Hacking .NET Applications: The Black Arts (v2)
SecTor 2012

Jon McCoy
www.DigitalBodyGuard.com
Hacking .NET Applications: The Black Arts(v2)
SecTor 2012

Jon McCoy
www.DigitalBodyGuard.com
Hacker VS Attacker
Everything New Is Old Again
IDA-Pro was good.....
IDA PRO &
SoftICE → 1987-2006 RIP
Syser follows $198

OllyDbg

ASM rocks….
IDA PRO
Back When
1 Thread(s)

1.337 kb of MEM

Back When

9 Classes

9 Object
IDA PRO WAS GOOD
private void bn_check_Click(object sender, EventArgs e)
{
    string user = string.Empty;
    string password = string.Empty;

    user = tb_user.Text;
    password = tb_password.Text;

    bool same = false;

    if (user.GetHashCode() == System.Convert.ToInt32(password))
        same = true;
    else
        same = false;

    if (same)
    {
        // true
        System.Windows.Forms.MessageBox.Show("SAME");
    }
    else
    {
        // false
        System.Windows.Forms.MessageBox.Show("NOT SAME");
    }
}
IL – Intermediate Language
Code of the Matrix |||| NEW ASM
private void bn_check_Click(object sender, EventArgs e) {
    string user = string.Empty;
    string password = string.Empty;

    user = tb_user.Text;
    password = tb_password.Text;

    bool same = false;

    if (user.GetHashCode() == System.Convert.ToInt32(password))
        same = true;
    else
        same = false;

    if (same)
    {
        // true
        System.Windows.Forms.MessageBox.Show("SAME");
    }
    else
    {
        // false
        System.Windows.Forms.MessageBox.Show("NOT SAME");
    }
}
private void bn_check_Click(object sender, EventArgs e)
{
    string user = string.Empty;
    string password = string.Empty;

    string user = tb_user.Text;
    string password = tb_password.Text;

    bool same = false;
    if (user.GetHashCode() == System.Convert.ToInt32(password))
    {
        System.Windows.Forms.MessageBox.Show("SAME");
        // true
    }
    else
    {
        System.Windows.Forms.MessageBox.Show("NOT SAME");
        // false
    }
}

IDA PRO WAS GOOD
YOU’RE DOING IT WRONG.

Suicide
You're doing it wrong.
why....
Over 9,000 Object
Over 90 Classes
Over 1,337 MB of MEM
15 Threads
private void bn_check_Click(object sender, EventArgs e)
{
    string user = string.Empty;
    string password = string.Empty;
    user = tb_user.Text;
    password = tb_password.Text;
    bool same = false;
    if (user.GetHashCode() == Convert.ToUInt32(password))
        same = true;
    else
        same = false;
    if (same)
    {
        // true
        System.Windows.Forms.MessageBox.Show("SAME");
    }
    else
    {
        // false
        System.Windows.Forms.MessageBox.Show("NOT SAME");
    }
}
Back When

I WILL BITE

YOUR FACE OFF
Attacking .NET

Attack

The code on disk
GrayWolf

On Disk edit
Attacking on Disk
Attack security

Microsoft Media Center
public static bool CheckPin(string pin)
{
    ParentalControl.Settings.PIN = null;
    ParentalControl.Settings.Load();
    string text = ParentalControl.Settings.PIN;
    if (text == null)
    {
        return 1;
    }
    if (text.Length > 0)
    {
        if (text.get_Chars(0) == 58)
        {
            goto Block_6;
        }
    }
    ParentalControlPin.StoreNewPin(text);
    return text == pin;
    Block_6:
    return text == ParentalControlPin.HashForPin(pin);
Crack

DEMO

GOD MODE
GSGE.ConfigOptions::cctor()
439 ldci4.1
public static bool CheckPin(string pin)
{
    return true;
}
Attacking .NET

Attack

While

The app is running
Attacking .NET Applications: At runtime
Graydragon

Injection
Run and Inject

SECURITY SYSTEMS
101 - Attack on Disk

- Connect/Open - Access Code
  - Decompile - Get code/tech
  - Infect - Change the target's code
  - Exploit - Take advantage
  - Remold/Recompile - WIN
The weak spots

- Flip The Check
- Set Value is “True”
- Cut The Logic
- Return True
- Access Value
SetFlipValue to true

```cpp
bool Registered = false;

if (a == b)
    bool Registered = true;
else
    bool Registered = false;
```
bool IsRegistered()
{
    Return TRUE;
}

Return True
string sqlClean(string x)
{
    Return x;
}

Hack The login

The Best keylogger

DEMO

pass the key
Show the key
Crack the Key

Public/Private == Change Key
3/B==Name*ID*7 == ASK what is /B?
Call Server == Hack the Call
Demo = True; == Set Value
Complex Math == Complex Math

1% of the time the KeyGen is given
Public/Private Key

If you can beat them
Why join them

Key = “F5PA11JS32DA”

Key = “123456ABCDEF”
Reg code replay

Name: JON DOE
Code: 98qf3uy

FAIL
Reg code replay

Name: *C

Code: 5G9P3
Reg code replay

Name: JON DOE
Code: 5G9P3

WIN
Server Call/Phone Home

1. Fake the Call => www.HackME.com
2. Fake the Request => ID=123456789
3. Fake the Reply => Reg Code = f3V541
4. Win => *Registered = True*
Complex math

1. Chop up the Math
2. Attack the Weak
3. ?????????????
4. Profit
Encrypted Data

- Static Crypto Key
- Vector init = 0
- Clear TXT Password Storage
What Stops this?

What is the security?
Crack - FAIL

Androsa FileProtector

Version 1.4.4

Copyright © AndrosaSoft 2009

DEMO

Fail
Protection on disk
0b fu$ca7 ed
Protection on disk

Shells
Pack/Encrypt the EXE
Like MalWareZ
Dotfuscator

Obfuscation will only slow the attacker.

Obfuscation applied programmatically is not 100% effective.

Phone Home

If tampered with, bugs will not add vulnerabilities.
Application hardening
Unprotected/Protected
the best defense is a good sniper

If you know the enemy and know yourself, you need not fear the results of a hundred battles.

- Sun Tzu
It can't be that ez

What is the security?
Visual Studio
Exploit – Run arbitrary code

First noted in 2004

Demo

Get developer Keys
Attack the SVN & DB

I LUV MALWARE == M$
Hacking/RE/Cracking

**SandBoxxie**

- Find your target
- Dissect your target
- Attack your target

www.sandboxie.com
Hacking/RE/Counterpoint

VirtualBox

• Trap your target
• Secure your target
• Lie/Deceive your target

www.virtualbox.org
Security

TOR
www.torproject.org

tRUEcRYPT
www.truecrypt.org

Convergence
www.convergence.io
HACKING

Windows 7 UAC whitelist

www.pretentiousname.com/misc/win7_uac_whitelist2.html

Encode EXE

POWERSHELL/CMD
Look inside
Don't look
Security

The Login security check is

- Does A == B
- Does MD5%5 == X
- Is the Pass the Crypto Key
DATA LEAK

The Data sent home is

- Application Info
- User / Registration Info
- Security / System Info
KEY

The Crypto Key is

- A Hard Coded Key
- The Licence Number
- A MD5 Hash of the Pass
- 6Salt 6MD5 Hash of the Pass
CRYPTO

The Crypto is

- DES 64
- Tripple DES 192
- Rijndael AES 256
- Home MIX (secure/unsecure)
Thanks

All the people that make SecTor happen
More information @:
www.DigitalBodyGuard.com
Jon.Mc@DigitalBodyGuard.com

FIN = 1