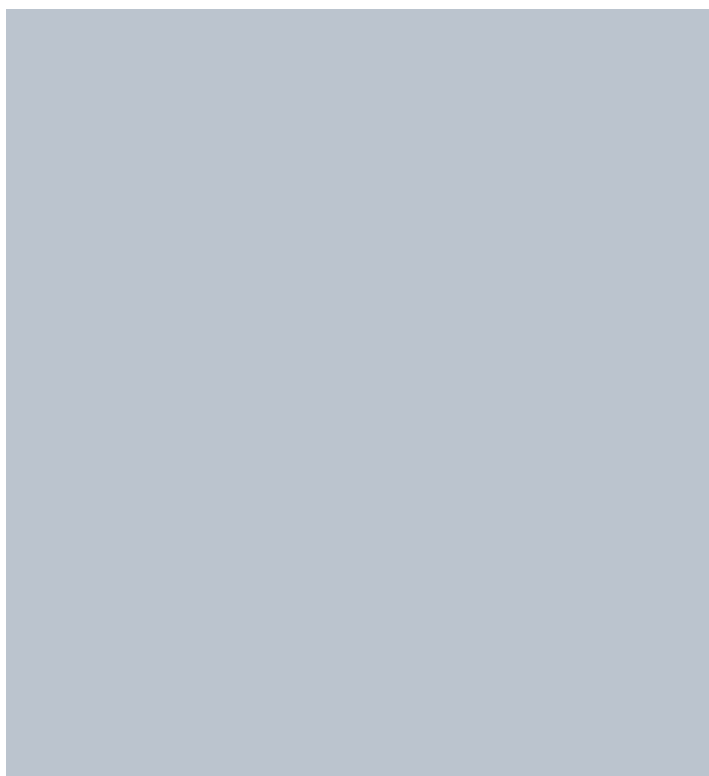


Un sistema aprende pautas para evitar ciberataques



Secciones

Políticas

I+D+i

Capital humano

Economía

Cultura

Estrategias verdes

Blogs



El Envés
Estoy libre si
todos somos
libres
José Carlos

EMPRESAS Y
RSC

Ampliar
+

Polémica en
Telefónica por los 5,7
millones de euros
cobrados por Eva
Castillo en 2014

BBVA lanza su
convocatoria de
ayudas por 2,2
millones a
investigadores y
creadores culturales

Las empresas no
responsables tendrán
riesgo de
desaparecer

ABENGOA

ABERTIS

ACCIONA

ACERINOX

ACS

ADECCO

AMADEUS

ARCELORMITTAL

BANCO POPULAR

BANCO SABADELL

BANCO SANTANDER

BANKIA



PUBLICIDAD

Investigadores de los grupos
Sistemas Inteligentes y
Minería de Datos (SiMiDat)
de la Universidad de Jaén y
Soft Computing y Sistemas
de Información Inteligentes
(SCI2S) de la Universidad de
Granada han diseñado un
sistema de detección de
intrusiones para hacer frente
a ciberataques. La
herramienta se basa en
técnicas de inteligencia
computacional con las que
aprende pautas que le
permiten anticiparse a los
intrusos que vulneran los
mecanismos de seguridad de
los sistemas de información.

Los dispositivos actuales de
detección de intrusos en la
red están limitados a la
información con la que fueron
entrenados y detectan sólo si
hay ataque o no. Otros
detectores incurrir en falsos
positivos. "No sólo consiste

Maestro Ciruela
Agustín Yanel:
"Periodistas y
fotógrafos son
autores"
Hipólito M.
Clavero



Solidarios
Deuda con los
nietos
Carlos Miguélez
Monroy

¿Quiere un blog
propio y leído en
todas las
universidades?
Infórmese aquí

Libros y Tesis

LIBROS

Reacciona-dos

DIARIO DE UN
MINISTRO. De la
tragedia del 11 M
al desafío
independentista
catalán

[illegible]

en identificar que el acceso es anómalo, sino que el sistema aprenda a detectarlos y responda ante ese ataque", explica el responsable del proyecto Alberto Fernández, de la Universidad de Jaén.

"No sólo hay que identificar que el acceso es anómalo, sino que el sistema aprenda a detectar y responda ante el ataque", dicen los investigadores

Los ataques cibernéticos presentan características diferentes, por lo que métodos estadísticos sencillos no resultan efectivos para su detección. Por ello, los expertos han utilizado Inteligencia Computacional que permite el entrenamiento del sistema para que extraiga conclusiones fruto de su experiencia. "Aplicamos estas técnicas para intentar que la herramienta avance hasta una solución factible con técnicas sofisticadas parecidas a las reglas propias del aprendizaje humano", detalla el investigador.

Para conseguir que el sistema ‘aprenda’ los investigadores lo someten a una batería de pruebas en las que tiene que procesar 4 millones de ejemplos disponibles en repositorios de datos. Con los comportamientos correctos, la herramienta va extrayendo conclusiones y discriminando si se trata de un acceso normal o anómalo.

La novedad de este modelo, que los expertos describen en su trabajo publicado en la revista *Expert Systems with Applications*, es la utilización de sistemas difusos evolutivos basados en las leyes de la naturaleza. “En nuestro caso, aplicamos este patrón y el algoritmo aprende por sí mismo con los conjuntos de datos que le hemos dado como entrenamiento. Empieza aportando soluciones aleatorias y evoluciona hasta quedarse con las que mayor calidad aportan al objetivo de identificación. Es como la teoría de la evolución de Darwin, combinamos soluciones y van quedando las mejores adaptadas”, indica Fernández.

La ventaja de este enfoque es la utilización de etiquetas lingüísticas, que permite una mejor comprensión del conjunto de reglas con las que opera el sistema. "En lugar de utilizar valores numéricos utiliza conceptos del lenguaje humano. Por ejemplo, en lugar de alertar sobre el riesgo de que alguien está intentando atacar el sistema es 10, dice que existe un riesgo alto. Esto facilita la interpretación, porque se parece a los conceptos que utilizamos en

	No, mi general		
	DEMOCRACIA DE PAPEL. Crítica al poder, desde la transición hasta la corrupción		
	Historia vivida de España. De Franco a Podemos. 1970-2020		

	RSC: Para superar la retórica		
	 TESIS Y TESINAS		
	Eficiencias del 9% al captar energía solar con electrodométricos y otros detectores		
	Avanzan las estrategias para optimizar los resultados de la cirugía electiva del cáncer colorrectal		

▣ Eficiencias del 9% al captar energía solar con electrodomésticos y otros detectores

▣ Un sistema aprende pautas para evitar ciberataques

▣ Ayudar a los niños con los deberes, contraproducente



nuestro día a día, donde en nuestras conversaciones no precisamos que la temperatura es de 30 grados, sino decimos que hace calor", aclara.

Aprendizaje 'divide y vencerás'

Otra de las novedades es la utilización del esquema de aprendizaje denominado 'divide y vencerás', que mejora la precisión cuando se producen ataques considerados raros. En este modelo se dividen los datos etiquetados por parejas (actividad normal y cada tipo de ataque y, a su vez, todos los tipos de ataques entre sí) y se introducen en el sistema con lo que se aporta una solución para cada binomio y la respuesta final agrega la de cada miembro individual.

"Es como el jurado de un concurso, cada persona elige un ganador y, al final, se toma una decisión conjunta. Así se traslada la responsabilidad de decidir a muchos puntos y cada punto o experto aborda una faceta, desgranando el problema. La decisión final integra la opinión de ese conjunto de expertos", ejemplifica. Esto supone que los tipos de alarmas están más definidos, porque dan distintas respuestas ante las alertas, aportando más robustez al sistema.

Este enfoque 'divide y vencerás', combinado con la lógica difusa evolutiva, ha permitido a los investigadores diseñar un sistema que identifica correctamente todos los tipos de ataques, incluyendo las categorías de ataque raras y que utiliza unos términos interpretables para la comprensión humana.

El sistema identifica todos los tipos de ataques, incluyendo las categorías raras

Las políticas de seguridad de la información de sistemas y redes están diseñadas para mantener la integridad de la confidencialidad y disponibilidad de los datos de sus usuarios de confianza. Sin embargo, los denominados ataques maliciosos analizan las vulnerabilidades de estos sistemas con el fin de obtener acceso no autorizado o comprometer la calidad del servicio.

Los expertos apuntan distintos tipos de ataques. Por un lado puede ocurrir un fallo del servicio, cuando se produce tanta cantidad de accesos denegados que al final saturan el sistema. Otras modalidades pasan por el escaneo de puertos para buscar vulnerabilidad en la red, adivinar la contraseña o intentar acceder como administrador, consiguiendo el control total del sistema.

Los investigadores continúan

La Responsabilidad Social Empresarial genera valor significativo, aunque debe adaptarse a cada caso

Muy positivos resultados del proceso de acreditación de pregrado en universidades de Chile

Creadores de opinión pública, diseñadores de comportamientos

Los Adolescentes como Actores en el Espacio Sanitario

Lo más leído

con este modelo, aún experimental, para trasladarlo al BigData, es decir, a la utilización de gran cantidad de datos con las herramientas capaces de analizarlos y procesarlos. "Si ahora trabajamos con un sistema de entrenamiento con cuatro millones de ejemplos, la idea sería incrementar esa cifra y adaptar el modelo para hacerlo escalable mediante su ejecución paralela sobre un conjunto de ordenadores para dividir el trabajo entre todos ellos", adelanta el investigador.

Referencia bibliográfica:

Elhag, S; Fernández, A; Bawakid, A ; Alshomrani, S ;Herrera, F. 'On the combination of genetic fuzzy systems and pairwise learning for improving detection rates on Intrusion Detection Systems'. *Expert Systems with Applications*, 2015.

Otros asuntos de Universidades

✓ [Comparación entre Klein y Lacan en base a sus abordajes de la transferencia](#)

✓ [El 16-M, lección conmemorativa del neurobiólogo Rafael Yuste en honor a Eladio Viñuela](#)

✓ [Coaching de grupo para ayudar a encontrar y crear empleo en Valladolid](#)

✓ [Bacterias y algas unicelulares para iluminar el ambiente sin consumo eléctrico](#)

1	Reacciona-dos	
2	El flato intestinal, detector de enfermedades	
3	La placenta donde creciste te pudo cambiar la vida	
4	Un sistema aprende pautas para evitar ciberataques	
5	Eficiencias del 9% al captar energía solar con electrodomésticos y otros detectores	

6	Ayudar a los niños con los deberes, contraproducente	
7	Avanzan las estrategias para optimizar los resultados de la cirugía electiva del cáncer colorrectal	
8	Son evitables dos millones de muertes anuales por el riñón	
9	La "E-Money Week" se hace global, salvo en España	
10	Comparación entre Klein y Lacan en base a sus abordajes de la transferencia	

✓ Multiplican por 10.000 el grosor de la seda de araña

✓ Homenaje a los estudiantes de magisterio desaparecidos en Ayotzinapa (México)

✓ IE Business School, líder mundial en MBA Online

✓ Científicos de tres países ejecutan la primera erradicación ecológica en la Antártida

✓ Las redes sociales, fuente más habitual del 90% de los periodistas

✓ Creanavarra organiza el Taller "La importancia de la moda en Televisión"

✓ Grecia: una oportunidad de repensar Europa

✓ El Consejo de la Complutense intentará desbloquear las elecciones

✓ Visita la UAM el líder europeo de investigación, interesado por su excelencia matemática

✓ El presidente de la Comunidad visita el Parque Científico de Madrid situado en la UAM

✓ Conferencia de Sergio Ramírez, secretario de

RANKING
WANABIS

Ampliar +

▣ De la 'formación online' a la 'presencia virtual'

▣ De la Formación Online al aprendizaje social y conectado

▣ La industria del e-learning duplicará su volumen hasta los 100.000 millones en 2015

escritor y ex vicepresidente de Nicaragua



Madrid suspende las elecciones a rector en la Universidad Complutense



El título de doctor, sometido a revisión crítica por académicos y universidades



Los 4 opositores a Carrillo en las elecciones de la Complutense denuncian "grave inestabilidad"



Descubierto tras 500 años el autor de la famosa fachada de la Universidad de Salamanca



La Cátedra UAM-Novartis celebra 10 años impulsando la investigación en atención primaria