Aprendizaje automático de modelos combinados para su aplicación a la detección de intrusos en el tráfico de Red.
Combined machine learning models for application to intrusion detection in network traffic.

Director: *CATANIA, Carlos Adrián*
Correo Electrónico: *ccatania@itu.uncu.edu.ar*

Co-Director: *BROMBERG, Facundo*

Integrantes: *MONGE, David; SALINAS, Sergio; PACINI, Elina; GARCIA GARINO, Carlos Gabriel.*

Palabras Clave: *Seguridad informática, aprendizaje de maquina, Inteligencia artificial, redes de datos*

Resumen Técnico: *Actualmente, los sistemas de redes informáticas se han convertido en una parte importante de nuestra vida. Resulta difícil de imaginar la realización de las actividades cotidianas sin tener acceso a la información disponible en Internet. Sin embargo, el crecimiento en las redes de computadoras ha traído aparejado un notable incremento en el número de incidentes de seguridad reportados. Frente a esto, los Sistemas de Detección de Intrusos basados en red (NIDS), surgen como una herramienta para ayudar al personal encargado de la seguridad de la red en el monitoreo y la identificación de ataques. Un NIDS se encarga de monitorear distintos dispositivos o segmentos de la red, analizando los protocolos en cada una de las capas con el objeto de encontrar actividad sospechosa. La búsqueda de actividad sospechosa en el tráfico red es una tarea que demanda una gran cantidad de recursos humanos y computacionales. Los procedimientos para la detección de intrusos deben ser capaces de hacer frente al constante incremento en el número de ataques junto a los grandes volúmenes de datos transferidos en las redes actuales. Durante los últimos años, se han aplicado un gran número de estrategias con la intención de aligerar la tarea de detección. Entre los enfoques más relevantes, se pueden mencionar desde métodos estadísticos y algoritmos de reconocimiento de patrones hasta aprendizaje de máquina. Las diferentes propuestas apuntan fundamentalmente a facilitar la tarea del personal de seguridad de la red, mejorando su capacidad de detección e intentando elevar el nivel de automatización en el proceso de detección de intrusos. A pesar de que muchas de estas técnicas han sido capaces de conseguir una alta taza de detección, se observa el hecho de que sólo algunas de estas han sido implementadas sobre redes con datos reales. Esto podría explicarse si se considera el hecho de que algunos de los supuestos sobre los cuales se basan estas técnicas, no siempre se cumplen. La disponibilidad de tráfico de red etiquetado como intrusión o normal, o la presencia de tráfico de red libre de ataques, son dos de las supuestos más comunes en las técnicas actuales. Por desgracia, asegurar tales supuestos exige grandes volúmenes de trabajo por parte del experto en seguridad de red, siendo esto lo que justamente se pretende evitar. Parecería que la mayoría de las propuestas actuales se orientan a la obtención de una alta taza de precisión en el proceso detección,*

dejando de lado un problema no menor como es la necesidad de reducir la interacción humana en dicho proceso. En este proyecto se propone investigar soluciones al problema de detección de intrusos mediante el análisis del tráfico de red. El principal objetivo de la investigación propuesta es proporcionar un sistema capaz de reconocer comportamiento intrusivo en el tráfico de red, junto a un alto grado de automatización durante todo el proceso de detección. Dicho proceso incluye la construcción del modelo de tráfico inicial, así como el ajuste periódico requerido a causa de la aparición de nuevas amenazas. El sistema propuesto debe ser capaz de adaptarse manteniendo la interacción con el personal de seguridad a un mínimo. Por lo tanto, la tesis descripta a lo largo de esta propuesta afirma que es posible reducir la interacción humana durante el proceso de detección y aun así mantener la taza de reconocimiento de intrusiones en niveles aceptables. A fin de alcanzar los objetivos planteados, se adopta un enfoque basado en modelos combinado para el proceso de detección, en donde se aplican algoritmos de aprendizaje automático no supervisados junto a métodos de computación evolutiva.

Keywords: *computer security, machine learning, artificial intelligence, data networks*

Summary: *Nowadays, network computer systems have become an important part of our life. It is difficult to image our daily activities without accessing at some point to information provided by interconnected computer systems. However, with the growth of computer networks, the number of security incidents has increased dramatically. In this sense, the use of Network Intrusion Detection Systems (NIDS) emerges as a tool aimed at helping network security staff to monitor and identify computer attacks. A NIDS monitors network segments or devices and performs analysis at different network protocol layers to identify suspicious activities. Looking for suspicious activities inside network traffic can be considered a challenging task which demands high human and computational resources. Detection approaches should be prepared for dealing with the rapid evolution on number of attacks and the large amount of Internet traffic volume. During the past years, a number of techniques have been proposed to address the intrusion detection problem. Techniques applying statistical methods, pattern recognition algorithms along with machine learning and data mining methods, are some of the most representative approaches applied to intrusion detection. These techniques aim at facilitating the work of the network security staff providing better detection capabilities along with some level of automation in the intrusion detection process. Despite many of these techniques have achieved the goal of getting high performance accuracy in a more automatic way, the fact is that only a few of them have actually been deployed on real life scenarios. This could be explained if we take into consideration that some of the assumptions in which these techniques rely on, do not always hold. The availability of network traffic labeled as intrusive or normal, or the presence of attack-free network traffic, are the two most usual assumptions followed by current techniques. Unfortunately, ensuring such assumptions demands a lot of work from security experts which is precisely what is wanted to avoid. It seems that most of current NDISapproaches focus on obtaining high detection*

accuracy leaving aside the goal of reducing human interaction (automatizing) into the whole intrusion detection process. This project proposes to investigate solutions to the intrusion detection problem focused on the analysis of network traffic. The main goal of the research is to provide a system capable of recognizing intrusive behavior on network traffic while improving the automation degree of the process. This includes the initial model construction as well as the periodic model adjustment caused by the occurrence of new threats. The proposed system should be able to adapt itself keeping the interaction with the security staff to a minimum. Therefore, the thesis outlined in this proposal is that is possible to reduce the human interaction required for performing still accurate network intrusion detection. In order to achieve these goals, the proposed research will adopt a combined detection approach based on unsupervised machine learning techniques along with evolutionary computation methods.