel de radiación. Dependiendo de esa clasificación, los equipos se utilizarán en los correspondientes locales y en el tratamiento de una determinada información.

Merecen especial mención los equipos con certificación TEMPEST, que están basados en sistemas comerciales especialmente modificados en cuanto a su apantallamiento, filtrado, etc., y son especialmente adecuados para la protección TEMPEST, aunque su coste es muy alto.

Organización y separación de líneas

La organización del cableado es un elemento fundamental para la protección TEMPEST. Es necesario un control muy riguroso en la instalación y mantenimiento del cableado de los equipos, especialmente en la separación de estos y de los cables rojos y negros.

Este control sobre el cableado es muy riguroso en las plataformas y en las instalaciones móviles (buques, aviones, helicópteros, vehículos, etc.), debido a la gran cantidad de equipos y al poco espacio del que disponen.

Es fundamental tener en cuenta ciertos conceptos, como la separación entre cables rojos y negros, la utilización de cables apantallados, la eliminación de conductores de fortuna y el filtrado de las líneas.

Acondicionamiento de equipos y locales

Un método utilizado a menudo para la protección TEMPEST es el acondicionamiento de equipos y locales con diferentes sistemas de apantallamiento, ya sean temporales o permanentes. Algunos de los sistemas más utilizados son:

— Armarios apantallados.
— Salas apantalladas.
— Apantallamientos fuertes, como Jaulas de Faraday.
— Apantallamientos débiles, como telas o pinturas metalizadas.

Diseño de infraestructuras. Evaluación ZONNING

La protección por zonas (ZONNING) es un método de control utilizado cuando se requieren diferentes niveles de protección. Se establece una clasificación de los locales en función de la atenuación hasta el perímetro de seguridad. Se deben tener en cuenta las propiedades de atenuación de un local y el espacio inspeccionable (1).

Por ejemplo, un generador «rugerizado» puede operar sin problemas en un área de muy baja atenuación, quizá únicamente con una instalación de tierra adecuadamente protegida. Una fuente de alimentación ininterrumpida (UPS) y sus equipos de comunicación asociados pueden requerir un nivel medio-bajo de protección, y una sala que albergue los ordenadores y equipos de proceso muy sensibles puede demandar niveles altos.

Una estrategia comúnmente utilizada consiste en definir zonas sucesivamente, cada una dentro de la siguiente, de forma que el nivel de protección es creciente conforme progresamos hacia el interior. Por ejemplo, podemos definir la zona 0, las más protegida, donde se puede poner cualquier instalación sin problema, o la zona 3, la más sensible para ordenadores y equipos de proceso y cifrado.

El método de protección ZONNING comporta lógicamente un ahorro de costes en blindajes, métodos y procedimientos de protección y en el mantenimiento de los mismos. Puede aplicarse a nivel de una instalación completa o solamente de elementos aislados, y sirve como una excelente herramienta para decidir lo que es crítico y cómo debe ser protegido.

En el Ministerio de Defensa, la evaluación ZONNING la realiza el Centro Criptológico Nacional (CCN), auxiliado por varios laboratorios acreditados.

Certificación TEMPEST

El procedimiento para asegurar que se cumplen los requisitos TEMPEST en los sistemas de proceso de información es la Certificación TEMPEST. El

(1) Espacio tridimensional alrededor de un equipo que procesa información clasificada, dentro del cual se tiene la Autoridad para identificar y expulsar a un potencial atacante dificultando el acceso a señales TEMPEST.

organismo encargado de realizarla es el CCN, que actúa como elemento de certificación del Esquema Nacional de Evaluación y Certificación de la Seguridad de las Tecnologías de la Información. Así lo estipula el R. D. 421/2004.

Una certificación TEMPEST consta de tres fases diferenciadas: inspección, evaluación y certificación. Solamente se certifica si, una vez inspeccionada y evaluada, cumple con todos los requisitos que dicta la ley.

TEMPEST en España

El lugar de referencia en el campo del TEMPEST en España es el Centro Criptológico Nacional, que depende orgánicamente del Centro Nacional de Inteligencia (CNI).

Su creación y sus cometidos están determinados por la Ley 11/2002, de 6 de mayo, reguladora del Centro Nacional de Inteligencia, y en el Real Decreto 421/2004, de 12 de marzo, por el que se rige el CCN, cuyos cometidos más importantes son los siguientes:

— Evaluación ZONNING de locales y equipos.
— Certificación TEMPEST de equipos.
— Evaluación de armarios y salas apantalladas.
— Desarrollo de normativa TEMPEST.
— Evaluación de plataformas.
— Inspecciones TEMPEST de locales.
— Asesoramiento y apoyo a Industria Nacional.

En su función de evaluación está auxiliado por diferentes laboratorios acreditados del Ministerio de Defensa. Estos centros se encargan de las evaluaciones ZONNING de instalaciones. Hasta el momento no se han realizado evaluaciones TEMPEST en las plataformas de la Armada.

Actualmente está en proceso la designación del Centro de Medidas Electromagnéticas de la Armada como organismo encargado de realizar las evaluaciones a las plataformas de nuestra Marina.

Conclusiones

Todos los equipos de generación, proceso y transmisión de la información producen emisiones comprometidas. Estas señales son un posible camino de fuga de información. Si un adversario tiene interés por esa información, y posee los recursos necesarios, esta puede llegar a sus manos.

En el ámbito de la Seguridad de la Información, el campo de la Seguridad de las Emanaciones es muy importante, sobre todo en el aspecto que cubre la confidencialidad de la información. Aparece entonces el TEMPEST.

Por sus características, el ataque TEMPEST es muy dañino. Es una amenaza real, por mucho que pueda parecer de ciencia ficción; no necesita que el atacante acceda físicamente a la instalación donde se trata la información, y no deja rastro. Un adversario con los medios adecuados, con tiempo y con paciencia, puede llegar a extraer información sensible.

Existe una variada metodología para defenderse de los ataques TEMPEST. En la utilización de los métodos de protección TEMPEST prima la optimización de recursos. Es por ello que el más utilizado es el ZONNING, que consiste en establecer una clasificación de los locales en función de la atenuación de la señal hasta el perímetro de seguridad.

El centro de referencia en España en el campo de TEMPEST es el CCN. Este organismo, con dependencia orgánica del CNI, es el encargado, entre otras misiones, de promulgar la normativa y realizar las evaluaciones y certificaciones TEMPEST, tanto a equipos como a dependencias.

Hasta el momento las medidas para las evaluaciones ZONNING de dependencias las realizaban organismos pertenecientes a los Ejércitos de Tierra y del Aire. Por la necesidad de evaluación TEMPEST de las plataformas en buques, está en proceso el nombramiento del CEMEDEM como centro TEMPEST de la Armada.

Es necesario que haya una mayor difusión de este fenómeno, en especial para los que tienen tareas en el campo de la operación y el mantenimiento de equipos de proceso y transmisión de la información, para que conozcan la normativa aplicable, los métodos de protección y se conciencien de la necesidad de mantener la Seguridad de las Emanaciones y en especial la protección contra ataques TEMPEST.

BIBLIOGRAFÍA

Guía/Norma de Seguridad de las TIC (CCN-STIC-400) del CCN, 2013.

KUHN, Markus G.; ROSS, J. A.: *Soft TEMPEST: Hidden Data Transmission Using Electromagnetic Emanations*. University of Cambridge. 1998.

MIL-STD-1680 Instalation and RED/BLACK Engineering Criteria for Secure Electrical Information Processing Systems.

NATO SDIP-28 NATO Zoning Procedures, 2009.

WRIGHT, Peter: Spycatcher: *The Candid Autobiography of a Senior Inteligente Officer*. W. Heinemann. 1987.

Real Decreto 421/2004, de 12 de marzo, por el que se regula el Centro Criptológico Nacional.

Transbordo de combustible en la mar.
(Foto: G. García Galán).