Diario de Burgos

Fundado el 1 de abril de 1891

Fecha: 05/12/12
Sección: Burgos
Página: 17

La UBU crea un sistema que detecta ataques informáticos

Lo ha hecho en colaboración con las universidades de Salamanca y Valencia

DB / BURGOS

Investigadores de la Universitat Politècnica de Valencia, 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). 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*.

Según explica Vicente Julián, investigador del Grupo de Tecnología Informática de la UPV, los ataques cibernéticos han crecido notablemente en los últimos años. «En EEUU, 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 Julián.

El objetivo 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 UBU. Álvaro Herrero, responsable del grupo de investigación GICAP de la UBU, 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. A diferencia del trabajo previo en este campo, el enfoque estaba más centrado en la visualización que en la clasificación del tráfico.