Global Information Assurance Certification Paper

ActiveX Controls - Risk and Control

Kam Ng

24 July 2000

Introduction

ActiveX is a Microsoft product consisting a set of technologies and services based on COM(Component Object Model). It embraces ActiveX documents, ActiveX controls, ActiveX Scripting and ActiveX Services.

ActiveX controls are most commonly known to computer users. It's Microsoft's response to the overwhelming market acceptance of Java applets at the time. These two technologies are similar. They are designed to be downloaded to World Web Browsers and executed. The browser is called the Container. Their difference is that ActiveX controls can interface with Microsoft Windows better than Java but the former offers very little cross-platform support.

ActiveX controls are small program building blocks that can be created using different flavors of computer programming languages. Once done, they can be downloaded to the Web-browser container through network for execution. Possible applications include data gathering, viewing certain kinds of files, displaying animation, special effects, etc.

The following characteristics contribute to the popularity of ActiveX's:

1. Reusability

Unlike Java applets, ActiveX programs resides on the user's hard drive. ActiveX controls a user download can be re-used by another Web-page without the need to download it again.

2. Extensibility

ActiveX controls can be created to accept parameters. This feature can be used to enhance the Web-surfing experience by changing the ActiveX controls appearance and action. This creates an advantage over Java.

3. Speed

ActiveX controls are stored in the local hard drive. There is no need to re-download the applet again. This minimizes the download time and the needed network bandwidth.

4. Power

ActiveX design allows running the ActiveX controls outside of the sandbox(see

Security Control Structure section below), it, therefore, can perform more complex and difficult tasks when compared to Java applets. It can write to the hard disk, send output to a program, access information of the computer system it resides and so on.

Security Control Structure

Like a virus, downloaded/mobile code is very difficult to manage and control. To make it more secure, Microsoft architects the ActiveX security based on Codesigning the applets and Sandboxing the applets. Also, Microsoft tries to educate developers on best design practice.

1. Codesigning

Codesigning is based on "authenticode" mechanism. The developer is required to sign his/her code with a digital certificate from CA(Certificate Authority). It provides the same level of accountability to end users of Internet software as buying a shrink-wrapped product in a store.

But this only serves the purpose to identify the code publisher who claims the integrity of the code has been validated. It does not prevent bugs or malicious operation.

This may not provide significant security improvement around ActiveX. The best it can do is to provide accountability for market and legal recourse. In fact, the classical Exploder Control just proved the point made here. It'll be described briefly below.

2. Sandboxing

ActiveX technology also uses security level control to improve the software security. There are two security component types with different level of system access control.

The first type are Sandbox components. They have limited access to the user system's resources such as the hard disk. This component type includes standard Java applets and libraries. Sandbox components are relatively safe but there'll never be any guarantee.

The second type is called full-access components. These are the components that run outside the sandbox such as ActiveX controls and trusted Java applets. ActiveX lets trusted Java applets access COM objects which are kept outside the
sandbox. Therefore, Java applets run under ActiveX can reduce the security level of the operating environment.

Security control for this component type is via authentication using Microsoft's authenticode technology.

The developer is responsible to validate and mark their ActiveX controls code with different levels of safety attributes. Web-browser bases on these attributes to ask the user for permission before running the code. This requires a good understanding of ActiveX security structure and the possible downloaded codes to determine the appropriate Web-browser setup to protect the users from running misbehaved codes.

Security Risks

1. Re-usability risk

ActiveX components are kept on the client's PC so they can be re-usable. As a result, they are accessible by other programs after the browser leaves the page.

2. Extensibility Risk

Being able to accept operating parameters, it's possible that malicious code writers can create ActiveX components that can selectively display malicious behavior depending on the passed parameters.

3. Power Risk

The power set given to ActiveX components can be used by malicious code to cause data damage to and information leak of the client systems.

Classical Security Breach Cases

1. Unsigned Malicious ActiveX Control - The Chaos Computer Control

On January 28, 1997, the Chaos Computer Club in Hamburg, Germany, claimed that they had created an ActiveX control that could modify and transmit a user's Quicken transaction file. In essence, the control was able to transmit electronic banking information such as account number and password to a third party computer and then update Quicken for the funds transfer.

2. Signed Malicious ActiveX Control - The Exploder Control

On June 17, 1996, the ActiveX Exploder control was posted on the Internet. As digitally signed, Exploder control contains an Authenticode certificate. When the control is downloaded to a PC with power conservation BIOS, it shut down

Windows95 and turns the PC off.

This case tells us that control with Authenticode certificate are not necessarily trustable. On the other hand, it often makes the user less wary about accepting a applet download which could turn out to be malicious even when it comes with a properly signed digital certificate. Also, aside from malicious intent, code coming from a well-known and trustworthy site is not a guarantee that it'll be properly behaving at all time.

Security Control

Like most viruses, ActiveX controls are being transported at the application layer.
Most of the time, ActiveX controls are sent using http protocol. This makes controlling ActiveX controls at lower network layers less effective.

Defense in depth at different points along the delivery chain is necessary to manage the ActiveX controls security risks. This includes the following security control points:

1. Corporate policies

Policies guide the security officers to make appropriate security decisions gearing towards the business needs of the organization. Without sound and easy
to understand policies, decision making will be very difficult to have all stake holders to come to a mutual agreement on how to deal with the security issues that come with business opportunities. This is particularly true for the e-business projects and organizations that need tighter coupling between the internal and external networks, either physically via computer network or logically via mobile/downloaded code such as ActiveX controls.

2. ActiveX scanning and behavior control at the network perimeter

All ActiveX code flowing into the corporate network should be scanned at the appropriate gateway before being allowed to it’s destinations.

Malicious code signature files should be kept up-to-date.

The control gateway should be able to be configured to detach all the ActiveX content if needed.

It should also be able to provide meaningful report for the administrator/security officers to act proactively to the downloaded/mobile code security problem.

Example of such control system is the SurfinGate from finjan (www.finjan.com)

3. At the Web-browser of the user frontend

There're security setup that can be used to further protect the user from malicious ActiveX malicious code. One example is to use Internet Explorer Security Zone. It is possible to configure the browser to only download or run ActiveX Controls located within the enterprise, the Intranet.

Some administrators may prefer to totally disable ActiveX and Java in the Web-browser. For Internet Explorer, try http://www.tiac.net/users/smiths/acctroj/howto.htm

4. User Education

Code Developers

All the developers coding for the organization should be made aware of the potential ActiveX risk and the security measures available. That way, the developers will be able to deliver ActiveX Controls and other components in such a way that the new code will be compatible with the best security practice for ActiveX.

Code Consumers

User education on ActiveX is one of the more effective defenses against the odds of being attacked by malicious applets. The principle is simple, if no user downloads ActiveX controls, there should be no risk because the organization is not vulnerable even if the threat is there.

But absolutely forbidding the use of ActiveX controls will be very difficult if not impossible to implement given the prevailing trend of more and more ebusiness.

Therefore, to mitigate the security risk, users should be made aware of why they should be concerned, what are the risks, when it can happen, where it would be coming from, who can be affected, how to use the Internet smartly to minimize the risk and lastly, how to handle the situation if infected by malicious ActiveX controls.

Conclusion

There is no and never will be solution that can provide 100% protection against ActiveX code or any other downloaded/mobile codes. The security risk is very much built in with the product. Security has been traded-off for functionality. There are partial solutions that can be used to mitigate the security risks that

come with its use.

Like other IS security issues, besides things suggested above in the "Security Control" section, the general guide-lines to be followed are "due diligence", "defense in depth" and "hope for the best but be well prepared for the worst".

Reference:

[1] Microsoft Corporation. "ActiveX Controls". 30 Mar 1999. URL: http://www.microsoft.com/com/tech/activex.asp

[2] Microsoft Corporation. "ActiveX Controls Overview". 23 Oct 1998. URL: http://msdn.microsoft.com/workshop/components/activex/ctrlovw.asp

[3] Microsoft Corporation. "How to write and use ActiveX controls for Microsoft Windows CE". June 1999. URL: http://msdn.microsoft.com/library/techart/activexce.htm

[4] Microsoft Corporation. "ActiveX Controls". URL: http://msdn.microsoft.com/workshop/components/activex/controls.asp#bk_activ
e
x_controls

[5] Indiana University knowledge Base. "What's ActiveX". 6 July 1999. URL: http://kb.indiana.edu/data/afoi.html

[6] Richard, Smith. "Accidental Trojan Horses: Security problems in Windows 98 PCs". 12 Aug 1999. URL: http://www.tiac.net/users/smiths/acctroj/

[7] Lars, Klander. "Hacker Proof". 1997. Published by Jamsa Press.

Last Updated: July 24th, 2017

Upcoming Training

SANS Prague 2017	Prague, Czech Republic	Aug 07, 2017 - Aug 12, 2017	Live Event
SANS Boston 2017	Boston, MA	Aug 07, 2017 - Aug 12, 2017	Live Event
Community SANS Omaha SEC401*	Omaha, NE	Aug 14, 2017 - Aug 19, 2017	Community SANS
SANS New York City 2017	New York City, NY	Aug 14, 2017 - Aug 19, 2017	Live Event
SANS Salt Lake City 2017	Salt Lake City, UT	Aug 14, 2017 - Aug 19, 2017	Live Event
SANS Virginia Beach 2017	Virginia Beach, VA	Aug 21, 2017 - Sep 01, 2017	Live Event
SANS Adelaide 2017	Adelaide, Australia	Aug 21, 2017 - Aug 26, 2017	Live Event
Community SANS Trenton SEC401	Trenton, NJ	Aug 21, 2017 - Aug 26, 2017	Community SANS
Virginia Beach 2017 - SEC401: Security Essentials Bootcamp Style	Virginia Beach, VA	Aug 21, 2017 - Aug 26, 2017	vLive
SANS Chicago 2017	Chicago, IL	Aug 21, 2017 - Aug 26, 2017	Live Event
Community SANS Pasadena SEC401 @ NASA	Pasadena, CA	Aug 23, 2017 - Aug 30, 2017	Community SANS
Mentor Session - SEC401	Minneapolis, MN	Aug 29, 2017 - Oct 10, 2017	Mentor
SANS San Francisco Fall 2017	San Francisco, CA	Sep 05, 2017 - Sep 10, 2017	Live Event
SANS Tampa - Clearwater 2017	Clearwater, FL	Sep 05, 2017 - Sep 10, 2017	Live Event
Mentor Session - SEC401	Edmonton, AB	Sep 06, 2017 - Oct 18, 2017	Mentor
SANS Network Security 2017	Las Vegas, NV	Sep 10, 2017 - Sep 17, 2017	Live Event
Community SANS Albany SEC401	Albany, NY	Sep 11, 2017 - Sep 16, 2017	Community SANS
Mentor Session - SEC401	Ventura, CA	Sep 11, 2017 - Oct 12, 2017	Mentor
Community SANS Columbia SEC401	Columbia, MD	Sep 18, 2017 - Sep 23, 2017	Community SANS
Community SANS Dallas SEC401	Dallas, TX	Sep 18, 2017 - Sep 23, 2017	Community SANS
Community SANS Boise SEC401	Boise, ID	Sep 25, 2017 - Sep 30, 2017	Community SANS
Baltimore Fall 2017 - SEC401: Security Essentials Bootcamp Style	Baltimore, MD	Sep 25, 2017 - Sep 30, 2017	vLive
Community SANS New York SEC401	New York, NY	Sep 25, 2017 - Sep 30, 2017	Community SANS
Rocky Mountain Fall 2017	Denver, CO	Sep 25, 2017 - Sep 30, 2017	Live Event
SANS London September 2017	London, United Kingdom	Sep 25, 2017 - Sep 30, 2017	Live Event
SANS Baltimore Fall 2017	Baltimore, MD	Sep 25, 2017 - Sep 30, 2017	Live Event
SANS Copenhagen 2017	Copenhagen, Denmark	Sep 25, 2017 - Sep 30, 2017	Live Event
Community SANS Sacramento SEC401	Sacramento, CA	Oct 02, 2017 - Oct 07, 2017	Community SANS
SANS DFIR Prague 2017	Prague, Czech Republic	Oct 02, 2017 - Oct 08, 2017	Live Event
Community SANS Charleston SEC401	Charleston, SC	Oct 02, 2017 - Oct 07, 2017	Community SANS
Mentor Session - SEC401	Arlington, VA	Oct 04, 2017 - Nov 15, 2017	Mentor