Detección en tiempo real de los ataques informáticos

abc@ABC_CValenciana / valencia
Día 04/12/2012

Varios investigadores desarollan una nueva herramienta para prevenir las intrusiones

Un ususario conectado a redes con su ordenador

Investigadores de la Universitat Politècnica de València (UPV), la Universidad de Burgos y la Universidad de Salamanca han desarrollado una nueva herramienta de ayuda a la detección precoz de ataques informáticos denominada 'RT-MOVICAB-IDS' (Real-Time MObile VIsualisation Connectionist Agent-Based IDS), informa la institución académica valenciana.

Su principal avance reside en la acotación temporal del proceso de detección de intrusiones mediante visualización gráfica del tráfico en una red de ordenadores. El sistema utiliza para ello técnicas de Inteligencia Artificial: la herramienta genera un informe visual que permite al administrador de red detectar de forma sencilla y rápida un posible ataque y, a partir de ahí, iniciar todo el protocolo de protección del servidor.

Los resultados de este trabajo han sido publicados en la prestigiosa revista internacional Future Generation Computer Systems, detalla la UPV en un comunicado. Según explica el investigador del Grupo de Tecnología Informática de la UPV Vicente Julián, los ataques cibernéticos han crecido notablemente en los últimos años. "En Estados Unidos, por ejemplo, estos ciberataques se han duplicado desde 2010 y el gasto incurrido por las empresas en respuesta a estos ataques se ha disparado un 40%", señala.

El objetivo de este trabajo de investigación era implementar un sistema que permitiera hacer un análisis de un gran conjunto de información en el menor tiempo posible y ofrecer sus conclusiones de una forma gráfica y muy fácilmente comprensible por el personal menos experimentado.

El trabajo se basa en la mejora del desarrollo previo MOVICAB-IDS, realizado en la Universidad de Burgos y publicado en el libro 'Mobile Hybrid Intrusion Detection: The MOVICAB-IDS System'.

Por su parte, el responsable del grupo de investigación GICAP de la Universidad de Burgos, Álvaro Herrero, destaca la importancia de este trabajo previo ya que supuso una contribución significativa al campo de los sistemas inteligentes híbridos aplicados a la

detección de intrusiones pues, a diferencia del amplio trabajo previo en este campo, el enfoque estaba más centrado en la visualización que en la clasificación del tráfico. "Imaginemos que alguien está intentando acceder con un barrido de direcciones o a la base de información para gestión de la red, mediante técnicas híbridas de Inteligencia Artificial podemos analizar ese tráfico que se produce on line de forma rápida para intentar prevenir el ataque", apunta Vicente Julián.

Redes neuronales

En concreto, el sistema se basa en el uso de redes neuronales y razonamiento basado en casos para tratar la información, tecnologías de agentes para una gestión distribuida del sistema y tecnologías de tiempo real para asegurar una respuesta en un tiempo máximo delimitado.

Según indica el profesor Herrero, el acotar los procesos deliberativos dentro del sistema de detección de intrusiones supone un avance muy positivo, ya que permite al personal de seguridad conocer el intervalo máximo de tiempo dentro del que se obtendrá una respuesta.

Además, se sigue trabajando en la mejora de este sistema con nuevas funcionalidades como la ejecución de mecanismos automáticos para la interrupción de estos ataques una vez detectados. "Aquí lo difícil es cómo compararte con otros: lo que hemos conseguido es ver que aún acotando temporalmente el tiempo de respuesta, los resultados son óptimos y podemos prevenir así el ataque", concluye Vicente Julián.

http://www.abc.es/local-comunidad-valenciana/20121204/abci-deteccion-tiempo-real-ataques-201212041405.html