Técnicas difusas para detección de ataques y vulnerabilidades

Óscar Riveros *Estudiante, P U J,* y Carlos Thompson, *Estudiante, P U J*

***Resumen*—La complejidad en la definición de medidas de seguridad y la complejidad de los sistemas a proteger, hacen necesario atacar el problema por fuera de la lógica dicotoma y el análisis lineal. Las técnicas difusas, tanto la lógica difusa (*fuzzy logic*), como las pruebas difusas (*fuzz testing*) permiten enfocar el análisis de seguridad.**

***Index Terms*—Fuzzy logic, network security, risk analysis, fuzz testing**

I. Introducción

LA SEGURIDAD de la información depende de muchos factores, los cuales no son fáciles de cuantificar. En un intento de medir la seguridad se establecen criterios de evaluación (*assestment*) el cual incluye gestión de riesgo. La complejidad de los sistemas de información genera una serie de vulnerabilidades escondidas; vulnerabilidades que serán buscadas por quienes intentan aprovecharlas y por lo tanto obligan al ingeniero de seguridad a anticiparse, pero aún los sistemas más efectivos de protección, al basarse en algoritmos predeterminados, pueden ser vulnerados por un atacante que aprovecha una falla oculta o tiene la paciencia suficiente para no disparar las alarmas.

Los mecanismos de la lógica dicotoma tradicional son insuficientes o demasiado complejos para medir el riesgo, detectar fallas ocultas, o enfrentarse a los ataques más elaborados, y esto nos obliga a salirnos del cuadro, a cambiar la lógica y recurrir a otro tipo de enfoques.

La lógica difusa (*fuzzy logic*) es una forma de romper los paradigmas.

II. Métricas de seguridad y evaluación de políticas

Enfrentados al dilema de proteger sistemas de infraestructura de llaves públicas (PKI) para que estas cumplan su objetivo, Casola et al.[4] en Italia han trabajado en la definición y evaluación de políticas de seguridad basados en técnicas de lógica difusa.

La lógica difusa se utiliza aquí, principalmente, para evaluar la idoneidad de los modelos de políticas de seguridad.

La estrategia sugerida no ofrece respuestas contundentes, pero logran establecer métricas para evaluar distintas soluciones como un apoyo en la toma de decisiones. Esta aproximación puede replicarse en otros sistemas de seguridad crítica, dentro de un proceso continuo de evaluación e implementación. La aproximación por lógica difusa les permitió también evidenciar problemas en las infraestructuras de llaves públicas, tanto en casos específicos como en las generalidades del concepto.

Uno de los mayores inconvenientes para definir una valoración del riesgo (*risk assessment*) y el nivel de seguridad, es encontrar la métrica adecuada. Liao et al.[2] en China han recurrido a métricas de similaridad difusa para acercarse al objetivo de medir la valoración del riesgo y medir así la seguridad de los sistemas.

Liao y sus compañeros establecen la factibilidad de crear sistemas que, basados en lógica difusa, puedan evaluar el riesgo de un sistema.

III. Mitigación de ataques distribuidos

El impacto de un ataque distribuido de denegación de servicio (DDoS) puede ser muy grande. Durante el ataque, sin duda, se perderán varias peticiones legítimas ante la avalancha de peticiones maliciosas y técnicas como los hoyos negros (*black holes*) no suelen ser selectivos ante peticiones legítimas y maliciosas.

Cualquier mecanismo que pueda aumentar el grado de probabilidad de prohibir un paquete malicioso y pemitir una petición legítima, ayudará a mejorar las condiciones de servicio de los elementos atacados. En este aspecto han trabajado Covarrubias et al. en México.

Si bien su modelo propuesto no es inmune a los falsos positivos, sí logran establecer sesiones en medio de ambientes infectados, y concluyen que su sistema podría mejorar aún más si utilizaran mayores herramientas de análisis de datos.

IV. Ataques difusos

Uno de los mayores campos de acción que se desarrolla actualmente consiste en descubrir vulnerabilidades por medio de ataques difusos. La técnica, conocida en inglés como *fuzz testing* o *fuzzing*, consiste en realizar pruebas de caja negra contra sistemas, verificando su reacción ante paquetes mal formados o información aleatoria.[1][6]

Un atacante (ético o malicioso), que conozca el código de un sistema puede aprovechar este conocimiento para explotar una vulnerabilidad, tal como una inyección de código, o enviar peticiones con valores no esperados que sabe de antemano logrará un efecto esperado en el sistema atacado.

Pero incluso con pleno conocimiento del código, un sistema complejo tendrá muchas líneas de lectura. En el caso de sistemas con código propietario, el atacante no posee siquiera

Óscar Riveros y Carlos Thompson son estudiantes de maestría en la Pontificia Universidad Javeriana

Este trabajo es el proyecto final de la asignatura de Seguridad en Redes, de la Pontificia Universidad Javeriana, y fue entregado el 5 de junio de 2008.

ese recurso (aunque podría utilizar métodos de ingeniería inversa).

Los ataques difusos, son pruebas de caja negra, en el sentido de que el atacante no conoce de antemano la reacción del sistema, y tienen su mayor efectividad en ambientes controlados de laboratorio. Aunque podrían ser también efectivos ante sistemas en producción mal administrados.

La técnica consiste en enviar peticiones aleatorias ante el sistema atacado para verificar si tiene una respuesta adecuada ante situaciones inesperadas. La mayor parte de los sistemas han sido diseñados para interactuar con otros sistemas por medio de estándares, pero la mayor parte de los estándares (y con ello de los fabricantes), no establecen procedimientos para cubrir todos los posibles casos de que un mensaje no se atenga a la norma.

La mayor parte de los sistemas tiene ciertas protecciones básicas. Los protocolos establecen firmas que sirven para reconocerse y para resincronizar. Una petición sin esas firmas será entonces ignorada. Pero una petición con las firmas correctas podrá tener, sin embargo, otros elementos no esperados.

Un ejemplo de esto consiste en paquetes o archivos que establecen secciones. En casos normales, los sistemas pueden leer los tamaños de las secciones y reservar recursos suficientes para atender el resto de la sección del mensaje, asumiendo que es un mensaje bien formado. Un potencial ataque podría reportar un número demasiado grande, el cual el sistema no podrá alojar, o el mensaje termina antes de completar el espacio asignado, dejando al sistema en una espera interminable, evitando que libere los recursos asignados.

Un mensaje que coincida con las firmas normales (y por lo tanto sea aceptado por el sistema), pero contenga luego información aleatoria, podría estar reportando este tipo de fronteras de sección erroneas y causar la excepción en el equipo evaluado.

La ventaja aquí es que el atacante no necesita conocer de antemano los pormenores del protocolo o del sistema atacado. Una vez generada la excepción podrá analisar lo que pasó para entender cómo funcionó el ataque.

Las mismas compañías desarrolladoras de software, utilizan técnicas difusas para probar sus propios sistemas,[5] ya que disponiendo de suficientes herramientas de cómputo, un ataque difuso puede lograr resultados más rápidos en encontrar fallas ocultas que un estudio del código y de las posibles excepciones.

En una prueba de vulnerabilidades por ataques difusos, es indispensable documentar el proceso, ya que el objetivo, normalmente, no es comprobar que el sistema es vulnerable a un ataque difuso, sino conocer cual fue el vector de ataque que generó la excepción del sistema, bien para poderlo replicar (y explotar, por ejemplo, esa vulnerabilidad para conseguir una acceso no autorizado a un sistema, no sólamente suspender el servicio) o prevenir.

V. Conclusión

En el mundo de la seguridad de la información hay pocas certezas, y eso hace indispensable buscar mecanismos que rompan la lógica dicotoma y el pensamiento lineal.

Las técnicas de pruebas por ataques difusos y la lógica difusa ofrecen respuestas a estos problemas. En el papel del oficial de seguridad, estas técnicas no ofrecen garantías absolutas, pero son un paso más al proceso de aseguramiento de los sistemas.

Estas técnicas son sin duda una ventaja. No reemplazan el análisis de los datos, pero permiten orientar mejor al investigador sobre dónde es prioritario enfocar los esfuerzos.

Apéndice A
Conjuntos Difusos

LOS conjuntos tradicionales se basan en la regla del tercero excluido, lo cual implica que un elemento pertenece completamente a un conjunto o no pertenece a él. Este hecho es expresado mediante la función característica, o de pertenecia, del conjunto dada por

$$\mu_A(x) = \begin{cases} 1, & \text{iff } x \in A \\ 0, & \text{iff } x \notin A \end{cases} \quad (1)$$

La lógica en la que se base esta definición es conocida como bivalente y ha sido la base de las matemáticas desde tiempo inmemoriales. Pero esta definición de conjuntos es suficiente para representar todo tipo de conocimiento?

El conocimiento humano está lleno de términos que parecieran tener una declaración precisa, pero que al tratar de llevarlos al lenguaje formal de los conjuntos clásicos, comienza a perder esa claridad. Por ejemplo, uno podría clasificar a las personas por las edades: niño, joven y viejo y decidir que niño es quien sea menor de 15 años, joven es quien tenga entre 15 años y 55 y viejo es quien sea mayor de 55 años. Esta clasificación implicaría que una persona de 35 años es joven y que una de 80 es vieja. Pero que pasa con quien tiene 54 años o 55 años? Es una persona vieja o joven? En estos casos de borde se podría decir que es una persona algo vieja, o no tan joven. Ahí es donde entra la lógica difusa, que asigna valores de verdad en todo el intervalo $[0, 1]$ y permite una gradualidad en la definición de pertenencia.

Un conjunto difuso es un conjunto con pertenencia gradual en el intervalo real $\mu_A(x) \in [0, 1]$. Esto quiere decir que un elemento pertenece al un conjunto en un cierto grado. De esta manera se pueden expresar matemáticamente definiciones vagas como frío, caliente, caro, barato, viejo, joven, etc.

Definición: Un conjunto difuso A en el universo X es un conjunto definido por la función de pertenencia $\mu_A(x)$ que es una relación del universo X en el intervalo $[0, 1]$:

$$\mu_A(x) : X \to [0, 1] \quad (2)$$

Si el valor de la función de pertenencia, llamado grado de pertenencia, es igual a uno entonces se dice que x pertenece completamente al conjunto difuso. Si es igual a cero, se dice que x no pertenece al conjunto y si se obtiene un valor intermedio, se dice que x es un miembro parcial del conjunto difuso [7] [8].

Operaciones entre conjuntos difusos. Se pueden extender las operaciones de la lógica tradicional a la lógica difusa. Presentamos las operaciones definidas por Zadeh [9].

Complemento: Sea A un conjunto difuso en X. El complemento de A es el conjunto difuso C, denotado $C = \bar{A}$ tal que para cada $x \in X$,

$$\mu_C(x) = 1 - \mu_A(x) \tag{3}$$

Intersección: Sean A y B dos conjuntos difusos en X. La intersección de A y B es el conjunto difuso C , denotado $C = A \cup B$ tal que para cada $x \in X$,

$$\mu_C(x) = min\{\mu_A(x), \mu_B(x)\} \tag{4}$$

Unión: Sean A y B dos conjuntos difusos en X. La unión de A y B es el conjunto difuso C , denotado $C = A \cup B$ tal que para cada $x \in X$,

$$\mu_C(x) = max\{\mu_A(x), \mu_B(x)\} \tag{5}$$

t-Norma: Una t-Norma T Es una operación binaria en el intervalo unidad que cumple con al menos las siguientes propiedades:

$$T(a,1) = a \quad \text{(condición de borde)}, \tag{6}$$
$$b \leq c \; implica \; T(a,b) \leq T(a,c) \quad \text{(monotonocidad)}, \tag{7}$$
$$T(a,b) = T(b,a) \quad \text{(reflexividad)}, \tag{8}$$
$$T(a,T(b,c)) = T(T(a,b),c) \quad \text{(asociatividad)} \tag{9}$$

Algunas t-Normas generalmente usadas:

intersección clásica (Zadeh):	$T(a,b) = min(a,b)$
producto algebraico:	$T(a,b) = ab$
Intersección de Lukasiewicz:	$T(a,b) = max(0, a+b-1)$

t-Conorma: Una t-Conorma S es una operación binaria en el intervalo unidad que cumple con al menos las siguientes propiedades:

$$S(a,0) = a \quad \text{(condición de borde)}, \tag{10}$$
$$b \leq c \; implica \; S(a,b) \leq s(a,c) \quad \text{(monotonocidad)}, \tag{11}$$
$$S(a,b) = S(b,a) \quad \text{(reflexividad)}, \tag{12}$$
$$S(a,S(b,c)) = S(S(a,b),c) \quad \text{(asociatividad)} \tag{13}$$

Algunas t-Normas generalmente usadas:

unión clásica (Zadeh):	$S(a,b) = max(a,b)$
producto algebraico:	$S(a,b) = ab$
unión de Lukasiewicz:	$S(a,b) = max(0, a+b-1)$

RECONOCIMIENTOS

Los autores reconocen a Julio Álvarez, Jeimi Cano, y Fabián Medina por el apoyo brindado en la elaboración de este trabajo.

REFERENCIAS

[1] M. Sutton, A. Greene y P. Amini *Fuzzing: Brute Force Vulnerability Discovery* ISBN 0321446119.
[2] Y. Liao, et al., *A New Fuzzy Risk Assessment Method for the Network Security Based on Fuzzy Similarity Measure**, Proceedings of the 6th World Congress on Intelligent Control and Automation, June 21 - 23, 2006, Dalian, China
[3] J. C. Covarrubias, A. Parra, J. A..Ñolazco, *FLF4DoS. Dynamic DDoS Mitigation based on TTL field using fuzzy logic* IEEE.
[4] V. Casola, M. Rak, R. Preziosi, L. Troiano, *Security Level Evaluation: Policy and Fuzzy Techniques* IEEE.
[5] Mu Security, *The Business Case and Return of Investment for Deploying the Mu-4000 Security Analysis Platform*
[6] J. Lämsä, R. Kaksonen y H. Kortti, *Codenomicon robustness testing – handling the infinite input space while breaking software*
[7] R. Babuška *Fuzzy modeling for control*. Kluwer Academic Publishers, 1998. Boston, Massachusetts.
[8] H.Ñguyen y E. Walker, *A first course in fuzzy logic*, Chapman & Hall, 2000. Boca Ratón.
[9] L. Zadeh *Fuzzy sets*. Information and Control 8, 338?353, 1965.



Óscar Andrés Riveros Moyano Informático-Matemático de la Pontificia Universidad Javeriana y estudiante de maestría en ingeniería electrónica en la misma universidad.

Se desempeña actualmente como contratista en seguridad informática en el fondo de pensiones del Distrito Capital de Bogotá .



Carlos Eugenio Thompson Pinzón Ingeniero electrónico de la Pontificia Universidad Javeriana y estudiante de maestría en ingeniería electrónica en la misma universidad. Ha trabajado en soporte técnico e implementación de redes de datos para Ericsson de Colombia y Huawei Technologies.

Se desempeñó como profesor y administrador de la red en la Universidad Antonio Nariño.

Actualmente trabaja como investigador en Digiware de Colombia, empresa líder en el país en seguridad de la información.

Primer puesto en Olimpiadas Colombianas de Matemáticas en nivel superior escolar y en olimpiadas universitarias, y tres veces ganador de medalla de bronce en las Olimpiadas Internacionales de Matemáticas.