Introducción a las técnicas antiforenses

Conceptos e implicaciones para investigadores

VII Jornada Nacional de Seguridad Informática

COMPUTACIÓN FORENSE: RASTREANDO LA INSEGURIDAD INFORMÁTICA

JUNIO 20, 21 Y 22 DE 2007
Biblioteca Luis Ángel Arango
Calle 11 No 4-14
Bogotá D.C., Colombia.

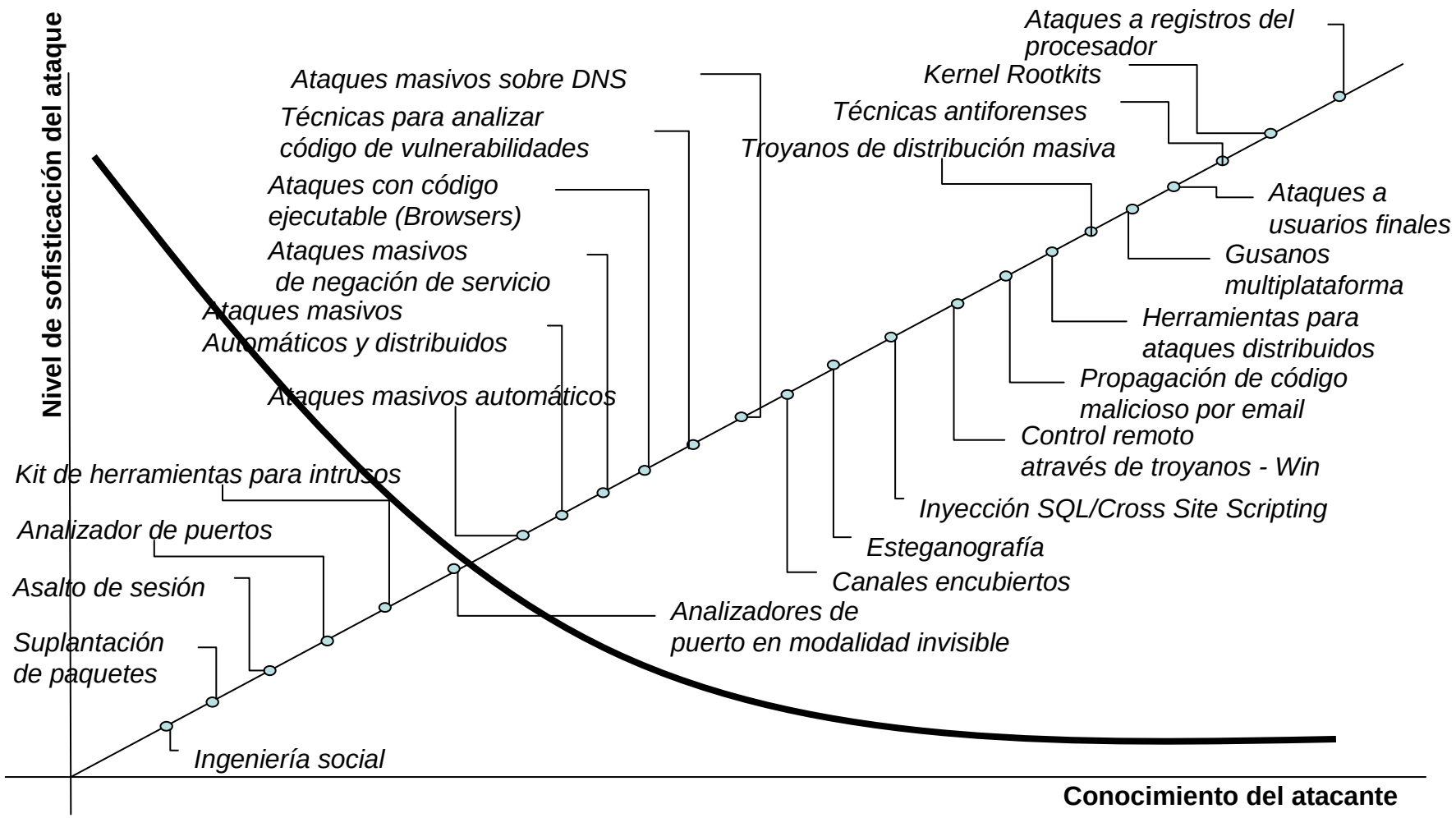
Conferencista:
Jeimy J. Cano, Ph.D, CFE
GECTI-Uniandes
jcano@uniandes.edu.co

ACIS

Agenda

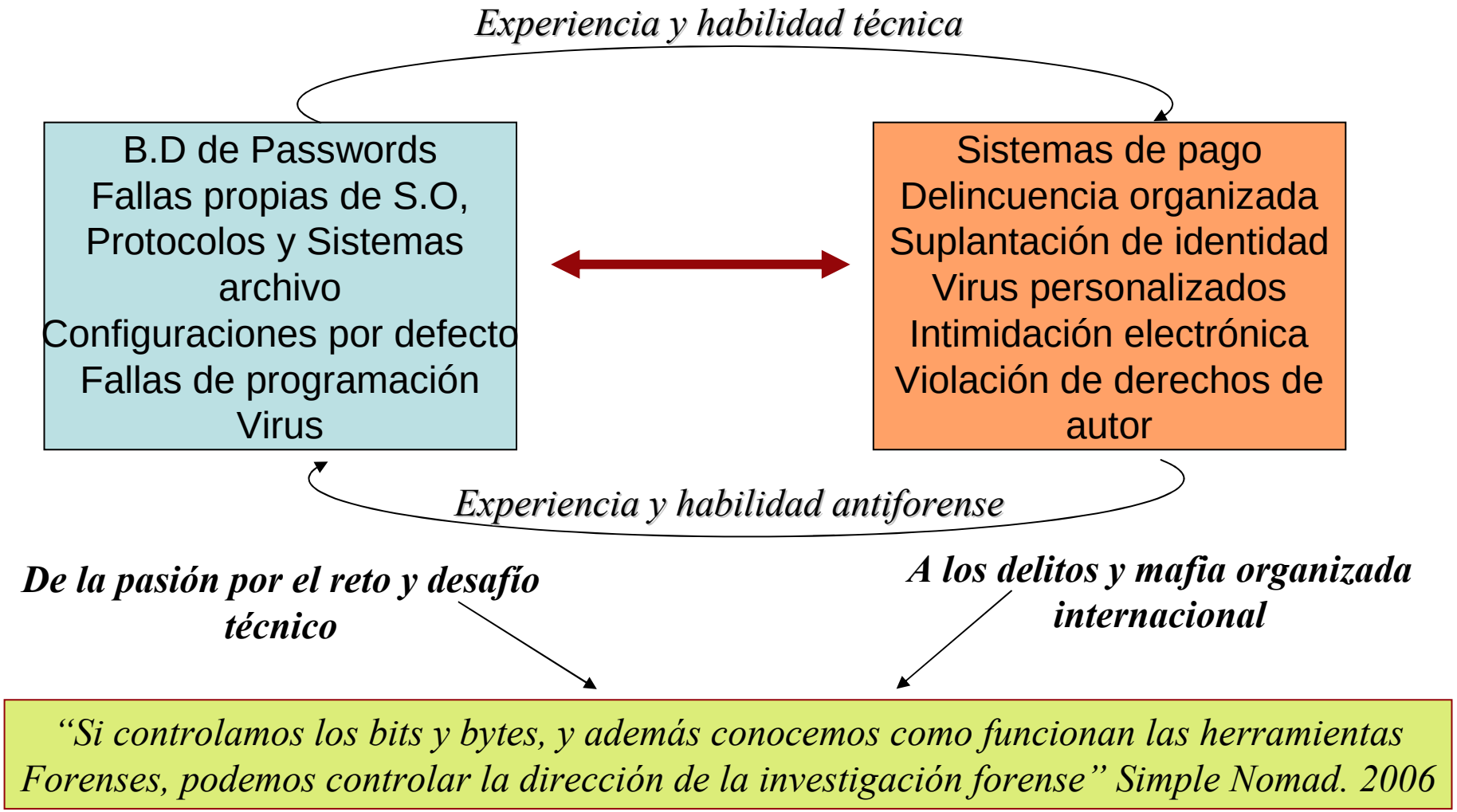
- Introducción
- Evolución de los ataques de seguridad
- Evolución de los atacantes: ¿hacia dónde vamos?
- ¿Qué son las técnicas antiforenses?
- Un modelo conceptual de detección y rastreo de técnicas antiforenses – MoDeRaTA
- Aplicación del modelo - MoDeRaTA
- Nuevos cuidados antes de iniciar una investigación
- Nuevas propuestas forenses
- Reflexiones finales
- Referencias

Evolución de los ataques de seguridad



Adaptado y extendido de: ALLEN, J.(2005) Information security as an institutional priority. Carnigie Mellon. Presentación Powerpoint. Disponible en: http://www.cert.org/archive/pdf/info-sec-ip.pdf (Consultado: 4/05/2007)

Evolución de los atacantes: ¿hacia dónde vamos?



¿Qué son las técnicas antiforenses?

- De acuerdo con Harris 2006, se tienen las siguientes definiciones
  - 1. "(…) *methods used to prevent (or act against) the application of science to those criminal and civil laws that are enforced by police agencies in a criminal justice system.* (…)"
  - 2. "*(..) limit the identification, collection, collation and validation of electronic data.(...)*"
  - 3. *"(...) attempting to limit the quantity and quality of forensic evidence (...)"*
  - 4. *" (...) any attempts to compromise the availability or usefulness of evidence to the forensics process. (...)"*

¿Qué son las técnicas antiforenses?

- Si tratamos de operacionalizar la cuarta definición, la podemos expandir como:
  - "*Cualquier intento exitoso efectuado por un individuo o proceso que impacte de manera negativa la identificación, la disponibilidad, la confiabilidad y la relevancia de la evidencia digital en un proceso forense*".

Modelo Conceptual de detección y rastreo de técnicas antiforenses – MoDeRaTA

MoDeRaTA - Consideraciones

- Niveles
  - Definen los elementos susceptibles donde se pueden materializar las técnicas antiforenses
- Detección y Rastreo
  - Establece los rangos y grados en los cuales es posible detectar y rastrear la materialización de técnicas antiforenses
  - Incluye en nivel de esfuerzo (sofisticación) requerido por el atacante para materializar la técnica antiforense
- Técnica utilizada
  - Destruir / Mimetizar / Manipular / Deshabilitar, las cuales se pueden materializar en todos los nivel definidos en el modelo

Modelo Conceptual de detección y rastreo de técnicas antiforenses – MoDeRaTA

Aplicación de MoDeRaTA - Memoria

- Ataques a regiones adyacentes en la memoria
  - Basada en usos de funciones estándar que no terminan automáticamente una cadena: Strncpy
  - Para obtener el control de la máquina objetivo, se debe materializar un desbordamiento de pila o heap, y puede ocurrir cuando la post-concatenación de un buffer es copiado en otro.

Aplicación de MoDeRaTA - Memoria

```
Void function hola (char buf5[32]){
char buf3[8];
Strcpy (buf3, buf5);
}

Int main{
Char buf1[8];
Char buf2[4];
Fgets (buf1, 8, stdin);
Strncpy (buf2, buf1, 4); /* Strncpy no copia el carácter nulo - \0 */
function hola (buf2);
}
```

Strcpy (Cadena-destino, cadena-origen)

• Copia la **<cadena origen>** sobre la **<cadena destino>**, a partir de su inicio (se perderá el contenido anterior de esta última).

Strncpy (x, y, len)

* Copia los primeros **len** caracteres de **x** dentro de **y**. No copia el caracter nulo.

Ejecución:

Buf2 = ?

Buf1 = “12345678” – ejecución del fgets

Luego del STRNCPY:

Buf2 = ?

Buf1= “?%*/5678”

Se ejecuta la función hola:

Buf5 = “? % * / -”

Buf3 = “- - - - - - - -”

Luego del STRCPY:

Buf3 = “ ? % * / - - - -” -

Tomado de: Rosiello, A. (2007) Ataques a regiones adyacentes de la memoria. *Hakin9*. No. 22. pp 14-19

Modelo Conceptual de detección y rastreo de técnicas antiforenses – MoDeRaTA

Aplicación de MoDeRaTA - Procesos

- Rootkits
  - "Es un programa o conjunto de programas que permiten al desarrollador ocultar en un computador su rastro y sus armas"
  - Un rootkit no es un virus, ni un código malicioso, lo que busca es modificar el comportamiento del sistema infiltrado para hacerse invisible.

Aplicación de MoDeRaTA - Procesos

COMPONENTES FUNCIONALES DEL KERNEL

Admon de procesos: Cada proceso tiene una estructura de datos en memoria para mantener el rastro de todos los hilos y procesos. *Modificando estas estructuras de datos, un atacante puede ocultar un proceso*

Acceso a los archivos: El kernel provee una interfase consistente al sistema de archivos. Modificando el código de la interfase, *un atacante puede ocultar archivos y directorios.*

Seguridad: En Unix y sistemas Windows, el Kernel hace cumplir los permisos establecidos y separa los rangos de memoria para cada proceso. *Sólo unos cambios en el código del kernel y es posible remover los mecanismos de seguridad.*

Admon Memoria: Cada vez que un proceso en memoria se carga, puede utilizar la misma dirección de memoria y leer datos diferentes. Es decir, la misma dirección de memoria en dos localizaciones físicas de memoria diferentes. *Un atacante puede explotar esta situación para ocultar datos a los depuradores o software de monitoreo activo.*

En el caso Windows XP

-Modo Usuario

- Uso de API que cada desarrollador puede usar.
- *Idea:* Reemplazar programa conocidos para hacerse invisible.

- Modo Kernel

- Los binarios ejecutados en este modo tienen acceso a todo el sistema sin restricciones.
- *Idea:* Escritos como *drivers* para windows, que tienen acceso a todos los objetos del sistema.

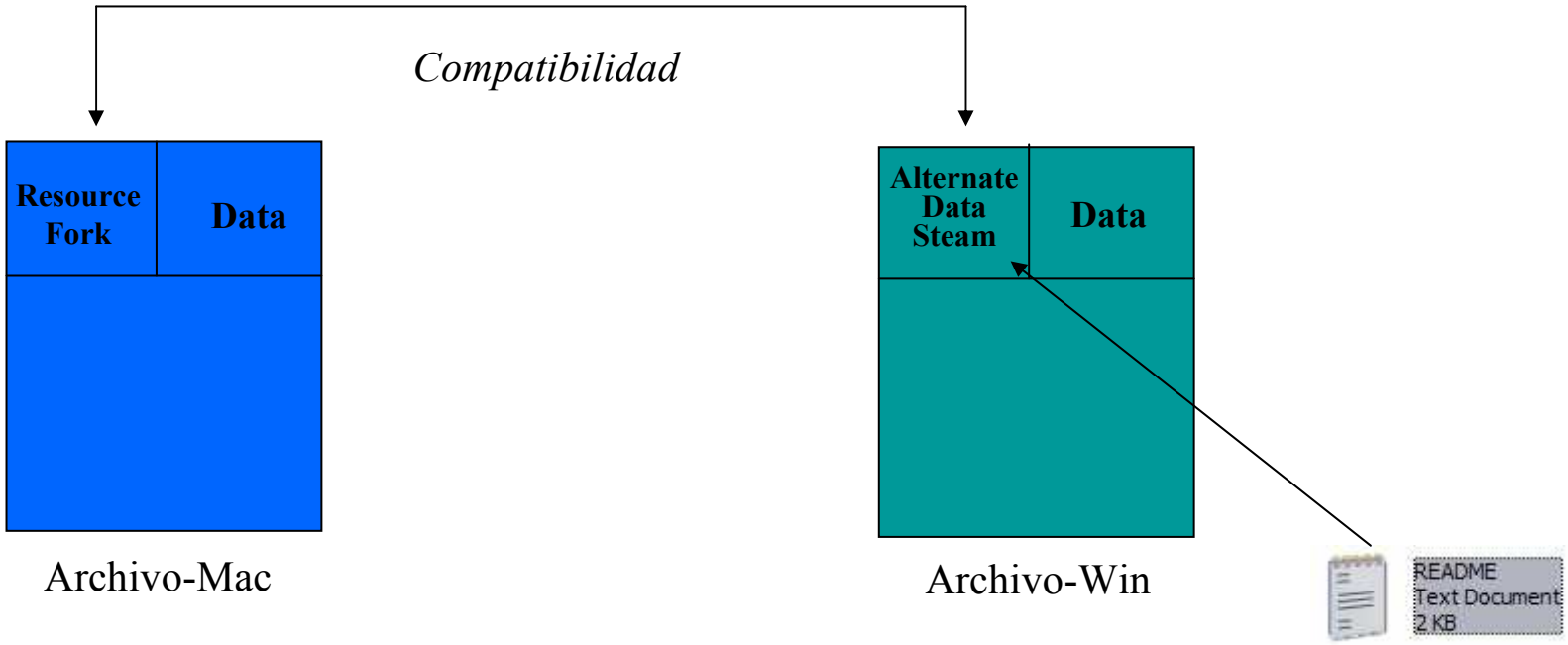
Tomado de: BUTLER, J. y HOGLUND, G. (2006) *Subverting the windows kernel. Rootkits*. Addison Wesley.

Modelo Conceptual de detección y rastreo de técnicas antiforenses – MoDeRaTA

Aplicación de MoDeRaTA – Sistemas de Archivo

- Alternate Data Streams
  - Característica propia de NTFS creada para mantener compatibilidad con los sistemas Macintosh.
  - Utilizada por los atacantes para ocultar información en medio de los archivos normales del sistema operacional o de los usuarios.

Aplicación de MoDeRaTA – Sistemas de Archivo



Macintosh
HFS

Windows NT
NTFS

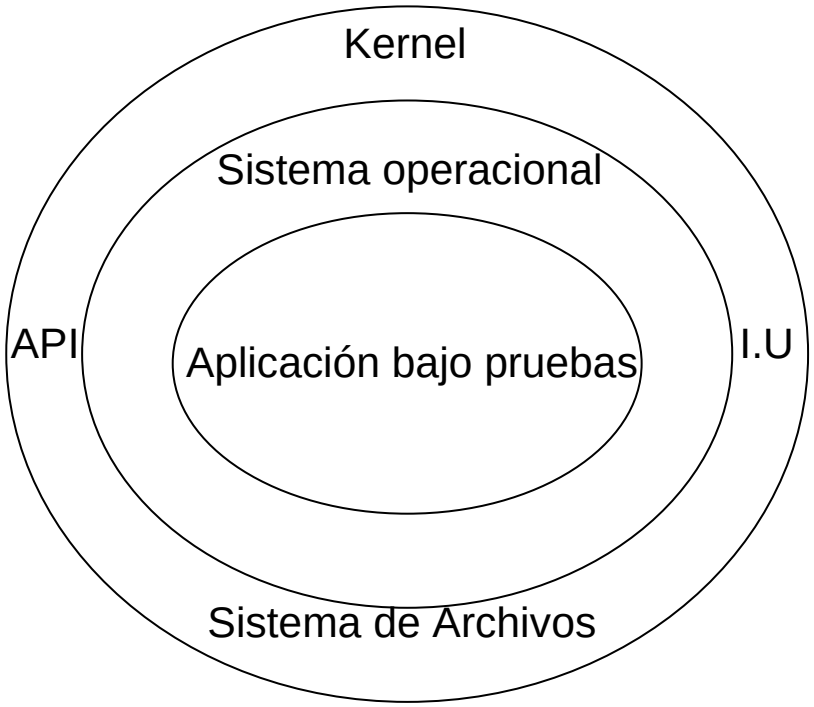
Alternate Data Stream - ADS

Modelo Conceptual de detección y rastreo de técnicas antiforenses – MoDeRaTA

Aplicación de MoDeRaTA – Aplicaciones

- Modelo de fallas en el software
  - La clave del manejo de la inseguridad de una aplicación es mantener información de los usos no documentados por agentes no autorizados
  - Los atacantes puede hacer uso de herramientas de ingeniería reversa (desensambladores) para tratar de inferir el funcionamiento de la aplicación.

Aplicación de MoDeRaTA – Aplicaciones



PLAN DE ATAQUE

¿Qué falla pudo haber causado esta vulnerabilidad?

-Cuando se tiene el código, es viable revisar la implementación del software.

- Cuando no, la ingeniería reversa puede ayudar.

¿Cuáles fueron los síntomas que pudieron haber alertado al ejecutor de las pruebas de la presencia de la vulnerabilidad?

- Las manifestaciones del software ante la presencia de la falla: degradación de la memoria, pérdida de acceso a los archivos, fallas de autenticación con usuarios, etc.

¿Qué técnica de pruebas pudo encontrar esta vulnerabilidad?

-No hay técnica ideal, sólo ideas y sugerencias: revisar dependencias del software y su plataforma, ataques a la interfase de usuario final – I.U, descubrimiento de fallas en el diseño de la aplicación y fallas en la implementación del diseño.

Tomado de: WHITTAKER, J. y THOMPSON, H. (2004) *How to break software security*. Addison Wesley

Modelo Conceptual de detección y rastreo de técnicas antiforenses – MoDeRaTA

Aplicación de MoDeRaTA – Gestión de (In)seguridad

- Taxonomía básica de la inseguridad de la información

  – Políticas, procesos y procedimientos de seguridad de la información que integren de manera sistémica la tecnología, la organización y los individuos.

  – Evidenciar y valorar las relaciones entre los elementos mencionados anteriormente para identificar, administrar la inseguridad propia de la organización.

Aplicación de MoDeRaTA – Gestión de (In)seguridad

Individuo		Tecnología		Procesos		Resultado		Objetivo
Intruso		Dispositivos de Hardware		Vulnerabilidades en la implementación		Interrupción		Fraude
Terrorista	→	Programas o aplicaciones	→	Vulnerabilidades en el diseño	→	Intercepción	→	Acto no intencionado
Delincuente		Manuales o documentación técnica		Vulnerabilidades en la configuración		Modificación		Negación del servicio
Insatisfecho						Fabricación		Destrucción

¿Cuáles son las nuevas consideraciones que debemos tener en cuenta ante esta realidad *antiforense*?

Nuevos cuidados antes de iniciar una investigación

- Fundamentos de las investigaciones en medios informáticos

Tomado de: IEONG, R. (2006) FORZA – Digital forensics investigation framework that incorporate legal issues. *Digital Investigation*. pp 29-36.

Nuevos cuidados antes de iniciar una investigación

- Fundamentos de las investigaciones en medios informáticos:
  - Reconocimiento
    - Utilización exhaustiva de diferentes métodos, prácticas y herramientas que han sido desarrolladas para operar en un ambiente particular para recolectar, recuperar, decodificar, extraer, analizar y convertir datos que serán mantenidos en medios de almacenamiento verificables y accesibles como evidencia.
  - Confiabilidad
    - Mantenimiento de la cadena de custodia durante la extracción, análisis, almacenamiento y transporte de los datos.
  - Relevancia
    - Está relacionada con el peso y la utilidad de la evidencia en el proceso. Si existe una orientación sobre qué se debe recoger durante el proceso, esto puede ayudar a mejorar el esquema de tiempos y costos.

Tomado de: IEONG, R. (2006) FORZA – Digital forensics investigation framework that incorporate legal issues. *Digital Investigation*. pp 29-36.

Nuevos cuidados antes de iniciar una investigación

- Desde el punto de vista legal
  - Motivación
    - ¿Cuál es la norma en cuestión?
    - ¿Es un caso civil o penal?
  - Los atributos de la situación
    - ¿Cuál es la información requerida y relacionada con los hechos?
    - ¿Qué datos deben ser recolectados?
  - Los procedimientos
    - ¿Se requiere una orden judicial?
    - ¿Cuáles son las acciones que deben ser aplicadas para proteger la evidencia?
  - Localización
    - ¿La situación está dentro de la jurisdicción de nuestro país?
  - Las personas
    - ¿Quiénes son las personas involucradas en la situación?
    - ¿Se conoce quién es el asesor legal, el fiscal o asesores que actuarán en el caso?
  - El tiempo
    - ¿Cuáles son los términos de vencimiento? / ¿Cuánto es el espacio de tiempo requerido para investigar el caso?

Tomado de: IEONG, R. (2006) FORZA – Digital forensics investigation framework that incorporate legal issues. *Digital Investigation*. pp 29-36.

Nuevos cuidados antes de iniciar una investigación

- Desde el punto de vista técnico-forense
  - Motivación
    - ¿Cuáles son los objetivos de la investigación?
    - ¿Cuál es el plan que se ha determinado para adelantar la investigación?
  - Los atributos de la situación
    - ¿Cuáles son las hipótesis o móviles de los hechos investigados?
    - ¿Existen políticas de seguridad de la información formales en la organización?
  - Los procedimientos
    - ¿Cuáles son las herramientas forenses a utilizar y la validación de las mismas?
    - ¿Verificación de la aplicación de los procedimientos establecidos para recolectar, recuperar, decodificar, extraer, analizar y convertir datos?
  - Localización
    - ¿Es posible obtener la ubicación del posible atacante?
  - Las personas
    - ¿Es posible identificar al atacante?
    - ¿Se requiere contactar a personal externo como proveedores o consultores para conducir la recolección o análisis de los datos?
  - El tiempo
    - ¿Es posible confirmar el primer momento del ataque? / ¿Es posible tener una línea de tiempo confiable a partir de la evidencia recolectada?

Tomado de: IEONG, R. (2006) FORZA – Digital forensics investigation framework that incorporate legal issues. *Digital Investigation*. pp 29-36.

Nuevos cuidados antes de iniciar una investigación

- Consideraciones para recordar (exigentes)
  - Valide el modelo **MoDeRaTA**, antes de continuar con los procedimientos forenses normales, particularmente en los temas de memoria y procesos
  - Cada vez que se enfrente a un sistema activo, recuerde que habrá una alta posibilidad de "alteración de información" del equipo analizado y por tanto, deberá extremar los cuidados, así como su respectiva documentación.
  - Generar librerías de ataques y sus rastros, como una forma proactiva, para avanzar en los análisis de los casos y su evidencia relacionada.

Nuevas propuestas forenses

- ¿Qué hacer ante la realidad de las técnicas antiforenses? *Algunas ideas en curso…*
  - *Tarjetas físicas (desactivadas) con propósitos forenses que son activadas en el momento del incidente para la recolección de evidencia en sitio.*
  - *Monitoreos y seguimiento de aplicaciones en memoria. Sistemas de alarmas de posibles fallas de funciones.*
  - *Verificación de integridad de archivos activos en memoria.*
  - *Evaluaciones periódicas de la confiabilidad de los procedimientos y las personas de la organización.*

Reflexiones finales

- A *mayor evolución técnica* de los ataques contra las infraestructuras de seguridad, *menor nivel de evidencia* disponible para el análisis.
- *Mientras existan mayores* elementos de gestión de la (in)seguridad informática, *habrá mayores oportunidades* para evidenciar posibles incidentes de seguridad en la organización.
- A *menor visibilidad* de la materialización de los ataques, *mayores los riesgos* contra la relevancia y confiabilidad de las investigaciones forenses en informática.
- A *mayor documentación* de incidentes y sus rastros asociados, *mayor capacidad* de inferencia y análisis del investigador.
- No es posible alcanzar *mayores niveles* de confiabilidad y relevancia en una investigación forense en informática, *sin un adecuado análisis* de técnicas antiforenses en la misma.

Referencias

- WHITTAKER, J. y THOMPSON, H. (2004) *How to break software security*. Addison Wesley
- OPPLEMAN, V., FRIEDRICHS, O. y WATSON, B. (2005) *Extreme exploits. Advanced defenses against hardcore attacks*. McGraw Hill.
- BUTLER, J. y HOGLUND, G. (2006) *Subverting the windows kernel. Rootkits*. Addison Wesley.
- EILAM, E. (2005) *Reversing. Secrets of reverse engineering*. John Wiley & Sons.
- ROSIELLO, A. (2007) Ataques a regiones adyacentes de la memoria. *Hakin9*. No. 22. pp 14-19
- HARRIS, R. (2006) Arriving at an anti-forensics consensus: Examining how to define and control the anti-forensic problem. *Digital Investigation*. pp 44-49.
- IEONG, R. (2006) FORZA – Digital forensics investigation framework that incorporate legal issues. *Digital Investigation*. pp 29-36.
- ALLEN, J.(2005) Information security as an institutional priority. Carnigie Mellon. Presentación Powerpoint. Disponible en: http://www.cert.org/archive/pdf/info-sec-ip.pdf (Consultado: 4/05/2007)
- HONEYNET PROJECT (2004) *Know your enemy. Learning about security threads*. Addison Wesley.
- DAVIS, C., PHILIPP, A. y COWEN, D. (2005) *Hacking Exposed. Computer Forensics*. McGraw-Hill.

Referencias

- KOVACICH, G y BONI, W. (2000) *High-technology crime investigator's handbook. Working in the global information environment*. Butterworth Heinemann.
- PAN, L. y BATTEN, L. (2005) Reproducibility of Digital Evidence in Forensic Investigations. *Proceedings of Digital Forensic Research Workshop 2005*. Disponible en: http://www.dfrws.org/2005/proceedings/pan_reproducibility.pdf (Consultado: 24/03/2007)
- PEIKARI, C y CHUVAKIN, A. (2004) *Security warrior*. O'Reilly.
- SIEFFER, M., FORBE, R., GREEN, C., POPYACK, L. y BLAKE, T. (2004) Stego intrusion detection system. *Proceedings of Digital Forensic Research Workshop 2004*. Disponible en: http://www.dfrws.org/2004/bios/day3/D3-Sieffert-SIDS.pdf (Consultado: 24/03/2007)
- CANO, J. (2007) Inseguridad informática y Computación anti-forense. Dos conceptos emergentes en seguridad informática. Disponible en: http://www.virusprot.com/computaci%F3n-anti-forense.htm (Consultado: 24/03/2007)
- CASEY, E. (2002) Practical approaches to recovering encrypted digital evidence. *Proceedings of Digital Forensic Research Workshop 2005*. Disponible en: http://www.dfrws.org/2002/papers/Papers/Eoghan_Casey.pdf (Consultado: 24/03/2007)
- CASEY, E. (2006) Investigating Sophisticated security breaches. *Communications of ACM*. Vol.49. No.2. Febrero. Pp 48-54. Disponible en: http://www.strozllc.com/docs/pdf/Casey-CACM-Sophisticated-Intruders.pdf (Consultado: 25/03/2007)

Introducción a las técnicas antiforenses

Conceptos e implicaciones para investigadores

VII Jornada Nacional de Seguridad Informática

COMPUTACIÓN FORENSE: RASTREANDO LA INSEGURIDAD INFORMÁTICA

JUNIO 20, 21 Y 22 DE 2007
Biblioteca Luis Ángel Arango
Calle 11 No 4-14
Bogotá D.C., Colombia.

Conferencista:
Jeimy J. Cano, Ph.D, CFE
GECTI-Uniandes
jcano@uniandes.edu.co

ACIS