TECNOLÓGICO DE MONTERREY

Primer ciclo de conferencias de seguridad informática
2-7 abril 2006
FES Acatlán

Ingenieria inversa vs antipirateria

Roberto Gómez Cárdenas

ITESM-CEM

http://webdia.cem.itesm.mx/ac/rogomez

rogomez@itesm.mx

TECNOLÓGICO DE MONTERREY

Para empezar dos preguntas

- ¿Cuánto estamos dispuestos a pagar por un software?
- ¿Cuántos estarían dispuestos a conseguirlo en lugares no recomendados?
- ¿Cuántos bajarían un programa para romper la llave?
- Y la última

¿Cuánto nos gustaría que nos pagaran, si la empresa que creó el software anterior nos contratara?

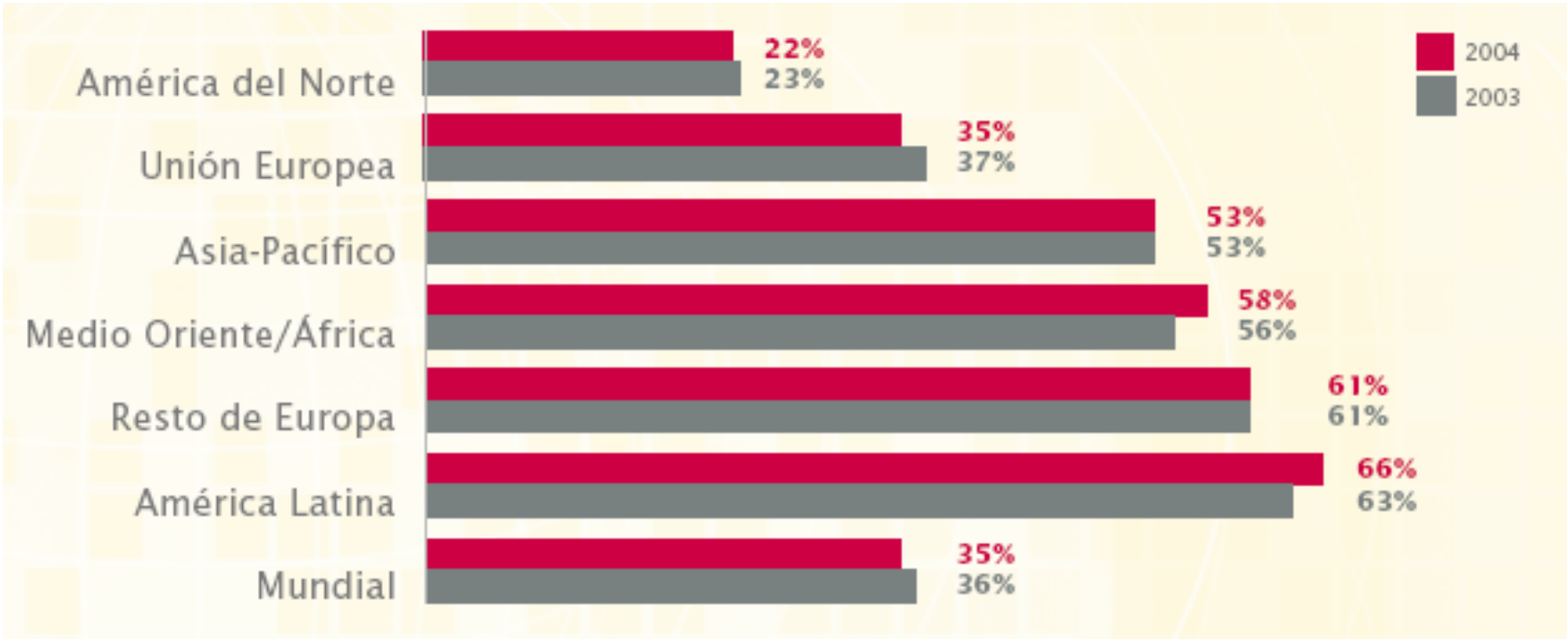
TECNOLÓGICO DE MONTERREY

Algunos números

- 36% por ciento del software que se utiliza en el mundo es ilegal.
- Tasas de piratería disminuyeron en 37 países pero aumentaron en 34 países
- Perdidas por piratería se incrementaron por 29 billones de dolares a 33 billones de dolares
- En 2004 mundo invirtió más de 59 billones en software de PC
  - más que los 51 millones en 2003
  - pero 90 millones se encuentra actualmente instalado
- Business Software Alliance:
  - http://www.bsa.org/mexico

TECNOLÓGICO DE MONTERREY

Tasas de piratería por región



TECNOLÓGICO DE MONTERREY

Clasificaciones de Piratería de Software

20 Países con Tasas de Piratería Más Altas

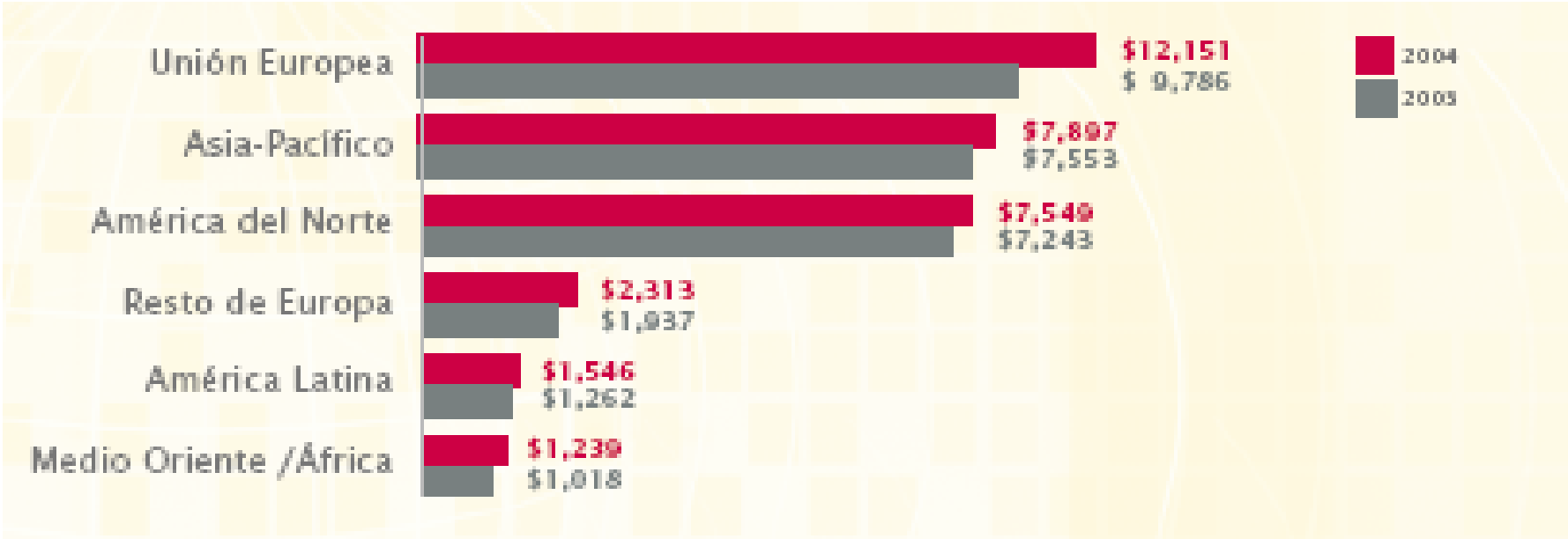
	2004	2003
Vietnam	92%	92%
Ucrania	91%	91%
China	90%	92%
Zimbabwe	90%	87%
Indonesia	87%	88%
Rusia	87%	87%
Nigeria	84%	84%
Túnez	84%	82%
Argelia	83%	84%
Kenia	83%	80%
Paraguay	83%	83%
Pakistán	82%	83%
Bolivia	80%	78%
El Salvador	80%	79%
Nicaragua	80%	79%
Tailandia	79%	80%
Venezuela	79%	72%
Guatemala	78%	77%
República Dominicana	77%	76%
El Líbano	75%	74%

20 Países con Tasas de Piratería Más Bajas

	2004	2003
Estados Unidos	21%	22%
Nueva Zelanda	23%	23%
Austria	25%	27%
Suecia	26%	27%
Reino Unido	27%	29%
Dinamarca	27%	26%
Suiza	28%	31%
Japón	28%	29%
Finlandia	29%	31%
Alemania	29%	30%
Bélgica	29%	29%
Holanda	30%	33%
Noruega	31%	32%
Australia	32%	31%
Israel	33%	35%
Emiratos Árabes Unidos	34%	34%
Canadá	36%	35%
Sudáfrica	37%	36%
Irlanda	38%	41%
Portugal	40%	41%

TECNOLÓGICO DE MONTERREY

Perdidas en dólares por región (millones)



TECNOLÓGICO DE MONTERREY

¿Qué es la ingeniería inversa?

- Metodología para analizar el diseño de un dispositivo o sistema, ya sea para estudiar el diseño o como un pre-requisito para un rediseño.
- Beneficios
  - desarrollar un enfoque sistemático para pensar sobre el diseño de ingeniería de dispositivos y sistemas
  - adquirir un banco de datos de soluciones mecánicas

TECNOLÓGICO DE MONTERREY

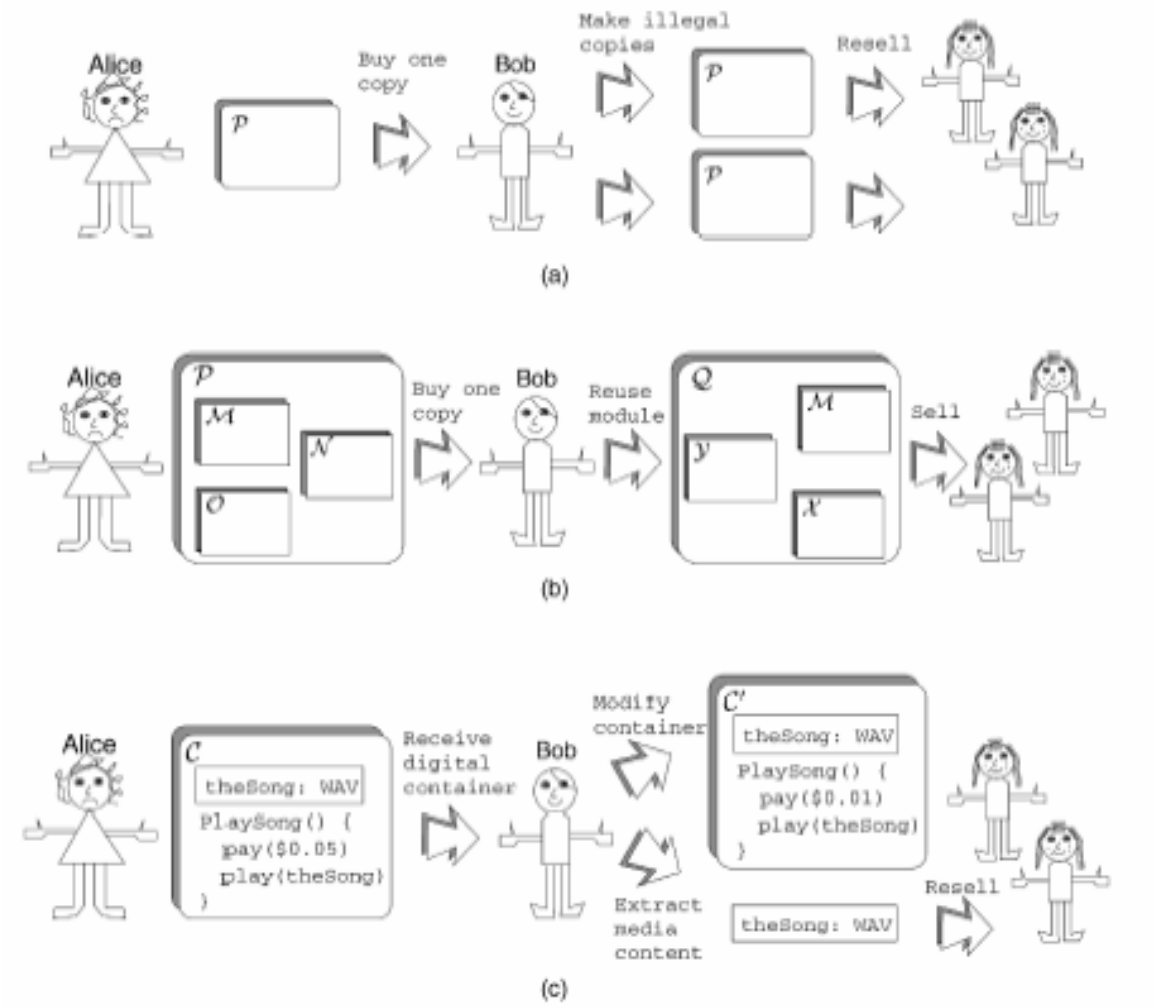
¿Ingeniería inversa o cracking?

- Proceso extraer el código fuente de una aplicación a partir del código objeto
- También llamada decompilación
  - quitar, remover o suspender uno más sistemas de protección de algún software en específico,
- El término cracking también se utiliza también cuando se burla al sistema de protección de algún software en específico para obtener una copia funcional de un software supuestamente protegido.

TECNOLÓGICO DE MONTERREY

Tipos de ataques

- Piratería software
- Ingeniería inversa maliciosa
- Software Tampering



Tomado sin permiso de: Watermarking, Tamper-Proofing, and Obfuscation Tools for Software Protection, Christian S. Collberg

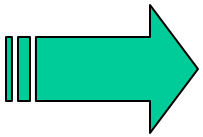
Algunos personajes relacionados

- cracker
  - persona lleva a cabo la ingeniería inversa
- shareware u honorware
  - usuarios envian un donativo a los autores mencionados al principio del programa
  - nag's screen
- wracker
  - programas shareware o freeware
- wares
  - intercambio programas comerciales pirateados

Una madrecita Aprendiendo a "Hackear".

TECNOLÓGICO DE MONTERREY

Un primer ejemplo



TECNOLÓGICO DE MONTERREY

Protegiendo la propiedad intelectual

- ¿Qué puedo hacer para proteger la propiedad intelectual de mis productos?
  - Esteganografia
  - Marcas de agua

TECNOLÓGICO DE MONTERREY

Estegano… que?

- Area similar a la de criptología.
- Viene del griego stegos (ocultar).
- Conjunto de técnicas que nos permiten ocultar o camuflar cualquier tipo de datos, dentro de información considerada como válida.
- La información puede esconderse de cualquier forma
  - diferentes métodos se han ido desarrollando

TECNOLÓGICO DE MONTERREY

Algunos ejemplos históricos

- Herodoto:
  - 440 ac: Aristagoras de Milet usa esclavos calvos para la revuelta contra los persas
  - Demeratus envía mensaje (tablones cubiertos de cera) a Esparta para avisar de que Xerxes (rey de Persa) tenía intenciones de invadir Grecia.

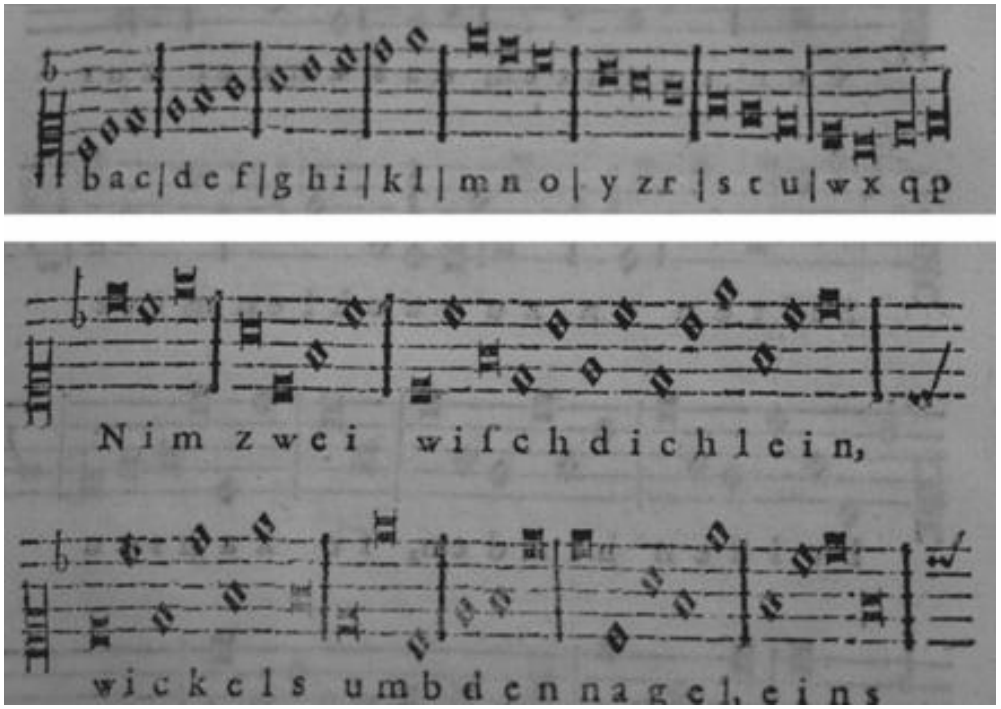
- Tintas invisibles
  - naturales: jugo limón, leche, orina, sal de amoniaco
  - química: alumbre y vinagre, traspasar cáscara huevo duro

- Chinos: texto escrito sobre seda china

TECNOLÓGICO DE MONTERREY

Algunos ejemplos históricos

- Siglo XVII: Schola Steganographica, Gaspar Schott partituras música
- Segunda Guerra mundial:
  - Microfilmes
  - prisioneros usan i, j, t, y f para ocultar mensaje en código morse
  - "Null Cipher"



Un primer ejemplo de Null Cipher

Tomando la primera letra de cada palabra

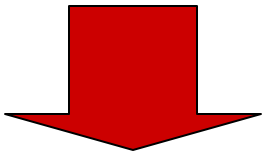
News Eight Weather: Tonight increasing snow. Unexpected precipitation smothers eastern towns. Be extremely cautious and use snowtires especially heading east. The highways are knowingly slippery. Highway evacuation is suspected. Police report emergency situations in downtown ending near Tuesday.

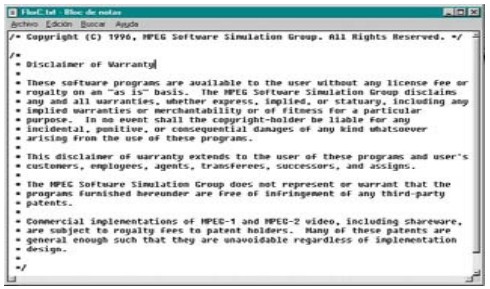
Hidden Information !

Newt is upset because he thinks he is President.

TECNOLÓGICO DE MONTERREY

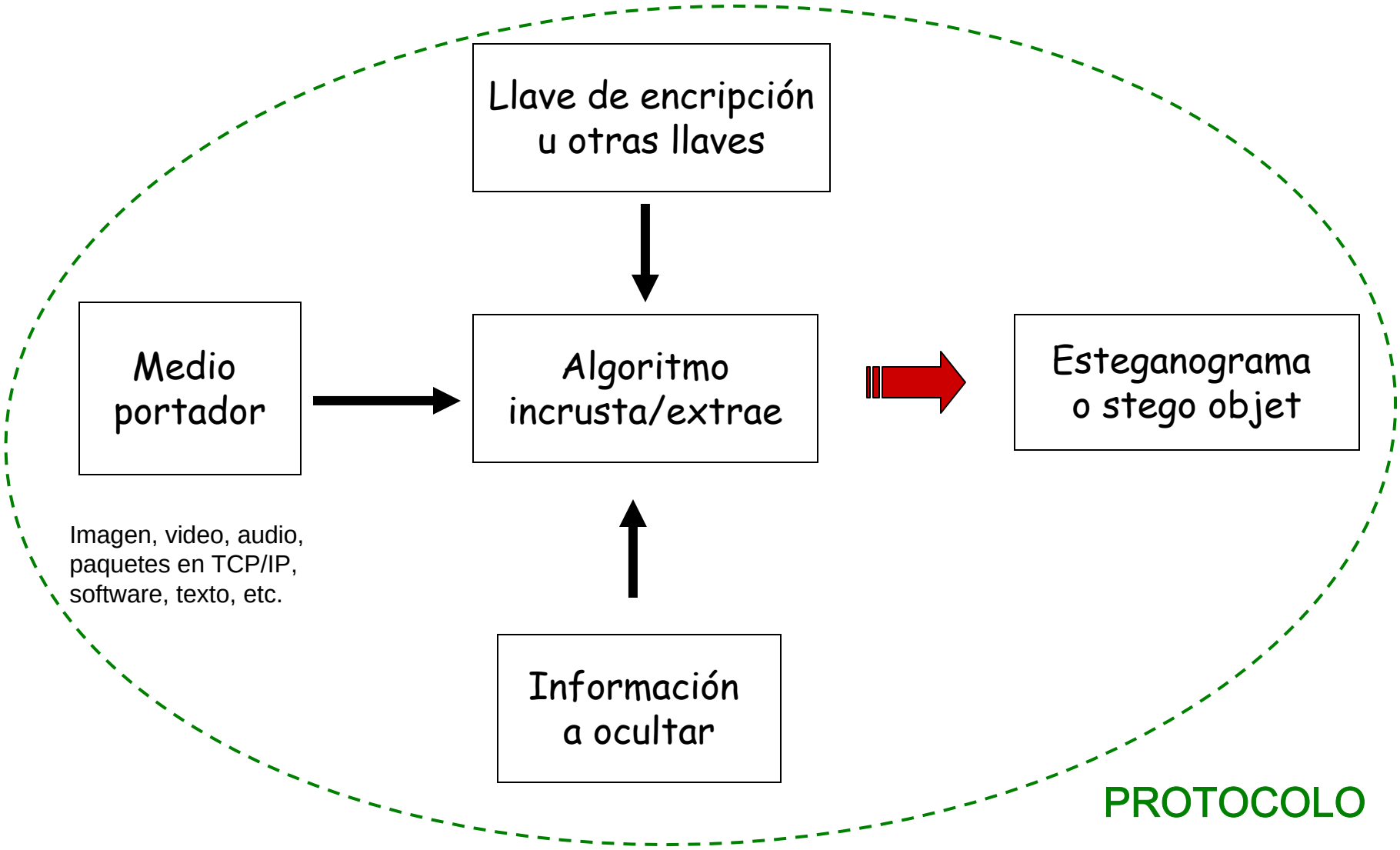
Usando imágenes digitales





TECNOLÓGICO DE MONTERREY

El proceso esteganografico



TECNOLÓGICO DE MONTERREY

¿Puedo insertar código ejecutable?

- Tesis: *Steganographic Computer Warfare*, Cochran J. T., USAF AirForce Institute of Technology, 2000
- Artículo: *A Possibility of Steganographic Trojan Installer*, Prakash; Nagesh; Singhal, 2002
- Conferencia: *Steganographic Trojans*, Rogers M, DefCON 10, 2002
- Virus PERRUN
- Exploit: *Buffer Overrun in JPEG Processing (GDI+)*
- Tesis: *Esteganografía de Código Ejecutable*, Gabriel Ramirez, ITESM-CEM, 2005

TECNOLÓGICO DE MONTERREY

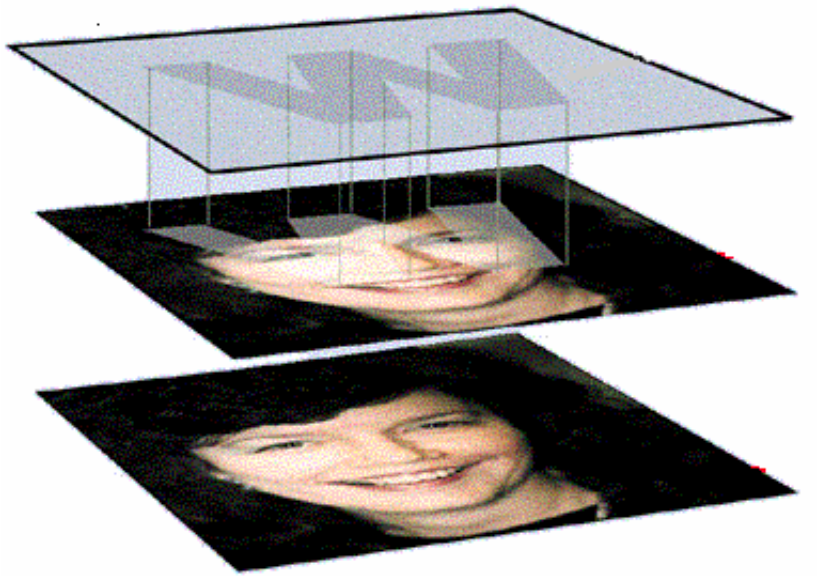
Herramientas esteganográficas

- EZStego
- Gif-It-Up v1.0
- Gifshuffle
- Hide and Seek
- JPEG-JSTEG
- MandelSteg and GIFExtract
- MP3Stego
- Nicetext
- OutGuess
- Pretty Good Envelope
- Publimark
- Stealth
- Snow
- Steganos
- Steghide
- Stegodos
- Stegonosaurus
- StegonoWav
- Stools
- wbStego (Werner Bailer)
- WhiteNoise Storm

Fuente: http://www.petitcolas.net/fabien/steganography/stego_soft.html

Marcas de agua: *watermarking*

- Misma características esteganografía
- Robustez en contra de posibles ataques
  - esteganografia esta relacionada con la detección de un mensaje oculto, mientras que watermarking involucra el borrado/duplicación de un pirata
- Watermarking no siempre necesita estar oculto
- Tipos
  - invisible
  - visible



TECNOLÓGICO DE MONTERREY

Watermarking visible vs invisible


Imagen sin marca

+


Marca de agua

=


Imagen con marca


Imagen sin marca


Imagen con marca


Marca de agua

TECNOLÓGICO DE MONTERREY

Esteganografia vs Watermarking

	Requerimientos	Watermarking		Steganografía
		Privado	Público	
Objetivo	Protección propiedad intelectual	++++		-
	Transmisión mensaje secreto sin despertar sospechas	-		++++
Especificación	Invisibilidad perceptual	++++		+++++
	Invisibilidad estadística o algorítmica	+		+++++
	Robustez contra borrado hostil, destrucción	+++++		-
	Resistencia contra un normal procesamiento de señales	++++		+
	Capaz sobrevivir códigos de compresión	++++		++
	Muy grande sobrecarga	++		++++
Detección/ extracción	Extracción/detección sin el host/objeto de cobertura	-	++++	++++
	Extracción con presencia del objeto/host de cobertura	++++	-	-
	Requerimiento de complejidad baja en extracción/detección	++		+++
	Capacidad opcional de bajado automático del objeto	+		++

Nota: Crucial +++++ Necesario: ++++ Importante +++ Deseable ++ Útil + Innecesario o irrelevante -

TECNOLÓGICO DE MONTERREY

Software watermarking

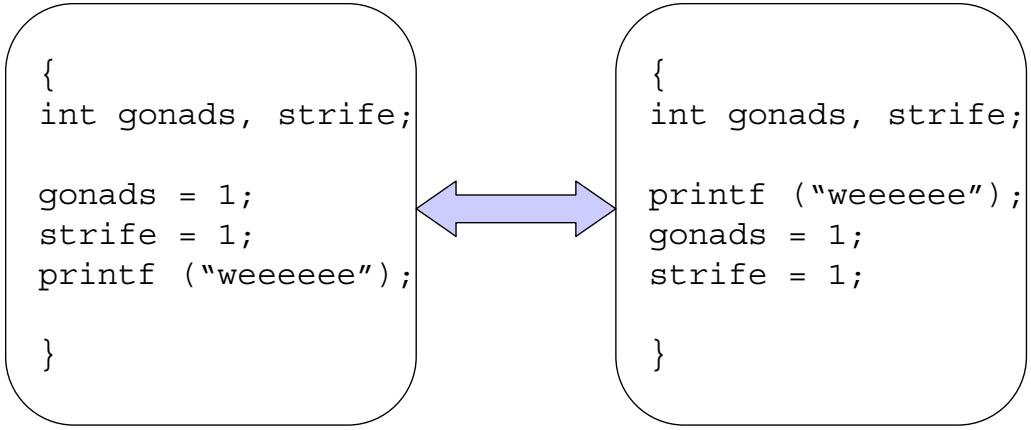
- Objetivo
  - proporcionar de una marca de agua al software
- Consideraciones a tomar en cuenta
  - longitud de la marca con respecto al programa
  - programa distribuido en un tipo de código de máquina virtual o en un código binario sin tipo
  - que tipos de ataques se esperan
  - como generar y distribuir un gran número de huellas únicas para diferentes programas
  - manejo de reporte de errores (bug reports)

TECNOLÓGICO DE MONTERREY

Marcas estáticas de datos

- Usado para protección de software (copyrigtht)
- Incluir la marca como una cadena de caracteres dentro de inicialización de las variables.

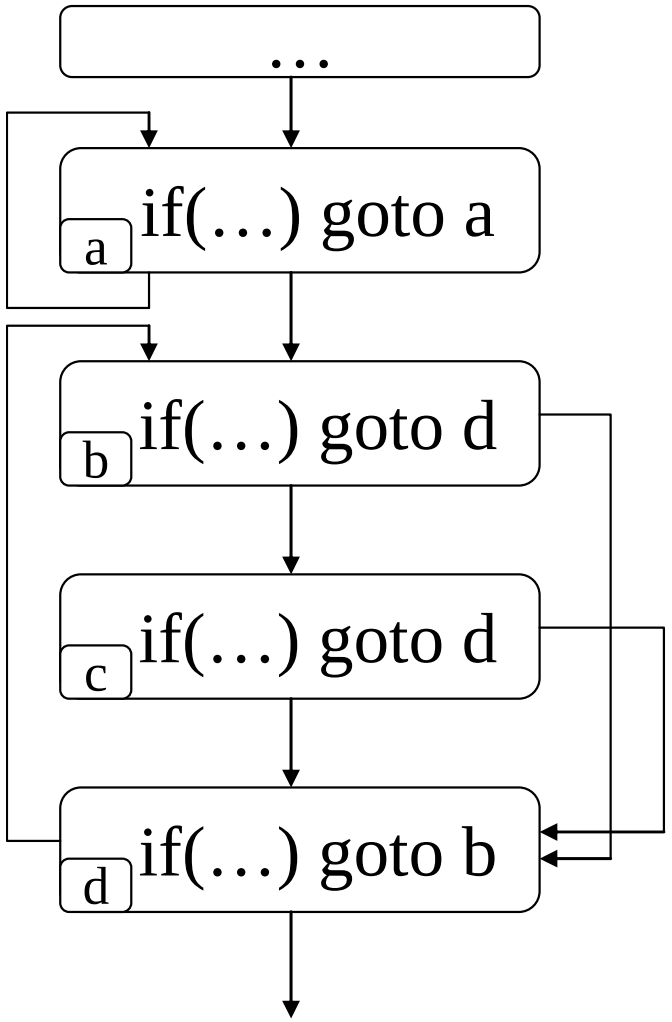
```
char mark[] = “All your base…”
switch (a) {
        case 1: return “are”;
        case 2: return “belong”;
        case 3: return “to us”;
    …
}
```



- Si no hay datos o dependencias de control entre dos enunciados adyacentes son S1 y S2
  - marca puede insertarse dependiendo si S1 y S2 se encuentran en un orden lexicográfico o no.

Secuencia de las gráficas de control

- Un número de software puede ser codificado dentro del bloque de secuencia de un grafo del flujo del programa



TECNOLÓGICO DE MONTERREY

Pros y contras

- Ventajas
  - fácil de implementar

```
> strings /usr/local/bin/netscape | \
     grep -i copyright
Copyright (C) 1995, Thomas G. Lane
```

- Desventajas
  - fácil de romper

TECNOLÓGICO DE MONTERREY

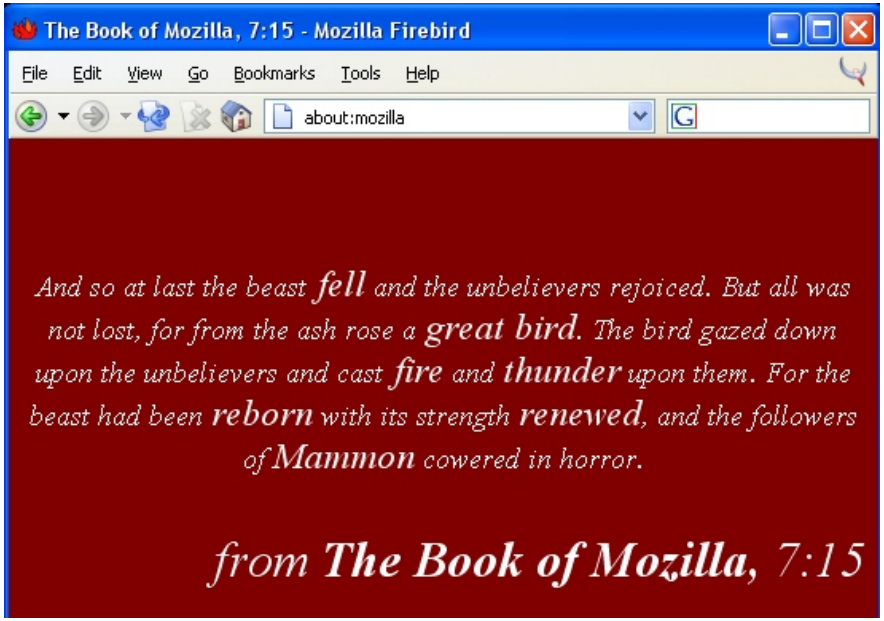
Marcas Dinámicas

- El usuario ejecuta el programa con un conjunto específico de entradas, después de los cuales el programa llega a un estado que representa la marca
- Tipos de marcas
  - marca del “easter egg”
  - estructuras de datos
  - trazado de ejecución

TECNOLÓGICO DE MONTERREY

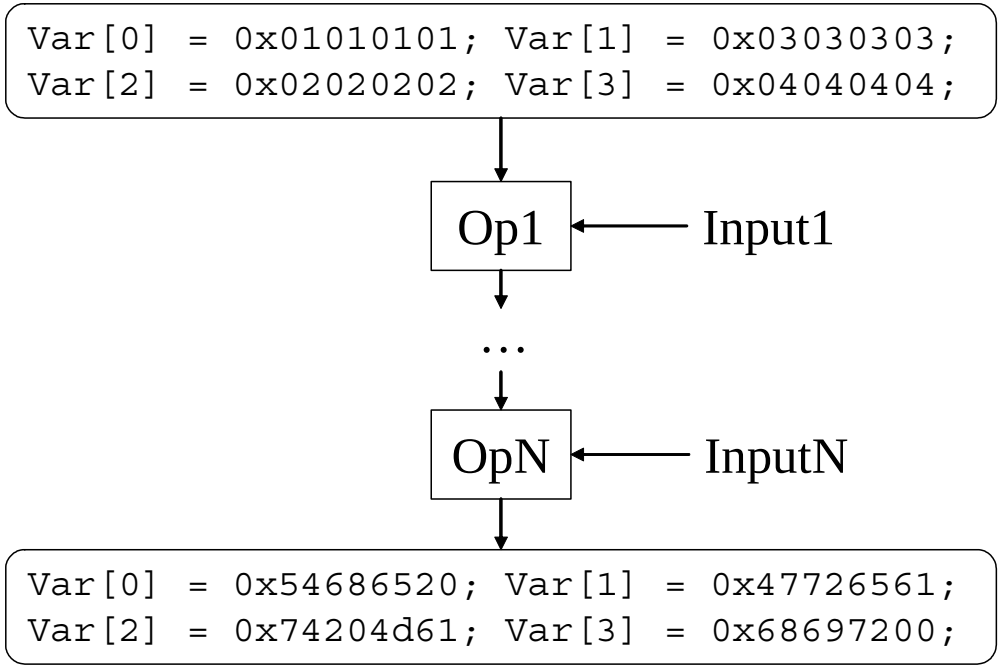
Easter egg

- Parte de código que es activada dada una entrada inusual a la aplicación.
- Característica esencial del easter egg: lleva a cabo alguna acción que es inmediatamente perceptible por el usuario
  - i.e. desplegar el mensaje oculto
- Por ejemplo:
  - entrar al URL about:mozilla en Netscape 4.0 provocará que una imagen aparezca



Ejemplo estructura datos dinámica

- El contenido de una estructura de datos cambia conforme el programa se ejecuta
- El estado final de la estructura representa la marca almacenada



"The Great Mahir"

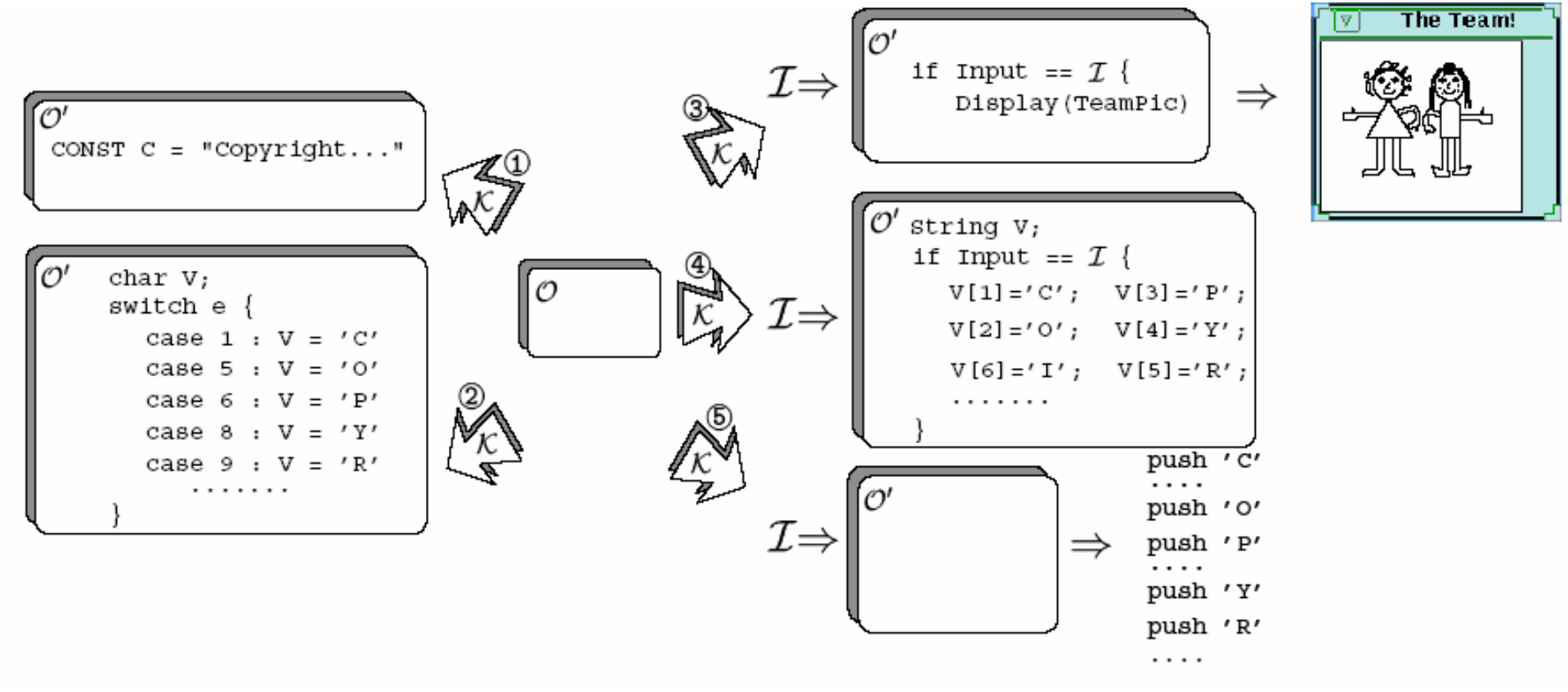
TECNOLÓGICO DE MONTERREY

Ejemplo trazado ejecución dinámico

- Similar al de la estructura de datos.
- La información se oculta dentro del trazo (ya sea instrucciones o direcciones, o ambos) del programas conforme va corriendo de acuerdo a una entrada partícular I
- La información se extrae con el monitoreo de algunas (tal vez estadísticas) propiedades del trazo de direcciones y/o de la secuencia de operadores utilizados

```
80480d3:    85 db              test   %ebx,%ebx
80480d5:    7e 29              jle    0x8048100
80480d7:    83 7d 08 00        cmpl   $0x0,0x8(%ebp)
80480db:    74 23              je     0x8048105
80480dd:    8b 45 08           mov    0x8(%ebp),%eax
80480e0:    a3 40 bc 08 08     mov    %eax,0x808bc40
80480e5:    80 38 00           cmpb   $0x0,(%eax)
                …
                …
8048100:    b8 00 00 00 00     mov    $0x0,%eax
8048105:    85 c0              test   %eax,%eax
8048107:    74 0c              je     0x8048115
8048109:    83 c4 f4           add    $0xfffffff4,%esp
```

Comparación entre las diferentes técnicas



Tomado sin permiso de: Software Watermarking: Models and Dynamic Embeddings, C, Collberg & C Thomborson

TECNOLÓGICO DE MONTERREY

Observaciones

- Marcas de agua:
  - diferenciar un original de una copia
- Protección piratería
  - no solo me interesa diferenciar entre el original y la copia
  - me interesa que no se pueda copiar
- Varios métodos de protección

TECNOLÓGICO DE MONTERREY

Tipos de protección

- Sistemas de protección por tiempo
- Sistemas de protección, CD Checks
  - comprobación del CD original
- Sistemas de protección anti-copia
  - usado en discos y CDs
- Sistemas de protección mediante hardware externo (mochilas)
- Sistemas de protección-defensa mediante comprobación de la integridad de los datos (CRC)
- Sistemas de protección contra banners-nags

TECNOLÓGICO DE MONTERREY

Tipos de protección

- Sistemas de protección mediante desactivación de funciones
- Sistemas de generación mediante generación de números de serie
- Serial Hardcoded
- Generación basada en Name introducido
- Generación con base en ID
- Generación de Serial Encriptado
- Validación de registro
- Validación de Keyfiles

TECNOLÓGICO DE MONTERREY

Herramientas básicas

- Editor hexadecimal
  - Winhex, Hex Workshop, Ultraedit, Hacker's View
- Des-ensamblador
  - IDA, WDasm, Sourcer 7,
- Descompresor
  - Deshrink, PeUNLOCK,
- Depurador
  - Debug, Soft-Ice (El más usado), TR, dbg,
- Analizador de archivos
  - File Monitor
- Dumpeadores de memoria
  - UserModeProcessDumper, Memory Dumper Pro
- Monitor del registro
  - Registry monitor (Win95).

TECNOLÓGICO DE MONTERREY

¿Qué es lo primero que se busca?

- Conocer el tipo de protección
- Lo que se necesita conocer depende del tipo de protección que se esta usando
  - puede ser un sistema de protección combinado
- Una vez detectado el sistema de protección se comprueban las posibles defensas del enemigo
  - Anti-debugging: detección de aplicaciones de depuración
  - Encripción-compresión de datos: ocultan verdadero código hasta que esté en ejecución, inutilizando cualquier intento de desensamblado del código.

TECNOLÓGICO DE MONTERREY

Técnicas para llegar el núcleo de la protección

- A lo retro
- Predicción
- Por referencia a una cadena conocida
- Por búsqueda de cadenas
- Por búsqueda de una secuencia de códigos de operación

A lo retro

- Depurar el programa hacia atrás
- Dejar que el sistema de protección se active y parar la ejecución justo después
  - cuando el software avise con un mensaje de error
- A partir de aquí se depura hacia atrás, examinando el código
  - se busca por un salto que nos aleje o nos aproxime a la función que muestra el mensaje
  - p.e. MessageBoxA, Message Box, DialogBoxParam, DialogBoxParamA

TECNOLÓGICO DE MONTERREY

Predicción

- Cuando se sospecha que una determinada función está siendo usada para el funcionamiento del sistema protección
- Se pone un breakpoint en la función sospechosa
- Cuando se llega a este punto se continúa depurando hasta llegar al punto clave
- Muy usado cuando se quiere buscar la función que pinta un banner o una pantalla nag de inicio, o cuando se conoce el sistema de protección que esta usando el enemigo

TECNOLÓGICO DE MONTERREY

Por referencia a una cadena conocida

- Método usado cuando el sistema de protección muestra un mensaje de error,
- Copiar el mensaje de error
- Desensamblar
- Buscar cadena en la lista de referencias a cadenas.
- Apuntar direcciones donde hay una posible referencia y examinar el código que hay alrededor.
  - se busca un salto que los aleje de la referencia dicha cadena
- Se examinan las llamadas previas al salto
  - estas pueden ser las llamadas de verificación

TECNOLÓGICO DE MONTERREY

Por búsqueda de cadenas

- Usado cuando se sospecha que una determinada cadena de caracteres está siendo utilizada y no se encuentra donde debería estar por el método de referencias.
- Se busca con un editor hexadecimal en el archivo que se sospecha contiene la cadena o se busca la cadena en memoria una vez ejecutado el programa.
- Si se encuentra en memoria se pone una instrucción para interrumpir al programa antes de realizar cualquier cálculo en ella.

Búsqueda secuencia códigos operación

- Se sospecha que una determinada secuencia de órdenes en ensamblador está siendo usada por el sistema de protección y/o defensa.
- Una vez que se cuenta con la cadena secuencia de códigos-bytes a buscar se realiza su búsqueda con el editor hexadecimal y se opera según sea el caso.
- Muy usada para la detección de trucos antidebbugging

TECNOLÓGICO DE MONTERREY

Sistema protección límite tiempo

- Pueden operar de las siguientes formas
  - Software comprueba si han transcurrido n días desde la instalación del mismo
    - procede a la salida inmediata o a su des-instalación
    - puede mostrar mensaje informando al usuario
  - software comprueba si se ha llegado a una fecha límite
    - software no funcionará si se vuelve a instalar
- Dándole la vuelta
  - se almacena la fecha de instalación en algún lugar
  - sistema debe comprobar la fecha actual y hacer los cálculos correspondiente

TECNOLÓGICO DE MONTERREY

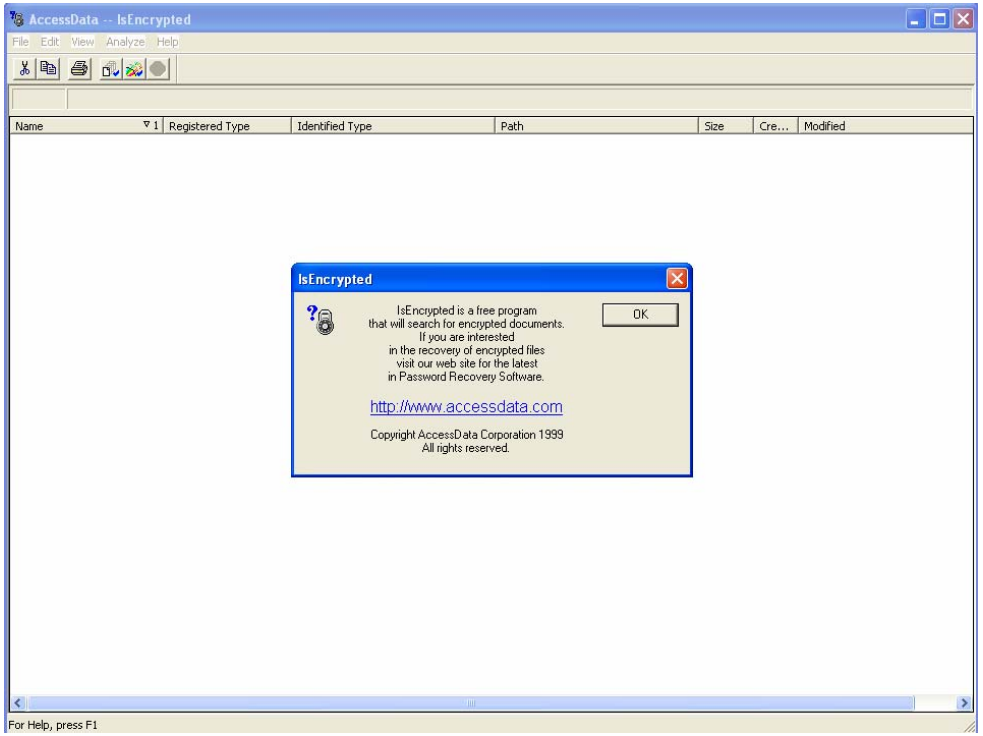
Técnicas banners y pantallas nags

- No son propiamente un sistema de protección
- Mensajes que recuerdan a los usuarios que adquiera el programa original
- Utilizados mucho en programas de visualización o de retoque de fotografías
  - se trata de textos o imágenes que tapan parcialmente el trabajo que se está viendo o haciendo, impidiendo su “correcta” visualizacón
- Los nags son pantallas o cuadros de diálogo que aparecen al inicio o al final de la aplicación
  - activos hasta que usuario presiona un determinado botón

Atacando a los nags

- Identificar el tipo de nag
  - es un cuadro de dialogo
  - es un cuadro de mensaje
- Examinar el estilo del nag
  - dos o menos botones: cuadro mensaje
  - no botones o más de dos: cuadro de diálogo
- Puede anticiparse a la creación del cuadro de diálogo-mensaje poniendo un breakpoint en las funciones usadas para crear un cuadro de diálogo
  - CreateDialogIndirectParamA, DialogBox, EndDialog

Ejemplos nag



TECNOLÓGICO DE MONTERREY

Protección de CDs

- Protección pasiva
  - diferencias entre la forma en que los tocadores de CD leen discos y la forma en que las computadoras leen discos
  - insertar “algo” en el disco de tal forma que las computadoras se confundan sin afectar a los tocadores
- Protección activa
  - permite computadora lee todos los archivos del CD
  - instala software que afecta todos intentos de lectura del disco
  - p.e. XCP (eXtended Copy Protection) y MediaMax

TECNOLÓGICO DE MONTERREY

Logos protección CDs

- Industria musical utiliza logos especiales para reconocer CDs que contienen protecciones contra copia

logo general que indica que el CD cuenta con una protección contra copia

logo establece que puede ser tocado en la mayoría de los cd/dvd pero no en una computadora

cd puede ser ejecutado en una computaora personal pero no puede ser copiado

TECNOLÓGICO DE MONTERREY

Detalles XCP y MediaMax

- Instala programa activo anti-copia
  - también instala un segundo componente que esconde la existencia del software
- Normalmente programas y dato no deben ser invisibles
  - particularmente a administradores de sistemas
  - pueden esconderse para simplificar el uso a los usuarios
  - comportamiento virus, spyware y rootkits
  - CD es insertado en una máquina Windows, el disco usa la opción de autorun para cargar en memoria la protección activa para interferir en la lectura del disco

Lo malo

- Software diseñado para resistir detección y borrado
  - se cargar sin des-instalador
- Sistema contacta el sitio Web de un vendedor cuando el usuario inserta un disco protegido
  - objetivo: bajar imágenes y publicidad mientras se toca la música
  - también crea en el servidor anotando dirección IP, el disco insertado así como tiempo y hora en que fue insertado
- Sitios Web aseguraron que nunca recopilaron información de las actividades de los usuarios

TECNOLÓGICO DE MONTERREY

La reacción de las compañías

- Revelación de spyware llega al público
- Compañía disquera recopila discos cambiándolos por discos “normales”
  - también deciden proporcionar des-instaladores
  - des-instaladores abren huecos seguridad
- Programas des-instalación se entregan vía ActiveX
  - programas destinados a embeberse en una página Web
  - página Web invoca el des-instalador
  - le pasa un URL a partir del cual baja el código del des-instalador
  - el controlador baja código del URL y lo ejecuta

TECNOLÓGICO DE MONTERREY

Pasando de lo malo a lo peor

- Ningún control X verifica si se le pasa un URL correcto o código aprobado
- Controles programados para bajar y ejecutar código de cualquier URL que recibieran
- Resultado
  - un servidor Web malicioso puede incluir un ActiveX del vendedor
  - este ActiveX puede bajar y correr código de un sitio malicioso
- Lo peor
  - los des-instaladores no borran el ActiveX, sino que lo dejan en la computadora del usuario

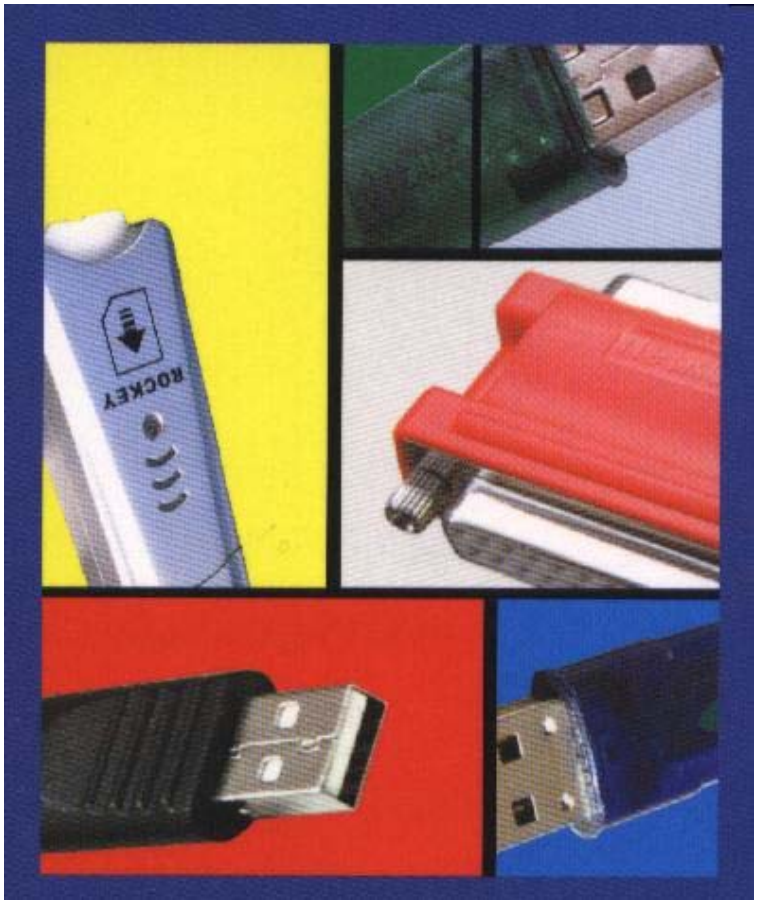
TECNOLÓGICO DE MONTERREY

Llaves físicas (dongles)

- Dongles = mochilas
- Una mochila no es más que una caja que contiene un circuito que puede variar en complejidad según el tipo de mochila.
- Algunas mochilas cuentan con memoria
  - unos pocos bytes
  - se almacenan datos usados por la propia mochila
- Mochilas más usadas
  - Sentinel Pro de Rainbow Technologies
  - HASP de Alladinn Systems

TECNOLÓGICO DE MONTERREY

Ejemplos mochilas



TECNOLÓGICO DE MONTERREY

¿Cómo funciona?

- Software a proteger se comunica con la mochila a través de rutinas que proporciona el fabricante.
- La protección depende de la habilidad del programador de implementar la protección
- Sugerencias
  - Mandar llamar a la mochila en varios lugares del programa
  - Mandar llamar a la mochila en intervalos de tiempo en el programa
  - Encriptar la llamada a la mochila
  - Obtener la huella del código que lleva a cabo la mochila

TECNOLÓGICO DE MONTERREY

Protección por empaquetados

- Autores software empaquetan sus programas
  - reducir el tamaño de los archivos del programa
  - complicar el trabajo de ingeniería inversa, ya que no se puede obtener un desensamblado exacto del archivo
- El programa original esta envuelto dentro del código del empaquetador, el cual esconde el código original
- Cuando se ejecuta el programa, se esta ejecutando en primer lugar el código empaquetador.
  - desempaqueta aplicación original en memoria
- Ejemplo: ASprotec, Aspack Armadillo, upx, etc

TECNOLÓGICO DE MONTERREY

Protección por CRC

- CRC= Código Redundancia Cíclica
- Detección de errores en la transmisión de datos en comunicaciones.
- Dispositivo calcula el CRC en base a un polinomio y envía información junto con su CRC
- Extremo recepción usa mismo polinomio para calcular el CRC de lo recibido y compara resultado.
  - si son iguales se ha transmitido con éxito
- Detección de que algún dato fue cambiado
- Posible usar huellas digitales

TECNOLÓGICO DE MONTERREY

Generación números serie

- Serial único (hardcoded)
  - peor de las protecciones
  - con desensamblar el ejecutable de la aplicación y viendo los strings se puede encontrar el serial
- Basada en serial creado con base en ID
  - se obtiene el serial en base a algún elemento del sistema huésped, p.e. número seria disco duro
  - dependiendo del método será la máquina donde pueda ser ejecutado
  - analizar el código de generación del ID y el serial para crear un generador de llave

Generación números serie

- Basada en serial encriptado
  - el número de serie se encripta con algún procedimiento de encripción
  - analizar el código para saber como encripta y saber como des-encriptarlo
  - ejemplo, el serial se puede generar de la siguiente forma:

a=+	c=%	e=!
b=%	d=@	f=*

TECNOLÓGICO DE MONTERREY

Conclusiones

- La ingeniería inversa no solo tiene su aplicación en el “lado obscuro de la fuerza”
- Posible aplicarlos para entender como funcionan virus computacionales y gusanos
  - desarrollar vacunas y protecciones
- Buen ejercicio para comprender diferentes áreas de la informática
  - http://crackmes.iespana.es
- Es importante conocer como funcionan los ataques para aprender a defendernos.
- No existe seguridad al 100%

Referencias

- Seguridad en software, Profesor X, Revista Conthackto, No 2, noviembre/diciembre 2005
- Digital Rigths Management, Spyware and Security, E.W. Felten and J. A. Halderman, IEEE Security & Privacy, Vol.4 No. 1, January/February 2006
- Electronic Frontier Foundation's Sony BMG Settlement FAQ
  - www.ef.org/IP/DRM/Sony-BMG/settlement_faq.php
- Armouring the ELF: Binary encryption on the UNIX platform, grugp, scut, Phrack Magazine
  - www.phrack.org

TECNOLÓGICO DE MONTERREY

Referencias

- Information Hiding, Steganography and Watermarking N. Johnson, Z Duric and S Jajodia, Kluder Academic Publishers, 2001
- Disappearing Cryptography, Peter Wayner, Ed. Morgan Kaufmann; 2da. edición, 2002
- Cracking sin secretos, Ataque y defensa de software, J. Zemánek, Ed. Alfaomega, 2005
- Hacker Disassembling Uncovered, K. Kaspersky, Ed. Alist, 2003
- Reversing, Secrets of Reverse Engineering, Eldad Eilam, Ed. Wiley Publishing, 2005

TECNOLÓGICO DE MONTERREY

Primer ciclo de conferencias de seguridad informática
2-7 abril 2006
FES Acatlán

Ingenieria inversa vs antipirateria

Roberto Gómez Cárdenas

ITESM-CEM

http://webdia.cem.itesm.mx/ac/rogomez

rogomez@itesm.mx