DETECCIÓN DE INTRUSOS MEDIANTE TÉCNICAS DE MINERÍA DE DATOS

RAFAEL CASTILLO SANTOS[1]

Resumen.

El presente artículo es una recopilación de información sobre sistemas informáticos relacionados con la detección de intrusos, utilizando herramientas de minería de datos.

La detección y control de accesos no autorizados en los sistemas de información ha sido un problema desde el mismo inicio de los sistemas de información computarizados, donde la seguridad y privacidad de la información son factores importantes. A su vez el conocimiento cada vez más profundo de los sistemas que soportan el desarrollo y aplicación de los sistemas informáticos, el conocimiento o detección de las fallas que estos presentan y el reto de vulnerarlos, ha llevado a que cada vez haya más personas interesadas en cometer tales actos ilícitos. Por otra parte estas mismas herramientas computacionales llevan a crear nuevas barreras o defensas, convirtiéndose en procesos de nunca acabar.

Sin embargo, normalmente el registro de los sucesos de ataques queda almacenado en medio magnético (ya que un hacker o un cracker la mayoría de las veces no deja huella), para ser posteriormente analizado y llevado a cifras estadísticas que muestran perfiles, tipos de ataques, número de intentos, etc. Si estos registros posteriormente se unen en una bodega de datos, se puede con técnicas de minería de datos, establecer por ejemplo, patrones de comportamiento que permitirán anticipar un ataque y por lo tanto activar las señales necesarias para su detección oportuna, como lo hacen sistemas como IDS, MADAM ID Y MINDS, entre otros.

Abstract.

The present article is a summary of information it has more than enough computer systems related with the detection of intruders, using tools of mining of data. The detection and control of accesses not authorized in the systems of information it has been a problem from the same beginning of the on-line systems of information, where the security and privacy of the information are important factors. In turn the more and more deep knowledge of the systems that you/they support the development and application of the computer systems, the knowledge or detection of the flaws that these they present and the challenge of harming them, it has taken to that every time there are more people interested in making such illicit acts. On the other hand these same tools computational take to create new barriers or defences, becoming processes of never to end up.

However, the registration of the events of attacks is usually stored between magnetic (since a hacker or a cracker most of the times don't leave print), to be analyzed later on and taken to statistical figures that show profiles, types of attacks, number of intents, etc. If these registrations later on unite in a cellar of data, one can with technical of mining of data, to settle down for example, behavior patterns that will allow to advance an attack and therefore to activate the necessary signs for its opportune detection, as they make it systems like IDS, MADAM GOES AND MINDS, among others.

Introducción.

El objetivo principal de un sistema para la detección de intrusos debe ser la detección oportuna del ilícito, lo ideal sería que fuera en el mismo momento que se está llevando a cabo. Pero cuando por falta de recursos suficientes o por funcionalidad del sistema, éste se aplica fuera de línea, es necesario que

[1] Rafael Castillo Santos Departamento de Sistemas e Informática Universidad Autónoma de Colombia rcastill@correo.fuac.edu.co

la detección se realice lo más pronto posible. Estudios realizados en universidades como Minessota, Columbia, George Mason, Corporación Mitre, entre muchas otras, han obtenido resultados positivos y bastante aproximados a lograr este objetivo. Algunos de estos se describirán al final del presente artículo (numeral 4). Previamente en el numeral 2, Antecedentes, se describen las condiciones que han motivado la mayoría de acciones tendientes a crear sistemas informáticos que eviten que un sistema sea vulnerado. En las áreas del conocimiento involucradas, numeral 3, se relacionan las áreas que contextualizan el conocimiento necesario para tratar el tema y su posterior desarrollo. Finalmente se presentan algunas conclusiones relacionadas con los resultados y aplicaciones obtenidas (Numeral 5)

La lectura está orientada a personas que conozcan de los temas expuestos, debido fundamentalmente a que cada tema puede constituirse en si mismo en toda una especialización. Pero no por ello se pretende excluir a quienes quieran empezar a conocer sobre los términos y áreas del conocimiento aquí tratadas, pues será una base para su posterior profundización.

Intencionalmente se han dejado varias palabras y términos en inglés, debido desafortunadamente para nuestro idioma, que es como se conocen en la argot técnico y muchos de ellos aún no tienen traducción o la traducción que se les da no es la más adecuada al significado real. La traducción cuando la tiene es la más comúnmente aceptada.

Antecedentes.

Según cifras estadísticas, los ataques a los sistemas informáticos siguen incrementándose día a día, dadas las nuevas facilidades proporcionadas por algunos sitios de *Hackers, Crackers*, etc, y por el mayor conocimiento tanto de las herramientas computacionales, como de las debilidades de las mismas (ejemplo de Windows en sus diferentes versiones, vulnerabilidad de puertos, puertas traseras, virus, troyanos, etc).

Los muros cortafuego (*firewall)* tanto en hardware como en software, proporcionan una barrera bastante eficiente a los ataques computacionales, pero dada la característica y amplitud de posibilidades de entrar a un sistema, éste se constituye en un obstáculo fácilmente salvable, utilizando software que engaña la identidad (*spoofing*), simulando ser quien no es.

Las claves de acceso (*passwords)* a las diferentes aplicaciones informáticas, desde el mismo ambiente de entrada al sistema operacional de la máquina y el de cada una de las aplicaciones de una organización, sigue siendo un problema de cultura organizacional que facilita en gran medida la entrada de intrusos, dado que muchas personas utilizan claves fácilmente descifrables, como palabras que están en un diccionario, nombres comunes de personas o mascotas.

El uso de software como *keyloggers*, *spyware*, y otros, permiten capturar información confidencial, como las claves de acceso, para luego a través de otros programas enviarla por Internet y de esta manera tener acceso al sistema y así tomar control del mismo o hacer uso de los datos.

Áreas del conocimiento involucradas.

En la actualidad cualquier actividad humana relacionada con sistemas de información computarizados, tiene que ver con muchas áreas del conocimiento. En el caso del presente artículo:

- Es necesario conocer cómo se almacenan y recuperan las grandes cantidades de información, proporcionadas por los registros permanentes de las actividades realizadas a través de un medio de comunicación, para lo cual la metodología, métodos y herramientas relacionados con las bodegas de datos y minería de datos son fundamentales.

- Se requiere identificar los comportamientos de los usuarios dentro del proceso que se lleva a cabo cuando se conectan a un sistema informático, a través de un medio de comunicación (sea éste público o no), para detectar cuando es normal, cuando es con fines delictivos o malintencionados (tumbar el sistema o conocer información confidencial) o cúando se trata realmente de un ataque informático. Por ello se deben conocer los diferentes tipos de ataques a los sistemas informáticos y los sistemas actualmente disponibles para la detección de intrusos.

- En este mismo marco de referencia es un requisito, determinar las deficiencias y fortalezas de los sistemas operativos (Windows, Unix, GNU-Linux, Solaris, AIX) con los cuales se llevan a cabo las diferentes aplicaciones informáticas de una organización (Contabilidad, Nómina, producción, etc.).

- También se deben identificar las fortalezas y debilidades de los medios de comunicación, de los equipos y del software utilizados para la transmisión de la información, pues ellos son otro punto vulnerable en la seguridad de un sistema de información.

- Finalmente, al interior de cada una de las aplicaciones, es imperativo saber la forma como cada una plantea el acceso y la seguridad de la información y necesariamente deben haberse tomado en cuenta las diferentes políticas de seguridad de una organización, pues como es bien conocido “el punto más débil de un sistema informático, en cuanto a su seguridad, lo constituye el usuario final”.

De cada uno de estos puntos se tratará brevemente a continuación.

Bodegas de datos y Minería de datos.

Las bodegas de datos (*Datawarehouse*) se consideran como la integración de conjuntos de datos muy grandes (del orden de los terabytes), existentes como consecuencia de cada una de las diferentes acciones que tiene una organización (datos de su acontecer diario), guardados probablemente en bases de datos, los cuales luego de ser agrupados y clasificados, pueden acelerar los procesos de análisis y consulta de información para la toma de decisiones. Empezaron a utilizarse debido a la necesidad de buscar patrones de comportamiento de clientes; de buscar intentos de fraude en tarjetas de crédito; a relacionar la forma y el cuándo los clientes compran productos; a buscar relaciones de afinidad entre los productos cuando son comprados o adquiridos por los usuarios, etc.

Algunas de las características de las bodegas de datos son [1]:

- Almacenan información de muchas fuentes, la cual ha sido tratada para garantizar la unicidad del dato y darle una única orientación más que una aplicación. Es decir, las bodegas de datos tratan un tema en particular (i.e Clientes, ventas, productos, etc), diferente a lo que hacen las bases de datos que tratan una aplicación del negocio (i.e nómina, inventarios, cartera, etc.).

- Los datos (una dirección, un teléfono o un nombre de un cliente, etc) han sido tratados para darles una única forma de representación en cuanto a nombre, formato (entero, carácter, *string*, etc), dominio de campo (Nit, CC. TI, etc), y unidad de medida (relacionada con el contenido del campo, i.e. metros, kilos, etc); unificando los existentes en diferentes sistemas informáticos de la organización (nómina, clientes, ventas, etc).

- Las bodegas de datos son estáticas y sus datos no son actualizables, es decir son no volátiles. Una vez almacenado el dato en una bodega de datos, éste permanecerá inalterable de ahí en adelante.

- Las bodegas de datos permiten solamente el ingreso de nueva información, lo cual indica que su contenido está variando en el tiempo.

- El factor tiempo es importante en una bodega de datos, pues debe reflejar un comportamiento en un intervalo de tiempo dado, permitiendo información redundante. En este aspecto las bodegas de datos constituyen una antítesis de las bases de datos, pues mientras las primeras tienen gran cantidad de información, mucha de ella redundante de alguna forma, las segundas tratan de garantizar la unicidad del dato.

Un factor diferenciador de las bodegas de datos es la *Metadata*, la cual se usa para:

- Ubicar los contenidos de la bodega de datos, comportándose como un directorio.

- Guiar la transformación de los datos de entrada desde el ambiente de las bases de datos a la bodega de datos (*mapping*).

- Guiar la utilización de los diferentes algoritmos en cuanto al grado de consolidación (resumen) de los datos.

El aporte de la minería de datos comienza por su definición: "La minería de datos es el proceso de extraer modelos o patrones útiles no previsualizados (ocultos) de grandes almacenes de datos [15]". Las técnicas de minería de datos, permiten la clasificación de datos según un contexto o comportamiento, por ejemplo de ataque o no ataque. Adicionalmente permite obtener comportamientos por medio del análisis secuencial; permite la totalización de datos y la visualización de los mismos por medio de diferentes representaciones (árboles de decisión, funciones lineales o no lineales, modelos de probabilidad, etc).

Etapas de desarrollo de minería de datos.

Los pasos que se siguen para el desarrollo de un trabajo de minería de datos, se basan en las etapas de la metodología propuesta por Michael Berry y Gordon Linoff en [1] son:

- Traducir el problema de negocio a un problema de minería de datos.
- Seleccionar los datos adecuados.
- Conocer los datos.
- Crear un *model set*
- Solucionar problemas con los datos
- Transformar los datos
- Construir modelos
- Evaluar modelos
- Desplegar modelos
- Evaluar resultados
- Volver a empezar

Estas pasos se pueden agrupar en las siguientes cuatro fases

Filtrado de datos: Debido a que para obtener los datos es necesario recurrir a diferentes fuentes, el formato de los datos nunca es el idóneo, y la mayoría de las veces no es posible utilizar algún algoritmo de minería. Por lo tanto es necesario realizar un preprocesado, filtrando los datos mediante eliminación de valores incorrectos, datos no válidos, datos desconocidos, etc. También se puede obtener muestras de los mismos dando mayor velocidad de respuesta del proceso, o se puede reducir el número de valores posibles mediante redondeo o agrupamiento.

Selección de variables: Se hace para reducir la cantidad de datos, eligiendo las variables más influyentes en el problema, sin sacrificar la calidad del modelo obtenido. Los métodos para la selección de características son dos:

- Los basados en la elección de los mejores atributos del problema.

- Los que buscan variables independientes mediante pruebas de sensibilidad, algoritmos de distancia o algoritmos heurísticos.

Extracción de Conocimiento: El objetivo es obtener un modelo de conocimiento, que represente patrones de comportamiento observados en los valores de las variables del problema o relaciones de asociación entre dichas variables.

Interpretación y evaluación: Finalmente se procede a su validación, comprobando que las conclusiones son válidas y satisfactorias. En el caso de haber obtenido varios modelos mediante el uso de distintas técnicas, se deben comparar los modelos en busca de aquel que se ajuste mejor al problema. Si ninguno de los modelos alcanza los resultados esperados, se alterará alguno de los procesos anteriores en busca de nuevos modelos.

En cuanto al software utilizado en la minería de datos se clasifica en:

- De consulta y de reporte (i.e. *Cristal reports, Impromtu, ReportSmith, Intelligent Query*, etc)

- OLAP (*On Line Analytical Processing*), Procesamiento analítico en línea y ROLAP (*Relational On Line Analytical Processing*), procesamiento analítico en línea relacional. Proveían inicialmente acceso a bases de datos multidimensionales (Cubos), que permitían capacidades de partir y unir (*Slice and Dice*) sistemas de información.

- Aplicaciones construidas sobre las herramientas de las bodegas de datos, para la gestión de una organización.

Por otra parte entre las herramientas más comúnmente usadas para extraer información de las bodegas de datos tales como clasificación, agrupación, predicción (*Dataminig* minería de datos), están: Modelamiento predictivo, redes neuronales, detección de desviación, programación genética y otras más.

Tipos de ataques a los sistemas informáticos.

Se puede entender como tal, a cualquier intento externo o interno que trate de burlar o pasar inadvertido por los sistemas o técnicas implementadas para garantizar la seguridad de cualquier sistema informático. Lo anterior se puede deber a una de las siguientes causas:

- Los mecanismos de seguridad de cualquier sistema de protección, pueden tener vulnerabilidades como huecos o fallas no detectadas oportunamente por quienes las implementan (Ing. de sistemas, Administradores del sistema, Usuarios, etc), pero sí detectadas por quienes tratan de burlarlas *hackers, crackers, lammers*, por ejemplo. [20].

- Los sistemas son muy fácilmente superados desde el perímetro interno de la red (*insider Atacks*), sin que los sistemas Cortafuegos puedan siquiera enterarse o actuar.

- Desde el perímetro externo cada vez existen técnicas más sofisticadas, de ingeniería social, virus, troyanos, etc que tratan de encontrar los huecos o fallas de los sistemas de protección o conocer claves o accesos a los sistemas a través de husmeadores (*Sniffers),* y burladores *(Spoofers), etc.*[21]

Algunos tipos de ataques conocidos son:

- DoS (*Denial of Service*, negación del servicio) trata de tumbar una red de computadores, un servidor o un proceso por un sin número de conexiones, peticiones al sistema o impidiendo el uso de recursos a los usuarios autorizados, causando un bloqueo o caída del mismo. Cuando el ataque se lleva a cabo desde diferentes sitios, se conoce como DoS distribuido.

- Exploración (*Probe*) o Escaneo. En este tipo de ataque los intrusos reúnen información relacionada con el equipo (Servidor) donde está ejecutándose la aplicación, para obtener listas de direcciones IP, servicios disponibles, usuarios, listas de correos, etc.

- Comprometer al sistema. Basándose en las debilidades y vulnerabilidades de algunos sistemas, tales como desbordamiento (*overflow*) o debilidades de seguridad, los atacantes tratan de obtener el control de una máquina en modo privilegiado.

- Dos formas usadas en este tipo de ataques son:

  - R2L (*Remote to Login*): Los atacantes usan su habilidad para enviar paquetes a un servidor sin tener una cuenta establecida en dicha máquina, obteniendo el acceso como usuario o administrador (*root*).

  - U2R (*User to Root*): Un usuario que tiene una cuenta establecida en un servidor, tiene la habilidad de escalar privilegios por medio de errores (*bugs*) del sistema operacional o aplicación a donde está conectado.

- Programas que llegan a una máquina sin ser detectados por los sistemas de seguridad y que utilizan la habilidad de replicarse o comunicarse con una dirección predeterminada, sin que el usuario se de cuenta de lo que está sucediendo, sino hasta cuando ya es tarde para tomar acciones correctivas o preventivas.

- Caballos de Troya, gusanos (*worms*) o virus.

- Ataques de fuerza bruta, ataques de diccionario, ataques *Smurf*, son otros tipos de ataques, entre muchos otros.

Sistemas de detección de intrusos (SDI).

Un sistema de detección de intrusos es todo aquel que resulta de la combinación tanto de software como hardware, que mediante alguna acción, alarma o indicador permite establecer con algún grado de precisión, cuándo se lleva o llevó un ataque a un sistema informático. Un sistema muy conocido es el SNORT [2], que provee mediante unas sentencias fáciles de implementar, crear un ambiente de detección de intrusos, pero a costa de poca flexibilidad y dinámica.

La mayoría de estudios que se han realizado hasta la fecha [4], están de acuerdo en que básicamente existen dos técnicas para realizar la detección de intrusos en los ataques a un sistema informático: Usos malintencionados o no permitidos de un sistema (*misuse*) y detección de anomalías (*anomaly detection*).

El primero enfoca la atención en el uso de patrones de ataques muy bien conocidos y/o en la detección de los puntos débiles de un sistema, para identificar una intrusión conocida. El segundo está basado en las desviaciones a una forma normal de comportamiento de un usuario frente a un sistema informático.

El uso de técnicas para la detección de intrusos, por medio de bodegas de datos y sus correspondientes técnicas de minería de datos, es relativamente reciente. En 1995 Ramakrishnan Srikant,[6], en su tesis doctoral, planteó el desarrollo de algoritmos rápidos para la búsqueda de reglas de asociación y patrones secuenciales, trabajo que fue tomado como base por Wenke Lee y Salvatore J. Stolfo de la Universidad de Columbia [3], en el planteamiento de modelos de minería de datos para la detección de intrusos.

En el trabajo realizado por estos autores, se plantea por medio de dos algoritmos: el de reglas de asociación y el de episodios frecuentes, determinar patrones consistentes, que describan el comportamiento de los usuarios por medio de clasificadores, que permitan reconocer anomalías e intrusiones conocidas.

Erick Bloedorn y otros [15] en Mitre Corporation, habían estado realizando trabajos relacionados con la detección de intrusos, sin tomar como herramientas la minería de datos. Dadas las dificultades en el manejo de grandes cantidades de información, debido al incremento permanente en el número y cantidad de ataques, comenzaron a utilizar otras formas para llevar a cabo el proceso. Básicamente tomaron en cuenta el trabajo de Lee (*ibidem*) en dos factores fundamentales [3]: desarrollar una manera de minimizar lo que los analistas de los sistemas de detección podían usar diariamente y si la minería de datos podía ayudar a encontrar ataques que las personas (analistas) y los sensores utilizados no detectaban. Sin embargo estos sistemas tienen un desempeño muy pobre en la detección de formas nuevas de ataques y un nivel alto de falsas alarmas.

Erick Bloedorn y otros [15] propusieron que la solución a estos inconvenientes podría darse con la aplicación de un conjunto de técnicas de minería de datos a las redes de comunicación de datos en ambientes fuera de línea, teniendo como base que existen multi-sensores y multi-métodos de correlación. El sistema propuesto para trabajar fuera de línea permite detectar exploraciones (*scan*) lentas y débiles, gusanos o la actividad no usual de un usuario basada en algún nuevo tipo o patrón de comportamiento. Adicionalmente estos sistemas permiten nuevos sistemas de comparación basados en métricas, que pueden usar datos históricos. También permiten a los administradores de los sistemas informáticos investigar sucesos acontecidos a priori, para ejecutar acciones preventivas o correctivas y disminuir en gran medida la cantidad de falsos positivos y por lo tanto el número de alarmas disparadas en el sistema.

Como lo anotó Bishop [7]: el análisis a tiempo está en la diferencia entre la detección de intrusos y el análisis pos mortem.

Fallas en sistemas operativos.

Los errores o *bugs* a la hora de programar código de un sistema operativo (como el núcleo de Unix), constituyen una de las amenazas a la seguridad que más dolores de cabeza proporcionan a la comunidad de la seguridad informática. En la mayoría de situaciones no se trata de desconocimiento a la hora de realizar programas seguros, sino del hecho que es prácticamente imposible no equivocarse en miles de líneas de código.

Todo sistema operativo debe proveer control sobre el área de memoria, para evitar que los diferentes programas que se están ejecutando simultáneamente se interfieran unos con otros. En la mayoría de ocasiones, cuando esto sucede, se presenta una falla del sistema y el usuario debe reanudar su sistema operativo. Pero como sucede con Unix, dependiendo de como haya entrado el usuario al sistema (como usuario normal o *root*) y del nivel donde se esté ejecutando la acción en el núcleo, por

[2] Mayor información se encuentra en www.snort.org

ejemplo, el sistema puede quedar totalmente desprotegido y bajo el control de un atacante.

Los desbordamientos de los *buffers* (*buffer overflow*) [21], es otro de los problemas más comunes y más antiguos, que puede hacer que el sistema quede en manos de un atacante. Este problema se presenta cuando en un arreglo se intenta utilizar o escribir en áreas que están por fuera de los límites del arreglo.

Si la intención es realmente originar este problema, el código que está en el *overflow*, código del intérprete de comandos creado en un archivo con privilegios de administrador, origina que el atacante también pueda tomar el control sobre el sistema.

También hay problemas con los sistemas operativos, en los cuales se puede originar un acceso indebido al sistema si se intenta utilizar un archivo al cual no se tiene permiso con el usuario actual. El caso concreto de Unix [21], las operaciones que se realizan son un *access*() y luego un *open*(). Debido a que las dos se ejecutan de manera independiente una de otra, un atacante puede realizar un cambio y direccionar a un archivo al cual no tiene permiso, cambiando el nombre y dirección del archivo luego de la operación *access*().

Esta situación se da debido a que el sistema ejecuta la acción *open*(), suponiendo que las condiciones dadas por el *access*() se mantienen. Afortunadamente estas situaciones ya están ampliamente detectadas y controladas.

Las puertas traseras (*back doors*) son condiciones dadas por los creadores de software, válido también para sistemas operativos, que permiten ingresar al sistema sin tener que someterse a algunos procesos de validación o de control por parte del mismo sistema. Normalmente estas condiciones son eliminadas antes de poner el sistema en funcionamiento o de realizar la entrega del mismo. También como consecuencia de la acción anterior, se pueden añadir nuevos servicios asignados a un puerto determinado, por medio del comando *telnet* ejecutando un comando del *kernel*

Equipos y medios de comunicación.

La sofisticación de un equipo o medio de comunicación, está asociado en un alto porcentaje a su costo, siendo por lo tanto los más costosos, los que en general tienen la forma de detectar intrusos o evitar su ingreso. Adicionalmente para que la información viaje a través de equipos y medios de comunicación, es necesario que lo haga de la forma más segura posible.

La mayoría de equipos y medios de comunicación, en la actualidad disponen de software, que garantiza en gran medida esta seguridad, ejemplos de él: los protocolos de comunicaciones SSL, (*Secure Socket Layer*), ipSec (*Internet protocol Security*); protocolo de Seguridad de internet; el software Estandar de Cifrado de datos DES (*Data Encription Standart*); PGP (*Pretty Good Privacy*); autenticación y firmas digitales. En cuanto a los equipos los conmutadores (*Switches*) y enrutadores (*Routers*) de comunicaciones en la actualidad permiten implementar seguridades adicionales a las tradicionales para impedir el acceso no autorizado de intrusos, por medio de barreras cortafuego, redes privadas virtuales (VPN, *Virtual Private Networks*) y otros mecanismos. Sin embargo, como ya es conocido, para cada nuevo procedimiento, técnica o método orientado a impedir accesos no autorizados, ya hay quien(es) está(n) creando las condiciones necesarias para evadirlo.

DES[10]: Estándar ampliamente usado en seguridad. Toma bloques de texto de 64 bits y los cifra en bloques de 64 bits. Se parametriza mediante una clave de 56 bits y tiene 19 etapas diferentes. La primera es una transposición independiente de la clave y la última es el inverso exacto de la primera. La etapa penúltima intercambia los 32 bits de la izquierda con los 32 de la derecha y las 16 etapas restantes se parametrizan mediante diferentes funciones de la clave. Para el descifrado se realiza el proceso inverso. En la versión original, este algoritmo ya no se usa. En la actualidad se utiliza el de 128 bits, el cual es exclusivo para Estados Unidos.

Existen otros algoritmos como el RSA (Rivest, Shamir, Adleman) el cual utiliza la factorización de números grandes para obtener luego números primos.

Teóricamente la factorización de un número de 200 dígitos, con las capacidades de cómputo actuales tardaría 400 mil millones de años y un número de 500 dígitos cerca de 10 a la 25 años, que es la razón en la cual está su seguridad. Adicionalmente utiliza también una llave pública y una llave privada.

El SSL[8] es el protocolo de comunicaciones utilizado hoy en día para realizar transacciones comerciales de manera segura, que involucren pago con algún medio de pago (normalmente tarjeta débito o crédito) utilizando una red de comunicaciones y sus equipos correspondientes.

El PGP[9] es un software que permite crear autenticación a través de claves públicas y privadas, proveyendo también la capacidad de firmas y certificados digitales. Utiliza el algoritmo RSA e IDEA. El procedimiento utilizado es el siguiente:

1. El emisor cifra el mensaje con la clave de cifrado IDEA.
2. El mensaje se cifra nuevamente con la clave pública RSA del receptor del mensaje.
3. Se envía el mensaje al receptor.
4. El receptor recibe el mensaje y utilizando la clave privada RSA, descifra el mensaje.

5. Finalmente descifra el mensaje con la clave IDEA descifrada.

El corta fuegos es software que se instala en un servidor o se construye en un enrutador (firewall en Hardware), para impedir que determinados tipos de programas, direcciones IP de red, sitios de Internet, personas, etc puedan ingresar a una red de comunicaciones.

Redes virtuales privadas. Una definición de estas redes "proceso de comunicación cifrado o encapsulado que transfiere datos desde un punto a otro de manera segura; la seguridad de los datos se logra mediante una tecnología segura de cifrado y los datos que se transfieren pasan a través de un red abierta insegura y enrutada" [11], permite entender su funcionamiento y objetivos. Cuando la definición se refiere a redes abiertas, se hace a cualquier tipo de red basada en un medio público, ATM, ISDN, xDSL, etc. Este tipo de redes permite crear grupos amplios de equipos utilizando medios de comunicación públicos, pero utilizando mecanismos tales como la tunelización (*tunneling*), donde los paquetes que llevan la información han sido previamente cifrados. Las redes privadas Virtuales, tratan de contrarrestar las intrusiones a las redes NDIS (*Network Detection Intrusion Systems*), Sistemas de detección de intrusos a nivel de red, en el nivel de enlace de datos y nivel físico del modelo de referencia ISO de la OSI.

Las redes privadas virtuales que actualmente se implementan pueden estar basadas en facilidades de muros cortafuego, en enrutador, en acceso remoto, en proxies, en software, etc [11].

Políticas de seguridad al interior de las organizaciones.

Debido a que la seguridad de la información es una de las mayores preocupaciones en una organización, es necesario conseguir que las personas que se desempeñan dentro de ellas logren un nivel de concientización suficiente para impedir que ellos sean el eslabón débil entre un intruso y la organización. Por lo tanto estas personas deben darse cuenta de la responsabilidad que tienen en la protección de la confidencialidad, integridad y disponibilidad de los activos de la organización y que comprendan que estos no deben ser solamente responsabilidad de los especialistas en dicho temas. Los retos que deben enfrentar el establecimiento de políticas, para lograr algunos de los objetivos planteados son [12]:

A. *Los usuarios normalmente son reacios a los cambios.* Esta parece una condición humana bastante común, debido a la formación de hábitos o costumbres, que impiden que las personas busquen o establezcan formas diferentes de hacer las cosas, la mayoría de las veces de manera mas fácil o más segura tanto para ellos como para las organizaciones para quien trabajan.
B. *No se reconoce que el problema de la seguridad es un problema de todos.* Las personas que se desempeñan en áreas no tecnológicas, normalmente creen que las funciones asociadas a la seguridad de la información es responsabilidad de los especialistas. Las políticas a establecer por lo tanto deben hacer énfasis en que la seguridad debe darse por medio de la colaboración de todos, definiéndolas claramente, divulgándolas y haciéndoles el seguimiento correspondiente.
C. *Introducción de nuevas tecnologías.* Estas originan problemas relacionados con errores involuntarios, mal uso (por desconocimiento) de todos los implicados y adicionalmente, la velocidad del cambio de estas tecnologías impide que se conozca al detalle sus fortalezas o debilidades, creando incertidumbre en quienes las aplican.
D. *Elaboración de programas únicos.* Un error frecuente en muchas organizaciones es el establecimiento de políticas únicas para todos los miembros de la organización, sin tener en cuenta la existencia de tipos de personalidades diferentes, edades, sexos, cargos, etc. Por este motivo es necesario segmentar estas políticas por medio de estrategias rápidas y fáciles de implementar, de manera que permitan el logro de los objetivos.
E. *Bombardeo de información a los usuarios.* Al igual que el defecto de información puede ocasionar problemas de desconocimiento, el exceso de información, puede provocar que las personas se saturen, y por lo tanto omitan o desconozcan la información que se les proporciona.
F. *No aplicar metodologías adecuadas.* La(s) metodología(s) escogida(s) para la aplicación de las políticas que tienen que ver con la seguridad de la información, puede(n) impedir que el entrenamiento o los canales de comunicación seleccionados no sean los adecuados y por lo tanto el logro de los objetivos perseguidos con la implementación de políticas de seguridad no se logren.
G. *Falla en el seguimiento del programa.* Todo programa o política que se implemente y no se le haga el seguimiento correspondiente, puede ser equivalente a que no exista. Por lo tanto es necesario escuchar, retroalimentar las opiniones de quienes están interviniendo y verificar los resultados para tomar oportunamente los correctivos necesarios.
H. *Ingeniería social.* Es una práctica bastante común por quienes están interesados en entrar de manera no autorizada (o ilegal) en un sistema informático.

Estado del Arte.

La tabla 1 a continuación, muestra los ambientes en los cuales se está llevando la detección de intrusiones y las dificultades en cuanto a su seguimiento.

Ambiente de los ataques	Intrusión a las redes de computadores
	Intrusión a los servidores
	Intrusión en ambientes de equipos clientes (P2P peer to peer)
	Intrusión en ambientes de redes inalámbricas
Dificultades en detectar intrusos	Ataques camuflados
	Ataques novedosos
	Ataques distribuidos y coordinados

Tabla 1. Ambientes y dificultades en la detección de intrusos.

Por otro lado, los elementos componentes de un sistema de detección de intrusos se muestran de manera esquematizada en la tabla 2, donde adicionalmente se indican algunos de sus componentes, áreas frecuentes de aplicación y nombres de algoritmos utilizados.

Estructura de un sistema de Detección de intrusos (IDS intrusion detection system)			
Fuentes de Información	**Servidores (HOSTS)**		
	Redes de computadores (Networks)		
	Redes inalámbricas		
	Registros de las aplicaciones		
	Sensores		
Estrategia de Análisis	**Detección de anomalías**	**No supervisadas**	
		supervisadas	**IDES, NIDES**
			EMERALD
			SPADE
			Computer Watch
			Wisdom & Sense
	Detección de formas de uso indebidas (Misuse detection)	**Minería de datos**	**Shadow**
		Transición de estados	**Network Flight Recorder**
			NetStat (UCSB)
			NetRanger (cisco)
		Sistemas Expertos	**P-Best (SRI)**
		Patrones	**SNORT**
Aspectos temporales	**Predicción en tiempo real**		
	Predicción fuera de línea		
Arquitectura	**Centralizada**		
	Heterogénea y distribuida		
Reacción	**Activa**	**Correctiva**	
		Proactiva	**Netprobe**
			CISCO Net Ranger
			Bellavista
	Pasiva		
Continualidad	**Monitoreo Continuo**		
	Análisis Periódico		

Tabla 2. Componentes, áreas frecuentes de aplicación y nombres de algoritmos utilizados, para la detección de intrusos con minería de datos.

Desde hace ya algunos años varias universidades de Norteamérica, principalmente, a nivel de investigación y de organizaciones con carácter comercial, han estado desarrollando algoritmos para la detección de intrusos en medios computarizados. Entre los cuales se tiene:

MINDS (*Minnesota Intrusión Detection System*) de la Universidad de Minnesota.

MADAM ID (*Mining Audit Data for Automated Models for Intrusión Detection*) de la Universidad de Columbia, Georgia Tech y Florida Tech.

ADAM (*Audit Data Análisis And Mining*) de la Universidad de George Mason.

IIDS (*Intelligent Intrusión Detection*) de la Universidad de Missippi.

Data Mining for Network Intrusión detection de la Corporación MITRE.

Agent based data mining system de la universidad de Iowa.

IDDM del departamento de defensa de Australia.

A continuación se describirá el estado actual de algunos de los estudios realizados y el planteamiento de los estudios futuros.

MINDS (Minessota Intrusión Detection System, Sistema de detección de Intrusos de la Universidad de Minessota) [13] [14].

La figura 1 muestra el esquema de algoritmo para la detección de intrusos creado por la Universidad de Minessota
El modelo está basado en las características:

- Está incorporado entre la arquitectura del interrogador del Centro de Monitoreo y Protección de Intrusiones (CIMP, *Center for Intrusión Monitoring and Proteccion*).
- Ayuda a analizar datos de múltiples sensores ubicados alrededor de Estados Unidos.
- Las anomalías en el modelo se usan como llaves primarias cuando se ven desde otras herramientas como el *Snort*.
- De manera rutinaria detecta ataques y comportamientos de intrusión, no detectados por otros sistemas ampliamente utilizados alrededor del mundo.

El módulo de extracción de características (*Features Extraccion module*) toma tres grupos de características para la detección de intrusos:

- Características básicas de las conexiones individuales TCP:
  - Dirección IP fuente/destino
  - Puerto fuente/destino
  - Protocolo
  - Duración
  - Bytes por paquete
  - Número de bytes

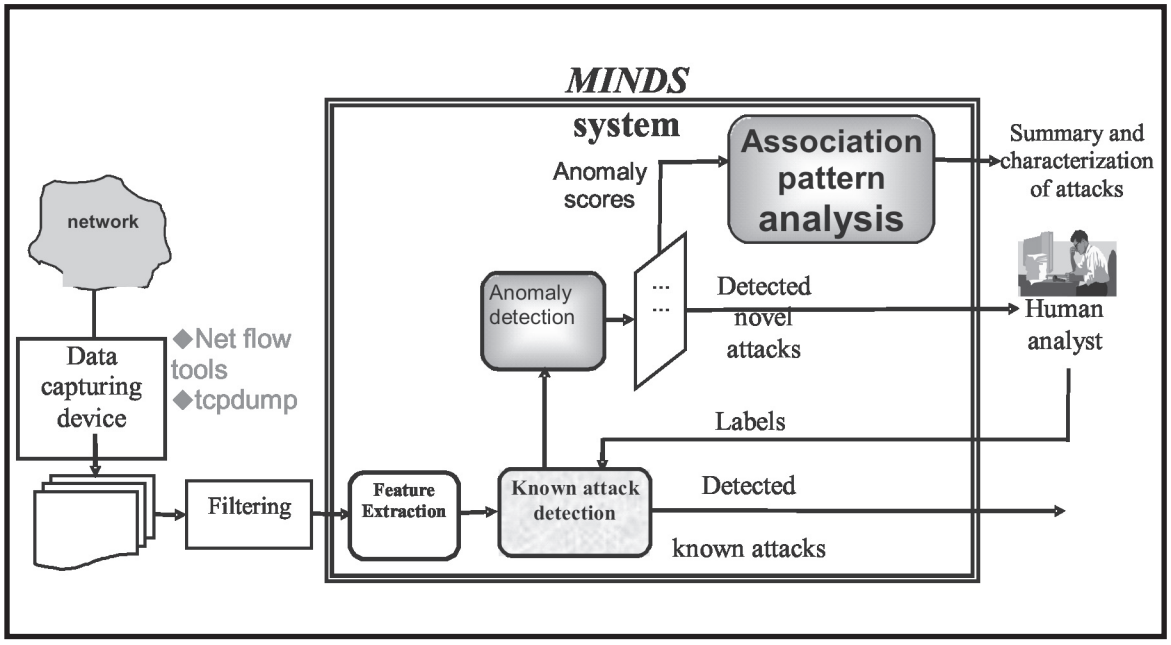

Figura 1. Modelo de implementación del MINDS [13].

- Características basadas en el tiempo:
  - Para la dirección IP fuente destino también se toma el número de destino/fuente único.
  - Los direccionamientos dentro de la red en los últimos T segundos.
  - El número de conexiones de la dirección fuente al destino en los últimos T segundos.

- Características basadas en la conexión:
  - Para la misma dirección IP fuente/destino, el número de destinos/fuente únicos de direcciones IP dentro de la reden las ultimas N conexiones.
  - El número de conexiones de la dirección IP fuente/destino al mismo puerto destino/fuente en las últimas N conexiones.

Otra manera resumida de ver el trabajo realizado por MINDS, se muestra en la figura 2. La cual muestra las investigaciones realizadas, los principales ataques y la forma cómo detectar su intrusión.

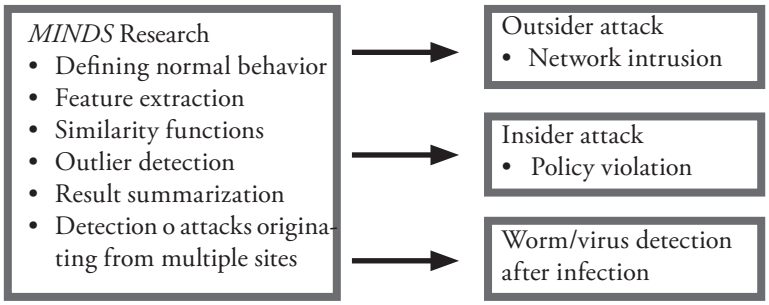

Figura 2. Áreas de investigación de MINDS y principales ataques[14].

Algunas acciones importantes detectadas por el algoritmo sobre datos reales:
En Agosto 13 de 2002, se detectó una exploración para el servicio distribuido de Microsoft, sobre el puerto 445 y el protocolo TCP, el cual no fue detectado por *Snort* [3].

Para la misma fecha también se detectó una exploración sobre un servidor Oracle, el cual fue reportado por CERT en junio 13 de 2002.

En octubre 10 de 2002 y enero 26 de 2003 se detectaron varias instancias del *Slapper worm* que tampoco fueron detectados por *Snort*, debido a la existencia de variantes del gusano.

En febrero 6 de 2003 se detectó un mensaje no solicitado *"ICMP ECHOREPLY"* a un computador previamente infectado con *Stacheldract worm*.

Adicionalmente también se han encontrado patrones de asociación descubiertos en la vida real, tales como: exploración Web (*Web scan*); ataques específicos a una máquina; alto número de conexiones TCP anómalas sobre el puerto 8888, que involucraba a una máquina con dirección IP "IP3".

Como estudios futuros planteados por MINDS está integrar el trabajo realizado con las potencialidades y fortalezas de *Snort*, complementando las acciones de los dos sistemas. Adicionalmente se plantea ampliar el espectro de aplicación del algoritmo fuera de ataques e intrusiones, como determinar fraudes en compañías de seguros y tarjetas de crédito; señales iniciales de riesgos potenciales en procesos industriales; condiciones médicas inusuales de arritmia cardiaca, etc.[14]

[3] La documentación completa de este caso se encuentra en: www.incidents.org

Estudios realizados por la corporación MITRE [15].

Un grupo de investigadores conformado por Eric Bloedorn, Alan D. Christiansen, William Hill, Clement Skorupka, Lisa M. Talbot, Jonathan Tivel, plantearon la forma de llevar a cabo la detección, tal como se muestra en la figura 3.

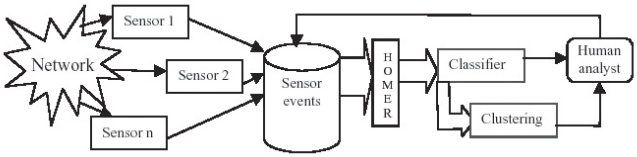

Figura 3. Ayuda de sensores en la detección de todo tipo de intrusiones, de acuerdo a estudios realizados por la corporación MITRE.[15]

Tal como lo muestra la figura 3, los sensores están permanentemente llevando datos al servidor central, para el acondicionamiento y entrada a una base de datos relacional. HOMER, filtra los eventos de los datos antes que estos pasen al análisis de clasificación y agrupamiento. Las herramientas de minería de datos filtran las falsas alarmas e identifican un comportamiento anómalo, en la gran cantidad de datos remanentes. Un servidor WEB está disponible como parte frontal del sistema en caso que sea necesario. El objetivo de este modelo es tener todas las alarmas revisadas por analistas humanos.

Estudios realizados en el departamento de Ciencias de la Computación de la Universidad de Columbia [16].

El estudio realizado se ha centrado principalmente en ambientes UNIX. Para ello se utilizó el modelo multivariado de Bernoulli, el modelo multinomial y el algoritmo SVM *(Suport Vector Machine,* Máquina soportada en vectores*)* de una clase. El proceso mostró que el entrenamiento para una clase, para realizar este trabajo, funciona tan bien como el entrenamiento Multiclase, con la ventaja de necesitar menos datos y un entrenamiento más eficiente. Las últimas investigaciones realizadas (junio de 2004), se han centrado en la detección de intrusiones por camuflaje (*Masquerade*) pues son éstas las que más problemas de seguridad causan.

Como estudio futuro, está planteado incluir comandos con argumentos, (no comandos truncados) con el fin de mejorar la precisión de la detección del engaño. Adicionalmente, tal como se vayan incrementando las características ha ser tenidas en cuenta, se plantea la necesidad de seleccionar las características más importantes, descartando las que no sean relevantes para el trabajo final.

MADAM ID (*Mining Audit Data for Automated Models for Intrusión Detection.* Datos auditados de minería para modelos automatizados en la detección de intrusos) [17].

Los principales componentes de MADAM ID son los programas de clasificación y meta-clasificación, las reglas de asociación, los episodios frecuentes, el sistema de construcción de características y un sistema de conversión que traslada las líneas de aprendizaje fuera de línea, en módulos de tiempo real. El producto final son reglas concisas e intuitivas que pueden detectar intrusiones.

Inductiva y automáticamente las reglas de aprendizaje son más generales que las reglas codificadas manualmente, porque las primeras pueden analizar grandes cantidades de datos auditados y extraídos de las reglas de descripción sobre intrusiones detectadas, mientras que los expertos humanos tienden a generar reglas muy especificas.

De otra parte teniendo en cuenta el desempeño de los componentes, se puede precisar que las reglas de asociación describen las correlaciones entre las características de los sistemas (i. e. qué comando está asociado con cuál argumento), mientras que los episodios frecuentes capturan las co-ocurrencias secuenciales de los eventos del sistema (i.e, qué conexión de red se realiza con una expansión corta de tiempo).

Estudios futuros. A pesar de las ventajas del uso de las herramientas de minería de datos para construir modelos de detección de intrusos, los dominios de conocimientos deben incorporarse en forma adecuada. La combinación de técnicas de ingeniería de conocimientos con el descubrimiento de conocimiento, deberán producir modelos más precisos y eficientes para la detección de intrusos.

IIDS (*Intelligent Intrusión Detection,* Deteccion de intrusos inteligente) [18].

Este sistema intenta evaluar la autenticación a través de una red UNIX, basada en reglas especificas, bien reconociendo logins como válidos, errores o actividad maliciosa.

Características.

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.

El FCM, es particularmente útil en ambientes dinámicos, tales como dominios de seguridad en una red.

El FCM, proporciona respuestas rápidas, lo cual es recomendable para un sistema de detección de intrusos en tiempo real.

En la arquitectura IIDS mostrada en la figura 4, 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 / uso indebido.

El sistema adicionalmente usa FCM, cuyo esquema se muestra en la figura 5. Este sistema modela el mundo como conceptos y relaciones casuales entre conceptos, en grupos estructurados. Los conceptos (nodos) son eventos que se originan en el sistema y cuyos valores pueden cambiar con el tiempo. Los enlaces entre los conceptos están representados por líneas que miden que tanto un concepto impacta a otro. Estos valores pueden ser positivos o negativos dependiendo de la naturaleza y dirección del efecto.

IDDM [19].

El objetivo del proyecto es determinar la factibilidad y efectividad de las técnicas de minería de datos en ambientes de tiempo real y generar soluciones a este respecto.

Una característica importante de este sistema es que no requiere de una base de conocimientos a priori, para comenzar su exploración y detección de intrusiones. El almacenamiento de los datos y las reglas de generación comienzan con datos reales, al tiempo de instalación. Como consecuencia de este proceso, inicialmente se encontrará un alto índice de falsas alarmas, hasta que el sistema llega a un modo más estable de operación.

Como muestra la figura 6, el sistema se enfoca principalmente en la detección de dos tipos de ataques: los que ya han sido encontrados y aquellos que aún no se han detectado, aunque el IDDM se concentra fundamentalmente en el reconocimiento de nuevos tipos de ataques o a las anomalías a las cuales se refieren particularmente.

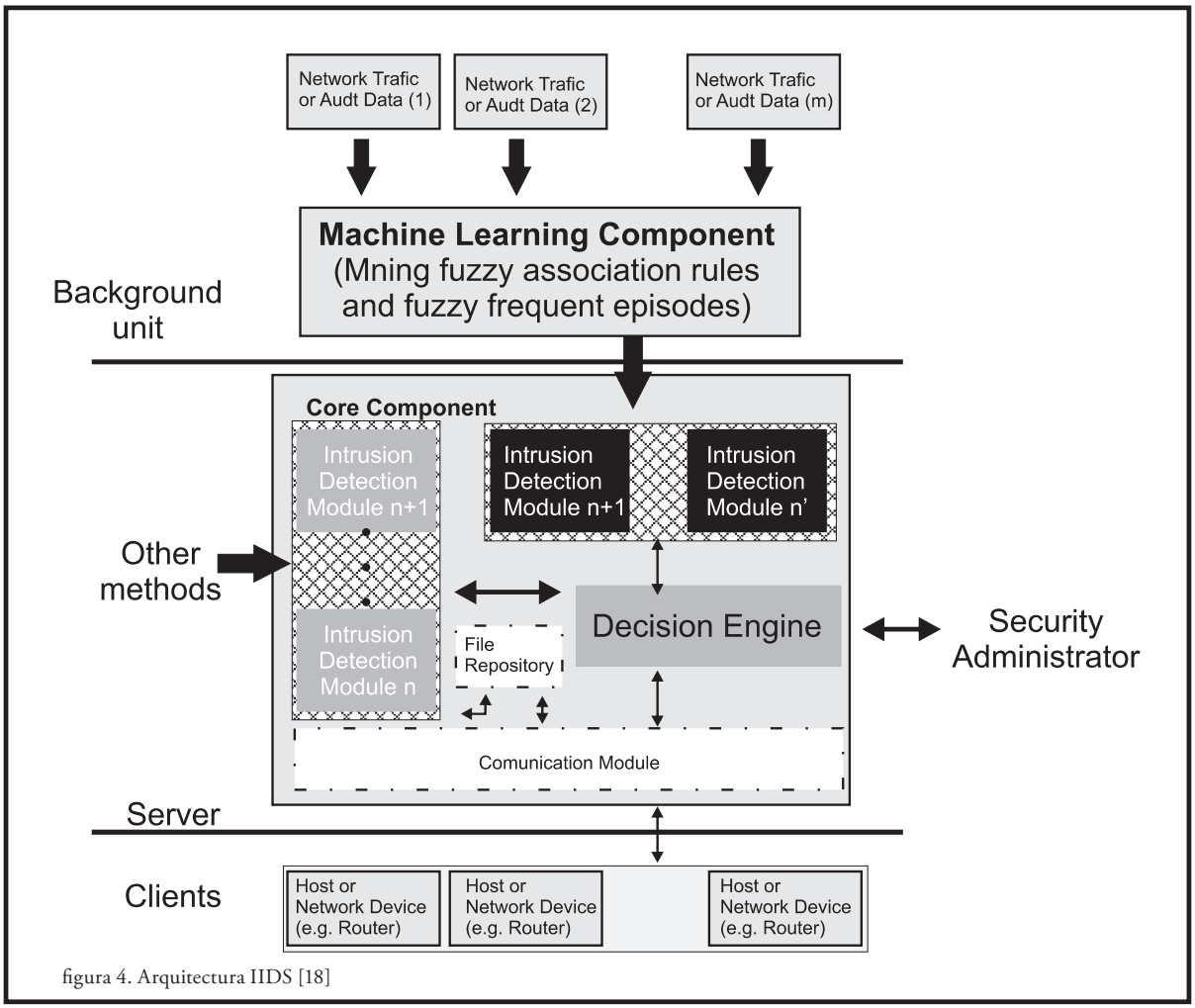

figura 4. Arquitectura IIDS [18]

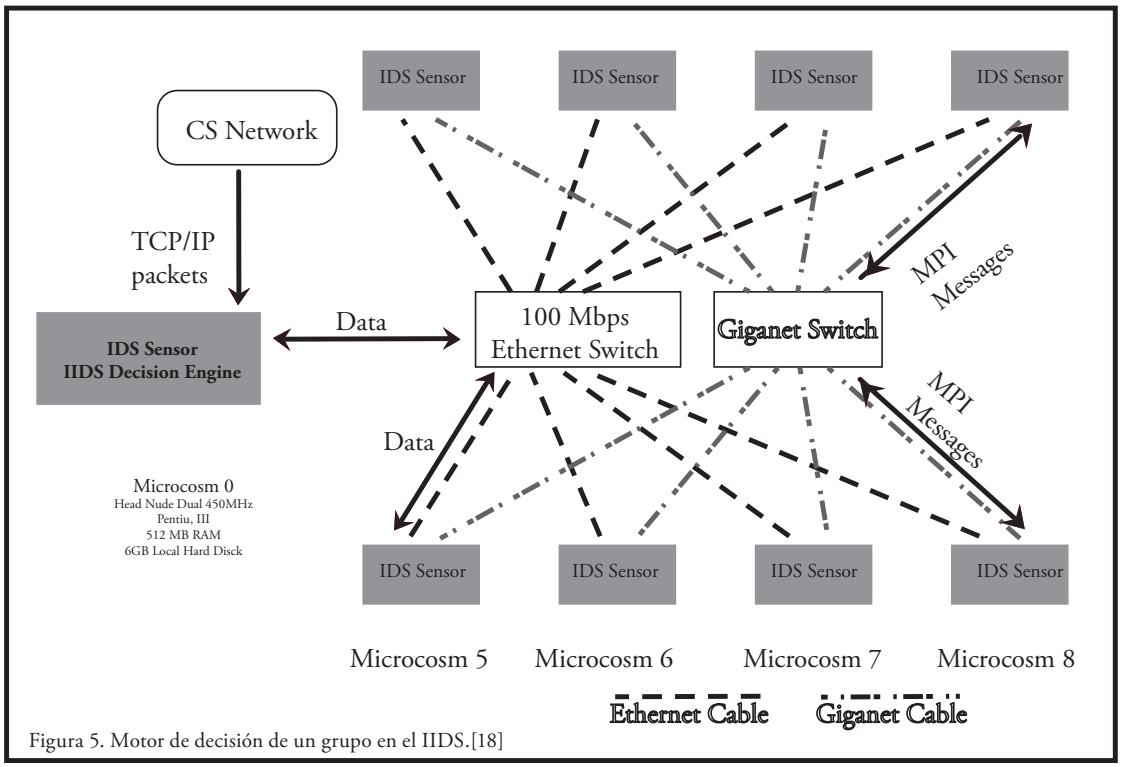

Figura 5. Motor de decisión de un grupo en el IIDS.[18]

Conclusiones.

Como se ve en esta breve reseña, los estudios que se están llevando a cabo en diferentes Universidades de Estados Unidos y Europa, así como entidades de carácter privado y oficial, permiten detectar oportunamente ataques a los sistemas informáticos, siempre y cuando hayan sido estos ataques usados y estudiados previamente. Sin embargo debido a la naturaleza dinámica como se llevan a cabo, resulta casi imposible anular cualquier nuevo ataque implementado de manera novedosa o no predeterminada. Todos los días surgen nuevas formas de ataque o modificaciones a las anteriores, que los hacen prácticamente imposibles de detectar en forma oportuna y antes de que causen daño.

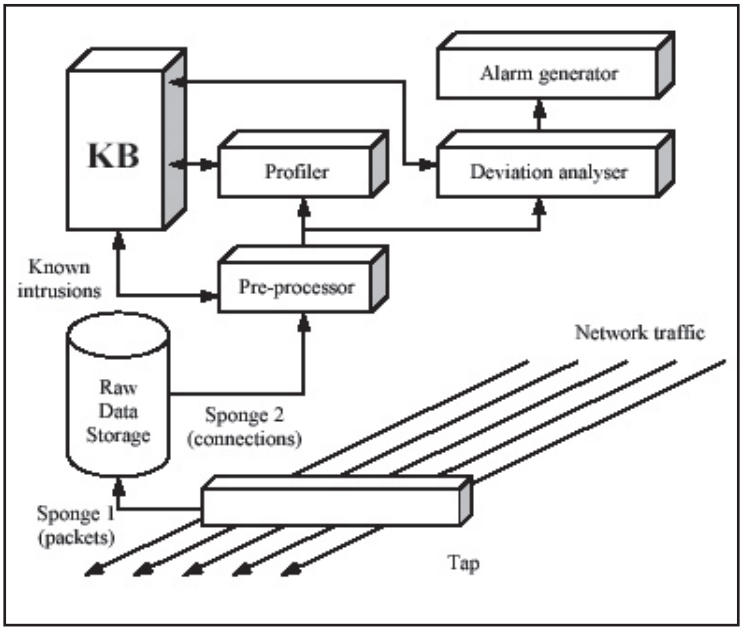

Figura 6. Arquitectura IDDM. [19]

La aplicación de la minería de datos, como resultado de modelos sobre grandes volúmenes de datos, permite anticipar algunas mutaciones de los ataques y crear por lo tanto barreras de defensa. Pero aún con la tecnología y potencia computacional actual, para muchas Organizaciones resulta inviable su aplicación en línea, debido a la degradación significativa del desempeño de las aplicaciones que son la razón de ser del negocio. Por esta razón cuando se aplican, se hacen para ser utilizados fuera de línea, como análisis de rutina o análisis *postMorten.*

Los desarrollos a realizar y las herramientas utilizadas son para la mayoría de Empresas u Organizaciones demasiado costosas, por lo tanto la relación costo beneficio, debe ser un soporte muy bien fundamentado.

La combinación de dos o más formas de detección, como por ejemplo una realizada con minería de datos y otra con otra herramienta, como *Snort*, hacen más seguro el sistema, pero no por ello totalmente invulnerable.

Los estudios en esta área siguen siendo un campo muy amplio y con grandes oportunidades de desarrollo y aplicación.

Bibliografía.

M. Berry, G. Linoff, "*Data mining techniques for marketing, sales and customer relationship management"*, Wiley Publishing, Inc. Indianapolis, 2004, pp. 43 – 86.

S. Stolfo et al, "*Cost-based Modeling and Evaluation for Data Mining With Application to Fraud and Intrusion Detection"*.

Lee, Wenke y Stolfo, Salvatore J. Data Mining Approaches for Intrusion Detection. Computer Science Department Columbia University.

Lazareviæ, Aleksandar; Srivastava, Jaideep; Kumar, Jaideep. *Tutorial on the Pacific-Asia Conference on Knowledge Discovery in Databases 2003*. Department of Computer Science, University of Minnesota.

BRUGGER, TERRY. *Data Mining Methods for Network Intrusion Detection*. University of California, Davis. 2004.

Srikant, Ramakrishnan. "*FAST ALGORITHMS FOR MINING ASSOCIATION RULES AND SEQUENTIAL PATTERNS*". Universidad de Wisconsin – Madison. 1996.

Bishop, M. ECS-253: *Data security and cryptography. Class Lecture*. (2001, 1 March).

J.D. Meier, Alex Mackman, Michael Dunner, and Srinath Vasireddy *Building Secure ASP.NET Applications: Authentication, Authorization, and Secure Communication*. Microsoft Corporation .November 2002

An introduction to Crytography. ftp://ftp.pgpi.org/pub/pgp/6.5/docs/english/IntroToCrypto.pdf

Tanenbaum, Andrew. Redes de computadoras. Tercera edición. Editorial Pearson.

Brown, Steven. Implementación de redes privadas virtuales. 2001. Editorial McGraw Hill.

Castillo, Rafael y otros. Concientizacion en seguridad de la información. Maestría en Sistemas y computación. Universidad de los Andes. 2004.

Vipin Kumar, *MINDS*: *Data Mining Based Network Intrusion Detection* System, Rome Labs, June 16, 2004.

Ertöz, Levent; Eilertson, Eric; Lazarevic, Aleksandar; y otros. *Detection and Summarization of Novel Network Attacks Using Data Mining. Computer* Science Department, University of Minnesota, Minneapolis, 2003.

Bloedorn, Eric; Christiansen, Alan D.; Hill, William; Skorupka, Clement; Talbot, Lisa M.; Tivel, Jonathan. *Data Mining for Network Intrusion Detection: How to Get Started.* 2000. The MITRE Corporation.

Wang, Ke; Stolfo, Salvatore J. *One-Class Training for Masquerade Detection*. Computer Science Department, Columbia University

Lee, Wenke (Department of Computer Science North Carolina State University) y Stolfo, Salvatore J (Department of Computer Science). *Combining Knowledge Discovery and Knowledge Engineering to Build IDSS*.

Rayford B, Ambareen Siraj y Bridges, Vaughn Susan M. *Intelligent Intrusion Detection System Architecture*.Department of Computer Science & Engineering Center for Computer Security Research Mississippi State University.

Abraham, Tamas. *IDDM: Intrusion Detection using Data Mining Techniques*. Information Technology División Electronics and Surveillance Research Laboratory.

http://es.tldp.org/Manuales-LuCAS/doc-unixsec/unixsec-html/node71.html. Fauna y otras amenazas. Bajado de internet el 16 de abril de 2005.

Villalon H, Antonio. Seguridad en Unix y redes. Version 2.1. Julio 2002.

Fuente de datos para análisis, http://kdd.ics.uci.edu

Descripción campos resumen de flag en modelset. http://www.icir.org/vern/bro-manual/node37.html#27494