EDITORIAL (Revista Telem@tica, Vol. XIII, No. 1)

Estimado lector

El presente número de la Revista de Telemática está dedicado a uno de los temas más importantes y apasionantes relacionados con las tecnologías de la información y las comunicaciones (TICs). El estado de la informatización global se caracteriza por una gran diversidad en los servicios, los protocolos, el equipamiento, los dispositivos de cliente, lasalternativas de acceso y otros elementos, que permiten trabajar con una cantidad y variedad monumental de información. Todas estas facilidades traen consigo, en igual medida, enormes retos a la seguridad.Es por eso que nuestro colectivo ha decidido dedicar todos nuestros artículos de la presente edición al tema de la seguridad en las tecnologías dela información y las comunicaciones.

Esta es una temática muy actual, que en nuestra sociedad va cobrando cada vez mayor jerarquía, dada la actualización no solo tecnológica, sino también económica y social del país. En un solo número no podemos abarcar todas las aristas del tema. Sin embargo, trataremos de ofrecer un acercamiento aalgunas de las más importantes tendencias en cuanto a problemas de seguridad ya las soluciones que actualmente se desarrollan.

Muchas son las amenazas reconocidas a la información y los servicios TIC. De todas ellas una de las más antiguas, y que permanece vigente, es la de los programas malignos. Puede decirse que la forma de ataque más común desde hace muchísimos años es la que vulgarmente todos llamamos virus. Ellos han evolucionado y hoy se encuentran en computadoras personales, teléfonos inteligentes y hasta atacando sistemas industriales. Es por eso que cuatro de los artículos de hoy, están dedicados a los antivirus y algunas tecnologías asociadas a su desarrollo.

Los componentes de identificación de código maligno o sospechoso constituyen el núcleo de cualquier solución antivirus. De sucapacidad de actualización y mejora progresiva depende en gran parte la calidad del programa antivirus en cuestión y su posibilidad de estar al día con las nuevas amenazas que aparecen para dar una respuesta rápida y efectiva. Para conseguir estos objetivos se ha desarrollado un importante trabajo que se muestra en el artículo *Motor antivirus de Segurmática: para el presente y el futuro*, donde se presenta el diseño y funcionamiento general del componente de identificación del Motor Antivirus de Segurmática, su arquitectura, sus prestaciones y una muestra de sus resultados.

Las tecnologías empleadas en el trabajo del Segurmática Antivirus, producto nacional de elevada calidad, siguen siendo protagonistas de los siguientes artículos, donde podremos conocer cómo se adicionan métodos heurísticos, que permiten la identificación de programas malignos que no se encuentren en sus bases de datos, aumentando la capacidad de detección de esta solución. Los detalles se podrán conocer gracias al artículo*Adición de heurística, basada en la estructura de los ficheros PE, a Segurmática Antivirus.*

Con el artículo *Identificación de texto en Segurmática Antivirus*, tendremos la oportunidad de estar al tanto de cómo se pretende optimizar el trabajo del antivirus a través deuna biblioteca que le permita identificar los distintos tipos de texto mediante el análisis del contenido de los archivos y extender su arquitectura de búsqueda de forma que se aplique a cada archivo analizado las técnicas y algoritmos que más se le avienen, manteniendo así una proporción eficiente entre el nivel de detección y la velocidad de escaneo.

Para cerrar el grupo de artículos que versan sobre el trabajo de detección de los motores antivirus y su optimización, el siguiente trabajo: S*istema para la gestión de enlaces o URL maliciosos*, busca mejorar el trabajo del antivirus mediante su actualización permanente. En esta ocasión se muestrala implementación de un sistema de búsqueda activa de código maligno en Internet capaz de encontrar, clasificar y descargarenlaces o sitios que apuntan a programas malignos recientes, lo cual permitiría obtener una base de datos de muestras de programas malignos muy actualizada.

Otro elemento importante, esencial en la seguridad delos sistemas, es el desarrollo seguro de las aplicaciones. Precisamente una buena parte de las causas de los problemas de seguridad están en desarrollos inseguros, que llenan los programas de debilidades a partir de las cuales se ejecutan numerosos ataques,especialmente de denegación de servicios. Asociado a este problema se han desarrollado múltiples soluciones para la detección de estas vulnerabilidades. En particular, el artículo*Herramienta para la detección de posibles vulnerabilidades en el código fuente del repositorio de GNU/Linux Nova,* muestra una interesante soluciónparaidentificar las vulnerabilidades de tipo desbordamiento de buffer, desbordamiento de pila y ataques de código remoto, en el código fuente de las aplicaciones que forman parte del conocido Linux Nova, producto que aporta en la línea de una informatización soberana de nuestra nación. Este detector de vulnerabilidades permite detectar de manera automática, las posibles vulnerabilidades existentes en dicho código fuente antes de que el producto final forme parte del repositorio de paquetes del sistema operativo.

Sin dudas, otros de los elementos que trae mayor preocupación a la comunidad internacional en la actualidad es el de la seguridad en las comunicaciones, sobre todo aquellas que se desarrollan a través de las redes inalámbricas, las cuales garantizan una conectividad casi ubicua en muchas ciudades del mundo, son ampliamente utilizadas por los proveedores y operadores como vías alternativas de tráfico, entre otras aplicaciones. En particular, las redes WiFi tienen un despliegue inmenso, *in crescendo*, y son parte habitual de la conexión de los usuarios de las redes de datos empresariales, Internet y muchasotras. Estas redes, de acuerdo a su empleo, pueden introducir numerosas vulnerabilidades para las entidades, las cuales no solo pueden atentar contra la confidencialidad de la comunicación, preocupación más habitual, sino también por el robo de la información empresarial, el desvío de tráfico, y demás. El artículo*Detección de nodos en el entorno inalámbrico(Wi-Fi)*, pretende ofrecer una alternativa para incrementar los niveles de seguridad en estos entornos pues propone algoritmos muy completos, basados en las tramas 802.11 y la información que brindan sus campos, que posibilitan la identificación de los nodos en el entorno inalámbrico, punto de partida para monitorizar y controlar la actividad de esas redes.

El empleo del cifrado es, históricamente, uno los mecanismos de seguridad más recurridos, sobre todo cuando se trata de dimensiones como la confidencialidad, la integridad y el no repudio. El cifrado, deja de estar solo en los grandes centros de datos para proteger la información almacenada en cualquier soporte o intercambiada sobre diversos medios, alambrados o inalámbricos. Entre los problemas tecnológicos más comunes que enfrentan las soluciones de cifrado actualmente están la velocidad de procesamiento y la fiabilidad del almacenamiento e intercambio de claves, entre otros. En el número de hoy se presentan dos artículos que ofrecen posibles solucionesa estos retos. En el primero de ellos*Componentes de cifrado simétrico sobre microblaze, basados en los estándares AES y GOST*se muestra, de forma muy ilustrativa, algunos pormenores del desarrollo de dos componentes de cifrado simétricos sobre FPGA (*Field ProgrammableGateArray*) de Xilinx: AES (*Advanced Encription Standard*) y GOST. En el segundo artículo sobre este tema, *Implementación del esquema de firma digital ECDSA sobre el procesador embebido microblaze*, se describe la implementación del Estándar de Firma Digital con Curvas Elípticas (ECDSA) sobre un dispositivo de hardware reconfigurable tipo FPGA, y se propone una arquitectura que sirve de base a la implementación del estándar de firma con curvas sobre el procesador de propósito general Microblaze. Ambos artículos dejan ver una tendencia muy interesante, la de embeber en sistemas electrónicos multipropósitos, soluciones de software de finalidad muy particular, como es el caso de estas soluciones de cifrado.

Es nuestra certeza que los temas presentados en el presente número resultarán atractivos paranuestra comunidad, que en este caso dirigirá su miradahacia la seguridad en las TIC. Aunque no es exhaustiva, se ofrece una panorámica sobrealgunas tendencias en la aplicación de diversas tecnologías en la solución de diferentes retos de los mecanismos de seguridad disponibles. Esperamos que este número sea de su interés, y que podamos compartir nuevamente en nuestra próxima publicación.

Walter Baluja García
Editor