Modelo basado en técnicas de aprendizaje automático permitirá detectar ataques a sistemas informáticos

Lorayne Solano Naizzir

Abstract

El PhD Emiro De la Hoz Franco realizó, en el marco de su formación doctoral, y en asocio con investigadores de las Universidades de Granada y Málaga (España), un modelo de detección de intrusos basado en Mapas Autorganizativos de Jerarquía Creciente-GHSOM, que de manera autónoma, y aplicando técnicas de aprendizaje automático, puede determinar si una red informática es sometida a ataques y detectar específicamente la tipología de este (denegación de Servicios – DoS, Usuario a Root – U2R, Remoto a Local – R2L y sondeo).

La ciberseguridad es un ámbito de trabajo bastante apetecido en la actualidad debido al alto volumen de ataques a los que están expuestos los sistemas informáticos empresariales. El acceso ilegal a información organizacional sensible y con fines maliciosos, haciendo uso de programas que secuestran los datos, como ransomware, ha generado pérdidas cuantiosas en múltiples organizaciones.

En mayo de 2017 se ejecutó un ciberataque masivo denominado 'WannaCry', del tipo ransomware, que generó considerables pérdidas económicas a destacadas empresas de diferentes sectores económicos (Telefónica, Iberdrola y Gas Natural, entre otras), mediante el cifrado de archivos y el bloqueo de accesos, con el propósito de exigir el pago en bitcoins por el rescate estos.

El alto y variado volumen actual de amenazas ha conllevado a que los investigadores desarrollen diferentes herramientas, metodologías y técnicas, con el fin de salvaguardar el activo más importante para las organizaciones hoy en día: la información. Algunas de estas soluciones son el control de

acceso remoto mediante la implementación de Redes Privadas Virtuales – VPR, el robustecimiento de la seguridad a través de la configuración de Listas de Control de Acceso – ACLs, la instalación de cortafuegos en zonas perimetrales de la red para filtrar el tráfico externo, el despliegue de sistemas antivirus, anti-spam y el monitoreo en tiempo real del tráfico en redes informáticas haciendo uso de Sistemas de Detección de Intrusos – IDS.

Si bien estas estrategias mitigan las vulnerabilidades de las redes computacionales, no son soluciones totalitarias, ya que, aunque evalúan el tráfico conocido y lo comparan con una base de datos de ataques previamente documentados, si se generan ataques que no tienen el mismo patrón de comportamiento a los ataques conocidos, sus respuestas son ineficaces.

De la Hoz, decano del Departamento de Ciencias de la Computación y Electrónica de la Universidad de la Costa, ha propuesto una robusta solución que tiene capacidad de autoaprendizaje para la detección de ataques desconocidos, debido a la implementación de técnicas de inteligencia artificial basadas en Redes Neuronales Artificiales (específicamente GHSOM), que no requiere la presencia del actor humano para la actualización de una base de datos de ataques, sino que analiza patrones de tráfico y detecta ataques basándose en la estimación de los mismos.

En el artículo ‘Modelo de selección de características mediante optimización multiobjetivo: aplicado a la detección de anomalías de red, basada en Mapas Auto-organizativos Jerárquicos’, publicado en la revista Knowledge-based Systems, los autores hacen una detallada descripción del sustento científico del modelo propuesto y de su funcionamiento. Un claro indicador de la validez del estudio descrito en el artículo es el reconocimiento que le ha dado la comunidad académica, evidenciado en un considerable número de citaciones en el ámbito internacional.

Los Sistemas de Detección de Intrusos (IDS) son programas computacionales que hacen un monitoreo periódico del tráfico que se genera en el interior de las redes informáticas y se clasifican en dos grandes categorías: basados en anomalías (Anomaly-based) y basados en mal uso (Misused-based). Estos últimos también se denominan como basados en firmas y su principal

funcionalidad es comparar el tráfico de red con una base de datos de ataques previamente documentados y al encontrar coincidencias exactas registran las incidencias para bloquear el acceso. «Este tipo de sistemas tiene una enorme limitante y es que en el momento en el que no esté actualizada la base de datos de ataques, un tráfico malicioso podría no ser detectado por el sistema y ello causaría un grave problema de seguridad al interior de la red», explica De la Hoz.

Al identificar esta falencia, y gracias a la dinámica colaborativa entre los departamentos de Ciencias Computacionales y Electrónica de la Universidad de la Costa, de Arquitectura del Computador y Tecnologías de la Información y la Comunicación de la Universidad de Granada y de Ingeniería de Comunicaciones de la Universidad de Málaga, con la orientación del PhD Julio Ortega, (catedrático de universidad de la Universidad de Granada) y el PhD Andrés Ortiz (profesor titular de la Universidad de Málaga), se desarrolló el modelo que soportará un Sistema de Detección de Intrusos basado en anomalías.

Este permite el entrenamiento de una técnica basada en inteligencia artificial que recrea el comportamiento de un cerebro humano y tiene la capacidad autónoma de clasificar el tráfico normal y el anómalo, y su tipología, sin hacer uso de una base de datos de amenazas previamente conocida, y de que a pesar de que no se tengan antecedentes de un determinado tipo de ataque, sea capaz de detectarlo con una muy alta tasa de aciertos.

Para el desarrollo de esta investigación se recreó un amplio repertorio de escenarios de simulación utilizando diferentes herramientas computacionales. A partir de ello, se comprobaron las métricas de calidad referidas al rendimiento del modelo propuesto (exactitud, precisión, sensibilidad, especificidad y curvas ROC) y cuando alcanzaron altos valores porcentuales en relación a los existentes en la literatura científica, se pudo evidenciar que el modelo propuesto aportaba un significativo avance en este ámbito de conocimiento.

La principal contribución de esta investigación es el haber desarrollado un modelo híbrido que permita detectar tráfico anormal o ataques, y la tipología de este tráfico en redes computacionales, como base para la implementación

de Sistemas de Detección de Intrusos en escenarios que analicen tráfico de red en tiempo real.

Las tasas de detección alcanzadas con la solución propuesta llegaron hasta el 99.8% con tráfico normal y hasta el 99.6% con tráfico anómalo, con una exactitud del 99.12%. En un trabajo futuro, este equipo planea analizar cómo se podría mejorar el actual modelo basado en GHSOM (Mapas Auto-organizativos de Jerarquía Creciente), mediante la hibridación con otras técnicas como el Modelo de Mezclas Gausianas o haciendo uso de Máquinas de Soporte Vectorial – SVM.

Lo que sigue en el proceso de esta investigación es tomar los resultados y hacer un desarrollo de software basado específicamente en este modelo para recrear una estructura de red computacional y embeberlo en un Sistema de Detección de Intrusos que pueda evaluar el tráfico, identifique el ataque y determine de qué tipo es.

Keywords

Investigación y desarrollo, Ingeniería electrónica, Tecnología de la información