Diseñan un sistema inteligente de detección de intrusos que aprende pautas para alertar de los ciberataques

Actualidad social

Diseñan un sistema inteligente de detección de intrusos que aprende pautas para alertar de los ciberataques

Agencias
@DiarioSigloXXI
jueves, 12 de marzo de 2015, 13:57 | Comentar

La herramienta identifica y se anticipa a las intromisiones que vulneran los mecanismos de seguridad de los sistemas de información

» Ampliar la imagen

GRANADA, 12 (EUROPA PRESS) Investigadores de los grupos Sistemas Inteligentes y Minería de Datos (SiMiDat) de la Universidad de Jaén (UJA) y Soft Computing y Sistemas de Información Inteligentes (SCI2S) de la Universidad de Granada (UGR) han diseñado un sistema de detección de intrusiones para hacer frente a ciberataques.

Según ha explicado la Universidad de Granada en una nota, la herramienta se basa en técnicas de Inteligencia Computacional con las que aprende pautas que le permiten anticiparse a los intrusos que vulneran los mecanismos de seguridad de los sistemas de información.

Los dispositivos actuales de detección de intrusos en la red están limitados a la información con la que fueron entrenados y detectan "sólo si hay ataque o no", indican los investigadores, quienes añaden que "otros detectores incurren en falsos positivos".

En este caso, "no sólo consiste en identificar que el acceso es anómalo, sino que el sistema aprenda a detectarlos y responda ante ese ataque", ha precisado a la Fundación Descubre el responsable del proyecto Alberto Fernández, de la Universidad de Jaén.

Los ataques cibernéticos presentan características diferentes, por lo que, según Fernández, "métodos estadísticos sencillos no resultan efectivos para su detección". Por ello, los expertos han utilizado Inteligencia Computacional que permite el entrenamiento del sistema para que extraiga conclusiones

Noticias relacionadas

El Gobierno catalán se lanza a captar universitarios extracomunitarios para aumentar sus ingresos

Manuela Carmena: "El poder judicial será realmente independiente cuando sus gobernantes tengan consenso ciudadano"

Una concentración en Madrid pide la paz en Siria

El Rey vuelve a Cataluña para constituir el comité de los Juegos de Tarragona 2017

Analizan los resultados de los sondeos con georradar en la zona donde podría estar enterrado Lorca

Vídeos de actualidad

fruto de su experiencia.

Así las cosas, ha explicado que aplican estas técnicas para intentar que la herramienta avance hasta una solución "factible" con técnicas "sofisticadas" parecidas a las reglas propias del aprendizaje humano.

Para conseguir que el sistema "aprenda", los investigadores lo someten a una batería de pruebas en las que tiene que procesar un total de cuatro millones de ejemplos disponibles en repositorios de datos. Con los comportamientos correctos, la herramienta va extrayendo conclusiones y discriminando si se trata de un acceso normal o anómalo.

La novedad de este modelo, que los expertos describen en su trabajo 'On the combination of genetic fuzzy systems and pair wise learning for improving detection rates on Intrusion Detection Systems', publicado en la revista Expert Systems with Applications, es la utilización de sistemas difusos evolutivos basados en las leyes de la naturaleza.

"En nuestro caso, aplicamos este patrón y el algoritmo aprende por sí mismo con los conjuntos de datos que le hemos dado como entrenamiento. Empieza aportando soluciones aleatorias y evoluciona hasta quedarse con las que mayor calidad aportan al objetivo de identificación. Es como la Teoría de la Evolución de Darwin, combinamos soluciones y van quedando las mejores adaptadas", ejemplifica.

La ventaja de este enfoque es la utilización de etiquetas lingüísticas, que permite una mejor comprensión del conjunto de reglas con las que opera el sistema. En lugar de utilizar valores numéricos utiliza conceptos del lenguaje humano.

En este sentido, ha indicado que en lugar de alertar sobre que el riesgo de que alguien está intentando atacar el sistema es diez, dice que existe un riesgo alto. "Esto facilita la interpretación, porque se parece a los conceptos que utilizamos en nuestro día a día, donde en nuestras conversación no precisamos que la temperatura es de 30 grados, sino que decimos que hace calor", insiste.

APRENDIZAJE 'DIVIDE Y VENCERÁS'

Otra de las novedades es la utilización del esquema de aprendizaje denominado 'Divide y vencerás', que mejora la precisión cuando se producen ataque considerados 'raros'.

En este modelo, se dividen los datos etiquetados por parejas (actividad normal y cada tipo de ataque y, a su vez, todos los tipos de ataques entre sí) y se introducen en el sistema con lo que se aporta una solución para cada binomio y la respuesta final agrega la de cada miembro individual.

"Es como el jurado de un concurso, cada persona elige un ganador y, al final, se toma una decisión conjunta. Así se traslada la responsabilidad de decidir a muchos puntos y cada punto o experto aborda una faceta, desgranando el problema. La decisión final integra la opinión de ese conjunto de expertos", explica.

Esto supone que los tipos de alarmas están más definidos, porque dan distintas respuestas ante las alertas, aportando más robustez al sistema.

Este enfoque 'divide y vencerás', combinado con la lógica

difusa evolutiva, ha permitido a los investigadores diseñar un sistema que identifica correctamente todos los tipos de ataques, incluyendo las categorías de ataque 'raras' y que utilizan unos términos "interpretables" para la comprensión humana.

TIPOS DE ATAQUES

Las políticas de seguridad de la información de sistemas y redes están diseñadas para mantener la integridad de la confidencialidad y disponibilidad de los datos de sus usuarios de confianza. Sin embargo, los denominados 'ataques maliciosos' analizan las vulnerabilidades de estos sistemas con el fin de obtener acceso no autorizado o comprometer la calidad del servicio.

Los expertos apuntan distintos tipos de ataques. Por un lado, puede ocurrir un fallo del servicio, cuando se produce tanta cantidad de accesos denegados que al final saturan el sistema. Otras modalidades pasan por el escaneo de puertos para buscar vulnerabilidad en la red, adivinar la contraseña o intentar acceder como administrador, consiguiendo el control total del sistema.

Los investigadores continúan con este modelo, aún experimental, para trasladarlo al Big Data, es decir, a la utilización de gran cantidad de datos con las herramientas capaces de analizarlos y procesarlos. "Si ahora trabajamos con un sistema de entrenamiento con un total de cuatro millones de ejemplos, la idea sería incrementar esa cifra y adaptar el modelo para hacerlo escalable mediante su ejecución paralela sobre un conjunto de ordenadores para dividir el trabajo entre todos ellos", ha concluido el investigador.

También te puede interesar

De la izquierda, un ministro y un sindicato MADRID, 13 (OTR/PRESS) Cuando se escribe para una agencia como es mi caso, al final uno nunca sabe para quién escribe; ni tan siquiera sabes cuándo... más ¡8 kg. en 10 días! ¿Cómo? Una figura ideal en tan sólo dos semanas. 1 cápsula al día es suficiente más Inmigración. Las ONG lamentan que el Gobierno no haya dado... MADRID, 13 (SERVIMEDIA)Asociaciones que trabajan en el sector de la inmigración lamentaron este viernes que finalmente haya salido adelante en la Ley... más Me cuesta mucho eyacular... no puedo Esta disfunción produce una gran preocupación en el hombre y en su pareja. Para ellos es difícil de entender y salta a la vista que el hombre está... más ¿Lo has probado? Este curioso truco está revolucionando las compras online. más La globalización en cuestión No solamente es global la historia, también lo es la más remota prehistoria. No estamos viviendo un fenómeno nuevo; la que vivimos es mucho más... más
Anúnciese Aquí powered by plista

Comentarios

Escriba su opinión

Comentario (máx. 1.000 caracteres)*

(*) Obligatorio