Hacking .NET Applications: The Black Arts

AppSec-DC 2012

Jon McCoy

www.DigitalBodyGuard.com
Hacking .NET Applications: The Black Arts

AppSec DC 2012

Jon McCoy

www.DigitalBodyGuard.com
WHY .NET

.NET new and cross platform
- Windows, OS-X, Linux, Android, IPhone, ARM

The attacks are not new nor only in .NET
- C++, Java, .............

Faster development time

Similar layout to JAVA

I happen to be good at .NET
HACKER VS ATTACKER
NOT AMS LEVEL
WHY NOT ASM?
NOT IDA PRO
NOT IDA PRO
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;

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

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

NOT IDA PRO
YOU'RE DOING IT WRONG.

Suicide
You're doing it wrong.
Attacking/Cracking

IN MEM  ||||  ON DISK
ATTACKING .NET

ATTACK THE CODE ON DISK
ATTACKING ON DISK
GRAYWOLF
ON DISK EDIT
GOD MODE
GSGE.CONFIGOPTIONS:::CCTOR()
439 LDC.I4.1
```csharp
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_Chat(0) == 58)
        {
            goto Block_6;
        }
    }
    ParentalControlPin.StoreNewPin(text);
    return text == pin;
    Block_6:
    return text == ParentalControlPin.HashForPin(pin);
}
```
public static bool CheckPin(string pin) {
    Return True;
}
ATTACKING .NET APPLICATIONS: AT RUNTIME
ATTACKING .NET

ATTACK WHILE THE APP IS RUNNING
ATTACK VECTOR (not new)
ASM THE OLD IS NEW

Shell Code - ASM
.NET has pointers
NO .NET Security

.............

THIS IS SCARY!!!!
NEVER LET ME CALL
UNMANNAGED
static public byte[] _ASM_Code_Calc = new byte[]
{
    0x31, 0xF6, 0x56, 0x64, 0x8B, 0x76, 0x30, 0x8B, 0x76, 0x0C, 0x8B,
    0x76, 0x1C, 0x8B, 0x6E, 0x08, 0x8B, 0x36, 0x8B, 0x5D, 0x3C, 0x8B,
    0x5C, 0x1D, 0x78, 0x01, 0xEB, 0x8B, 0x4B, 0x18, 0x67, 0xE3, 0xEC,
    0x8B, 0x7B, 0x20, 0x01, 0xEF, 0x8B, 0x7C, 0x8F, 0xFC, 0x01, 0xEF,
    0x31, 0xC0, 0x99, 0x32, 0x17, 0x66, 0xC1, 0xCA, 0x01, 0xAE, 0x75,
    0xF7, 0x66, 0x81, 0xFA, 0x10, 0xF5, 0xE0, 0xE2, 0x75, 0xCC, 0x8B,
    0x53, 0x24, 0x01, 0xEA, 0x0F, 0xB7, 0x14, 0x4A, 0x8B, 0x7B, 0x1C,
    0x01, 0xEF, 0x03, 0x2C, 0x97, 0x68, 0x2E, 0x65, 0x78, 0x65, 0x68,
    0x63, 0x61, 0x6C, 0x63, 0x54, 0x87, 0x04, 0x24, 0x50, 0xFF, 0xD5,
    0xC3
};
public delegate int funPointer();

// windows call to alloc space in the process
[System.Runtime.InteropServices.DllImport("kernel32.dll", SetLastError = true)]
static extern IntPtr VirtualAlloc(IntPtr lpAddress, UIntPtr dwSize,
   AllocationType flAllocationType, MemoryProtection flProtection);

// windows call to free space in the process
[System.Runtime.InteropServices.DllImport("kernel32")]
private static extern bool VirtualFree(IntPtr lpAddress, UInt32 dwSize, UInt32 dwFreeType);

static public void runASM()
{
    IntPtr p = VirtualAlloc(IntPtr.Zero, new UIntPtr((uint)_ASM_Code.Length),
        AllocationType.COMMIT | AllocationType.RESERVE, MemoryProtection.EXECUTE_READWRITE);

    //copy the ASM code into memory(code memory)

    //build the function pointer to the ASM code
    funPointer ASM_Function = (funPointer)

    // Run ASM
    v = ASM_Function();

    //free up the ASM code in mem:
    VirtualFree(p, 0, 0x8000);
}
Run and Inject

SECURITY SYSTEMS

PROCESS
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
SET VALUE TO "TRUE"

bool Registered = false;

if(a!=b)
if(a==b)
bool IsRegistered()
{
    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”
1. Fake the Call
2. Fake the Request
3. Fake the Reply
4. Win

“Send”
SystemID = 123456789
Reg Code = f3V541

*Registered = True*
REG CODE REPLAY

Name: JON DOE

Code: 98qf3uy

5G9P3

FAIL
REG CODE REPLAY

Name: *C

Code: 5G9P3
REG CODE REPLAY

Name: JON DOE
Code: 5G9P3

WIN

Code: 5G9P3
COMPLEX MATH

1. Chop up the Math
2. Attack the Weak
3. ????????????
4. Profit
HACK THE KEY

The Best keylogger

DEMO

APPSEC-USA 2011
999ca10a050f4bdb31f7e1f39d9a0dda
Encrypted Data

- Static Crypto Key
- Vector init = 0
- Clear TXT Password Storage
WHAT STOPS THIS?

What is the security?
PROTECTION ON DISK

Protection – Security
- Signed code (1024 bit CRYPTO)
- Verify the creator
- Strong Names
- ACLs…….. M$ stuff

Try to SHUTDOWN
Tampering
PRIVET KEY SIGNING

Signed code is based on

- Private Key - 1024 bit
- Signed Hash of Code

Identify and Verify the Author
PROTECTION ON DISK

Protection - Security by $\text{0bscur17y}$

- Code Obfuscation
- Logic Obfuscation
- Unmanaged calls…to C/C++/ASM
- Shells / Packers / Encrypted(code)

Try to SHUTDOWN

Decompilation
Secure App

Crypto

Phone

Record

Update

DB

Call

Twitter

Secure USB Dongle

Return True;
Phone Home
Reg Check
API
Update
DB Call
Twitter

Secure USB Dongle
CRACK - FAIL
PROTECTION ON DISK

DEMObfuscated

DEMO
Obfuscation will only slow the attacker. Obfuscation applied programmatically is not 100% effective. Causes low or no bugs. Does not add vulnerabilities. Phone home if tampered.
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
PROTECTION ON DISK

Shells

Pack/Encrypt the EXE
IT CAN’T BE THAT EZ

What is the security?
STRONG NAME HACKING
Signed code is based on

- Private Key - 1024 bit
- Signed Hash of Code

SIGNED CODE CHECKING IS OFF BY DEFAULT
FAKE SIGNED DLL

genuine Microsoft software

EX

PRIVATE

DLL
FAKE SIGNED DLL

Turn Key Checking ON

[HKEY_LOCAL_MACHINE
\SOFTWARE\Microsoft\.NETFramework]
"AllowStrongNameBypass"=dword:00000000
We the People of the United States, in Order to form a more perfect Union, establish Justice, insure domestic Tranquility, provide for the common Defence, promote the general Welfare, and secure the Blessings of Liberty to ourselves and our Posterity, do ordain and establish this Constitution for the United States of America.

Article 1.

Section 1.

All legislative Powers herein granted shall be vested in a Congress of the United States, which shall consist of a Senate and House of Representatives.

Section 2.

The House of Representatives shall be composed of Members chosen every second Year by the People of the several States, and the Electors in each State shall have the Qualifications requisite for Electors of the most numerous Branch of the State Legislature.

No Person shall be a Representative who shall not have attained to the Age of thirty-five Years, and been a Citizen of the United States for seven Years, and who shall not, when elected, be an Inhabitant of that State in which he shall be chosen.

Representatives and Direct Taxes shall be apportioned among the several States which may be included within this Union, according to their respective Numbers, which shall be determined by adding to the whole Number of free Persons, including those bound to Service for a term of Years, and excluding those not taxed, three- fifths of all other Persons.

The actual Enumeration shall be made within three Years after the first Meeting of the Congress of the United States, and within every subsequent Term of ten Years, in such Manner as they shall by Law direct. The Number of Representatives shall not exceed one for every thirty Thousand, but the States having less than thirty Thousand Inhabitants, shall be entitled to have one Representative; and when the Number of any State shall be increased in such Manner as to render it necessary to add to the Representation therein, two or more new Houses shall be added, as may be necessary, but not exceeding in the aggregate one for every forty Thousand People, according to the last Federal Census.

The Houses of Representatives shall choose their Speaker and other Officers; and shall have the sole Power of Impeachment.

Section 3.

The Senate of the United States shall be composed of two Senators from each State, chosen by the Legislature thereof, for six Years; and each Senator shall have one Vote.

Immediately after they shall be assembled in Consequence of the last Election, they shall be on Duty, to choose a President of the United States, and if the Senate and House of Representatives shall not agree upon the choice of President within the time appointed in the Constitution, then the House of Representatives shall choose a President, from the two Members proposed by the Senate.

In the meantime, the Congress may apportion among the States, the Unappropriated revenues of the United States, and keep account of the public Money, and pass all other Laws which may be necessary for the Administration of the Union; and for the interior Protection and Defence thereof; and for the Punishment of Offences against the Laws thereof, but the Trial of all Crimes, except in Cases of impeachment, shall be by a Federal Court.

The Congress shall have Power to deport or expel any Aliens in Cases of Impeachment, or other Convictions, to which the Punishment of Fine or imprisonment doth not extend.

Section 4.

The Congress shall have Power to determine the Rules of Procedure, and the Times, Places, and Manner of holding Elections for Senators and Representatives, except as this Constitution may otherwise provide; and the Congress may at any time, by the most absolute Majority of both Houses, vote a public Reward or Punishment to any of the Judges in the Cases stated in the next Article.

Section 5.

The Congress shall have power to make all Laws which shall be necessary and proper for carrying into Execution the foregoing Powers, and all other Powers vested by this Constitution in the Government of the United States, or in any Department or Officer thereof.
VISUAL STUDIO
Exploit – Run arbitrary code
First noted in 2004

Demo
PowerShell - Matrix
Get developer Keys
Attack the SVN & DB

www.pretentiousname.com/misc/win7_uac_whitelist2.html
YOU’RE NOT A HACKER
WHY SHOULD YOU CARE?

Defend your Applications
Defend your Systems
Verify your Tools\Programs
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
The Crypto is

- DES 64
- Tripple DES 192
- Rijndael AES 256
- Home MIX (secure/unsecure)
FIN
MORE INFORMATION @:
www.DigitalBodyGuard.com
Jon.Mc@DigitalBodyGuard.com

FIN = 1