Global Information Assurance Certification Paper

Microsoft Java VM Identity Hijacking Vulnerability
By: Andrew Tang
SANS GIAC Level 2 – GCIH Assignment
Option 2
SANS Parliament Hill 2000 – Ottawa
Aug 2000

Exploit Details

Name: Microsoft Java VM identity hijacking vulnerability

Operating System: Microsoft Windows 95, 98, NT & 2000

Protocols/Services: Java Virtual Machine

Brief Discription: Attacker can masquerade as the unsuspected user, while the user is browsing the Attacker's malicious web site. Attacker can browser other sites with the users identity and have the information relay back to the attacker.

Background Information

This Microsoft VM vulnerability has to do with how java applets are run on a Microsoft platform. Therefore without understanding what Java is, it is virtually impossible to understand how this vulnerability works and the potential scope and danger of it. With Java's promise of "write once, run anyway" it has become the most popular programming language over the Internet. Most of the Web pages nowadays have some Java applet embedded in it. Over the next paragraph in this section we will go over some of Java's basic concepts, Java language, Java applets and Java Virtual Machine.

Java was a language created mainly by Sun Microsystems, it is intended to be the computer language that can cross system barrier. The major distinguishing factor for java is that its source code is complied into a "byte code" instead. Normal programming language is platform dependent because source code is compiled into machine code which the specific OS / Platform would understand. If the program needs to be run on a different platform, the source code has to be recompiled for that platform. In the case of Java, we eliminated this platform dependency by using the same "byte code" across all

platforms. Each platform / OS would have their own Java Virtual Machine, which runs as a program in the background. When the JVM receive a Java byte code, it will run the instructions imbedded in the byte code. Therefore instead of the application being platform specific, only the JVM have to be platform specific.

Java applet is a common type of java program that can be found of the web. There is actually two major type of Java program, Java application and Java applet. Java applications like any other application are programs that user install on their machine. The code resides on the user machine and therefore is trusted. On the other hand Java applets are hosted on web sites and run on user's machine while they visit the site. Due to the foreign nature of the applet, it is not trusted. When the JVM run a java applet, it uses a "sand box" to restrict the action of the applet. The sand box is designed to prevent an applet form performing any inappropriate action on the user's machine. Also because these java applets are foreign code, designer can attach a digital signature to the code. When the applet is first ran, information on the digital signature will be shown to the user. Therefore the user can decide to trust or not trust the applet. Non-trusted or unsigned applets are treated by the JVM differently than trusted ones. This Microsoft JVM vulnerability has to do with unsigned java applets.

The Virtual Machine works by reading Java byte codes and converting them to the native language of the machine the virtual machine is running on. Therefore the virtual machine is critical to how Java applications and applets are executed. It is also responsible for applying the "sandbox" restrictions to untrusted codes, like applets. If there are any bugs to the virtual machine, it can produce vulnerabilities in the operating system. Which is exactly our case here. Some versions of Microsoft VM have flaws where the "sandbox" restriction is not applied properly. The Microsoft VM is a virtual machine for the Win32 operating environment. It runs on top of the Microsoft Windows(r) 95, 98, or Windows

NT, or Windows 2000. It ships as part of each operating system, and also as part of Microsoft Internet Explorer. The version of the Microsoft VM that ships with Microsoft Internet Explorer 4.x and Internet Explorer 5.x contains the security vulnerability that could allow a Java applet to operate outside the bounds set by the sandbox.

Variants

Since this report focus on the Microsoft Java VM identity hijacking vulnerability, which is a vulnerability instead of class of attack, there isn't any considerable variants. Yet there are two major ways that this vulnerability can be exploited. Detail explanation will be given in the next section.

How does it work

The VM identity hijacking vulnerability has to do with how Microsoft VM deals with Java applets. As mentioned before, due to the foreign nature of Java applets, virtual machine uses a sandbox to restrict the activity of the applets. The sandbox is designed so that applets will not be able to perform inappropriate function on user's computer. Different codes are given different limitation from the sandbox, Java application, java applets and unsigned java applets are all treated differently.

One of the sandbox restrictions is to block untrusted code from communicating with other web sites. Normally applet is allowed to communicate with its hosting server only. In some cases signed applet is allowed to communicate with other server as well, but unsigned applet since it is untrusted code should not be allow to communicate with other servers. Yet a flaw in Microsoft VM sandbox can allow an unsigned applet to talk to any servers.

Microsoft Java VM Identity Hijacking Vulnerability
By: Andrew Tang
SANS GIAC Level 2 – GCIH Assignment
Option 2
SANS Parliament Hill 2000 – Ottawa
Aug 2000

This flaw in the VM can let an attacker obtain information from web site while disguising as another user. An attacker can create a malicious web site, which contains an applet that can exploit the VM vulnerability. When an innocent user browses the malicious web site, the applet will be downloaded to the user's machine and run by the java virtual machine. Due to the flaw in the sand box this applet will be able to communicate with other web sites. From the other web site's point of view, the request is coming from the user's machine instead of the attacker's machine. The information obtain from the other sites will be relayed back to the attacker by the applet. Therefore the attacker is effectively browsing the other web site under the user's identity.

On the surface, this might not seem to be a big problem. Web site are generally design to provide information and the hosts seldom cares about the user who is obtaining the information. Yet in some cases this vulnerability poses a great threat. For one, this vulnerability provides a possible path for an attacker to obtain information which is stored on a corporate intranet website. Normally the corporate website is behind the corporate firewall and is inaccessible to attackers on the outside world, yet if any user on the corporate network who have access to the intranet site, browse the attacker site, then a pathway exists for the attack steal information from the intranet site which normally would not exist, if it is not for the VM vulnerability.

Microsoft Java VM Identity Hijacking Vulnerability
By: Andrew Tang
SANS GIAC Level 2 – GCIH Assignment
Option 2
SANS Parliament Hill 2000 – Ottawa
Aug 2000

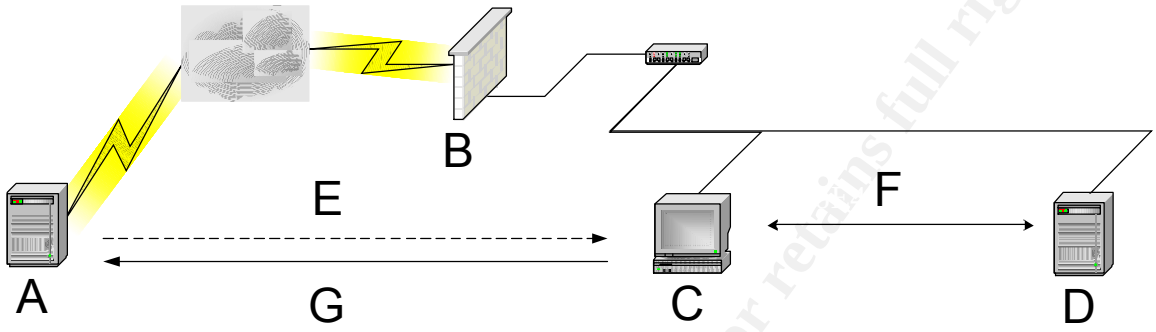

Diagram 1. Exploit to steal information from intranet site

A. Attacker's Malicious Web server
B. Firewall
C. User's Workstation which contains the VM vulnerability
D. Company's Intranet Web server
E. Applet Downloaded
F. Information transfer requested by the malicious applet
G. Stolen information for Intranet site relay back to the attacker by the Applet

Another problem that can be caused by this vulnerability has to do with the fact that browsers cache user information when they access websites. If a user browses an Internet site that requires authentication, this information can be cached. If the user then visits the attacker's malicious site, the attacker can utilize the vulnerability to obtain the password-protected information. By exploiting the VM vulnerability, the applet can cause the request for the information to be sent from the user's machine instead of the attacker's machine, the cached password information will be sent along with the request. Assuming the password was right while the user was accessing the site, the request will go through and information obtain from the site will be relayed back to the attacker by the applet. A successful attack will mean the attacker can obtain information without knowing the user's password.

Microsoft Java VM Identity Hijacking Vulnerability
By: Andrew Tang
SANS GIAC Level 2 – GCIH Assignment
Option 2
SANS Parliament Hill 2000 – Ottawa
Aug 2000

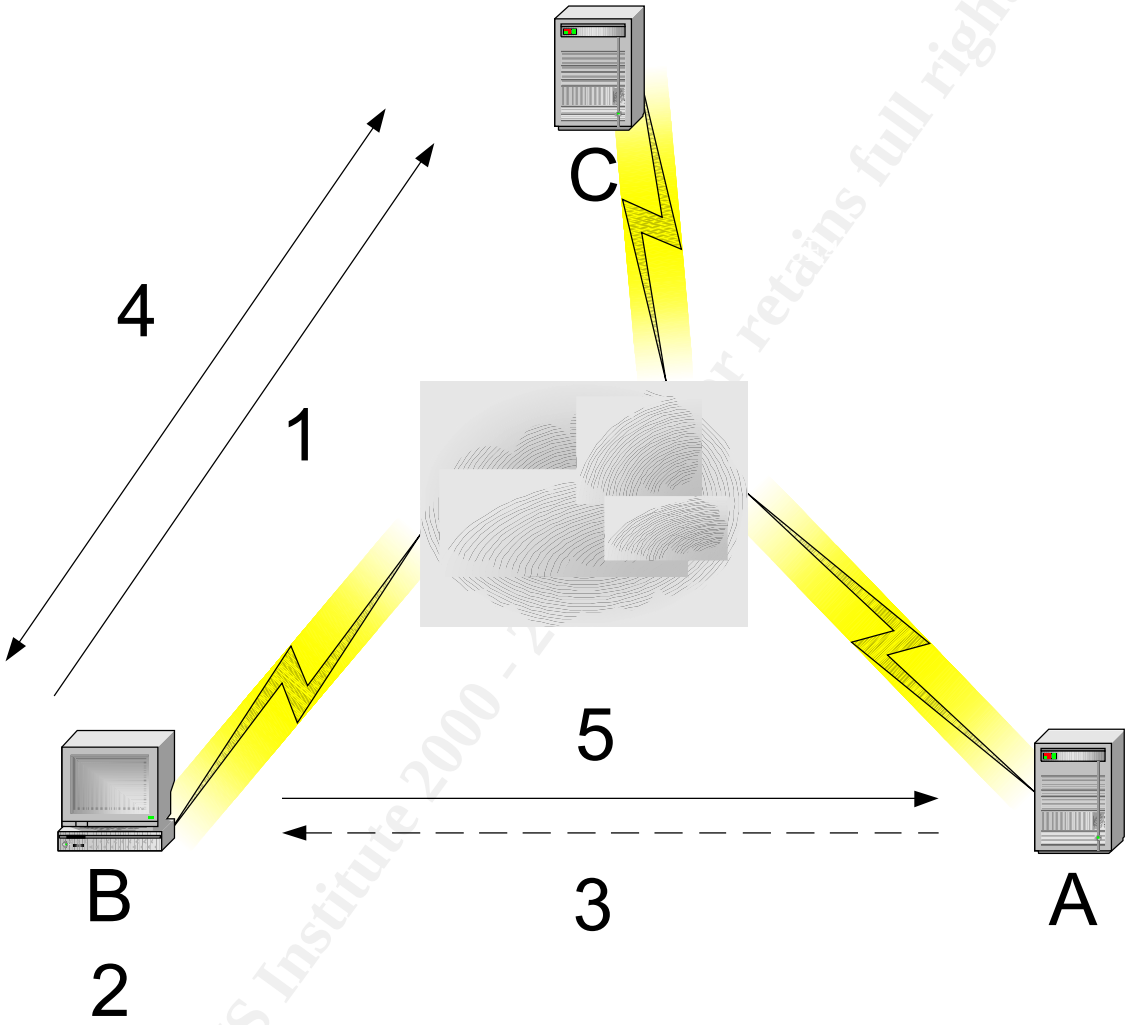

Diagram 2 Exploit using cached password information

A. Attacker's Malicious Web Server
B. User's Workstation containing the VM vulnerability
C. Web Server which requires password authentication
1. User visiting site which requires authentication
2. User password information cached on user's machine
3. User visit the attacker's malicious site and the malicious applet is downloaded
4. Applet request information from password protected site, User's machine sends cached password information along with the request
5. Stolen information is relay back to the attackers machine

As we seen from above this vulnerability have potential to be a great threat, but there are some difficulties and limitation for the attacker to use this exploit as well. For one the attacker has to know the server's name before hand. Since the applet has to be pre-build before the attack, the target server name has to be included in the applet; a change while the user is browsing the attacker's site is difficult. Also this vulnerability provides no information about where the user has visited lately, therefore it is also very hard to know which site's password information is stored in the cache. Another major limitation to this vulnerability would be that even though as presented before, the personal information stored on the machine can be reused by the attacker, this vulnerability does not expose this information to the attacker. The password information is always sent with the request to the target website and it is never sent back to the attacker. Using this vulnerability alone the attacker will not be able to obtain any cached personal information on the user's machine.

As we can see, this vulnerability has some potential to cause major security problems especially in the information thief area. It provides a path for protected intranet server to be accessed externally, and it also allows the attacker to use a user's identity and password to access password protected information on servers. Although the limitation might make the vulnerability hard to exploit, even useless in some situations, we have to remember that attack seldom use a single trick to attack. When the vulnerability is used in conjunction with sniffers and other tools, where the tools can provide information like which server have the user accessed and the name or IP address of the server, it can potentially be very dangerous.

Microsoft Java VM Identity Hijacking Vulnerability
By: Andrew Tang
SANS GIAC Level 2 – GCIH Assignment
Option 2
SANS Parliament Hill 2000 – Ottawa
Aug 2000

Program to Exploit the Vulnerability

There is no known program that exists to exploit this vulnerability; the exploits that we talk about in this paper are just hypothetical. Since the vulnerability has been found to exist, there is really nothing stopping an attacker to create such an applet that can exploit this vulnerability.

Detection

Due to the natural of this vulnerability, exploits are very hard to detect. From the server point of view there is no way to distinguish between normal information request and a malicious request from the attacker, which is spawn from the applet. Even the firewall log will only show that the machine is having connection to more than one site, but this is hardly evidence for this type of attack as there are many other normal user activity which would cause these type of entries to show up on the log. A more efficient way to detect this type of attack would be from the user's machine. If the user is monitoring his/her network connection, and the network activity is up even long after the page is loaded, then this can be a sign of trouble but still far from being the definite signature of this attack.

On the other hand the vulnerability is much easier to detect, all you have to do is to find out what version of Microsoft VM is running on the machine, if it is one of the affected ones then the vulnerability is exploitable. Full detail on how to find out what version of VM a machine is running and which version is affected is listed in the next section.

Microsoft Java VM Identity Hijacking Vulnerability
By: Andrew Tang
SANS GIAC Level 2 – GCIH Assignment
Option 2
SANS Parliament Hill 2000 – Ottawa
Aug 2000

Protection & Prevention

Microsoft after recognizing the potential danger of this vulnerability, had released a patch to correct the problem in the affected Microsoft VM. As mentioned earlier only a few version of the Microsoft VM is affected, here is the list:

- All builds in the 2000 – 2445 range
- All builds in the 3000 – 3194 range
- All builds in the 3229 – 3240 range
- All builds in the 3300 – 3313 range

To find out which build of Microsoft VM is running on a machine follow the following steps:

1. Open a command prompt window

   For Windows 2000 & Windows NT

   - Click lower left "Start" button
   - From the menu choose "Run"
   - Enter the command "CMD"

   For Windows 95 & Windows 98

   - Click lower left "Start" button
   - From the menu choose "Run"
   - Enter the command "COMMAND"

2. In the command prompt window enter the command "JVIEW"
3. From the first line of the results notice the version number

> The version number will be presented in the "5.00.xxxx" format, where the xxxx is the build number. (e.g. if the version reads 5.00.2134, then the build number of the VM is 2134)

After determining the build of the machine, if it is one of the affected once. You should apply the Microsoft patch. Notice, different builds requires a different patch here are the different patch path:

> All 2000 series Microsoft VM customers:
> Install Microsoft VM build 2446
>
> All 3100 series Microsoft VM customers:
> Upgrade to build 3309 and install the 3314 security patch
>
> 3200 series Microsoft VM customers should do one of the following:
> * All 3200 builds:
> Upgrade to build 3309 and install the 3314 security patch
> * Builds 3229-3234:
> Install the security patch from Bulletin MS00-011 before installing this new 3314 security patch
> * Build 3240:
> Install the 3314 security patch
>
> All 3300 series Microsoft VM customers should install the 3314 security patch

In a perfect world one would only need to inform the administrator and users to apply the patch and the problem will go away, yet the world we live in is far from being perfect,

user and administrator often need to reinstall the OS or IE but yet forget the reapply the security patch. Therefore there are a few extra precaution steps we can take to make this vulnerability harder to be exploited. First setup intranet servers to challenge for a password. Since the applet has no capacity for answering the password challenge, as long as the password is not cached, the attack will fail.

The second way to increase protecting against the exploit of this vulnerability is to configure the browser not to cache personal information. A lot of user will not like this, because they will have to enter authentication information all the time, but from a security standpoint it is very important. Leaving a password cached or saved on a machine is very dangerous, it allows this exploit to go through much more easily also since it is saved on the machine if the machine become compromise, the password will be stolen too. Having a saved password on the browser is like leaving a key under your door met, it might be convenient but it can make the lock on the door virtually useless.

Reference:

Microsoft VM
http://www.microsoft.com/java/resource/vm.htm
Microsoft Security Bulletin on this Vulnerability
http://www.microsoft.com/technet/security/bulletin/fq00-059.asp

Other Sources
http://neworder.box.sk/showme.php3?id=2598
http://neworder.box.sk/showme.php3?id=2547

Last Updated: October 19th, 2017

Upcoming Training

SANS Berlin 2017	Berlin, Germany	Oct 23, 2017 - Oct 28, 2017	Live Event
Community SANS Columbus SEC504	Columbus, OH	Oct 23, 2017 - Oct 28, 2017	Community SANS
SANS Seattle 2017	Seattle, WA	Oct 30, 2017 - Nov 04, 2017	Live Event
SANS San Diego 2017	San Diego, CA	Oct 30, 2017 - Nov 04, 2017	Live Event
SANS Gulf Region 2017	Dubai, United Arab Emirates	Nov 04, 2017 - Nov 16, 2017	Live Event
SANS Milan November 2017	Milan, Italy	Nov 06, 2017 - Nov 11, 2017	Live Event
Community SANS New York SEC504^	New York, NY	Nov 06, 2017 - Nov 11, 2017	Community SANS
Mentor Session AW - SEC504	Houston, TX	Nov 06, 2017 - Jan 29, 2018	Mentor
SANS Miami 2017	Miami, FL	Nov 06, 2017 - Nov 11, 2017	Live Event
Community SANS Raleigh SEC504	Raleigh, NC	Nov 06, 2017 - Nov 11, 2017	Community SANS
SANS Amsterdam 2017	Amsterdam, Netherlands	Nov 06, 2017 - Nov 11, 2017	Live Event
Pen Test Hackfest Summit & Training 2017	Bethesda, MD	Nov 13, 2017 - Nov 20, 2017	Live Event
Community SANS Toronto SEC504	Toronto, ON	Nov 13, 2017 - Nov 18, 2017	Community SANS
Mentor Session SEC504	Houston, TX	Nov 13, 2017 - Dec 11, 2017	Mentor
SANS Sydney 2017	Sydney, Australia	Nov 13, 2017 - Nov 25, 2017	Live Event
SANS San Francisco Winter 2017	San Francisco, CA	Nov 27, 2017 - Dec 02, 2017	Live Event
Community SANS Detroit SEC504~	Detroit, MI	Nov 27, 2017 - Dec 02, 2017	Community SANS
SANS London November 2017	London, United Kingdom	Nov 27, 2017 - Dec 02, 2017	Live Event
SANS Austin Winter 2017	Austin, TX	Dec 04, 2017 - Dec 09, 2017	Live Event
SANS Frankfurt 2017	Frankfurt, Germany	Dec 11, 2017 - Dec 16, 2017	Live Event
SANS Cyber Defense Initiative 2017	Washington, DC	Dec 12, 2017 - Dec 19, 2017	Live Event
SANS Cyber Defense Initiative 2017 - SEC504: Hacker Tools, Techniques, Exploits, and Incident Handling	Washington, DC	Dec 14, 2017 - Dec 19, 2017	vLive
SANS Security East 2018	New Orleans, LA	Jan 08, 2018 - Jan 13, 2018	Live Event
Community SANS Honolulu SEC504	Honolulu, HI	Jan 08, 2018 - Jan 13, 2018	Community SANS
Mentor Session - SEC504	San Antonio, TX	Jan 09, 2018 - Mar 13, 2018	Mentor
SANS Amsterdam January 2018	Amsterdam, Netherlands	Jan 15, 2018 - Jan 20, 2018	Live Event
Community SANS Ottawa SEC504	Ottawa, ON	Jan 15, 2018 - Jan 20, 2018	Community SANS
Community SANS St Louis SEC504	St Louis, MO	Jan 15, 2018 - Jan 20, 2018	Community SANS
Northern VA Winter - Reston 2018	Reston, VA	Jan 15, 2018 - Jan 20, 2018	Live Event
SANS vLive - SEC504: Hacker Tools, Techniques, Exploits, and Incident Handling	SEC504 - 201801,	Jan 16, 2018 - Feb 22, 2018	vLive
SANS Dubai 2018	Dubai, United Arab Emirates	Jan 27, 2018 - Feb 01, 2018	Live Event