PUNTO SEGURIDAD, DEFENSA DIGITAL I NÚMERO 11 I AGOSTO 2011 I ISSN EN TRÁMITE
REVISTA BIMESTRAL

.Seguridad

¿A dónde va tu información?

La Geoetiquetación: Los riesgos de hacer pública tu ubicación

No. 11

En este número

Editorial

Actualmente, las tecnologías de la información y comunicación despuntan como un paradigma que inmiscuye a la sociedad que las consume en su totalidad desde el usuario casero hasta los sitios gubernamentales o foros internacionales.

En esta edición 11 de la revista **.Seguridad**, quisimos ofrecer nuevamente a nuestros lectores temas diversos que hoy por hoy están dejando huella en la era digital.

Como ya es costumbre, abordamos temas de gran actualidad sobre seguridad informática, con los que pretendemos transmitir ese vínculo directo que tienen con nuestra vida cotidiana, tópicos como las geoetiquetas, la seguridad de las redes inalámbricas, buenas prácticas y los sistemas de detección de intrusos. En nuestra sección de consejos, te presentamos tips prácticos para que puedas cifrar desde un archivo hasta todo tu disco duro.

Esperamos que este número sea de tu agrado no olvides enviarnos tus sugerencias u opiniones al correo de contacto revista@seguridad.unam.mx

Bienvenido nuevamente a .Seguridad, defensa digital.

Galvy Ilvey Cruz Valencia
Subdirección de Seguridad de la Información

¿Crees que tu red inalámbrica es segura?

Por Erika Gladys De León Guerrero*

Cada vez es más frecuente el uso de tecnologías inalámbricas, ellas representan movilidad, una característica sumamente importante en nuestros tiempos.

Una particularidad que define a este tipo de tecnologías, es el uso de ondas electromagnéticas como medio de transmisión, lo cual conduce a un alto grado de descontrol en los límites geográficos por los cuales se extiende una red. Una red cableada está limitada en cuanto a extensión con base en elementos físicos internos en la infraestructura de la organización, en cambio, una red inalámbrica se extiende más allá de los limites organizacionales, ampliando su alcance a algunos metros fuera del área destinada para la red, permitiendo el acceso incluso a kilómetros si se cuenta con la antena indicada.

Sin una detección oportuna, esta falta de control facilita el acceso no autorizado a la red. Para atender esta problemática, surgieron protocolos de seguridad para redes inalámbricas, sin embargo, no todos ellos dieron el resultado deseado, pero sí cierta confusión, ya que el usuario usa como medida preventiva un protocolo que brinda la falsa sensación de seguridad al permitir la intrusión, nos referimos al protocolo WEP (Wired Equivalency Privacy), un protocolo que estructuralmente presenta vulnerabilidades significativas que atentan contra la seguridad de la red.

La problemática de WEP

WEP está diseñado con la finalidad de proporcionar seguridad a una red inalámbrica, pero lamentablemente, su estructura da lugar a muchas vulnerabilidades.

La primera vulnerabilidad la localizamos en cómo este protocolo maneja estáticamente las claves. Por otro lado, el protocolo WEP opera vectores de inicialización *VI* utilizados para obtener claves distintas para cada trama. Para generar las claves son necesarias dos partes, una configurada por el usuario (clave compartida) y la otra es el vector de inicialización (Figura 1). Este vector de 24 bits, resulta insuficiente para la cantidad de paquetes manejados, lo que implica la repetición de claves.

Un intruso puede recolectar una cantidad pequeña de paquetes para determinar el valor del flujo de bits y de la clave compartida, es decir, la parte de la clave configurada con el usuario, y de esta manera, tener acceso a la red inalámbrica.

* Ingeniera en Computación por la UNAM. Colaboradora de la Subdirección de Seguridad de la Información (SSI/UNAM-CERT) en el Área de Auditoría y Nuevas Tecnologías, realizando pruebas de Penetración y Análisis de Vulnerabilidades, así como investigación sobre nuevas tecnologías de seguridad para la emisión de recomendaciones. Fue miembro del Plan de Becarios de Seguridad en Cómputo impartido por el UNAM-CERT a través de la Dirección General de Servicios y Cómputo Académico. Se encuentra desarrollando un sistema de prevención de intrusiones para Redes Inalámbricas.

Figura 1. Estructura de clave WEP

La segunda problemática presente en el protocolo WEP está en el sistema de integridad empleado, ya que posee un error de implementación grave, utiliza el algoritmo CRC-32[i] pensado para problemas producidos de forma involuntaria por el sistema de transmisión, los paquetes cuyo CRC-32 sea incorrecto, simplemente serán rechazados. Sin embargo, el sistema no contempla las modificaciones maliciosas que puedan realizarse a los paquetes, ya que al ser un algoritmo lineal, permite la reconstrucción de códigos, admitiendo que un intruso altere ciertos bits en los datos para mantener coherencia en el resultado de la aplicación del algoritmo CRC-32. Esta vulnerabilidad permite a un intruso insertar paquetes en la red con contenido apócrifo. Por si fuera poco, existen herramientas que facilitan esta labor, un ejemplo se muestra en la *Figura 2*.

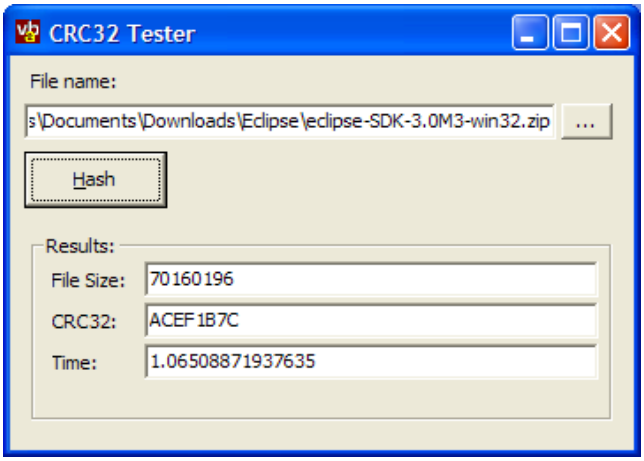

Figura 2. Calculador de checksums CRC-32

Después de revisar las vulnerabilidades presentes en el protocolo WEP, podría creerse que es un protocolo caduco, sin embargo, existen actualmente muchos Access Points que ejecutan este protocolo, y algunos ISP (Internet Service Provider) lo configuran como protocolo de protección por default. Este dato lo podemos constatar mediante una toma de la identificación de redes y sus protocolos en un lugar aleatorio (*Figura 3*).

[i] Cyclic Redundancy Check. Código detector de errores. Número calculado en función de un mensaje, para validación de integridad.

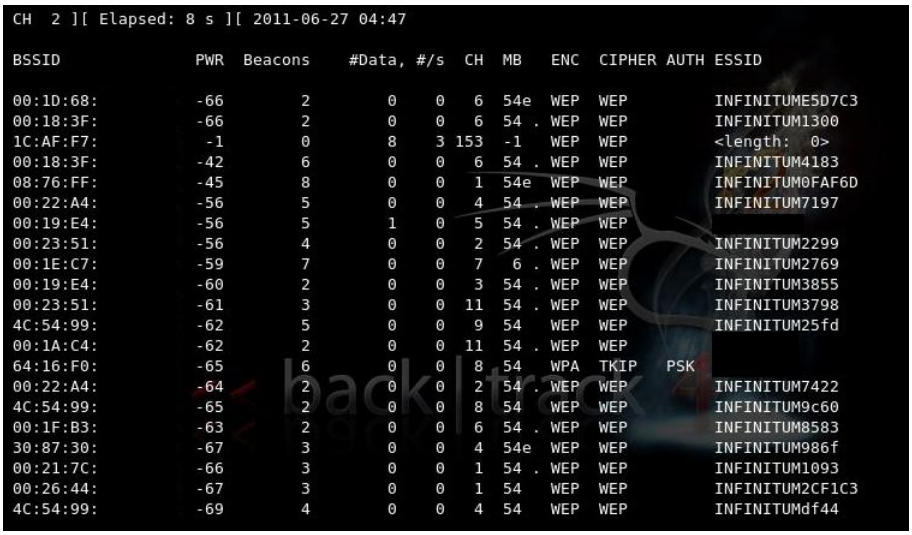

Figura 3. Identificación de redes inalámbricas y su protocolo de seguridad.

Como puede observarse, aún existen redes empleando este protocolo de protección, pero ¿qué implica esto? Un usuario común, confía en que su red está protegida por un protocolo de seguridad, lo que no sabe es el grado de seguridad proporcionado. Esta confianza excesiva, lo lleva a no implementar medidas alternas como el uso de cifrado tanto en conversaciones de Messenger como en el envío de correos electrónicos por esa red supuestamente segura. Lo cierto es que basta una tarjeta de red inalámbrica con capacidad de inyección de paquetes para obtener en cuestión de segundos la clave de acceso a una red inalámbrica protegida con protocolo WEP.

¿Qué pasa con WPA y WPA2?

Al identificar las vulnerabilidades del protocolo WEP, surgen otros protocolos, como WPA y WPA2, los cuales reparan las vulnerabilidades surgidas en el primer protocolo, pero añaden debilidades nuevas.

Vale aclarar que existen dos distintos tipos de implementación en estos protocolos: WPA/WPA2 Enterprise y WPA/WPA2 con PSK (Llave pre compartida).

La primera implementación se encuentra basada en certificados, validados mediante un servidor de autenticación, generalmente RADIUS. WPA/WPA2 con PSK valida una clave configurada por el usuario con tamaño de 128 ó 256 bits, se complementa con un vector de inicialización de 48 bits, aclárese, que WPA y WPA2 fortalecen WEP, esto quiere decir que toman gran parte de la arquitectura de este protocolo, pero implementan medidas para eliminar las vulnerabilidades.

Para permanecer protegido con estos protocolos, se deben dar ciertas condiciones. WPA/WPA2 PSK tiene como punto medular el establecimiento de una contraseña segura, lo cual implica el uso de caracteres alfanuméricos, mayúsculas y minúsculas, caracteres especiales, así como evitar el empleo de palabras que puedan encontrarse en un diccionario y sus derivados (no importando el idioma), por ejemplo, la sustitución de ciertas letras por

números, y por supuesto, que su longitud sea mayor a 8 caracteres. En el caso de WPA/WPA2 Enterprise, es necesario un resguardo celoso de los certificados de autenticación.

Si la clave configurada no presentara los requisitos necesarios para una contraseña suficientemente segura, la clave en WPA y WPA2 PSK podría ser descubierta por un intruso, comprometiéndolos, ya que la fortaleza de este par de protocolos se basa en la clave configurada por el usuario.

El tipo de ataques que permiten la identificación de la clave precompartida son los de fuerza bruta y diccionario. Si se cuenta con un diccionario lo suficientemente completo, con combinaciones adecuadas entre números y letras, es posible obtener un gran cantidad de claves. Si los recursos y diccionarios no fueran adecuados, existen sitios en Internet que proporcionan los medios necesarios para la obtención de claves, procesamiento y diccionarios, un ejemplo es http://www.wpacracker.com/ (Figura 4), en el que basta con proporcionar el archivo *.cap* que contiene el handshake[ii] entre un usuario conectado y el Access Point para que WPA Cracker obtenga la clave en 20 minutos.

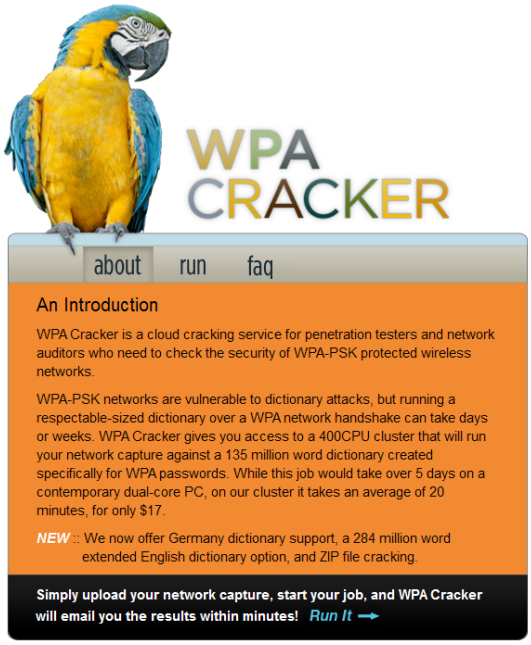

Figura 4. Sitio que proporciona recursos para obtener claves WPA

Consecuencias

Una vez que el intruso haya obtenido la clave de acceso, ya sea de WPA, WPA2 o WEP, puede con facilidad entrar a la red y aplicar algún método de suplantación de identidad, por ejemplo el ataque conocido como "*Man in the middle*", y capturar los paquetes que transiten de un usuario a otro dentro de la red, lo que implica pérdida de confidencialidad, y en algunos casos, de integridad de los paquetes que atraviesan la red afectada.

[ii] Mecanismo con el cual, un cliente y un Access Point inician una comunicación inalámbrica.

¿Qué hacer para evitar la conexión de usuarios no permitidos a una red?

Se expusieron los problemas existentes en los distintos protocolos de seguridad de las redes inalámbricas, ahora el lector sabe que es necesario estar conscientes del riesgo que se corre al no tomar las medidas precautorias necesarias.

A continuación, se exponen algunos puntos recomendados para evitar ser víctimas de usuarios malintencionados que busquen irrumpir en una red inalámbrica.

- Es necesario cambiar el protocolo de seguridad usado por la red, en caso de ser WEP, configurar WPA ó WPA2.
- El protocolo mas recomendado es WPA/WPA2 Enterprise, pero en caso de tratarse de una red casera o que existan dificultades para la instalación de un servidor RADIUS, puede optarse por WPA/WPA2 PSK, con una clave fuerte.
- En caso de tener configurado WPA ó WPA2, siempre es necesario configurar una contraseña robusta y cambiarla cada determinado tiempo, 1 vez cada 3 meses es lo idóneo.
- Modificar la contraseña configurada por default por el ISP.
- Proteger el Access Point con una contraseña de interfaz de administración fuerte.
- Regular la frecuencia con la que se transmitirá.
- Monitorear constantemente el Access Point, verificando el historial de los usuarios conectados.
- En caso de detectar usuarios desconocidos en el historial de usuarios conectados, modificar de inmediato la contraseña, tanto la de administración del Access Point como la de acceso a la red.
- Mantener prendido el Access Point sólo cuando sea necesario.
- Aplicar medidas de seguridad recomendadas en el sitio http://www.seguridad.unam.mx/usuario-casero/

Sitios de interés

- http://www.wi-fiplanet.com/tutorials/article.php/1368661/80211-WEP-Concepts-and-Vulnerability.html
- http://www.netcraftsmen.net/resources/archived-articles/578-how-secure-is-wep-anyway.html
- http://www.wi-fiplanet.com/news/article.php/3784251/WPA-Vulnerability-Discovered.htm

Geoetiquetación: Los riesgos de hacer pública tu ubicación

Por Israel Andrade y Cecilia Espinosa*

Hoy en día, el fácil acceso a la tecnología nos permite compartir ideas y experiencias por medio de imágenes, videos, texto y sonidos de manera ágil a través de las redes sociales. Además nos permite enriquecer nuestras formas de comunicación al combinar diferentes contenidos entre sí y con otras tecnologías.

La Geoetiquetación es una tecnología con la que podemos vincular datos de localización geográfica a los contenidos digitales como imágenes, texto, videos, etc., logrando un impacto en la comunicación relacional.

Ejemplos de lo anterior es la fotografía digital y los mensajes de texto. La fotografía digital al integrarse con tecnologías GPS (Global Position System) permite conocer la ubicación geográfica de las fotografías; mientras que en el caso de mensajes de texto, se puede llegar a conocer el origen del mensaje. Redes sociales como Flickr, Twitter y Facebook han popularizado y facilitado el consumo de esta tecnología y cada vez son más los usuarios que aprovechan los beneficios de estos servicios (*Figura 1 y Figura 2*).

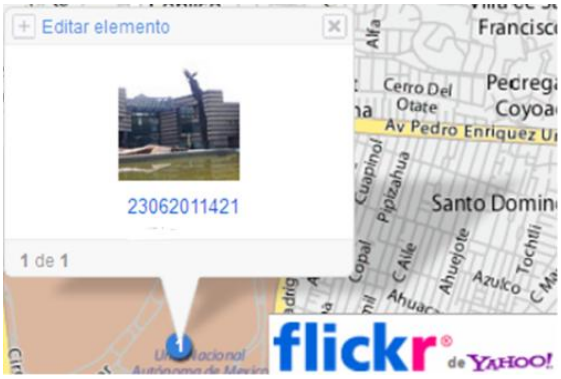

Figura 1. *Flickr* permite ubicar en un mapa las fotografías que contengan datos GPS incrustados. En la figura se observa el "Amoxcalli" dentro de Ciudad Universitaria en la Ciudad de México.

Figura 2. *Twitter* permite vincular un mensaje de texto con la ubicación geográfica del autor en el momento de la publicación.

---

* **Israel Andrade** es Ingeniero en Computación, por FES Aragón. Se desempeña como Auditor interno de la SSI. Actualmente cursa una maestría.

Cecilia Espinosa. Ingeniera en Computación por la Facultad de Ingeniería, UNAM. Laboró en el Departamento de Seguridad en Sistemas de la Subdirección de Seguridad de la Información/UNAM-CERT como responsable de seguridad de base de datos. Posteriormente, se incorporó al Departamento de Auditoría y Nuevas Tecnologías, en la que se desempeña hasta la fecha como analista de vulnerabilidades. Actualmente, colabora en el análisis de riesgos de la misma subdirección y cursa una maestría.

Es importante enfatizar que cualquier tipo de dato que haga referencia a nuestra ubicación debe ser considerado “privado", por la simple razón de brindar información relacionada con lugares que frecuentamos o con actividades que realizamos cotidianamente. Por ejemplo, las fotografías geoetiquetadas podrían generar un mapa ilustrando de nuestras actividades diarias (Figura 3), los lugares de convivencia con nuestra familia y amigos, así como la ubicación de nuestras pertenencias.

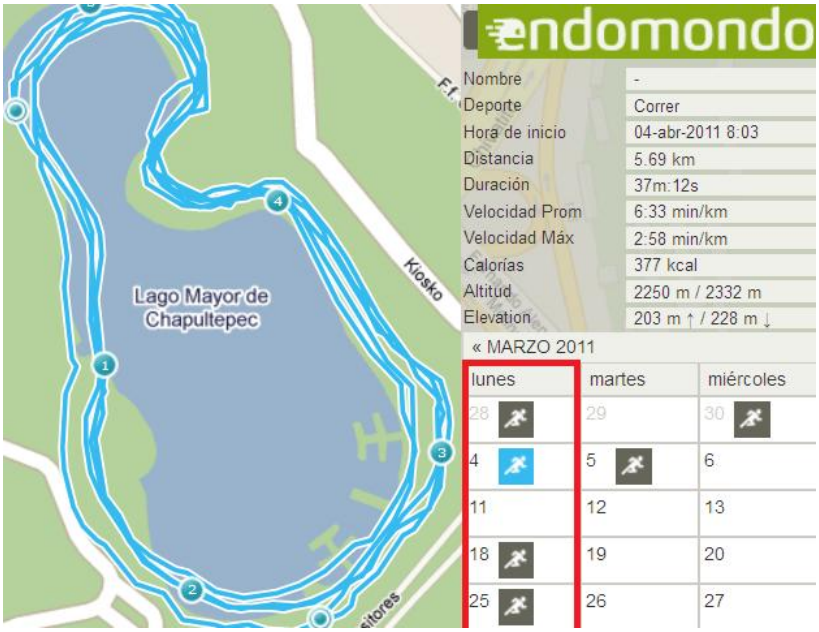

Figura 3. El servicio de *“endomondo”* permite llevar un registro de actividades deportivas referenciadas con datos GPS. En la figura se ilustra un ejemplo de información de actividades cotidianas.

Riesgos de seguridad

1. **Fuga de datos**

   El primer y principal riesgo de seguridad a la que nos enfrentamos con el uso de la geoetiquetación, es la fuga inconsciente de datos de ubicación a través de las redes sociales Esto ocurre por desconocimiento sobre el funcionamiento de estas tecnologías en nuestros dispositivos móviles, ya que algunos de ellos están configurados para incrustar geoetiquetas de forma automática (*Figura 4)*.

   En agosto del 2010, Adam Savage, conductor del programa Cazadores de Mitos (MythBusters), publicó en Twitter una fotografía de un automóvil estacionado fuera de su casa, la imagen contenía una geoetiqueta con información exacta del lugar en el que se tomó la foto, revelando la dirección de su casa. Además el mensaje de la imagen decía “Voy al trabajo”. Con toda esta información publicada inconscientemente, el famoso conductor proporcionó datos muy valiosos que pudieron ser aprovechados por ladrones. [1]

[1] http://www.nytimes.com/2010/08/12/technology/personaltech/12basics.html?_r=2

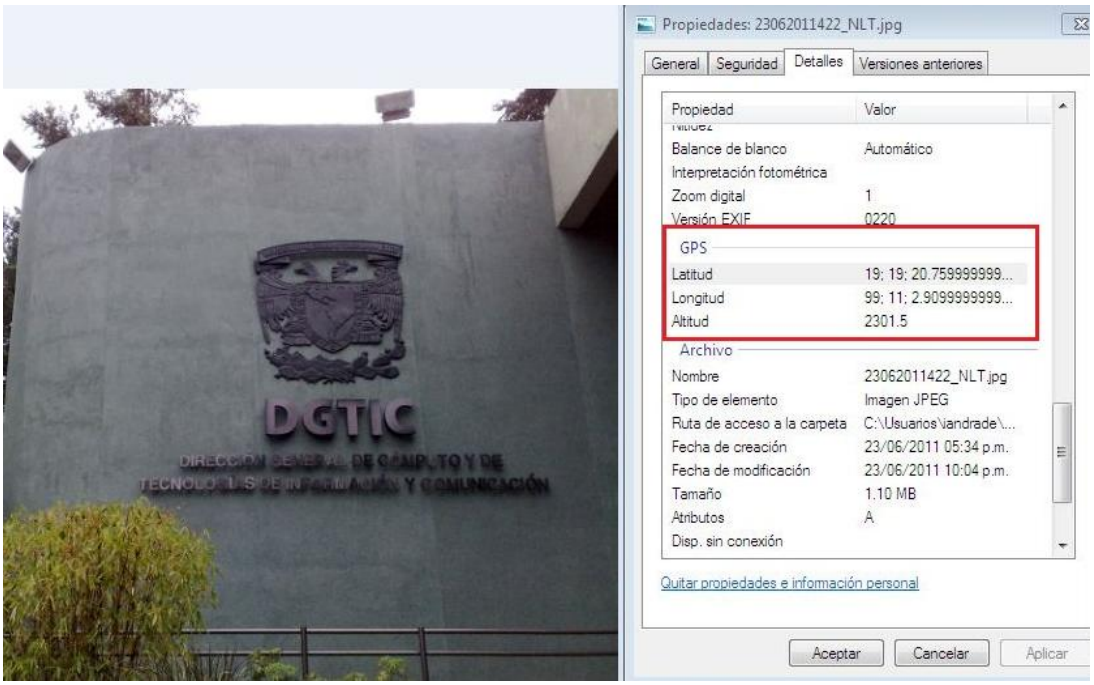

Figura 4. Datos de ubicación (georreferencia) incrustados automáticamente por la cámara digital.

2. Configuraciones deficientes

El segundo riesgo, es la deficiencia en las configuraciones de privacidad específicamente con los servicios y aplicaciones de redes sociales donde compartimos información georreferenciada. Una configuración deficiente (*Figura 5*) podría permitir que personas mal intencionadas tengan acceso a datos de nuestra ubicación, aprovechándose de esto para realizar acciones criminales. Por ejemplo, a través de mensajes o imágenes georreferenciadas se puede conocer el comportamiento y rutinas de una persona, datos suficientes para realizar un secuestro.

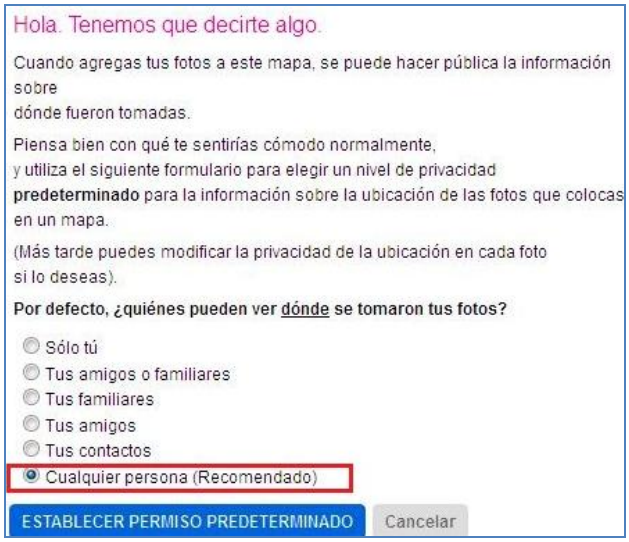

Figura 5. Ejemplo del panel de configuración predeterminada de Geoetiquetación. En la figura se resalta una mala práctica de privacidad, la cual permite que cualquier persona tenga acceso a nuestros datos de ubicación.

3. **Pérdida o robo de dispositivos móviles**

Muchos dispositivos móviles integran sistemas GPS que pueden almacenar la ubicación geográfica, sitios de interés, números telefónicos y fotografías de contactos, si estos dispositivos son robados o extraviados y no están protegidos mediante contraseña, toda esta información se verá seriamente comprometida y podría ser usada para extorsiones y secuestros, *(Figura 6)*.

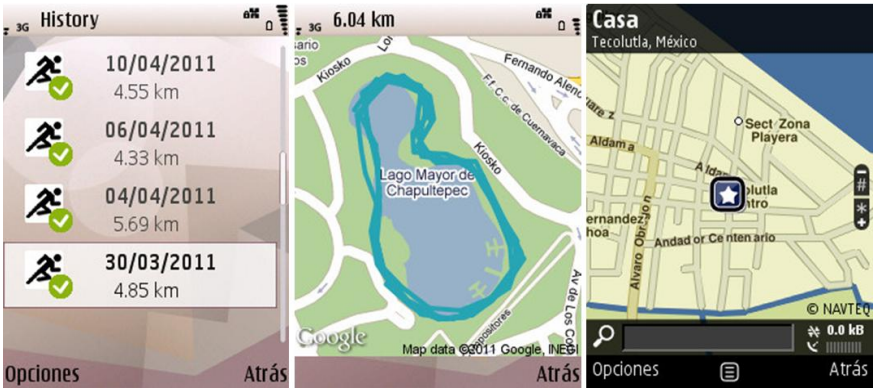

Figura 6. Ejemplo de datos privados geoetiquetados que pueden ser encontrados en un dispositivo móvil.

Prevenir el mal uso de tu información

A continuación, te exponemos algunas sugerencias que pueden ayudar a aprovechar al máximo los beneficios de esta tecnología minimizando los riesgos:

- Lee el instructivo de tu cámara digital o teléfono móvil para que conozcas su funcionamiento y puedas configurar adecuadamente el GPS. Desactiva la funcionalidad del GPS y sólo actívala cuando vayas a utilizarla.
- Si vas a publicar un contenido digital que contenga datos de tu ubicación, asegúrate que sólo esté disponible para personas de confianza, esto lo puedes realizar al restringir el acceso a tu información visitando la sección de configuración de tus redes sociales.
- Recuerda que una fotografía puede decir más que mil palabras, ésta puede dar información de los sitios que más frecuentas, horarios de visita y ubicación geográfica. Piensa dos veces antes publicarla.
- Muchos dispositivos móviles o GPS tienen la capacidad de almacenar ubicaciones para acceder a ellas rápidamente, evita poner nombres que den información extra como: “Mi Casa”, “Trabajo de mi hermano”, “oficina”, “casa de mi novia”, etc.
- Asegura con contraseña el acceso a tu dispositivo móvil, ya que existe el riesgo de extravío o robo del mismo y por lo tanto de tu información.

El empleo de tecnologías innovadoras o emergentes siempre debe ir acompañado de medidas básicas de seguridad, sé consciente del tipo de información que generas, transformas, almacenas o comunicas, sin olvidar los riesgos que implica. Contribuye a mantener una cultura

de seguridad de la información que propiciará un ambiente en el que se confíe en las nuevas tecnologías y sus aplicaciones.

Referencias:

- http://es.wikipedia.org/wiki/Geoetiquetado
- http://icanstalku.com/how.php#disable
- https://support.twitter.com/articles/20169204-sobre-los-tweets-con-ubicacion
- http://www.google.com/url?sa=t&source=web&cd=1&ved=0CBcQFjAA&url=http%3A%2F%2Fwww.icsi.berkeley.edu%2Fpubs%2Fnetworking%2Fcybercasinghotsec10.pdf&ei=VRZfTKWOKYH48Aaxt5m2DQ&usg=AFQjCNFao3oZgrGHMocb6OaezV_K4Rpckg&sig2=2r3Dc2r2KRTW6wWIz_NVLg
- https://support.twitter.com/articles/20169204-sobre-los-tweets-con-ubicacion
- http://www.icsi.berkeley.edu/pubs/networking/cybercasinghotsec10.pdf

Buenas prácticas, estándares y normas, un punto de partida para la seguridad de la información

Por Ing. Jeffrey Steve Borbón Sanabria*

"La seguridad de la información es parte activa de nuestra actualidad"

La anterior frase ilustra el momento que enfrentamos actualmente en diferentes entornos como el laboral, el educativo y cada vez más, en el hogar. Términos como copia de seguridad, privacidad, antivirus, cifrado, son con el paso de los días parte de nuestro léxico y lo seguirán siendo aún más con la popularización del uso de recursos tecnológicos en casi todos los entornos y espacios.

En la medida que se trabaja inmerso en el mundo de la seguridad de la información y la seguridad informática, aumenta la necesidad de difundir la educación en estos temas; sin embargo, en espacios laborales o educativos no es tan simple como el compartir con un amigo y decirle qué antivirus emplear o cómo proteger su teléfono celular del robo de información. Por ello, es necesario buscar guías y documentos que ilustren cómo abordar la seguridad de una forma responsable, procedimental y orientada al cumplimiento de los estándares mínimos requeridos para la tecnología actual.

Pero surge una duda, ¿qué es un estándar y por qué son tan mencionados en la actualidad? Pues bien, un estándar es un documento con un contenido de tipo técnico-legal que establece un modelo o norma que refiriere lineamientos a seguir para cumplir una actividad o procedimientos. Su uso se ha popularizado en la actualidad debido a que se busca que los procesos y actividades de organizaciones y sus personas sean repetibles, organizados, y estructurados. Por ello, entidades como ISO[1] (International Standard Organization), IEEE[2] (Institute of Electrical and Electronics Engineers), entre otras proponen estos documentos, los cuales se crean a partir de la experiencia de diferentes grupos que participan durante el proceso de definición y al finalizar son documentos de tipo público.

¿Qué se puede encontrar?

Entrando en materia, observemos algunos estándares internacionales, guías y manuales de buenas prácticas que en la actualidad son ampliamente empleados para buscar el aseguramiento de la información, el activo más valioso de toda organización, en el constante proceso de la consecución de protección a nivel de integridad, disponibilidad y confidencialidad:

ISO 27001[3]

Es un estándar para la seguridad de la información denominado ISO/IEC 27001 (Information technology - Security techniques - Information security management systems - Requirements) adoptado por ISO, basado en un estándar británico denominado BS 7799. Es certificable y su primera publicación fue en el año 2005.

En éste se determinan los requisitos necesarios para establecer, implantar, mantener y

*Ingeniero en Sistemas Computacionales por la Universidad Distrital Francisco José de Caldas. Actualmente, estudia el máster de seguridad informática de la Universidad Oberta de Catalunya. Se ha desempeñado como hacker ético, pentester, administrador de sistemas, servidores y comunicaciones en varias organizaciones. Colabora con el blog http://hacking.mx, cuenta con varias certificaciones.

mejorar un Sistema de Gestión de la Seguridad de la Información (SGSI) a través del ciclo de Deming-PHVA por medio de los procesos de planificar, hacer, verificar y actuar.

ISO 27002[4]

Se trata de una guía de buenas prácticas a partir de objetivos de control y controles recomendables a nivel de seguridad de la información. A diferencia de ISO 27001, no es un estándar certificable. Cuenta con 39 objetivos de control y 133 controles agrupados en 11 dominios, abordando más controles y dominios que los establecidos en el estándar certificable ISO 27001.

A través de este documento se puede identificar un marco de trabajo más amplio para una organización cuando se desea implementar políticas de seguridad, establecer un sistema de gestión de la seguridad de la información y con la madurez adecuada lograr la certificación ISO 27001 que evalúa menos dominios.

ISO 27005[5]

Se trata de un estándar internacional denominado ISO 27005:2008, Information technology – Security Techniques – Information Security Risk Management. Fue creado en el año 2008 y provee pautas para la gestión del riesgo de seguridad de la información.

Como procedimiento vital, al hablar de seguridad de la información aparece el análisis, evaluación y gestión de los riesgos, por ello este documento ilustra un marco de referencia para el tratamiento de las actividades antes mencionadas.

CoBIT[6]

Este documento establece un marco de trabajo basado en dominios y procesos, a través del cual se ofrecen unas buenas prácticas enfocadas a optimizar la inversión de recursos en áreas de IT, brindando así calidad, gestión y correcta administración en los servicios prestados, abordando también, temas de seguridad asociados a los servicios.

ITIL[7]

Este compendio de documentos, conocido como la Biblioteca de Infraestructura de Tecnologías de Información, aborda recursos orientados a la correcta gestión de los servicios de IT a través de un ciclo de vida de los servicios, evaluando inmerso en cada una de las fases del ciclo temas de seguridad, capacidad y continuidad.

NIST SP 800-30[8]

Este documento contiene una guía desarrollada por el National Institute of Standards and Technology (NIST). “Risk Management Guide for Information Technology Systems – Recommendations of the National Institute of standards and Technology”. Este documento fue creado en el año 2002 y ofrece pautas para la gestión del riesgo buscando su evaluación, gestión, control y mitigación.

A través de este documento, en conjunto con ISO 27005, es posible identificar y establecer métodos a través de los cuales gestionar los riesgos identificados en una organización, diseñar y aplicar controles para la correcta mitigación de estos.

BS 25999[9]

Este estándar de origen británico, aborda los lineamientos que deben contemplarse para la administración de la continuidad del negocio. A través de 2 partes. La primera ofrece un marco de referencia para procesos, principios y terminología asociado a la continuidad del negocio. En la segunda, se encuentran los requerimientos para implementar, operar y mejorar un sistema de administración de la continuidad del negocio.

Interactuando entre sí

Lograr una alineación entre los documentos antes indicados tiene un alto grado de dificultad, pero a la vez es una oportunidad para crear un conjunto de métodos y procedimientos complementarios que abarquen gran cantidad de puntos, logrando uno a uno el aseguramiento de los activos, procesos y recursos tecnológicos de la organización. Además, permiten crear consciencia en la importancia de la seguridad de la información al personal que forma parte de la organización.

Observemos un caso práctico de una organización que considera la necesidad de implementar un sistema de gestión de la seguridad de la información para así ofrecer confianza a sus clientes y proveedores respecto al manejo y aseguramiento de la información:

Se inicia realizando el inventario de activos de información de la organización y sobre ellos se realiza un análisis de riesgos a través del uso de NIST SP 800-30 e ISO 27005, definiendo amenazas y vulnerabilidades, se establecen así, los controles correspondientes siguiendo las buenas prácticas de ISO 27002.

Una vez terminado el anterior grupo de actividades, se procede a identificar cómo se prestan los servicios en el área de Tecnologías de la Información (TI) dentro de la organización, evalúan temas de seguridad, y se procede a la gestión de estos servicios siguiendo las buenas prácticas de ITIL y CoBIT. S e establece así, la administración y gestión del área de servicios de TI, siempre pensando en seguridad.

Pero no se puede dejar de lado que la continuidad del negocio es primordial para toda organización, así que tomando como base BS 25999, se establecen los planes de continuidad, los comités y grupos asociados al proceso.

Así quedaría constituido un sistema de gestión de la seguridad de la información, que una vez auditada y evaluada, permitirá lograr la certificación en ISO 27001.

Conclusiones

Uno de los mayores errores que pueden presentarse es creer que el cumplimiento de una lista de chequeo o contar con un sello que certifica a una organización en estándares internacionales como ISO 27001 significa que es una organización segura. Por otra parte, es vital entender que este proceso de aplicación de normas o estándares a su vez tiene implicaciones adicionales, como la necesidad de constantes actualizaciones de acuerdo con los cambios que se presentan a nivel de los activos de información y tecnológicos a través de los que se accede a ésta.

Sin embargo, el seguimiento de los documentos y guías antes mencionados permiten en conjunto una creación de políticas y procedimientos que establecen controles de seguridad para la información y los activos asociados, brindando protección desde lo procedimental hasta lo técnico dentro de la organización, ofreciéndole confianza a nivel interno y externo gracias al nivel de seguridad provisto.

Entonces, podemos ver que existen múltiples opciones y podemos usarlas en conjunto o progresivamente para lograr así hablar de seguridad de la información.

Para conocer más sobre los documentos antes mencionados, consulta los siguientes enlaces de interés:

[1] http://www.iso.org/iso/home.html

[2] http://www.ieee.org/index.html

[3] https://mmujica.files.wordpress.com/2007/07/iso-27001-2005-espanol.pdf

[4] https://mmujica.files.wordpress.com/2007/07/iso-17799-2005-castellano.pdf

[5] http://www.27000.org/iso-27005.htm

[6] http://www.isaca.org/Knowledge-Center/cobit/Documents/CobiT_4.1.pdf

[7] http://itil.osiatis.es/Curso_ITIL/

[8] http://csrc.nist.gov/publications/nistpubs/800-30/sp800-30.pdf

[9]http://www.bsigroup.com/en/Assessment-and-certification-services/management-systems/Standards-and-Schemes/BS-25999/

Trece años del foro académico de seguridad informática más importante de México

Por Célica Martínez Aponte y Galvy Ilvey Cruz Valencia*

La seguridad de la información representa en nuestros días un cúmulo de aspectos tecnológicos en los que convergen ya no sólo unos cuantos individuos. La apertura y acercamiento de distintos medios en la llamada era digital han comenzado a aproximar a una gran cantidad de personas.

La inquietud sobre los problemas que comprometen a la información personal o de las organizaciones también ha cobrado una creciente relevancia. Hoy se escuchan noticias desafortunadas sobre robo de dinero, datos e identidad a través de acciones en línea.

La UNAM, a través de la Dirección General de Cómputo y de Tecnologías de Información y Comunicación (DGTIC), ha organizado desde 1997 el Congreso Seguridad en Cómputo, en el que se realizan cursos de alta especialización y reúne a destacados especialistas de seguridad informática a nivel internacional con la comunidad académica, expertos de la industria, área comercial, estudiantes y profesionales interesados en la seguridad de la información.

Líneas de especialización

El interés creciente y la demanda de una comunidad cada vez más especializada hicieron imperante que el entonces Departamento de Seguridad en Cómputo decidera implementar talleres y cursos específicos. Así, en el congreso de 2003 se configuró lo que hoy se conoce como Líneas de Especialización.

Estos cursos se desarrollan en espacios académicos que cumplen con todas las características necesarias para llevarlas a cabo. Este año se realizarán en las instalaciones de Centro de Extensión Tlatelolco de la UNAM.

Las líneas a impartir son:

- Administración y seguridad en Windows
- Cómputo forense y legislación relacionada
- Análisis de vulnerabilidades, técnicas de intrusión y pentest
- Detección de intrusos y tecnologías honeypots
- Seguridad en aplicaciones web y técnicas defensivas

---

* **Célica Martínez.** Licenciada en Administración por la Facultad de Contaduría y Administración. Coordinadora de proyectos y responsable de logística de eventos especializados de seguridad, entre ellos el Congreso Seguridad en Cómputo, actividad que desarrolla hasta ahora. **Galvy Cruz.** Licenciado en Ciencias de la Comunicación por la Facultad de Ciencias Políticas y Sociales. Se ha desempeñado como difusor de tecnologías de la información y la comunicación. Actualmente, es editor de la revista .Seguridad y otros contenidos de la Subdirección de Seguridad de la Información/UNAM-CERT.

Otros talleres ofertados:

- Análisis de software malicioso
- Seguridad perimetral
- Hardening en sistemas operativos Linux
- Infraestructura Library, ITIL
- Análisis de riesgos
- Implementación del SGSI
- Fundamentos de COBIT

A través de este esfuerzo académico, la Subdirección de Seguridad de la Información/UNAM-CERT de la DGTIC, busca impulsar la seguridad de la información desde el usuario de tecnologías hasta CEOs de TI.

Conferencias magistrales

El liderazgo que la UNAM ha mantenido en seguridad informática, ha permitido convocar en cada una de sus emisiones a prestigiados ponentes, quienes han intercambiado experiencias con la comunidad.

Las conferencias magistrales se realizan en una sede diferente a la de las líneas de especialización; este año, tendrá lugar en el Palacio de Minería.

En ediciones anteriores se ha contado con la presencia de personalidades reconocidas en el ámbito como Alan Paller (SANS Intitute), Wietse Venema (Internet Systems Consortium, Inc.), Eugene Schultz (Berkeley Lab), Ralph Logan (The Honeynet Proyect), Mikko H. Hyppönen (F-Secure Corp.), Raffael Marty (Loggly), entre otros.

Durante los días de conferencias, se desarrollan dos eventos importantes en el área: La Reunión Anual de la Red Nacional de Seguridad en Cómputo (RENASEC) y el Día Internacional de Seguridad en Cómputo (DISC).

Reunión Anual RENASEC

En este evento se reúnen responsables de diversas Instituciones de Educación Superior del país con el objetivo de contrarrestar los problemas de seguridad en cómputo en las labores académicas.

DISC

El Día Internacional de Seguridad en Cómputo (DISC) es un evento celebrado en varios países. México se une a esta celebración a través del UNAM-CERT.

Esta emisión se transmitirá por webcast y podrás participar pegando los posters conmemorativos para difundir mejores prácticas de seguridad.

Asiste al Congreso Seguridad en Cómputo 2011 del 18 al 25 de noviembre, contando con la misma calidad y excelencia que durante más de una década lo han caracterizado.

¡No te quedes fuera! Consulta la página: http://congreso.seguridad.unam.mx/2011/, llama al (0155) 56228169 ó escribe a congreso@seguridad.unam.mx.

Mesografía

http://www.seguridad.unam.mx
http://congreso.seguridad.unam.mx/
http://renasec.anuies.mx/reunion/index.php
http://www.disc.unam.mx/2010/
http://www.acm.org/

Sistemas de detección, los siguientes pasos

Por Javier Ulises Santillán Arenas*

En nuestro artículo anterior, se abordó cómo, los sistemas de detección de intrusos (IDS), los de prevención (IPS o IDP) los correlacionadores de eventos, entre otros, permiten a los administradores de red y a los encargados del monitoreo de la actividad de tráfico tener un panorama general y poder establecer el estado de su infraestructura en relación con la posible actividad maliciosa dentro de ella.

Durante los últimos años, las características de estos sistemas han ido evolucionando, adaptándose a las necesidades de la industria y, sobre todo, siguiendo las tendencias y patrones de las amenazas existentes que atentan en contra de la seguridad de la información.

Imagínese el panorama de hace algunos años. Una organización con una infraestructura de mediano tamaño, pero con un diseño un tanto complejo, es usada por contadores, abogados, secretarias, líderes de proyecto, investigadoras, analistas de negocios, etc. Ellos realizan sus actividades diarias y no necesariamente consideran las medidas de seguridad relacionadas a su equipo de cómputo. Para ellos, el uso de dispositivos móviles de almacenamiento, el acceso a sitios web que ofrecen descarga de contenido multimedia o los "inofensivos y útiles" programas para compartir archivos de música, representan una parte de las actividades en sus computadoras.

Al dar el medio día, hora pico en el uso de la red de la organización, se percibe un comportamiento anormal en la velocidad de transmisión de la red, traducido en una evidente incapacidad para continuar con sus actividades de enviar correos electrónicos, descargar alguna imagen de Internet para una presentación, llevar a cabo la junta por videoconferencia que se tenía agendada con la casa matriz y, en algunos casos, algunas cámaras de vigilancia han quedado con una imagen congelada porque no pueden sincronizarse con el servidor correspondiente. Se presiente un caos y empiezan a sonar los teléfonos del departamento de soporte técnico y de operación de TI. Los usuarios en realidad suponen que el problema es ocasionado por una falla en los sistemas debido a alguna mala configuración, administración o un simple descuido.

---

* Ingeniero en Computación por la Facultad de Ingeniería de la UNAM. Perteneció a la tercera generación del plan de becarios de seguridad en cómputo de la Dirección General de Servicios de Cómputo Académico (ahora DGTIC). Labora desde 2008 en la Subdirección de Seguridad de la Información/UNAM-CERT como líder del proyecto Honeynet-UNAM, donde realiza diversas actividades enfocadas al desarrollo e investigación de tecnologías de detección, análisis y procesamiento de tráfico de red malicioso. Tiene la certificación GIAC Certified Intrusion Analysts (GCIA) y ha tomado cursos relacionados con análisis de tráfico de red en el SANS Institute.

Del otro lado, en el cuarto del soporte técnico, los sistemas se ven saturados, la actividad entre los equipos internos con algunos servidores externos es inusual y existe demasiada transferencia de información. La solución temporal pero más inmediata, como en muchos casos, es limitar o desconectar el acceso a Internet para analizar dónde está el problema.

Después de algunos minutos, los administradores de la red se dan cuenta de que existen decenas de equipos que intentan enviar peticiones de conexión a un servidor externo a la organización y esto ha ocasionado que se inunde el medio de transmisión por donde tienen acceso la mayoría de los equipos en la red. ¡Voilá!, se ha identificado el problema. La propagación de un *bot*, malware que hace que un equipo sea parte de una botnet, ha ocasionado que se infecten equipos de la organización, es decir, el problema estaba *dentro de casa,* ya que seguramente la infección pudo llegar desde una USB o mediante un archivo infectado, pero el ataque fue generado desde el interior.

En este panorama, muchas veces el usuario cree que es inocente, pero en realidad, por una falta de conocimiento y cultura de seguridad informática, son el eslabón más débil y participan directa e indirectamente en los problemas de la red de la organización, apoyados con la falta de una adecuada administración de la seguridad.

En este ejemplo se pueden analizar varios aspectos.

1) Los problemas causados durante el incidente, ¿en realidad sólo fue una interrupción en el servicio? La información es el activo más importante de las organizaciones y el acceso no autorizado a ella por parte de terceros podría implicar un compromiso serio a la integridad de la propia organización.

2) Tener la capacidad de saber dónde se generó el ataque, o dónde fue el punto de entrada a la red por parte de la entidad maliciosa, son aspectos que un sistema de detección de intrusos común, con las características de hace algunos años, podía indicar al administrador, sin embargo, actualmente esto no es suficiente; se necesitan mejores características. La llegada de sistemas de prevención de intrusos que cuentan con una correcta administración y configuración, no solo alertarán de una posible actividad maliciosa, sino que actuarán automáticamente para poder mitigar con un tiempo de respuesta adecuado a toda la actividad maliciosa identificada.

Muchas nuevas tecnologías en los sistemas de detección y prevención están siendo implementadas. Entre ellas se encuentran aspectos como inteligencia artificial, detección de anomalías, mejoras en firmas de identificación de patrones maliciosos, etc. Todas estas nuevas características se están complementando con el desarrollo de nuevas herramientas como los correlacionadores de eventos o los analizadores de bitácoras, que permiten identificar de manera muy específica, los puntos en donde se ha tenido actividad anómala o maliciosa en los sistemas de una organización.

Siguiendo el ejemplo del incidente, con las nuevas características de los sistemas actuales y de los futuros, acompañados con una correcta metodología de implementación y seguimiento, podría detectarse en tiempo real el inicio de la propagación del malware y la fuente del mismo. A su vez, podría identificarse si existe algún tipo de fuga de información y con un análisis casi automático el administrador podría saber qué tipo de malware es el que ocasiona el problema. Con la correcta configuración, el ataque podría mitigarse de manera automática lo cual se traduciría, en el peor de los casos, en una mínima percepción por parte de los usuarios acerca del incidente. Así, los tiempos y costos relacionados con el mismo disminuirían al máximo, e irónicamente, toda la inversión de tiempo y costo para la implementación de las soluciones de seguridad habrán valido la pena.

Actualmente existe una gran variedad de soluciones de seguridad basadas en software libre y comercial. Dependiendo del tipo y de sus características, algunas son más complejas que otras y ofrecen una mayor versatilidad de detección, administración y aprovechamiento costo-beneficio. El punto importante es que para la correcta selección de un mecanismo de seguridad, se tiene que hacer un análisis completo de la infraestructura de la organización.

Es interesante también observar cómo a partir de modelos que han nacido de la investigación en seguridad en cómputo, como la tecnología honeypot, sistemas darknet, spiders, etc., muchas de las soluciones comerciales y no comerciales han adquirido dentro de sus características este tipo de tecnologías adaptándolas a su esquema y ofreciendo alternativas que complementen una detección de tráfico malicioso.

Los sistemas que solo ofrecen alertas sobre las amenazas más comunes ya han quedado rezagados. Por esa razón, la mayoría de las nuevas soluciones tanto comerciales como de software libre, buscan ser soluciones integrales con diversas tecnologías complementadas mutuamente, así como ofrecer al administrador una mayor capacidad de monitoreo y detección de amenazas de seguridad dentro de la organización.

En este punto se debe tener aún ciertas reservas, ya que muchos debates en cuanto a las tecnologías de los IPS, IDP, etcétera siguen existiendo pese a no representar la solución final de los problemas de seguridad de las organizaciones. Muchas de ellas, al adquirir este tipo de soluciones integrales, tienen más problemas de los que inicialmente habían tenido. Esto se debe a que independientemente de las capacidades y características de este tipo de tecnologías, la correcta capacitación para la implantación, configuración, administración y mantenimiento de ellas es esencial para aprovecharlas de manea correcta y eficiente, por lo que la adopción y adaptación toma cierto tiempo.

Algunas tendencias indican que el software provee cada vez más información al usuario técnico, es decir, debe decir de manera más detallada cuándo, cómo, por qué, etcétera se presentó el problema y así proporcionar parte de la evidencia.

En conclusión, podremos siempre contar con un sistema de detección y monitoreo de seguridad en cómputo, pero varios factores deben tomarse en cuenta para su correcto aprovechamiento:

- ✓ Capacidades de detección y mitigación adecuadas al entorno de implementación
- ✓ Correcta capacitación de los administradores para su configuración y mantenimiento
- ✓ Definición de políticas en la organización y seguimiento de una metodología de atención a incidentes
- ✓ Adopción de un modelo de educación para los usuarios en relación con la seguridad informática

Los sistemas de detección seguirán evolucionando, adaptándose a las necesidades de las organizaciones y siguiendo las tendencias que imponen las nuevas amenazas en Internet, pero siempre el límite que separa la amenaza latente de la organización, será definido por el conjunto de todos los mecanismos implementados, entre ellos, una cultura de seguridad de la información.

Referencias

- http://www.sans.org/security-resources/idfaq/
- http://www.sans.org/reading_room/whitepapers/detection/
- http://www.google.com/url?sa=t&source=web&cd=7&ved=0CEMQFjAG&url=http%3A%2F%2Fbiblioteca.utec.edu.sv%2Fsiab%2Fvirtual%2Farticulos_soft_libre%2Fintrusos.pdf&rct=j&q=historia%20de%20los%20sistemas%20de%20deteccion%20de%20intrusos&ei=7MuaTYXgGPCQ0QH03LXcBg&usg=AFQjCNGEhkHJFV1kkrUYYFaYhYCHHC7Lew&cad=rja

La criptografía: El secreto de las comunicaciones seguras

Por David Eduardo Bernal Michelena

Desde los tiempos remotos, las grandes civilizaciones han tratado a toda costa de proteger sus posesiones preciadas. Más valioso que el oro y que los diamantes puede ser el conocimiento, porque puede ser la clave para crear una poderosa arma para ganar una guerra o para producir comida y alimentar a la población. ¿Pero cómo podían las personas asegurarse de que sólo los destinatarios del conocimiento pudieran usarlo y entenderlo y no sus adversarios?

Plasmando el conocimiento en una representación simbólica, normalmente escrita y luego transformándola, mediante una clave secreta, en una representación equivalente (criptograma) e ininteligible para aquellos que la desconozcan y que sólo aquellos conocedores de la clave y el método para ello podrían regresarla a su forma original. Pues bien, al arte de aplicar estas transformaciones hasta llegar a una representación enigmática mediante una clave secreta, se le llama criptografía.

La criptografía moderna, creada a partir de 1948 con la Teoría de la Información de Claude Shannon, se divide en simétrica y asimétrica, una de las principales diferencias, es que en esta última se utiliza la clave pública del destinatario del mensaje para cifrar el mensaje y el destinatario usa su clave privada para descifrarlo. Otra de las diferencias, es que la criptografía asimétrica puede proveer autenticidad, con lo que el destinatario puede corroborar la identidad del remitente.

Fascinante, ¿pero cómo funciona?

La criptografía asimétrica utiliza dos claves distintas, pero que matemáticamente son equivalentes. Así, la información que es cifrada con una, puede ser descifrada con la otra. Sin embargo, el hecho de conocer la clave pública no revela la clave privada.

Para proveer integridad, se calcula un valor único (hash) para el mensaje utilizando algún algoritmo de digestión (md5, sha1, etc.). Para proveer autenticidad, se cifra ese valor con la clave privada del emisor, la cual se agrega al final del mensaje enviado, junto con el nombre del algoritmo utilizado.

Cuando el destinatario recibe el mensaje firmado, calcula el valor único del mensaje utilizando el algoritmo de digestión que se indica al final del mensaje recibido, descifra el valor único (hash) enviado por el usuario con la clave pública del emisor y los compara. Si son iguales, se comprueba la integridad y la autenticidad del mensaje.

Tips en criptografía simétrica

1) Ya que en la criptografía simétrica, se utiliza la misma clave para cifrar y descifrar, cuida los mecanismos de transmisión y almacenamiento de la misma, para reducir el riesgo de que ésta pueda ser usada por usuarios no autorizados. Una de las opciones que permiten la transmisión de la clave a través de un medio inseguro es el algoritmo

Diffie Hellman, ampliamente conocido y que precisamente es la base de la criptografía asimétrica.

2) Utiliza un algoritmo de cifrado acorde con la importancia de la información, la eficiencia de la aplicación y que se encuentre vigente y avalado por organizaciones internacionales como ISO e IEEE. Evita utilizar algoritmos obsoletos como DES.

Tips criptografía asimétrica

1) Ten siempre en mente que al utilizar la criptografía asimétrica se provee de autenticidad e integridad. Cuando se envía un mensaje cuya autenticidad e integridad es verificable, se dice que está firmado digitalmente. Así, el usuario tiene la posibilidad de enviar mensajes firmados y/o cifrados a sus destinatarios. Sé consiente y selectivo de la información que debes firmar y/o cifrar.
2) Recuerda que la criptografía asimétrica se usa para proteger una gran variedad de comunicaciones, por ejemplo el correo electrónico, que es uno de los medios de comunicación más utilizados en la actualidad
3) Crea un revocado del certificado de tu clave. Así, en caso de que por algún motivo tu clave privada fuera comprometida, puedes revocarla y evitar que los usuarios no autorizados puedan hacer mal uso de ella.

Tips cifrado en general:

1) Utiliza una clave robusta para proteger tu información. Si la clave es débil es probable que un atacante logre adivinarla con facilidad, utilizando una variedad de ataques de diccionario, fuerza bruta y estadísticos.
2) Establece un mecanismo para recuperar la clave de cifrado en caso de olvidarla. Si no lo haces, es probable que no haya manera de recuperar los archivos y se pierdan para siempre. Es recomendable que la clave usada para cifrar un activo de información, a su vez sea cifrada y almacenada utilizando una clave maestra, con el fin de recuperarla en caso de que se olvide.
3) Dependiendo del tamaño y de la importancia de la información cifrada, puede ser recomendable realizar una o varias copias de ésta, de manera que si ocurre algún problema con el medio de almacenamiento (disco duro, CD/DVD, memoria usb, etc.), haya forma de recuperar la información original. La criptografía puede usarse para proteger cualquier información digital. Se usa para proteger discos completos, particiones, carpetas y archivos, incluyendo la información que se transmite de un sistema de cómputo a otro. Determina qué grado de protección requieres en tus sistemas, en función del grado de protección que desees proveer a la información y el grado de funcionalidad y eficiencia que necesites.

4) Durante el proceso de generación de claves, en ocasiones se permite indicar una “frase de contraseña”, la cual se usa para proteger tu clave y controlar tu acceso. De esta manera, funciona como una capa de protección adicional, para que en caso de que te sea robada no pueda ser usada de manera no autorizada. Proporciona una frase de contraseña robusta pero que puedas recordar.

Normalmente el correo electrónico sólo provee cifrado en el proceso de autenticación. Es decir, cuando un usuario inicia sesión en su correo electrónico, la contraseña va protegida en su transmisión, pero el resto de la información, incluyendo los correos electrónicos viaja en claro, por lo que pueden ser capturados y leídos por usuarios no autorizados.

Es importante cifrar el correo electrónico para asegurar que los mensajes son leídos sólo por los usuarios autorizados, así como firmar los correos electrónicos enviados para permitir que los destinatarios de nuestros mensajes corroboren la autenticidad de los mismos.

Una de las tecnologías más utilizadas para la implementación de criptografía asimétrica en el correo electrónico es PGP (Pretty Good Privacy), la cual se distribuye gratuitamente y puede ser agregada a interfaces existentes de correo como Horde o Squirrelmail, desde donde los usuarios pueden crear y administrar sus claves. También existen alternativas como Enigmail que permiten cifrar el correo desde clientes de coreo como Thunderbird, siempre y cuando sea soportada por el proveedor del servicio de correo.

Es importante mencionar que la criptografía asimétrica es normalmente más costosa computacionalmente que la criptografía simétrica, es decir, que una computadora necesita realizar más cálculos para cifrar y descifrar los mensajes cifrados con criptografía asimétrica.

Para **cifrar archivos y carpetas** con criptografía simétrica existen varias tecnologías. Es conveniente consultar la especificación de cada herramienta para determinar si es capaz de proveer la seguridad que se requiere. Una de las herramientas gratuitas, multiplataforma que es capaz de proveer un fuerte cifrado AES de 256 bits es 7zip. Winzip y Winrar proveen también cifrado AES, en sus versiones actuales. Para cifrar un archivo o carpeta con estas herramientas, es necesario ir al apartado de seguridad y establecer una contraseña. En caso de que se pregunte, seleccionar el algoritmo y la longitud de preferencia del usuario, con base en las necesidades de seguridad que desee implementar.

Otra herramienta multiplataforma que provee una mayor versatilidad de uso, ya que no sólo puede cifrar archivos y carpetas, sino volúmenes completos es TrueCrypt, la cual incorpora una gran variedad de algoritmos de cifrado y de digestión, además de que incluye un generador de números aleatorios con base en los movimientos del mouse del usuario. Una de las herramientas disponibles en GNU/LINUX para cifrar volúmenes virtuales es eCrpytfs.

Windows 7 Professional, Windows 7 Ultimate y Windows 7 Enterprise permiten cifrar carpetas o archivos de una manera relativamente fácil. Para hacerlo, se da clic con el botón secundario en el archivo o carpeta y se selecciona propiedades, opciones avanzadas, cifrar contenido para proteger datos. El sistema abre un asistente que permite al usuario proporcionar una contraseña para crear un certificado con el que cifran los datos, así como cualquier archivo o carpeta que se cifre con esta opción en el futuro.

Otra de las herramientas de Windows sólo disponible en sus versiones más avanzadas es Bitlocker, la cual es una manera fácil de implementar cifrado transparente en toda una unidad. Existe una gran variedad de herramientas de cifrado disponibles, algunas son gratuitas y otras

de paga y existen para una diversidad de sistemas operativos. Algunas se enfocan sólo a cifrar un archivo, otras permiten cifrar volúmenes completos.

Debemos tener en cuenta que muchos protocolos de Internet no fueron creados pensando en la seguridad, por lo tanto, es posible que al usarlos sin cifrado, dejemos la puerta abierta a usuarios no autorizados para que capturen nuestra información confidencial. Para evitarlo, se puede implementar la criptografía asimétrica tanto para cifrar la información y asegurar que sólo los usuarios autorizados pueden verla; como para firmar los mensajes y asegurar que la autenticidad de nuestros mensajes puede ser verificable. Así como fomentar que nuestros contactos nos envíen mensajes firmados para asegurar que realmente vienen de ellos.

Referencias

- LÓPEZ, Barrientos Ma. Jaquelina. *Criptografía*, México, Universidad Nacional Autónoma de México, Facultad de Ingeniería, 2009.

  SCHNEIER, Bruce*, Applied Cryptography*, Second Edition. John Wiley & Sons, 1996 ISBN 0-471-11709-9

  ÁNGEL, Ángel José de Jesús, *Criptografía para todos* [en línea], México, CINVESTAV, Formato html. Disponible en Internet: http://computacion.cs.cinvestav.mx/~jjangel/chiapas/criptografia.pdf.