Programas inteligentes para la protección de entornos informáticos

Antes la idea de delincuencia hacía pensar en un ladrón entrando en una casa o robando un coche. Hoy en día, los delincuentes utilizan ordenadores para cometer sus delitos. No importa si se encuentra a 500km o en la manzana de enfrente: la tecnología actual facilita a los deli...

Antes la idea de delincuencia hacía pensar en un ladrón entrando en una casa o robando un coche. Hoy en día, los delincuentes utilizan ordenadores para cometer sus delitos. No importa si se encuentra a 500km o en la manzana de enfrente: la tecnología actual facilita a los delincuentes la invasión de su privacidad. Investigadores de la Universidad Carlos III de Madrid (UC3M, España) han diseñado un sistema capaz de detectar intromisiones informáticas y activar una respuesta automática.

Los sistemas de detección de intrusos (SDI) son herramientas de seguridad desarrolladas con el objetivo de detectar cualquier acto sospechoso en sistemas informáticos. Se trata de «sistemas multiagente» compuestos de agentes autónomos coordinados que interactúan entre sí atendiendo a una serie de atributos de programación como la predictibilidad y la adaptabilidad.

Para parar cualquier tipo de intrusión, el dispositivo localiza estos sucesos y decide automáticamente si se debe llevar a cabo alguna acción. «Ambas capacidades son necesarias en un SDI», explicó el profesor Agustín Orfila del Departamento de Informática de la UC3M.

Los datos actuales muestran que España carece de la capacidad que poseen otros países para ejecutar investigaciones avanzadas en arquitecturas multiagente dedicadas a SDI.

En este estudio, el equipo español buscó la forma de utilizar agentes deliberativos que fueran capaces de adaptarse a su entorno y tener en cuenta intervenciones eficaces anteriores de forma independiente. El investigador comentó que de esta forma se puede estar seguro de si una respuesta es realmente necesaria al enfrentarse a un suceso sospechoso.

La utilización de «un modelo cuantitativo que sopesa el daño que provocaría un intruso frente al coste que supone ejecutar una acción de respuesta» es lo que hace este sistema posible, informó el profesor Orfila. El resultado es que el multiagente SDI decide qué configuración del sistema debería utilizarse en cada caso y determina si una respuesta es acertada o no. Esta maniobra cuantifica el grado de respaldo del SDI a la decisión adoptada.

Se ha demostrado mediante investigaciones que el «ataque por escáner de puertos» (cuando alguien busca puertos abiertos) y el ataque de denegación de servicio son las dos formas de intrusión más comunes. De esta forma los «hackers» pueden conseguir acceso ilimitado a los ordenadores atacados y controlarlos de forma remota, afirman los expertos.

El Instituto Nacional de Estándares y Tecnología de los Estados Unidos afirma que «la detección de intrusos es el proceso por el que se detecta un uso no autorizado de, o un ataque sobre, un ordenador o una red. Los SDI son componentes de software o hardware que detectan ese tipo de abusos.»

Un agente debe estar dotado de capacidad de adaptación y reacción e incluso ser capaz de sustituir a un ser humano, subrayó el profesor Orfila. «De esta forma, la arquitectura multiagente SDI nos permite repartir las tareas dedicadas a la detección y coordinar mejor el proceso, con lo que la detección es más eficiente», añadió.

Los más indicados para utilizarlo serían los administradores de sistemas, porque «les permitiría cuantificar el valor que el SDI asigna a sus decisiones y, además, sería capaz de indicar la mejor forma de ajustar el SDI a su entorno», declaró el profesor Orfila.

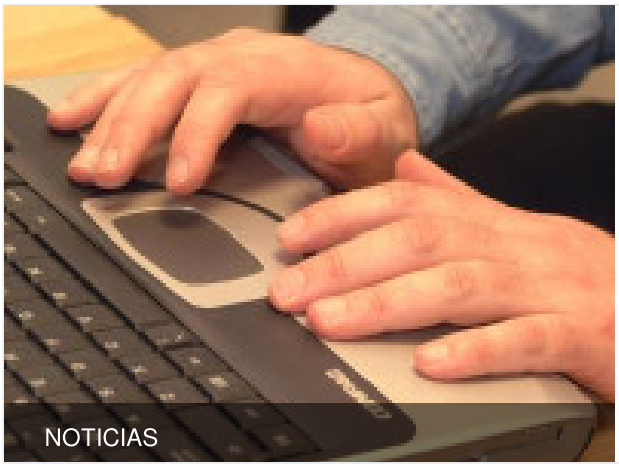
Éste aclaró, no obstante, que para funcionar correctamente el SDI necesitaría una adaptación al tráfico de la red real. También sería necesario configurar el sistema con arreglo a su verdadero entorno de seguridad y evaluarlo en esas condiciones.

Este estudio se publicó en la revista Computer Communication.

Países

España

Artículos conexos



Un nuevo proyecto de la UE promoverá la seguridad en línea

7 Abril 2008

Última actualización: 25 Noviembre 2008

Permalink: https://cordis.europa.eu/article/id/30170-intelligent-programs-protect-computer-environment/es