SITEMAS DETECCIÓN DE INTRUSOS Y SISTEMAS EXPERTOS EN LA SEGURIDAD INFORMÁTICAS.

Ing. Juliet Díaz Lazo, MSc. Adriana Pérez Gutiérrez, Dr.C. René Florido Bacallao
Instituto Nacional de Ciencias Agrícolas, carretera Tapaste Km. 3 ½ San José, Mayabeque
juliet@inca.edu.cu

Resumen:

En este artículo se podrá ver la aplicación de los sistemas informáticos inteligentes (SII) para la detección de intrusos en la actualidad. Las temáticas van desde las más triviales como son los virus, los cortafuegos, el cifrado de información, los sistemas de detección de intrusos (SDI), agentes móviles, lógica difusa, hasta las más complejas como técnicas para la detección de intrusos, sistemas de expertos, redes neuronales y minería de datos. Algo muy interesante que caracteriza el artículo son los ejemplos que se exponen de los sistemas de detección de intrusos que utilizan sistemas expertos, su utilidad y características específicas de cada uno de ellos. El objetivo de este trabajo es que sea ampliamente consultado con el propósito que cada vez más toda esta comunidad este consciente de la importancia que tiene la seguridad informática y el auge que existe en los sistemas informáticos inteligentes que utilizan sistemas de expertos.

Palabras claves: Sistemas Expertos, sistema de detección de intrusos, seguridad informática, sistemas informáticos inteligentes.

Abstract:

By reading this article you can see the see the implementation of intelligent computer systems (SII) for intrusion detection today. The topics range from the most trivial as they are viruses, firewalls, encryption of information, intrusion detection systems (IDS), mobile agents, fuzzy logic, even the most complex techniques for intrusion detection expert systems, neural networks, data mining. An interesting that characterized the paper are the examples presented of intrusion detection systems using expert systems, its utility and specific characteristics of each one of them. The aim of this work is to be widely consulted by teachers and students of computer science in order that more and more throughout this community be aware of the importance of computer security and the growth that exists in computer systems that use smart expert systems.
KEY WORDS: Expert System, intrusion detection system, information security, intelligent computer systems.

Introducción

La seguridad informática tiene como objetivo principal disminuir los riesgos a que se exponen los sistemas informáticos.
Las vulnerabilidades de software contribuyen el factor principal a los problemas de seguridad de Internet desde hace mucho tiempo, oportunidad que utilizan los hacker para apropiarse de información, intercambiarla o distribuirla a otras personas, así como alterar o modificar el comportamiento de las aplicaciones, todas estas causas han originado técnicas, métodos y sistemas inspirados en estrategias de defensa, ataque y contraataque teniendo como propósito general proteger la información almacenada e

instalada en los medios de cómputos, convirtiéndose en un medio de defensa para que la información que existe en un sistema no se vea comprometida. Por lo general los mecanismos de seguridad necesitan obrar de manera conjunta para complementarse unas con otras y perfeccionar sus debilidades y alcances.
En la actualidad se ha logrado disminuir los ataques ya conocidos y un retrazo en los que no se conocen. En la seguridad informática se utilizan herramientas entre las que encontramos:

Los antivirus:
Son programas que exploran periódicamente el contenido del ordenador donde está instalado, detecta si hay virus y los elimina. Están compuestos por un motor y un conjunto de vacunas que se actualizan de manera automática en el servidor.
Los antivirus son esenciales en sistemas operativos cuya seguridad es baja, como Microsoft Windows, pero existen situaciones en las que es necesario instalarlos en sistemas más seguros, como Unix y similares(1).

Cortafuegos:
Es un sistema que previene el uso y el acceso desautorizados a tu ordenador o a las redes privadas conectadas con Internet, especialmente intranets.
Es importante recordar que un cortafuego no elimina problemas de virus del ordenador, sino que cuando se utiliza conjuntamente con actualizaciones regulares del sistema operativo y un buen software antivirus, añadirá cierta seguridad y protección adicionales para tu ordenador o red(2).

Cifrado de la información:
Es una técnica muy usada para aumentar la seguridad de las redes informáticas. Esta técnica convierte el texto normal en algo ilegible, por medio de algún esquema reversible de codificación desarrollado en torno a un clave privada que sólo conocen el emisor y el receptor(3).
Estos mecanismos de seguridad controlan y restringen el acceso a un sistema pero teniéndolos debidamente instalados y configurados no quiere decir que nuestra computadora este totalmente protegida ya que los atacantes pueden utilizar técnicas de evasión que les permite penetrar el sistema, esta situación a provocado que nos encontremos inmersos en una continua revolución para mejorar las estrategias de seguridad en aplicaciones.
Los sistemas de detección de intrusos (IDS) es otra de las herramientas de seguridad que informa cuando un atacante quiere penetrar o se encuentra dentro de un sistema, permitiéndole realizar una revisión detallada y profunda con el propósito de clasificar los datos y determinar cuales son los que pueden comprometer el sistema, los IDS son el complemento de los cortafuegos y antivirus

Sistema de detección de intrusos (IDS)
Los IDS se encuentran integrados por módulos que trabajan de forma conjunta y con funciones específicas para monitorear el tráfico de una red y los sistemas de una organización en busca de señales de intrusión, actividades de usuarios no autorizados y la ocurrencia de malas prácticas, como en el caso de los usuarios autorizados que intentan sobrepasar sus límites de restricción de acceso a la información(4).

Tipos de IDS
Existen varios tipos de IDS, clasificados según el tipo de situación física, del tipo de detección que posee o de su naturaleza y reacción cuando detecta un posible ataque.

Clasificación por situación

Según la función del software IDS, estos pueden ser:

- NIDS (Network Intrusion Detection System)
- HIDS (Host Intrusion Detection System)

Los NIDS analizan el tráfico de la red completa, examinando los paquetes individualmente, comprendiendo todas las diferentes opciones que pueden coexistir dentro de un paquete de red y detectando paquetes armados maliciosamente y diseñados para no ser detectados por los cortafuegos.

Los NIDS tienen dos componentes:

- Un sensor: situado en un segmento de la red, la monitoriza en busca de tráfico sospechoso
- Una Consola: recibe las alarmas del sensor o sensores y dependiendo de la configuración reacciona a las alarmas recibidas.

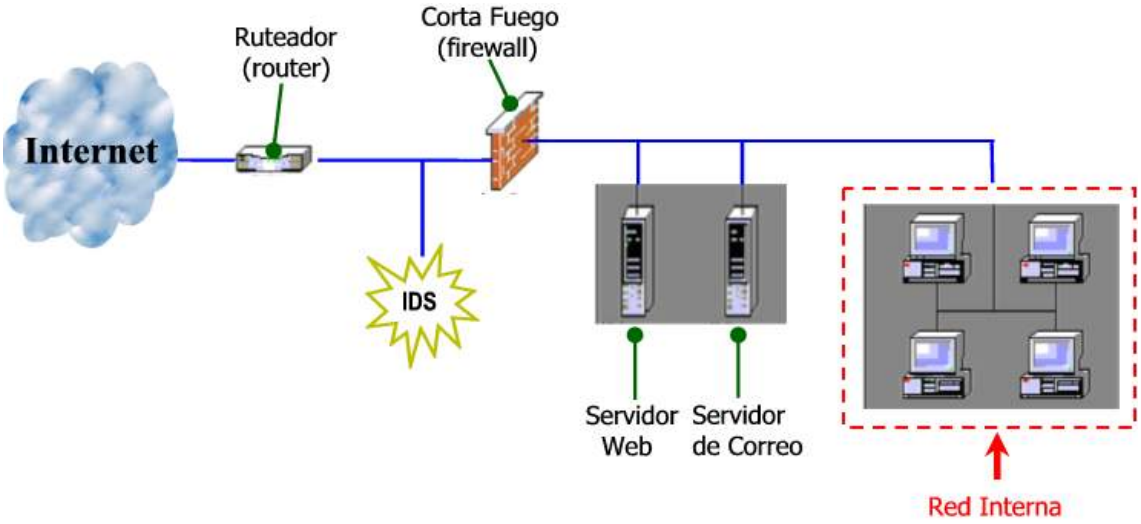
En cambio, los HIDS analizan el tráfico sobre un servidor o un PC, se preocupan de lo que está sucediendo en cada host y son capaces de detectar situaciones como los intentos fallidos de acceso o modificaciones en archivos considerados críticos.

Clasificación según los modelos de detecciones

Los dos tipos de detecciones que pueden realizar los IDS son:

- Detección del mal uso: La detección del mal uso involucra la verificación sobre tipos ilegales de tráfico de red. Este tipo de detección puede incluir los intentos de un usuario por ejecutar programas sin permiso.
- Detección del uso anómalo: se apoya en estadísticas tras comprender cual es el tráfico “normal” en la red del que no lo es. Esto se consigue realizando un modelo estadístico que contenga una métrica definida y compararlo con los datos reales analizados en busca de desviaciones estadísticas significantes.

Mosmo



Modelo IDS en una red simple

Modelos de IDS.

Desarrollar un modelo de un sistema de detección de intrusos requiere considerar los factores que lo integran y la vulnerabilidad que es inherente a éste, a través del uso de la terminología que denote la interacción con el entorno y la secuencia de pasos que describen el proceso de intrusión(5).

Sistema
Es un conjunto de equipos de cómputo o programas que brindan servicios que son utilizados por los usuarios.
Usuario
Persona que tiene acceso a un sistema por medio de permisos otorgados por el propietario del sistema.
Propietario
Persona que es dueña de la información contenida en el sistema.
Normal
Parámetro que sólo se puede establecer a criterio personal por el propietario de un sistema.
Anormal
Todo lo que se encuentra fuera del parámetro denotado como normal.
Anómalo (Anomalía)
Es la alteración o desviación que se presenta en un parámetro normal.
Intruso (Interno o Externo)
Puede ser una persona que accede local o remotamente a un sistema de forma ilegal, así como un programa que no se ha registrado previamente como parte de un sistema, y sus intenciones son de irrupción a la privacidad del propio sistema.
Atacante
Una persona o programa que trata de acceder de manera ilegal a un sistema y busca comprometer (poner en riesgo) su seguridad**.**
Las *técnicas de detección no pueden ser generalizadas dentro de un Modelo*, esto se debe a que en la búsqueda de un mejor análisis y clasificación de la información que recibe, se ha propiciado un ambiente idóneo para la exploración de nuevas técnicas y el empleo de diferentes ramas científicas que pueden ser aplicadas a los Sistemas de Detección.

Modelo propuesto por CIDF
Otra propuesta para tratar de hallar un modelo de Sistemas de Detección de Intrusos fue hecha por el CIDF (Common Intrusion Detection Framework).
Ésta sugiere la utilización de GIDO (Generalizad Intrusión Detection Object) como componente de intercambio de datos entre los diferentes módulos y la utilización de CISL como lenguaje para crear las reglas de detección, el cual tiene cierta similitud al lenguaje LISP. La Arquitectura está integrada por 4 módulos:

- *Generadores de Eventos*
- *Analizadores de Eventos*
- *Base de Datos*
- *Unidades de Respuesta*

El modelo que ha desarrollado el CIDF describe una arquitectura a seguir para definir los componentes que constituirán a un Sistema de Detección de Intrusos y la interoperabilidad entre diferentes fabricantes de IDS. Sin embargo, éste no ha sido considerado como un estándar, debido a la complejidad que presenta su lenguaje en la sintaxis misma y en el uso de GIDO para intercambiar información entre diferentes fabricantes de IDS.
GIDO (Generalized Intrusion Detection Objects) fue creado para establecer intercambio de información entre los diferentes módulos que constituyen un IDS, así como permitir la interoperabilidad entre otros IDS(5).

Modelo propuesto por IDWG del IETF

Otro modelo ha sido desarrollado por el IDWG (Intrusión Detection Working Group), que a diferencia del anterior, no propone una arquitectura específica, sino adaptarse a cualquiera existente.

Este modelo a diferencia de los descritos anteriormente, se puede considerar atractivo por el hecho de tratar de dar respuesta a la interoperabilidad entre los diferentes fabricantes de Sistemas de Detección de Intrusos. Sugiriendo para dicha solución la intercomunicación entre componentes, y la generación de reportes adaptables a las necesidades de información que se requieren conocer del sistema que se protege. Esto es posible a través de la utilización de las características que ofrece el lenguaje XML, el cual fue diseñado y propuesto como un estándar para el intercambio de información entre diferentes plataformas, obteniendo con esto la compatibilidad entre sistemas(5).

Modelo propuesto por Dorothy Denning

Modelo descrito por Dorothy Denning explica sobre similitudes informáticas que es lo que representaría cada componente en la detección de la instrucción específicamente para un solo equipo y no para una red.

El modelo esta constituido por sujetos, objetos, registro de auditoria, perfiles, registro de anomalías, reglas de actividades y análisis.

En esta propuesta se presenta como sistema al conjunto integrado por sujetos y objetos, donde su interacción es registrada y observada (almacenamiento de perfiles) en espera de sucesos (anomalías), que al ser comparados con las reglas establecidas y validándose éstas, se traducirán como intrusión; efectuándose con ello las alertas pertinentes a través de reportes. Este modelo recibió el nombre de IDES que implementó un sistema experto (SE) como técnica de detección de intrusiones(6).

Técnicas para le detección de intrusos

Los Sistemas de Detección de Intrusos (IDS), tienen como objetivo el detectar si existe o no una intrusión dentro de un sistema. Esto es posible efectuar, por medio del uso de diferentes áreas de investigación, de las cuales podemos citar: la Inteligencia Artificial, Métodos Estadísticos, Redes Neuronales, Minería de datos, entre otras. Las técnicas empleadas en una detección se ocupan de manera aislada o conjunta, en base a su flexibilidad y potencialidad para detectar intrusos(7).

Agentes Móviles

Los agentes son una entidad que actúa de manera autónoma, pero en colaboración con otros agentes para detectar una intrusión en un sistema. El agente obtiene información que permita reconocer la presencia de un intruso y la envía a un motor de análisis, quién dictamina si existe o no una intrusión. Si se halla algo importante es comunicado a los otros agentes para tomar las medidas apropiadas(8).

Agentes Inteligentes

Es una entidad que percibe y actúa sobre un entorno de forma razonada que puede realizar tareas específicas para un usuario y posee un grado de inteligencia suficiente para ejecutar partes de sus tareas de forma autónoma y para interactuar con su entorno de forma útil(9).

Lógica Difusa

Es una rama de la inteligencia artificial que se funda en el concepto "Todo es cuestión de grado". Los valores de salida de las relaciones difusas no son ambivalentes, 0 ó 1, sino que puede tomar valores reales entre 0 y 1(10).

Minería de Datos
Esta técnica permite extraer patrones o modelos de ataques desconocidos, de un conjunto de datos recolectados por un IDS(11). La minería de datos es una herramienta fundamental para la toma de decisiones. El proceso de aprendizaje de los datos juega un papel muy importante en muchas áreas de la ciencia, las finanzas y la industria, dónde las entidades o empresas han de minimizar los riesgos en la toma de decisiones estratégicas, es decir a partir de una base de datos, se adquieren nuevos conocimientos válidos, potencialmente útiles y, sobre todo, comprensibles.

Redes Neuronales
Es un área que está incursionando al igual que otras áreas como los Algoritmos Genéticos y el Sistema Inmune, en el campo de la detección de intrusos. La red neuronal es entrenada con compartimiento normales o anormales (estos valores dependen de la forma en que se desee detectar una intrusión). Mediante su empleo es posible detectar variaciones de ataques o de carácter desconocidos, que difieren de los patrones iniciales con que fue entrenada la red(12). Las redes neuronales (RNAs) están inspiradas en el sistema lógico natural, como es conocido en este sistema la neurona es la unidad de procesamiento y aunque las (RNAs) sean mucho menos complejas en un sistema informático también realizan cálculos complejos para procesar información.

Métodos Heurísticos
Emplea el resultado que es generalmente obtenido a través de algún método estadístico, para ajustar un umbral de detección de lo normal y anormal que se presenta en un sistema. Tratando con ello, de aminorar el número de falsos positivos y negativos en un IDS.

Sistemas Expertos
Los sistemas expertos, también llamados sistemas basados en conocimiento, pueden considerarse el primer producto verdaderamente operacional de la Inteligencia Artificial y son esquemas diseñados para emular a un especialista humano en un dominio particular o área de conocimiento. Entre esas aplicaciones cabe destacar el campo de la Automática, donde se utilizan en supervisión y monitorización, robótica, y control en general(13). Estos sistemas imitan las actividades de un humano para resolver problemas de distinta índole. También se dice que un SE, se basa en el conocimiento declarativo (hechos sobre objetos, situaciones) y el conocimiento de control (información sobre el seguimiento de una acción). Para que un sistema experto sea herramienta efectiva, los usuarios deben interactuar de una forma fácil.

Sistema de Detección de Intrusos que utilizan Sistemas Expertos

IDES 1980 (Intrussion Detection Expert System) es un sistema experto cuyo motor de detección está basado en conocimiento. Posee un detector de anomalías estadístico(14).

HayStack 1988 El proyecto Haystack, del Centro de Soporte Criptológico las Fuerzas Aéreas de EEUU fue usado para ayudar a los oficiales a encontrar signos de ataques internos en los ordenadores principales de sus bases. Estas máquinas eran principalmente "mainframes" (servidores corporativos) que manejaban información no clasificada pero confidencial. El sistema estaba escrito en C ANSI y SQL. Examinaba los datos de forma periódica, recogiendo colas de eventos de forma periódica. Utilizaba dos

fases de análisis para detectar las posibles anomalías. El principal responsable del proyecto fue Steve Smaha(15)

Wisdom & Sense 1989: El sistema "Wisdom and Sense" fue un detector de anomalías creado en el Laboratorio Nacional de Los Alamos en cooperación con el Laboratorio Nacional de Oak Ridge. Utilizaba técnicas no paramétricas ("nonparametric techniques"), que eran técnicas estadísticas que no hacían suposiciones sobre la distribución de los datos. Usaban este método para crear su propio conjunto de reglas. Luego analizaba los "logs" de las auditorias en busca de excepciones de esas reglas, las cuales estaban organizadas en "arrays" con forma de árbol. Definían lo que era el comportamiento normal desde un punto de vista cronológico de los datos de auditoria(16).

ISOA 1990 Estos sistemas transfieren la información de múltiples anfitriones supervisados a un sitio central para el tratamiento. Estos emplean los mismos algoritmos que en los sistemas basados en host sin supervisar ningún tráfico de red.
ISOA (Information Security Officer's Assistant) es un sistema que considera una gran variedad de estrategias incluyendo estadísticas, un comprobador y un sistema experto(17).

NADIR 1990: "Network Audit Director and Intrusion Reporter" (NADIR) fue desarrollado en Laboratorio Nacional de Los Alamos, para monitorizar el "Integrated Computing Network" (ICN). Esta red estaba inicialmente compuesta por unos 9.000 usuarios. NADIR usaba técnicas de detección similares a los sistemas de su tiempo como el IDES o MIDAS. Fue uno de los sistemas con más éxito de los años ochenta. La principal responsable de NADIR fue Kathleen Jackson(14)

Shadow 1994 (Secondary Heuristic Analysis for Defensive Online Warfare) procesa los archivos de log de tcpdump y puede identificar ataques. Fue desarrollado como respuesta a los falsos positivos de un IDS anterior, NID. La interfaz permitiría al analista evaluar gran cantidad de información de red y decidir de qué eventos informar.
Shadow almacena el tráfico de red en una base de datos y se ejecuta por la noche. Los resultados esperan a que el analista llegue a la mañana siguiente.
Al no ser en tiempo real, es inviable que Shadow analice él contenido de los paquetes, por lo qué tan solo se centra en las cabeceras. Esto le hace inútil para análisis forense(4).

IIDS 2000 IIDS (Detección de intrusos inteligente): Este sistema intenta evaluar la autenticación a través de una red UNIX, basada en reglas específicas, errores o actividad maliciosa.
El módulo de mapa cognitivo (FCM, *Fuzzy cognitive Maps*), núcleo del IIDS, provee una forma natural de adquisición de conocimiento, que representa el conocimiento de un experto de manera tal que es muy fácil de entender por un experto humano.
En la arquitectura IIDS, los sensores de detección de anomalías y formas no autorizadas de uso que están permanentemente monitoreando el sistema, sirven como expertos, en las estaciones de trabajo de usuarios finales, y de tráfico de la red.
Estos componentes usan métodos tales como aprendizaje de máquina o sistemas expertos, para detectar información de intrusión y transferirla luego a al sistema de anomalías o uso indebido(18).

Conclusiones

Este artículo muestra la unión entre el campo de la Inteligencia Artificial y el de la Seguridad Informática, lo que fortifica la seguridad minimizando las vulnerabilidades y aprovechando los avances en las técnicas de inteligencia artificial, específicamente los sistemas expertos.
Se logro ampliar los conocimientos acerca de los sistemas de detección de intrusos que utilizan sistemas expertos con el objetivo de minimizar los riesgos en aplicaciones informáticas.

Bibliografía

1. Ficarra, F., ANTIVIRUS Y SEGURIDAD INFORMÁTICA: EL NUEVO DESAFÍO CIBERNÉTICO DEL SIGLO XXI, in *CHASQUI*, Vol. 79, pp. 72 (2002).
2. SORIANO, M., ¿CÓMO FUNCIONA LA SEGURIDAD EN INTERNET?, 77 (2007).
3. Jajodia, S., *Advances in Information Security*, Vol. 46 (2007).
4. Alfaro, E. J. M., Implantación de un Sistema de Detección de Intrusos en la Universidad de Valencia, in *Ingeniería Informatica*, Universidad de Valencia, Valencia (2002).
5. Sezer, E. C., Conferencia sobre la Seguridad Informática y Comunicaciones, in *El software de seguridad*, EE.UU., A. f. C. M. N. Y., Ed., pp. 562 a 572 (2007).
6. Denning, D., Modelo detección de intrusos, in *Modelo detección de intrusos*, IEEE, IEEE (1986).
7. Arroyave, J. D., Herrera, Jonathan y Vásquez, Esteban., Propuesta de modelo para un Sistema Inteligente de Detección de Intrusos en Redes Informáticas, Escuela de Ingeniería de Antioquia. Arroyave, Herrera, Vásquez., pp. 9 (2007).
8. Echeverry, G. A. I., Sanz, A. G. C., and Méndez, N. D. D., Técnicas inteligentes, agentes adaptativos y representaciones ontológicas en sistemas de detección de intrusos, Vol. 6, pp. 53 (2007).
9. Nestor Dario Duque Mendez, J. C. C. P., Ricardo Moreno Laverde, Seguridad Inteligente, in *Revista Científica de América Latina y el Caribe (REDALYC)*, Vol. 13, pp. 389 (2007).
10. Retamales, F. E. Q., Navegación robótica basada en aprendizaje evolutivo de acciones mediante lógica difusa, in *Departamento de electrónica*, Universidad Técnica Federico Santa María, pp. 39 (2006).
11. Bettini, C., Wang, X. S., and Jajodia, S., *Privacidad en aplicaciones basadas en localización* (2009).
12. Zurutuza, U., and Uribeetxeberria, R., Revisión del estado actual de la investigación en el uso de data

mining para la detección de intrusiones, Dpto. Informática
Escuela Politécnica Superior, Mondragón pp. 8 (2005).

13. Ribas, M. M., and Alfonso, J. M. d., Los agentes inteligentes o electrónicos: aceptar o no aceptar sus contratos (2002).
14. Santos, R. C., DETECCIÓN DE INTRUSOS MEDIANTE TÉCNICAS DE MINERÍA DE DATOS, in *Revista Clepsidra*, Vol. 2, pp. 31 (2006).

15. Samaha, S., An Intrusion Detection System for the Air Force, in *Proceedings of the Fourth Aurospace Computer Security Applications Conference*, Orlando, F., Ed. (diciembre 1988).
16. Vaccaro, H., Detection of Anomalous Computer Session Activity, in *Proceedings of the 1989 IEEE Symposium on Security and Privacy* Oakland, C., Ed. (mayo 1989).
17. Márquez, V. E. G., Sistema de detección de intrusos basado en sistema experto, in *Centro de Investigación en Computación*, Instituto Politécnico Nacional, México, pp. 138 (2010).
18. García, M. I. G., Utilización de Sistemas de Detección de Intrusos como Elemento de Seguridad Perimetral, Universidad de Almería, Almeria, pp. 307 (2008).