(ISC)² Twin Cities Chapter
October 2012
24 October 2012, 3.00pm-4.00pm

Java Exploits
Offense and Defense

Matthew J. Harmon
IT Risk Limited, LLC

Hello!

- Matthew J. Harmon - 20 years of Information Security
  CISSP, GSEC, GCIH, CISO, ISO 27001 Lead Auditor

- Community SANS Instructor
  SEC 401 - Security Essentials Bootcamp
  SEC 504 - Incident Handling, Exploits and Hacking Techniques
  SEC 464 - Hacker Guard for Systems Administrators

- Security Researcher, Interim CISO and Security Director
  Penetration Tester, Security Architect
  Incident Handler, Computer Archeologist (Forensic Analyst)

- ISO Standards Developer
  Chairman of US Technical Advisory Group 7 - Security
  Liaison to Sub-Committee 27 - IT Security Techniques

Why we are here today.

- Client-side (Java, Flash, iTunes) vulnerabilities are a serious attack vector that is largely uncontrolled
- We as security practitioners need to raise awareness of these risks and recommend business appropriate controls

What we are going to talk about...

- Oracle Java Vulnerabilities and Exploits
- Technical Defense Measures
- Policy based Defensive Measures

...and what not.

- No exploit code release and demo today, sorry.
- Many effective exploits in the wild, no need to add insult to injury.
- When this presentation was originally planned it was expected the October Java SE 7 Update 7 patch would fix the sandbox, it didn't and the next expected update is in February 2013.

However...

- Other security researchers have well documented vulnerabilities in the Oracle Java Sandbox:
- **Joshua J. Drake** (August 2012)
  http://pastie.org/4594319
- **Adam Gowdiak** (September 2012)
  http://seclists.org/fulldisclosure/2012/Sep/170
  http://www.security-explorations.com/en/SE-2012-01-press.html
- **Sami Koivu** (April 2010)
  http://slightlyrandombrokenthoughts.blogspot.com.ar/2010/04/java-trusted-method-chaining-cve-2010.html

and the problem is built-in

```
public void disableSecurity() throws Throwable {
    Statement localStatement = new Statement(System.class, "setSecurityManager", new
Object[1]);
     Permissions localPermissions = new Permissions();
     localPermissions.add(new AllPermission());
     ProtectionDomain localProtectionDomain = new ProtectionDomain(new
CodeSource(new URL("file:///"), new Certificate[0]), localPermissions);
    AccessControlContext localAccessControlContext = new AccessControlContext(new
ProtectionDomain[]{localProtectionDomain});
     this.SetField(Statement.class, "acc", localStatement, localAccessControlContext);
     localStatement.execute();
   }

private void SetField(Class paramClass, String paramString, Object paramObject1, Object
paramObject2) throws Throwable {
    Object[] arrayOfObject = new Object[]{paramClass, paramString};
    Expression localExpression = new
Expression(this.GetClass("sun.awt.SunToolkit"), "getField", arrayOfObject);
    localExpression.execute();
    ((Field)localExpression.getValue()).set(paramObject1, paramObject2);
  }
```

Oracle Java Vulnerabilities and Exploits

Numbers Speak Volumes

23 of the 50 Oracle JRE vulnerabilities released in 2012 have a CVSS Score of 10

- CVSS Score of 10 means Game Over
- Complete Compromise of Confidentiality, Integrity and Availability, without Authentication
- Execute Code, Denial of Service, Bypass

http://www.cvedetails.com/vulnerability-list/vendor_id-93/product_id-19117/Oracle-JRE.html

Oracle's Secure Coding Guidelines for Java

Is Oracle following their own guidelines?

- SEC00-J Do not allow privileged blocks to leak sensitive information across a trust boundary

- SEC05-J Do not use reflection to increase accessibility of classes, methods, or fields

http://www.kb.cert.org/vuls/id/636312
http://www.oracle.com/technetwork/java/seccodeguide-139067.html

Technical Defense Measures

Whitelisting

Until the track record of Oracle's Java improves, applets should be considered hostile

- The good news is under Windows, Group Policies have Zone Mappings
- To Forbid Java in the Internet Zone, set:

HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\Zones\3
Key 1C00 = 0

http://laws.qualys.com/2012/08/new-java-0-day-disclosed.html

Click-to-Run

Default Deny Java Applets

- Google Chrome and Firefox have the option of requiring the user to click on Java Applets before activating them
- Click-to-Run helps prevent drive-by exploitation
- Not as effective as whitelisting, but a good control

http://laws.qualys.com/2012/08/new-java-0-day-disclosed.html

A Stronger Local Sandbox

Invincea

- Runs all major client side applications in a virtual machine
- Evaluates application behavior against known good baseline
- Appears similar to Cube OS - Every application runs in its own virtual machine
- Strength in numbers

http://www.invincea.com/

An In-Line Sandbox

FireEye

- Similar to Invincea, however runs as an in-line appliance
- Ties in with malware analysis services
- Strength in numbers

http://www.fireeye.com/

Policy based Defensive Measures

Security Policies

What is the business case for keeping Java around?

- If you don't have a business requirement for allowing Java in your environment, remove it.
- Certification and Accreditation doesn't only apply to computers that run in your environment, but it applies to the software running on those machines as well.
- Evaluate the risk of allowing Java to run uncontrolled

http://arstechnica.com/information-technology/2012/10/ars-asks-is-using-java-on-a-desktop-worth-the-security-risks/

Critical Security Controls

Controls 1 through 5

1. Inventory of Authorized and Unauthorized Devices
2. Inventory of Authorized and Unauthorized Software
3. Secure Configurations for Hardware and Software on Laptops, Workstations, and Servers
4. Continuous Vulnerability Assessment and Remediation
5. Malware Defenses

http://www.sans.org/critical-security-controls/

Final comments

We've reached a point where client side exploitable vulnerabilities are far more common than daemon or service vulnerabilities.

These exploits, tied with social engineering and specifically phishing, leave our user populations vulnerable.

Patching alone isn't an effective measure, hostile software is running in our environments and we are not in control. Our adversaries aren't disclosing the vulnerabilities they discover so we shouldn't wait.

IT Risk Limited, LLC

matthew@itriskltd.com

IT Risk Ltd. performs IT risk assessments, penetration testing and incident response.
We lead security research and participate in international standards development,
and if you couldn't tell, we are passionate about what we do.

Thank you!

Questions?

I hope you enjoyed this presentation, it can be downloaded after this event from:

https://github.com/itriskltd