Hacking .NET Applications: The Black Arts

Jon McCoy
www.DigitalBodyGuard.com
TOPICS

- How-To Attack .NET Applications
- Tools and Methodology of Attacking
- Overcome “secure” .NET Applications
- Building KeyGen/Crack/Hacks/Malware
- Reverse Engineering for Protection
Attacking/Cracking

IN MEM

|||

ON DISK
ATTACK OVERVIEW

Attack on Disk
- Access Logic
- Infect Logic
- Hook Logic
- Decompile
- Recompile
- Debug

Attack in Memory/Runtime
- Injecting Structure
- Navigating Structure
- Editing/Controlling Structure
ATTACKING .NET APPLICATIONS: AT RUNTIME
ATTACKING ON DISK
DEMO
GrayWolf – IL_Spy – Reflector
101 - Recon
Windows Media Center

Core File Location
C:\Windows\ehome\ehshell.dll

StrongName KEY
d:\w7rtm.public.x86fre\internal\strongnamekeys\fake\windows.snk

Registry  CurrentUser OR LocalMachine
SOFTWARE\Microsoft\Windows\CurrentVersion\Media Center\

Web Host Address
www.microsoft.com/WindowsMedia/Services/2003/10/10/movie
101 - ATTACK ON DISK

Connect/Open - Access Code

- Decompile - Get code/tech
- Infect - Change the target's code
- Exploit - Take advantage
- Remold Application - WIN
THE WEAK SPOTS

Flip The Checks
Cut The Logic
Controlling Objects
Accessing Value
Set Value is “True”
SET VALUE TO "TRUE"

```cpp
bool Registered = false;
```

```cpp
if (a != b)
```

```cpp
if (a == b)
```
IL – Intermediate Language
Code of the Matrix |||| NEW ASM
REGISTRATION CHECK

- KeyGens
- Cracks
IT CAN’T BE THAT EZ

NO

What can stop this!!
IT CAN'T BE THAT EZ

NO  YES

What can stop this!!!
MORE INFORMATION @:
www.DigitalBodyGuard.com

FIN = 1