

200 Milliseconds To Owned: Walking Tour of a Drive By Exploit

Patrick Thomas

4/17/10

Me

- Cal Poly Computer Science, BS
- Intuit
 - Software engineer, QuickBooks Online backend
- Qualys
 - Vulnerability Detection Engineer (now in research)
- InfoSec Community:
 - OWASP*, BlackHat/DefCon (speaker? We'll see...)
- CoffeeToCode.net

Obligatory Ethics Slide

- Laws are new
 - Things we do can be viewed as good or bad
 - Want to set good precedent and win public opinion
- It's not just important to be doing the right thing
 - ... you have to *look* like you're doing the right thing
- Toyota black box?
- Voting machines?
- Society should be able to trust hackers to tackle these
- Okay, on with the fun stuff...

Some Terminology

- Vulnerability (n.)
 - [MS definition](#) is pretty good
 - Essentially “a weakness in a computer system that allows something bad to happen”
 - Many have a CVE number, eg [CVE-2010-0249](#)
- Exploit (n., v.)
 - Often casually conflated with “vulnerability”
 - A specific technique or tool that makes something bad happen
 - Often used as proof of a vulnerability
- Payload (n.)
 - What an attacker actually does to a machine if an exploit attempt is successful
 - Usually bundled with, but distinct from, an exploit

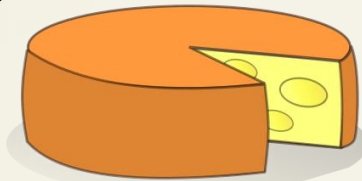
Attack Surface

- Useful concept -- internalize it
- What's the attack surface of a server just sitting there?
- When browsing the web, what's your attack surface?
- How do you find out?



The Browser

- What browsers do you use?
- Swiss cheese, basically...
- Vulns in 2008 ([Secunia](#)):
 - IE: 31
 - Safari: 32
 - Opera: 30
 - Firefox: 115
 - ActiveX: 366
 - Java: 54
 - Flash: 19
 - PDF: [51](#) (2009)



We Want Out...

- We want to run code in the context of the OS
- Can't do much with plain javascript or html
- Browser is a foothold; it has real power

Breaking the Browser

- Programming errors everywhere
- Goal: Cross the line between data and code
- Lots of ways to do that
- [Month of Browser Bugs](#)
 - I <3 HD Moore

Going Deeper (just for a moment)

- Don't let your eyes glaze over
 - This is where the magic happens
- Computers are simple, code is just bytes
- He who controls the next instruction to be run wins

Going Deeper (just for a moment)

- Holy Grail: Get Instruction Pointer to point to something we control → Game Over.
 - Buffer Overflow, Format String, Heap Corruption
- Just as good: "Mother May I" vulns
 - These are stupid. Really, really dumb. Hopefully MS is past this. Adobe & Sun/Oracle, not so much.
 - MS06-014
 - `var s = CreateO(a, 'WScript.Shell');`
 - `var o = CreateO(a, 'ADODB.Stream');`
 - `var e = s.Environment('Process');`

Going Deeper (just for a moment)

- The “stack” is working memory
- A “buffer overflow” is an attack against this working memory

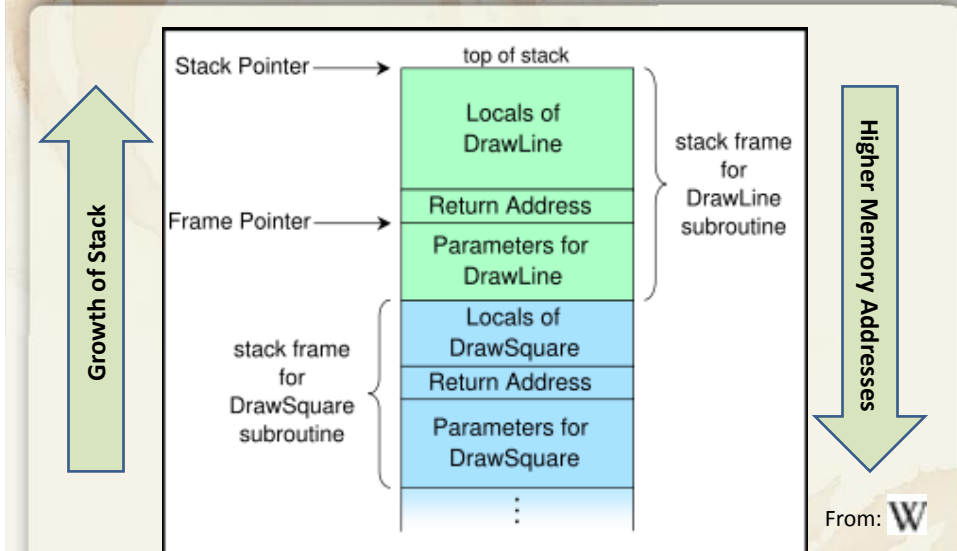
```
DrawSquare(Point* a, Point* b, Point* c, Point* d)
{
    //use some locals here, then call to draw lines..
    DrawLine(a, b);
    DrawLine(b, c);
    DrawLine(c, d);
    DrawLine(d, a);
}
```

Going Deeper (just for a moment)

Dump of assembler code for function DrawSquare:

```
0x080483c3 <DrawSquare+0>:    push  %ebp
0x080483c4 <DrawSquare+1>:    mov   %esp,%ebp
0x080483c6 <DrawSquare+3>:    sub   $0x8,%esp
0x080483c9 <DrawSquare+6>:    mov   0xc(%ebp),%eax
0x080483cc <DrawSquare+9>:    mov   %eax,0x4(%esp)
0x080483d0 <DrawSquare+13>:   mov   0x8(%ebp),%eax
0x080483d3 <DrawSquare+16>:   mov   %eax,(%esp)
0x080483d6 <DrawSquare+19>:   call  0x80483b9 <DrawLine>
...
0x0804840c <DrawSquare+73>:   call  0x80483b9 <DrawLine>
0x08048411 <DrawSquare+78>:   leave
0x08048412 <DrawSquare+79>:   ret
```

Going Deeper (just for a moment)



Going Deeper (just for a moment)

- The Schneier 7-11 Analogy
- Volunteers?



Detecting Bad Stuff (1)

- Sure, just search for that in a page right?
 - Static Detection (aka signature-based)
- Right! (Once.) Now it's an arms race.
 - Alan Turing says the bad guys win in an obfuscation game
 - We don't have to play to the end though...
- End result: Bad stuff is almost always obfuscated

Detecting Bad Stuff (2)

- Behavioral Detection
 - Let it do its thing, judge based on what it does
- Sweet, this is a powerful technique
- General lesson: Always whitelist

Alright already, lets own something

- MS06-014 Demo
- MS10-002 "Aurora" Demo
- Disclaimer: Don't expect fireworks... the cool stuff happens inside the machine.

So, what happened? (1)

- Webpage made browser do something it shouldn't
- Attacker was on the net... now on your box
- He's not done yet...

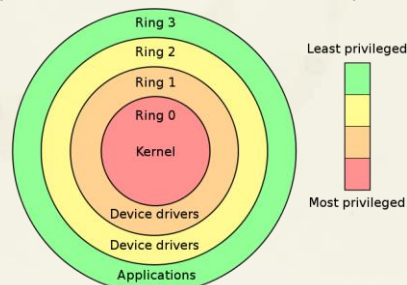
So, what happened? (2)

12:08:39.461		Click on Malicious URL
12:08:40.128	↓	L1 Payload Process Start
12:08:41.645	Owned ↓	L2 Payload Written
12:08:41.663	Really Owned ↓	L2 Payload System Hook Written
12:08:41.668	Really Owned ↓	L1 Payload Cleanup File Written
12:08:41.851	Really Owned ↓	L1 Payload Cleanup Process Start
12:08:41.855 – .88	Owned ↓	More System Hooks Written
12:08:41.888	Really, Really Owned ↓	L1 Payload Process End
~12:08:42.000	Really, Really Owned ↓	L1 Payload File Deleted

<1 seconds to Ownage*, **

More Terminology

- Ring0 - Ring3 (aka Kernel to User)
 - *nix/Windows differentiate, DOS didn't



- Ever wonder about CTRL-ALT-DELETE?

Programs are just bytes

- How to defang malware
- Demo
- Though it's not always this easy...

Some practical advice

- Run a modern, patched OS and browser
 - Take advantage of DEP, ASLR, SELinux
 - It's time for XP and IE 6 to die
- Run adblocker and scriptblocker
 - if you can stand it...
- Don't browse as admin
- Don't install random plugins in your browser
- Oh, and ditch Adobe Reader
 - Though Foxit just [got egg in their face](#)
- (A/V isn't on this list)

Skills for InfoSec Industry

- Learn to speak and write well
- Politics is a skill
- Econ (depends who you ask; I [think it's huge](#))
- Not so much about *"OMG H4xx0rs at teh gates!"*
 - More about "Hmm, that's funny" ([P. Nico](#))

Obligatory "Getting into InfoSec" Slides

- There's no one way
 - I'm biased toward getting a technical background
- Take a broad range of technical classes
 - You'll need approaches and techniques from many different fields
- Work with the smartest people you can find
- Mostly: "Be proactive"

Obligatory “Getting into InfoSec” Slides

- [Marissa Fagan's talk](#) on ErrataSec
- [Securiosis](#) post
- [SecureConsulting](#) post

- Read blogs → Have a blog
- Get on Twitter (... I hate it as much as you do)

Questions?

psthomas@gmail.com

@coffeetocode

Slides and more at

<http://CoffeeToCode.net>