ActiveX vs. Java
By: Blake Stockslager

Anyone that uses a computer today mainly uses it for access to the internet. While what that person is actually doing on the internet might seem perfectly harmless, they could be putting their entire computer at risk. Many web pages use technology called ActiveX or Java. These two technologies allow web pages to come more alive and interactive, and the developers of those web pages as well as the users have to choose to use ActiveX or Java applets to make this effect. In the following paragraphs, I am going to explain what ActiveX and Java is, what risks are involved when using them, and ways to safely use these technologies.

First, what is ActiveX? Microsoft developed ActiveX in 1996, and it is only useable on the system they are complied for, most commonly seen in Internet Explorer. There are however plug-ins available to use ActiveX with Netscape or FireFox. “The technology can exist within the framework of an Internet browser or a standalone Windows application” (Lee). ActiveX is a tool for building applications from another language, like perhaps Visual Basic or C++. “ActiveX Controls are small programs that are also a set of rules for how applications should share information, which can be automatically downloaded and executed by a Web browser. Programmers can develop ActiveX controls in a variety of languages. ActiveX controls have full access to the Windows operating system. This gives them much more power than other Web technologies. To control this, Microsoft developed a registration system so that browsers can identify and
authenticate an ActiveX control before downloading it.” (Broadband Glossary A)
The method of controlling use of ActiveX will be explained later. Before ActiveX was introduced to web page developers, their pages were just text and graphics. No manipulation of the page was possible, it was used just to read the information it contained. With ActiveX web pages become interactive, display animations, stream video and sound files, play games, interact with applications, and much more. A good way to think of the power that an ActiveX control has been stated as “If you can do it in Windows, you can do it on the web” (ActiveX versus Java).

Second is Java, Java is a technology developed by JavaSoft, a division of Sun Microsystems. It is not platform dependant, meaning it can be used across any operating system that has java installed on it. When Java is installed on a computer, it installs the complier, which is called the Java Virtual Machine (JVM). Whenever a web page is accessed that has a java program embedded in it, the client side of Java comes into play. The web page containing the Java code is interpreted by the JVM and compiled in a secured section of your computer’s memory, also called a sandbox. Within this area, the code is executed, keeping the instructions separate from your hard-drive to provide security. Java can also be used also in mobile devices such as cell phones or PDA’s.

Since ActiveX and Java have such power to control a user’s computer, security measures had to be set in place. The way Microsoft achieves security with ActiveX is use of certificates. Each ActiveX control must have a digitally signed certificate with it. When your browser looks at the certificate it will display
whom the author of the control is, and whether or not if the certificate has been altered meaning that ActiveX control could be compromised. Based the validity of the certificate and who made the control will give the end user a choice of accepting it or not. If that program is accepted to run on the webpage, it could have full reign of your computer, but if the certificate is rejected it will not be allowed to install. ActiveX security is almost completely up to the user to make the judgment to use.

An example of an ActiveX control is the Windows Update website. Before the website can check if your version of Windows is up to date, it must inspect some system files on your hard drive. In order to do so, the user is asked whether to install the ActiveX control. This allows Microsoft to gather information and display a list of needed updates. Without installing it, nothing could be done. Although not all Controls are meant for good use, many viruses, worms, Trojans, and spyware will attempt to use ActiveX as a gateway to your computer. One example of using ActiveX for malicious purposes is exploiting the Certificate Enrollment Control. “Attackers could exploit the flaw with a specially designed Web page "through an extremely complex process" to use the control to delete certificates on remote systems, Microsoft said in an advisory. Potentially susceptible certificates include: root certificates, EFS encryption certificates and e-mail signing certificates. If the flaw is exploited, users could have trouble using secured Web sites and encrypting and decrypting data.” (Hurley). If this situation happens, this mean any banking websites, websites that require personal information, digitally signed and encrypted emails, or anything else that needs to
be completed over a secured connection cannot be done. Most compromises are done by visiting websites or opening unknown emails.

Java on the other hand is only similar to ActiveX “in one respect in that it allows downloading and remote execution of code. However, that’s where the similarity ends” (Grossman); the way it operates is completely different. “A Java virtual machine places severe limits on what a Java applet you download from elsewhere can do. It is the responsibility of the Java virtual machine to make sure that all the ways an applet could potentially damage or alter your system without your knowledge are strictly controlled” (Chong). Because all java applets are executed in a secured area of memory, called a sandbox, so it is limited, but the way java is usually compromised is exploiting the flaws in the sandbox. If this is done, then the java applet can reign freely over the user's machine, kill other applets in use, perform processor intensive tasks that will eventually cause the system to freeze, or learn the contents of a computer's hard drive.

Now that we have covered the basics of what ActiveX and Java is, and the security vulnerabilities, what are ways to prevent this from happening? One simple way is to keep your software up to date. Usually all security leaks have been or will be patched, fixed, with an update from the developers. The software to keep current would be the operating system, web browsers, and applications that are commonly used. To be more specific when securing ActiveX, “Internet Explorer allows the user to set three different security levels…The highest security setting will not allow your browser to download any unsigned ActiveX controls. The medium setting warns you if you are about to download an
unsigned ActiveX control and lets you choose whether or not to continue. The low setting lets your browser automatically download any ActiveX control, signed or unsigned, without notifying you. By default, Explorer is set at the highest level of security. It can also maintain a list of developers you will accept controls from or certificate providers whom you trust” (Dugan). As Sean Dugan stated above, browsers can be also configured to allow or reject ActiveX controls as well as email clients. It is also possible to configure firewalls not allow ActiveX come into the network, but using ActiveX controls that stay within the intranet is not as bad of a threat. The most important way to safeguard a computer from ActiveX attacks is to know who the certificate came from, and where. If by some unfortunate event a malicious ActiveX control is used on a computer, the best way to find out where it came from is to look at the certificate, it will tell you the name and organization of where that control came from. After learning that information, the author could then be easily contacted.

With the information provided in this report, you should now have a basic understanding of what ActiveX and Java is, what they are used for, and the security risks involved in using them. These two growing technologies can be very useful, helpful, and fun if used correctly. Depending on the environment of your network, and if transmission of classified information like health records, it might be best if ActiveX is not used or if it is make sure to have a very close eye on it. ActiveX has a lot of power, but with careful planning, and a good security model you should feel safe using it.
References


