

VIII Evento Internacional de Redes y Telecomunicaciones  
CITMATEL 2003

# Actualidad de la tecnología de detección de intrusos en las redes



MSc. **Walter Baluja García**  
[walter@tesla.cujae.edu.cu](mailto:walter@tesla.cujae.edu.cu)

*Dpto. Telemática*  
*CUJAE. CUBA*

# Introducción

- Actualmente, las redes de computadoras y sus problemas de seguridad tienen características que no son las mismas de 5 o 10 años atrás.
- Estas situaciones adicionan complejidad a las medidas o mecanismos de protección y al trabajo del personal que se ocupa de estos menesteres.

# Diversidad, fuerza y profundidad de los ataques

- Persisten en su efectividad ataques de denegación de servicios.
- Cobran fuerza los ataques distribuidos, los ataques a sitios web y a sus bases de datos.
- La mayor parte de los ataques reflejan un gran conocimiento de las características y debilidades de los sistemas.

# Cantidad de incidentes

## 2000-2003

Year	2000	2001	2002	1Q-3Q 2003
Incidents	21,756	52,658	82,094	114,855

Total de incidentes (1988-3Q 2003): **297,318**

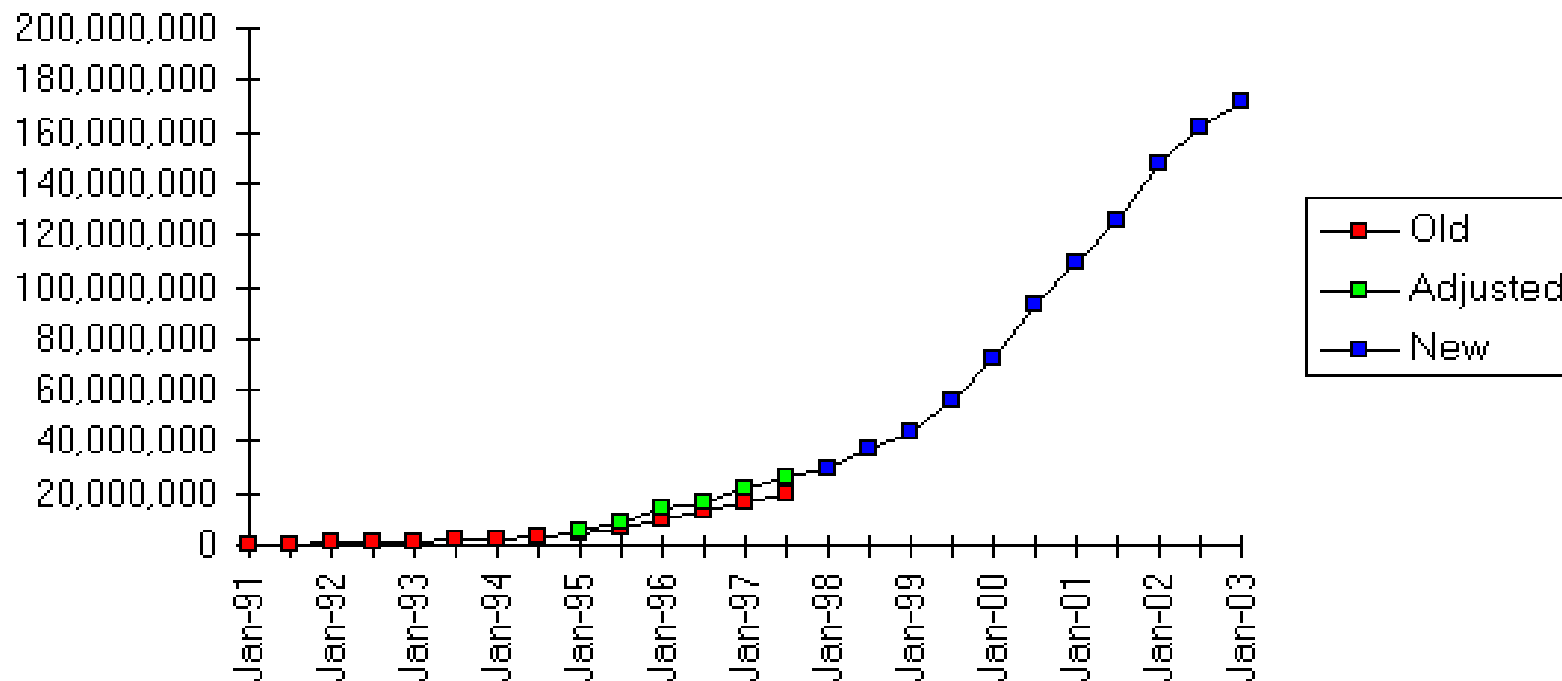
Fuente: CERT/CC (<http://www.cert.org/>)

# Cada vez más computadoras que proteger

- Cada entidad, posee una red que llega a todos los rincones de la misma y que es utilizada por la mayor parte del personal correspondiente.
- Crece el número de servidores y la cantidad y variedad de servicios.
- Esto multiplica el número de posibles puntos vulnerables, intrusos y otros.

# Cada vez más computadoras que proteger

Internet Domain Survey Host Count



Source: Internet Software Consortium ([www.isc.org](http://www.isc.org))

Enero del 2003: **171,638,297** hosts

# Cada vez más computadoras que proteger

	2002	2003	2004	2005	2006
North America	212,625,000	222,882,250	234,422,143	244,682,327	256,154,022
Central/South America	25,603,581	32,653,405	43,793,278	59,450,160	80,780,979
Europe	163,532,970	195,513,220	224,840,203	240,579,018	257,419,549
Middle East/Africa	9,235,050	10,707,998	11,571,220	12,535,406	13,616,264
Asia/Pacific	151,284,715	203,625,480	238,007,338	273,034,857	313,433,527
<b>Total Worldwide</b>	<b>562,281,316</b>	<b>665,382,353</b>	<b>752,634,182</b>	<b>830,281,767</b>	<b>921,404,341</b>

Usuarios de Internet

Fuente: Internet Software Consortium (<http://www.isoc.org/>)

# Distribución de puntos a proteger por toda la red

- Son decenas y hasta cientos las computadoras cuya protección se hace indispensable en cada lugar.
- La información sensible de cada entidad y los servicios de la misma se hallan dispersos en diferentes segmentos de red por diferentes causas.

# Enlaces numerosos y veloces

- Las soluciones de acceso telefónico enlaces a Internet, conexiones a redes experimentales, corporativas o con otros fines son muy comunes.
- Esto hace crecer el número de puntos de acceso a una red y por tanto la complejidad de control del flujo de información en cada acceso.

# Redes corporativas

- Es muy común que cada empresa o entidad tenga una red nacional o regional.
- Existen numerosos enlaces de alta velocidad y gran cantidad de servidores a proteger ubicados en una especie de backbone controlado por la empresa.

# Sistemas Detectores de Intrusos

- Herramientas con cierta inteligencia que automatizan la detección de intentos de intrusión en una red de computadoras.



(nfr)(security)



# Sistemas Detectores de Intrusos

- Sistemas basados en normas: actúan a partir de bases de datos que contienen los patrones de ataques.
- Sistemas adaptables: se trata de incorporar técnicas avanzadas, como la inteligencia artificial, para reconocer y aprender nuevos patrones de ataques.

# ¿Qué pueden hacer?

- Detectar ataques en el momento que está ocurriendo o poco tiempo después de haber ocurrido.
- Automatizar la búsqueda de nuevos patrones de ataque.
- Monitorizar y análisis de las actividades de los usuarios.



# ¿Qué pueden hacer?

- Auditoria de configuraciones y vulnerabilidades de determinados sistemas.
- Analizar comportamientos anormales.
- Disminuir la complejidad de las tareas de administración de la seguridad en la red.

# Reacciones

- Reconfiguración del cortafuegos.
- Emisión de sonido de alerta.
- Emisión de un *trap* SNMP.
- Envío de mensaje de correo.
- Registro del ataque en *logs*.
- Salva de evidencias.
- Ejecución de programas.
- Cierre de conexión TCP.



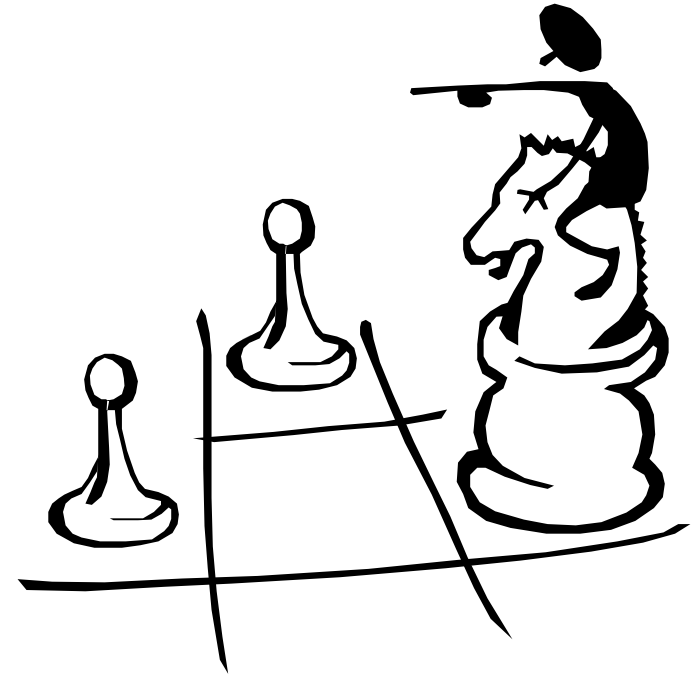
# Características

- Balance entre complejidad en la administración y potencialidad de la herramienta.
- Costo elevado.
- Falta de integración de las herramientas.



# Retos

- Automatización y sofisticación de los ataques.
- Descubrimiento veloz de las vulnerabilidades.
- Incremento de ataques a la infraestructura.
- Empleo de cifrado para ocultar información de ataques.
- Aumento del tráfico y los servicios en las redes.
- Operación en entornos de alta automatización de tareas.



# Tendencias

- Integrar la información proveniente de diferentes sensores.
- Mejorar las posibilidades de capturar información útil para el trabajo forense.
- Ampliar las posibilidades de detectar código maligno.
- Desarrollar facilidades para la detección de ataques DoS (Denial of Services), ataques distribuidos y otros.
- Identificar nuevas formas de ataques.

# Soluciones:

## Operación distribuida

- Una misma herramienta debe estar funcionando en varias computadoras al mismo tiempo.
- Esto se había resuelto instalando el o los programas en cada lugar y esto significa repetir bases, reportes, configuración y multiplicar los esfuerzos de administración.
- Actualmente se comparten las bases de datos y configuración.

# Soluciones:

## Administración centralizada

- Concentrar todo el esfuerzo de administración en un solo lugar.
- Desde allí se configura, actualiza, analiza el funcionamiento, se estudian los reportes y se toman decisiones.
- La comunicación entre las estaciones vigilantes y la estación de control debe ser segura.

# Soluciones:

## Fusión de datos de diferentes sensores

- En ambientes distribuidos se requiere la recolección y análisis de datos en un solo punto central.
- A partir de este trabajo se evalúan situaciones, se toman decisiones y se ejecutan tareas.
- La aplicación de la fusión de datos requiere de algoritmos matemáticos y heurísticos, inteligencia artificial, reconocimiento de patrones y otros.

# Soluciones: Minería de datos

- Con este trabajo se filtra, transforma y organizan extensos volúmenes de información que se obtienen mediante la recolección.



- Permite reconocer nuevos patrones de ataques y nuevos ataques en sí.

# Soluciones: Redes Neuronales

- En los IDS, se pueden usar para decidir si un paquete o un grupo de estos constituyen un ataque o no.
- Un cambio significativo en la red (por ejemplo, la aparición de tráfico nuevo) puede producir multitud de falsos positivos.
- Además, la actualización del IDS es complicada.
- Aunque carece de elementos que automaticen su configuración, entrenamiento y otros, se perfila como uno de los grandes motores que impulsará la adaptabilidad de los IDS.

# Soluciones: Agentes Móviles

- Disminución de la carga o el tráfico en la red en entornos de trabajo distribuido, independencia de plataforma, adaptación y configuración dinámica, escalabilidad y otros.
- Representa un cambio radical en el modo de ejecutar algunas tareas.

# Facilidades

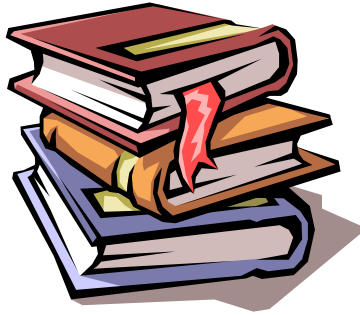
- La aplicación de las técnicas expuestas arriba les permite desarrollar un trabajo más efectivo y completo a la hora de detectar intrusiones.
- El hecho de analizar los datos de todos los nodos en un punto común permite obtener conclusiones imposibles de alcanzar con los análisis independientes que se puedan realizar en cada nodo.

# Facilidades

- Detección de ataques simultáneos.
- Detección reconocimientos.
- Detección de ataques distribuidos.
- Ejecución de reacciones defensivas globales.

# Conclusiones

- Las características de la operación y desarrollo de las redes exigen herramientas de seguridad más capaces, eficientes y robustas.
- Los diseñadores y desarrolladores se enfrentan a retos mayores.
- Hoy se empieza a dar los primeros pasos para convertir realmente a los IDS en sistemas inteligentes.



# Bibliografía

- Ant, Allan, “Intrusion Detection Systems (IDSs): Perspective”. 2002.
- Baluja, Walter, “Acercamiento a los sistemas detectores de intrusos.” Revista Telem@tica, Año I No. 2 ISSN: 1729-3804. 2001.
- Bass, Tim, “Intrusion detection systems and multisensor data fusion”, Communications of the acm, April 2000/Vol. 43, No. 4.
- Díaz Vizcaíno, Luis Miguel, “Sistemas de Detección de Intrusos”, Universidad Carlos III de Madrid. 2002.
- Krugel, Christopher, Toth Thomas, “Applying Mobile Agent Technology to Intrusion Detection”, Distributed Systems Group Technical University Vienna. 2001.
- Networked Systems Survivability Program, “State of the Practice of Intrusion Detection Technologies”. CERT. January 2000.