Pedro Bados Aguilar

Pedro Bados Aguilar nació en Soria en Diciembre de 1979 y desde 2003 es Ingeniero Superior de Telecomunicaciones por el Centro Politécnico Superior de la Universidad de Zaragoza. Especializado en Telemática, la mayor parte de su investigación se centra en la combinación de técnicas de Inteligencia Artificial en el dominio de la seguridad informática.

Desde su Proyecto Fin de Carrera se encuentra fuertemente vinculado al Laboratorio de Inteligencia Artificial de la Universidad de Tecnología de Suiza donde ha desarrollado un nuevo sistema de modelado de comportamiento en redes, recientemente patentado por dicha universidad.

En Julio de 2004, Pedro Bados ha conseguido reunir los fondos así como a un grupo de expertos altamente cualificados para fundar NEXThink, una start-up especializada en sistemas de seguridad inteligentes con sede en Lausana donde inicialmente asume la responsabilidad tecnica.

Modelado del Comportamiento del Usuario en Red para Detección de Intrusos (Resumen breve)

El presente documento constituye una introducción al proyecto fin de carrera titulado ***Modelling User Network Behaviour For Intrusion Detection*** realizado por **Pedro Bados Aguilar** bajo la supervisión de **Omar Belakhdar** en el **Instituto Politécnico Federal de Suiza en Lausanne.** Este trabajo fue presentado y defendido en la Universidad de Zaragoza en Septiembre de 2003.

La estructura de esta breve introducción estará compuesta por tres puntos básicos :

1. Introducción y antecedentes.
2. Idea central de nuestro proyecto.
3. Necesidades y requerimientos de nuestro nuevo contexto.
4. Breves conclusiones

1. Introducción y antecedentes.

Todos conocemos que el desarrollo tecnológico está revolucionando nuestro mundo. Innumerables actividades comerciales, gubernamentales e incluso sociales están cambiando sus medios así como su contexto, trasladándonos a unas poco intuitivas coordenadas digitales. Este profundo cambio en el tratamiento de la información, afectando fundamentalmente a su forma más que al contenido, nos crea en ocasiones grandes dificultades para proyectar en nuestro mundo cotidiano algunos términos hasta ahora claramente definidos.

Las personas abandonan ocasionalmente su personalidad físicas para iconizarse en direcciones de correo electrónico asociadas a uno o varios dominios igualmente digitales. La tecnología ha introducido curiosas y complejas reglas de trasiego y almacenaje de información fuera de la tangible realidad. Éstas, además de ofrecer una serie de ventajas innegables, también añaden una cierta incertidumbre a conceptos como confidencialidad, seguridad o integridad de los datos transmitidos.

El área de investigación de la seguridad informática ofrece actualmente un historial de consistente a la vez que frustrante progreso. Los grandes avances en complejos sistemas criptográficos y de detección de intrusos han sido habitualmente superados por las noticias de su derrota frente al brillante ingenio del pirata informático. De esta forma, nosotros creemos que se hace necesario afrontar los problemas desde nuevas perspectivas y en nuevos contextos de análisis, considerando el problema de la seguridad informática también en sus aspectos *humanos*.

Este trabajo se centrará en el objetivo de ofrecer un nuevo eje control de lo que ocurre en una red informática como aproximación para la detección de intrusos. En el resto de este documento y en especial en las secciones 2 y 3 veremos las ideas básicas en el diseño de un nuevo contexto. Ahora, para un correcto enfoque posterior, vamos a resumir brevemente las actuales lineas de investigación y desarrollo en el panorama de la seguridad informática.

Principales campos de seguridad.

El concepto de seguridad normalmente se vincula a una serie de problemas en la integridad y la confidencialidad de la información en diferentes planos de acción. Nosotros hemos querido comentar muy brevemente cada una de estas cuatro ramas principales.

- **Sistemas criptográficos**. Su misión fundamental es la protección de la información mediante procesos de codificación de datos y claves de acceso. Por supuesto, para aquellos elementos en el sistema con autorización para disponer de dicha información se deben habilitar métodos para la decodificación y lectura. Estas técnicas afectan en diferentes niveles del proceso de almacenaje y transporte. Sistemas de intercambio de claves, codificación de la información o *trusted hosts* son algunas de las actuales ramas de investigación.

- **Firewalls y routers de selección**. Estos dispositivos vienen asociados a la política de seguridad en el trasiego de información. Comúnmente referidos a redes TCP/IP, los firewalls y routers de selección se sitúan el lugares físicamente estratégicos de los canales de transporte (ej : tras los routers externos) para evaluar las diferentes conexiones. De esta forma, según una preestablecida política de seguridad esta evaluación puede permitir el paso de la información , redirigirla o simplemente desecharla si la considera desautorizada o potencialmente peligrosa.

- **Sistemas de análisis forense.** Dentro del numeroso grupo herramientas de seguridad, merecen una mención aparte los procedimientos para la detección de ataques y vulneraciones de integridad *a posteriori*. En otras palabras, después de constatar la existencia de un problema de seguridad, este tipo de sistemas ayudan a profundizar en sus causas con el fin de tomar las medidas necesarias para evitar futuras incidencias similares.

- **Sistemas de detección de intrusos.** Posiblemente el área más heterogénea en los actuales métodos de seguridad de redes de computadoras son los sistemas de detección de intrusos. Comúnmente denominados IDS, estos elementos basan su comportamiento en la extracción y monitorización de diversas variables con el fin de detectar y notificar una posible intrusión en curso. Las evidencias extraídas y los motores de detección difieren en gran medida según las estrategias utilizadas. Nosotros nos centraremos en estos sistemas de detección de intrusiones tomando un nuevo e innovador contexto de análisis basado en ***el estudio y modelado de los usuarios reales así como de sus propias motivaciones*** para operar en la red.

Es importante tener en cuenta que debido al extenso trabajo y a las actuales soluciones tecnológicas, la clasificación anterior es inevitablemente general y posiblemente escasa. No obstante, consideramos que es importante contar con un primer enfoque dentro del panorama actual de la seguridad informática para pasar a continuación a una descripción algo mas detallada de los sistemas de detección de intrusos.

Sistemas de detección de intrusos

Una amplia definición del concepto de detección de intrusos (IDS) ha sido la cual lo describe como *el problema de identificación de individuos que utilizan redes o sistemas sin autorización, así como aquellos que aun teniendo acceso legítimo, abusan de sus privilegio*s. Es importante notar que el denominado intruso, ha dejado ya de ser únicamente una o un conjunto de persona físicas, sino que debemos incluir agentes de software (virus), o incluso una combinación mixta de seres humanos y ciertos *robots*.

Nos encontramos por tanto en escenarios donde los IDS son diseñados inteligentemente para tratar de identificar aquella actividad maligna provocada por uno o varios agentes intrusivos. Por tanto, en ocasiones nos resulta difícil evitar el símil de este escenario con el de un complejo juego donde dos jugadores luchan por sus objetivos, el primero por llevar a cabo su ilegítima acción y el segundo por detectar dicha operación. Ambos están inevitablemente sometidos a una particulares reglas del juego digitales basadas en decenas de protocolos, estándares y sistemas de información.

Otro elemento muy importante es establecer el **rango de acción de los IDS como fundamentalmente interno** en entornos corporativos e intranets. Numerosos análisis actuales cifran los incidentes de seguridad dentro del perímetro de la red por encima del 80 %. Existen importantes medidas de seguridad como firewalls o incluso external IDS que vigilan que esta penetración no se origine del exterior. A pesar de ello, si esta primera barrera se sobrepasa o el si el origen proviene de un intruso interno (trabajador, social engineering ...) es aquí cuando estos sistemas deben mostrarse realmente eficaces. Este punto es capital para enfocar nuestro trabajo principalmente en el **interior de una red.**

Los sistemas de detección de intrusos se componen de tres elementos fundamentales : fuentes de información, motor de análisis y el sistema de notificación. La naturaleza básica de los dos primeros elementos definirán principalmente el tipo sistema. De esta forma, atendiendo al lugar de extracción de información existen dos estrategias fundamentales :

- **Sistemas Host-based.** La fuente de extracción de información de se encuentra en el propio sistema operativo. Un ejemplo habitual de este tipo de mecanismos son los antivirus.

- **Sistemas Network-based**. La fuente de información son los datos transmitidos por la red. El IDS de código libre más conocido, SNORT, es un conocido ejemplo de este tipo de sistemas.

De la misma manera, según sea la estrategia del motor de análisis se pueden establer fundamentalmente dos clases diferenciadas :

- **Sistemas misuse.** Son aquellos sistemas cuya detección viene guiada por una serie de reglas extrictas previamente introducidas. Su misión principal es encontrar evidencias de estos patrones en la información revisada. Tanto SNORT como cualquier antivirus son ejemplos de sistemas basados en reglas.
- **Sistemas de detección de anomalías.** Estos sistemas son más complejos. Cuentan con la adquisición un conocimiento autónomo, de la situación de la red. De esta forma se realiza una evaluación estadística de diferentes parámetros según sea la estrategia utilizada. A pesar de ello, los parámetros y técnicas no suelen ser demasiado sofisticadas, destacando las escasas que cuentan con algoritmos inteligencia artificial y en especial aquellas utilizadas en *machine learning*.

Por supuesto, los puntos presentados en ambas clasificaciones no son necesariamente excluyentes, sino que en realidad pueden existir sistemas híbridos que combinen alternativas de ambos lados. No obstante, cada estrategia conlleva una serie de ventajas e inconvenientes que es necesario evaluar, y en ocasiones la suma de tecnologías trae consigo la multiplicación de desventajas.

Nuestro trabajo se centrara particularmente en un sistema **network-based basado en la detección de anomalías**. Esta alternativa es idealmente la menos vulnerable pero también tradicionalmente la mas imprecisa. No obstante, en este documento introduciremos un nuevo contexto de estudio de anomalías, basado en el **comportamiento en red de los usuario** mediante una serie de postulados básicos.

2. Idea central de nuestro trabajo.

Como hemos comentado en el punto anterior, los sistema de detección de intrusos basan su análisis en los procesos de extracción de información y detección de anomalías ya sea con ayude de patrones fijos establecidos o mediante cálculos estadísticos. No obstante, sea cual sea el tipo de evaluación, la información puede ser considerada en su análisis desde muy diferentes puntos de vista. Por ejemplo, una conexión puede ser estudiada comprobando su correcto seguimiento de los estándares, chequeando su ajuste a la política de seguridad de la red, o incluso desde ciertos criterios estadísticos como la duración, tamaño, etc.

Nuestro trabajo se va a concentrar en establecer un ambicioso e intuitivo contexto al considerar todos eventos en la red **asociados a las características personales de los diferentes usuarios,** siendo éstas **evidencias de sus verdaderas motivaciones**.

Conceptos fundamentales.

Las ideas presentadas en este apartado formarán el núcleo conceptualmente innovador. Es importante aclarar que estas ideas introducen grandes dificultades técnicas que abordaremos más tarde, especialmente en la secciones 4 y 6. De esta manera, los elementos y problemas expuestos de una cierta forma abstracta contarán con una serie de implementaciones reales para traer a la realidad nuestros conceptos básicos :

1. *Los usuarios operan el la red guiados por una serie de **motivaciones** concretas***.*** El trabajo en un proyecto, el trabajo en asuntos personales o incluso el tiempo de ocio tienen un reflejo inequívoco en la manera de comportarse el usuario en la red. Nosotros veremos como estas motivaciones son una característica muy personal de cada usuario.
2. *Estas motivaciones y objetivos provocan un particular intercambio de información en forma de **conexiones**.* Como es evidente que una misma motivación puede contener varias conexiones, nosotros crearemos el concepto de ***servicio*** donde intentaremos agrupar un conjunto de conexiones con un

objetivo común. Recomendamos el capitulo 3 del documento original donde hemos desarrollado una serie de definiciones y relaciones básicas para estudiar la especificidad de las conexiones en relación a su motivación y objetivos de operación.

3. E*ste conjunto de servicios se nos presentan como secuencias de eventos creando un verdadero reflejo del* ***comportamiento*** *del usuario.* Es muy importante notar que uno de los objetivos fundamentales de nuestro trabajo es asegurar que efectivamente podemos llegar a modelar este comportamiento como reflejo de sus motivaciones. Por tanto, el comportamiento es también, como veremos, una característica muy personal.

Debemos consideraremos un escenario con usuarios localizados en sistemas, que generan una serie de conexiones de acuerdo a sus motivaciones y objetivos de uso de la red. Toda información perceptible que circule tendrá necesariamente asociado este contexto de comportamiento de usuario. Al encontrarnos en entornos intranet, como comentamos anteriormente, incluso el tráfico maligno deberá estar identificado como perteneciente a un usuario a priori legítimo en dicha red. **Si suponemos que somos capaces de definir el comportamiento así como su correcto modelado, es posible verificar la normalidad o no de las nuevas acciones de este usuario, estableciendo si corresponde a su identidad o es en realidad una posible intrusión.**

En resumen, nos encontramos con un numero finito de usuarios de los cuales somo capaces de obtener los modelos de comportamiento como reflejo en red de sus motivaciones de trabajo. Cada nuevo comportamiento de dichos usuarios sera validado con su modelo legítimo. De esta manera, el proceso nos permitirá detectar anomalías e intrusiones en curso debido a que este contexto es inevitable para cada nueva conexión, independientemente de su naturaleza. Pongámonos en la piel del atacante y observemos el panorama :

1. El comportamiento particular de un individuo es una **característica a priori desconocida** y muy **difícil de aprender** para un potencial intruso que lo intente imitar. Aprenderlo y reproducirlo son tareas complejas.
2. Aunque el intruso quiera utilizar una cierta identidad de usuario que conozca y sea capaz de imitar, llevar a cabo cualquier ataque, acción dañina o incluso simplemente algo anómalo es una tarea realmente complicada de ejecutar si para ello solo puede *utilizar* un comportamiento posible. El lector debe notar que esta única forma de actuar admisible, la manera habitual del usuario legítimo, obedece a unas motivaciones distintas de la intrusión. Por tanto, el intruso se encuentra con **un solo comportamiento posible** si no quiere ser detectado y que **no obedece a sus objetivos**. Su misión se complica aún más.

3. Necesidades y requerimientos de nuestro nuevo contexto.

Un desarrollo teórico sobre un nuevo contexto de análisis basado en usuarios y motivaciones resulta inevitablemente abstracto e infructífero sin las pertinentes soluciones reales. Por ello, es necesario enumerar los principales requerimientos para la implementación practica de nuestro sistema. A nivel conceptual, hemos de diseñar tres procesos son fundamentales :

- Una **definición** concreta y exacta de lo que es **comportamiento del usuario**.
- Un **proceso para modelar** este comportamiento considerando su origen y sus características particulares.
- Un **proceso para evaluar** el futuro comportamiento y decidir si es normal o no para el usuario legítimo.

De forma que a nivel técnico debemos habilitar :

- Un mecanismo para **separar los flujos de red de los diferentes usuarios**.
- Necesitamos diseñar e implementar **una plataforma de modelado y análisis** de comportamiento**.**

4. Breves conclusiones

Este documento constituye una introducción a las ideas básicas y teóricas para diseñar un sistema de detección de intrusos basado en el comportamiento personal de los usuarios. A pesar del gran contenido abstracto de los conceptos expuestos en los puntos 2 y 3, existe un proyecto que se encuentra actualmente en fase experimental de implementación y desarrollo para construir un sistema de seguridad basado en la protección de identidades personales a través del comportamiento humano en el ámbito de redes corporativas.