

## Inseguridad en Software e Ingeniería Inversa

Federico G. Pacheco  
Training Manager X-Lambda

Héctor R. Jara  
IT Manager X-Lambda

## Temario

- Introducción
- Seguridad del software
  - Algunos problemas del software
  - Programación segura
- Ingeniería Inversa
  - Protecciones
  - Herramientas
- Demostración 1 – Herramientas
- Demostración 2 – Caso de estudio
- Discusiones

## Introducción

- Alcances de la charla
  - Los NO
    - NO se pretende enseñar a crackear
    - NO se quiere hacer apología de la ilegalidad
    - El instructor NO es cracker
  - Los SI
    - SI se pretende dar una visión global de los problemas relacionados a la seguridad del software
    - SI se pretende demostrar prácticamente algunas técnicas y herramientas de ingeniería inversa
    - SI se pretende dar un panorama sobre los métodos de protección de software e ingeniería inversa

## Algunos problemas del software

- Vulnerabilidades
  - En sistemas operativos
  - En aplicaciones
- Piratería
  - Distribución y copias ilegales
  - Desprotección del software

## Algunas soluciones técnicas

- A las vulnerabilidades
  - Entornos de ejecución seguros
  - Programación segura
- A la piratería
  - Aumentar las protecciones ☹
  - Utilizar software libre ☺

## Programación segura

- ¿Por que hay código inseguro?
  - Los programadores son humanos y los humanos se equivocan
  - No se acostumbra a hacer foco cuando se enseña
  - Los lenguajes en sí contienen elementos inseguros (funciones, librerías)
  - La mayoría de los programadores no son expertos en seguridad
  - La mayoría de los expertos en seguridad no son programadores
  - Así como existen malos amigos existen malos programadores
  - La programación segura cuesta mas dinero, esfuerzo y tiempo de desarrollo.
  - La auditoria de código es muy costosa

## Programación segura

- Errores propios de la programación
  - Falta de validación de parámetros y buffers
  - Armado de algoritmos ineficientes
  - Errores desapercibidos en la sintaxis y uso del lenguaje
  - Omitir el concepto del mínimo privilegio

## Ingeniería Inversa

- Proceso de aislar y analizar con detalle una obra de ingeniería con el objeto de obtener información relevante acerca de su diseño, implementación y funcionamiento.
  - No es ilegal, es una herramienta
  - Se aprovecha en muchos ámbitos
  - Tiene usos científicos
  - No es solo aplicable al software

## Ingeniería Inversa de Software

- Aplicación de técnicas de Ing. Inversa para obtener o modificar un comportamiento específico de un programa.
- Objetivo
  - Uso de programas protegidos (cracking)
  - Alteración de funciones (crack-modding)
  - Adaptación de programas

## Un poco de teoría ...

- Un programa puede estar escrito en algún lenguaje de programación (pascal, c, delphi, visual basic...)
- Cuando los compilamos y los hacemos ejecutables para poder usarlos, el compilador interpreta las instrucciones y las pasa a un lenguaje universal: el lenguaje ensamblador (Assembler, ASM)
- Este ASM, que tiene sus propias instrucciones, se traduce a su vez en códigos binarios que interpreta la CPU y se ejecutan en un equipo

## Algunos tipos de protecciones

- Tiempo de uso limitado
- Cantidad de ejecuciones limitadas
- Número de serie (propios o dinámicos)
- Mensajes molestos y/o nags
- Funciones deshabilitadas
- CD-ROM Ausente
- Archivos llave
- Antidebugging, Obfuscation
- Ejecutable comprimido y/o encriptado
- Protecciones por hardware
- Protecciones comerciales

## Algunas Herramientas

- Debugger (Ej: SoftICE, TRW2000, OllyDBG)
- Desensamblador (Ej: W32Asm, IdaPro.)
- Editor Hexadecimal (Ej: UltraEdit, Hview, HexWorkshop)
- Monitor de Archivos (Ej: FileMon)
- Monitor de Registro (Ej: RegMon)
- Monitor de Funciones API (Ej: APIS32)
- Descompresor (Ej: ProcDump)
- Patchers
- Utilidades varias (Resource Tools, PE Tools, etc.)

## Antidebugging

- Verificación de tiempo de ejecución
- Verificar flags del CPU (Trap Flag)
- Manipulación del stack
- Modificación del código
- Alterando las interrupciones

## Compresores de Ejecutables

- Devuelven un ejecutable comprimido pero totalmente funcional que se ejecutan en memoria sin necesidad de crear otro archivo adicional
- Usos:
  - Esconder virus reconocidos: el archivo resultante varía respecto al original que detectan los antivirus
  - Optimizar los ejecutables que devuelven los compiladores de alto nivel

## Encriptadores Comerciales

Nombre	Version	Autor	Link
EXECryptor	2.1.20	StrongBit	<a href="http://www.strongbit.com/">http://www.strongbit.com/</a>
Obsidium	1.25	Obsidium Software	<a href="http://www.obsidium.de/">http://www.obsidium.de/</a>
UltraProtect	1.35 (2004)	Risco Software	<a href="http://www.ultraprotect.com/">http://www.ultraprotect.com/</a>
Armadillo	4.05	Silicon Realms Toolworks	<a href="http://www.siliconrealms.com/">http://www.siliconrealms.com/</a>
ASProtect	1.34	Solodovnikov Alexey	<a href="http://www.aspack.com">http://www.aspack.com</a>
Themida	1.0.0.5	Rafael Ahucha & Sergio Lara	<a href="http://www.xprotector.com">http://www.xprotector.com</a>
Code-Lock	2.35	RTSoft	<a href="http://www.rtsoftware.org">http://www.rtsoftware.org</a>
EXE Stealth	3.04	WebtoolMaster	<a href="http://www.webtoolmaster.com">http://www.webtoolmaster.com</a>

## Encriptadores Freeware ☺

Nombre	Version	Autor	Link
[MSLRH]	0.32	emadicius	<a href="http://www.emadicius.tk/">http://www.emadicius.tk/</a>
Arm Protector	0.3	SMoKE	<a href="http://protocols.reverse-engineering.net/files/packer/s/armp.zip">http://protocols.reverse-engineering.net/files/packer/s/armp.zip</a>
PESpin	1.1	cyberbob	<a href="http://pespin.w.interia.pl/">http://pespin.w.interia.pl/</a>
yoda's Protector	1.03.2.02	yoda & Ashkbiz Danehkar	<a href="http://yodap.cjb.net/">http://yodap.cjb.net/</a>
yoda's Crypter	1.2	yoda.	<a href="http://protocols.reverse-engineering.net/files/packer/s/yc.zip">http://protocols.reverse-engineering.net/files/packer/s/yc.zip</a>

## Compresores Comerciales

Nombre	Version	Autor	Link
eXPressor	1.2.0.1	CGSoftLabs	<a href="http://www.softpedia.com/get/Programming/Packers-Crypters-Protectors/eXPressor.shtml">http://www.softpedia.com/get/Programming/Packers-Crypters-Protectors/eXPressor.shtml</a>
Thinstall	2.526	Jonathan Clark	<a href="http://thinstall.com/">http://thinstall.com/</a>
Petite (shareware)	2.3	Ian Luck	<a href="http://www.un4seen.com/petite">http://www.un4seen.com/petite</a>
PECompact	2.5	DevelTek	<a href="http://www.sharewareplaza.com/">http://www.sharewareplaza.com/</a>
PEBundle	3.20	Jeremy Collake	<a href="http://www.softpedia.com/get/Programming/Packers-Crypters-Protectors/PEBundle.shtml">http://www.softpedia.com/get/Programming/Packers-Crypters-Protectors/PEBundle.shtml</a>

## Compresores Freeware ☺

Nombre	Version	Autor	Link
Upack	0.25	Dwing	<a href="http://dwing.go.nease.net/">http://dwing.go.nease.net/</a>
Mew	11 SE 1.2	Northfox	<a href="http://northfox.uw.hu/">http://northfox.uw.hu/</a>
UPX	1.25	Laszlo & Markus	<a href="http://upx.sourceforge.net/">http://upx.sourceforge.net/</a>
Packman	0.0.0.1	bubba.	<a href="http://packman.cjb.net/">http://packman.cjb.net/</a>
exe32pack	1.42	SteelBytes	<a href="http://www.steelbytes.com">http://www.steelbytes.com</a>
Dropper	2.0	Gem	<a href="http://gem.intro.hu/">http://gem.intro.hu/</a>
FSG	2.0	Bart	<a href="http://protocols.reverse-engineering.net/">http://protocols.reverse-engineering.net/</a>

## Paranoia: Mas protecciones!!!

- Parallel Keys
- USB Keys
- PCI Card Keys



## Protecciones para medios físicos

- Data CD Protections
- Audio CD Protections
- DVD Protections
- Técnicas de protección:
  - Commercial Protections
  - CD-Checks
  - Dummy Files
  - Illegal TOC
  - OverSize/OverBurn the CD
  - Physical Errors

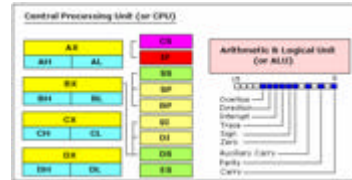
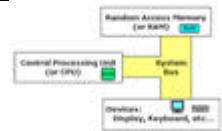
## Antes de comenzar una práctica ...

- Obtener las herramientas
- Introducirse en ASM
- Practicar con "crackmes"
- Leer tutoriales!!!

## Arquitectura 8086

### REGISTROS DE PROPOSITO GENERAL

- AX - the accumulator register (AH / AL).
- BX - the base address register (BH / BL).
- CX - the count register (CH / CL).
- DX - the data register (DH / DL).
- SI - source index register.
- DI - destination index register.
- BP - base pointer.
- SP - stack pointer.



## Arquitectura 8086

- REGISTROS DE SEGMENTO
  - CS – apunta al segmento que contiene el programa actual
  - DS – apunta al segmento donde se definen las variables
  - ES - extra segment register, a definir por el programador
  - SS – apunta al segmento del stack
- REGISTROS DE PROPOSITOS ESPECIALES
  - IP - instruction pointer, puntero a las instrucciones
  - Flags Register – estado actual del procesador

## Ejemplos de instrucciones ASM

90		nop	no operation
	EB	jmp	jump directly to
0F83	73	jae	jump if above or equal
0F84	74	je	jump if equal
0F84	74	jz	jump if zero
0F85	75	jne	jump if not equal
0F85	75	jnz	jump if not zero

LAIIBDA  
Tecnología y Capacitación

## Demostración 1 - Herramientas

- Herramientas típicas (Freeware)
  - Debugger: OIlyDBG
  - Dissassembler: Win32Dasm
  - Hex Editor: Hackman
  - Resourcer: Resource Hacker
  - PE: PE Tools, PEid
  - Varios (Patchers, Dumpers)
- Ayudas
  - Intel OPCODEs
  - Win32 APIs
  - ASCII Data

LAIIBDA  
Tecnología y Capacitación

## Demostración 2 - Caso de estudio

- Archivo del tipo "crackme"
- Uso de debugger OIlyDBG
- Protección por serial
  - Registración por método drástico
  - Registración por generación de clave
- Creación de Loader
- Patcheo de ejecutable

LAIIBDA  
Tecnología y Capacitación

## Realidad Actual

- Crackear es considerado ilegal
- Los crackers son perseguidos
- Los sitios duran poco online
- La información está muy desactualizada
- A pesar de esto, diariamente aparecen cracks => Los creadores trabajan desde la oscuridad.

LAIIBDA  
Tecnología y Capacitación

## ¿A quién pertenece el conocimiento?

LIBERTAD DE LA INFORMACION  
↓  
Caso particular: *Tecnología libre*  
↓  
Caso particular: *Software Libre*  
↓  
Caso particular: *GNU/Linux*

LAIIBDA  
Tecnología y Capacitación

## ¿Y las grandes empresas ...?

- Noviembre de 2004
  - "Microsoft ha usado una copia crackeada del programa SoundForge 4.5 para la edición de archivos wav que vienen incluidos de serie con el Windows Media Player."
- Fuentes:
  - Slashdot, Barrapunto, Tomshardware, Pcwelt.

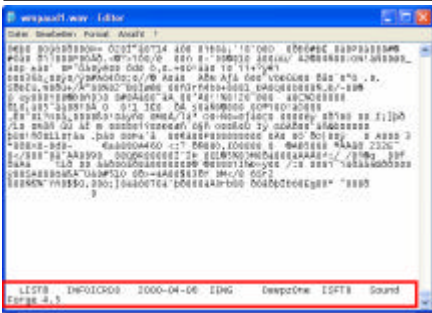
LAIIBDA  
Tecnología y Capacitación

## ¿Y las grandes empresas ...?



C:\WINDOWS\Help\Tours\WindowsMediaPlayer\Audio\Wav

## ¿Y las grandes empresas ...?



## Muchas gracias

Federico G. Pacheco  
Training Manager  
federicop@x-lambda.com.ar

Héctor R. Jara  
IT Manager X-Lambda  
hectorj@x-lambda.com.ar

X-Lambda – Tecnología y Capacitación