Auditing ActiveX Controls

Cesar Cerrudo Independent Security Researcher/Consultant

Outline

ActiveX definition
ActiveX security
Auditing ActiveX
Demo
Preventing ActiveX exploitation
References

ActiveX control

Basically an ActiveX Control (formerly known as OLE control) is software based on the Component Object Model(COM). ActiveX controls are portable and reusable and can be used in many programming and scripting languages. They are widely used by web based applications to extend their functionality (ie: Windows Update site, etc.).

ActiveX security is most based on "trust"

If you trust the author.
If you trust IE.
If you trust the site, etc.

No sandbox to restrict access to system resources.
Once an ActiveX is run it can perform any

action on the system.

ActiveX controls can be signed or unsigned

- Signed doesn't mean that the control is safe.
- Signing only helps to identify the control's author and that the control wasn't modified.
- Ignored when controls are not installed from Internet Explorer.

ActiveX controls can be marked as safe

- Again, this doesn't mean that the control is safe.
- By the existence of some registry subkeys: subkey {7DD95801-9882-11CF-9FA9-00AA006C42C4} means safe for scripting, subkey {7DD95802-9882-11CF-9FA9-00AA006C42C4} means safe for initialization.
 By IObjectSafety interface.

ActiveX controls can be restricted to run only under specific domains

- Using SiteLock template or custom code.
- After the control is run the actual URL is checked against allowed domains, if it doesn't match, execution can be aborted.
- Can be easily defeated by XSS and IE cross domain issues.

ActiveX security options can be set on IE
– ActiveX execution can be restricted.
– Restrictions can be bypassed by exploiting XSS or IE cross domain issues on trusted sites, exploiting IE cross zone issues. What about a XSS on Microsoft.com ☺

Conclusion

- ActiveX security mechanisms only help to mitigate risks, they don't prevent.
- ActiveX controls can be abused bypassing security mechanisms.
- A "really safe" ActiveX should not perform any dangerous action on the system and be vulnerability free.
- ActiveX controls are dangerous.

Auditing ActiveX (why?)

To perform QA.
To detect security vulnerabilities.
To check if a control is "really safe".
Sometimes people are forced to run ActiveX controls because they are used by "must use" applications, auditing could help you to sleep better at night ©.

- Microsoft OLE/COM object viewer (OleView)
 - Tool that allows easy access to OLE/COM objects information, interfaces, methods, properties, etc.
 - Helps to get ActiveX controls information and to enumerate methods and properties.

Registry monitor (www.sysinternals.com)
Tool that monitor registry access, it allows to see what application is performing some action on some registry key and value.
Helps to detect if an ActiveX control is accessing registry and what actions it is performing.

File monitor (www.sysinternals.com)

- Tool that monitor file system access, it allows to see what application is performing some action on some file/folder.
- Helps to detect if an ActiveX control is accessing file system and what actions it is performing.

TCPView (www.sysinternals.com) - Tool that shows TCP/UDP ports opened and TCP connections made by processes. Helps to detect if an ActiveX is opening ports or making outbound connections. Microsoft Windows Debugger (WinDbg) – Windows based debugging tool. Helps to detect ActiveX buffer overflows.

Any protocol analyzer/sniffer

Helps to determine what data is being sent and received by an ActiveX.

Strings (www.sysinternals.com)

Tool for searching text strings in binary files.
Helps to look for ActiveX methods and properties when an ActiveX does not have a type library.

Getting information about the control

- Run OleView tool to determine if the control is marked as safe, to enumerate methods and properties, etc.
- If the control does not have a type library, use Strings tool to find methods and properties in ActiveX binary.
- Find out initialization parameters.
- Determine if the control is restricted to run only under some specific domains.

After finding all the ActiveX related information, we can start auditing it.
Best way to audit an ActiveX is creating an HTML page to invoke the control.
The HTML page is opened with IE while it's attached to a debugger and monitoring tools are running.

What to look for?
Registry and file system access.
Buffer overflows.
Information leakage.
Dangerous methods.
Opened ports.

Auditing buffer overflows

- Identify all string inputs on ActiveX initialization parameters, properties and methods.
- Try with a long string value on every input and open the HTML page with IE.
- Look if the debugger halt on an exception, if not debugging look if IE crash (if the exception is handled IE may not crash).

Auditing file and registry access
Try with a test string value on every input.
Look at monitoring tools if file system or registry is accessed.
Identify what kind of access occurs.
Try to read, write, delete arbitrary files and

registry values.

Auditing (Misc.)

- Use TcpView to identify if IE is opening additional ports and making outbound connections.
- Run a protocol analyzer/sniffer to see data transmitted and received.
- Test ActiveX properties and methods to determine if sensitive information is exposed.
 Test ActiveX for dangerous methods.

Basic guide for auditing

- Learn control logic and functionality by trial an error, by error messages, etc.
- Sometimes properties and/or methods must be set and/or executed before executing other actions.
- Sometimes ActiveX controls do a weak validation, use test strings mixed with right values (ie. If a method has a URL as parameter try with "http://XXXXXXX...", etc.).

Basic guide for auditing (cont.)

- Try to trick the ActiveX to do things that it's not supposed to do.
- Don't frustrate yourself if you didn't find anything, stop, think and continue.
- When you think that there are not more holes, relax and continue, sure you will find another. (Cesar Law [©])

DEMO

- Getting information about the control.
- Building an HTML test page.
- Enumerating initialization parameters.
- Detecting if the control only runs under specific sites.

DEMO

- Auditing buffer overflows.
- Auditing file and registry access.
- Determining if sensitive information is exposed.
- Detecting if the control has dangerous methods.

Preventing ActiveX exploitation

Set Kill Bit

 Set Compatibility Flags DWORD value to 00000400 under key HKLM\SOFTWARE\Microsoft\Internet Explorer\ActiveX Compatibility\CLSID of the ActiveX control

Only prevent ActiveX from running on IE.

Remove ActiveX controls.

References

Results of the Security in ActiveX Workshop

http://www.cert.org/reports/activex_report.pdf

MSDN

http://msdn.microsoft.com/

SiteLock Template

http://msdn.microsoft.com/downloads/samples/internet/components/SiteLock/default.asp

References

Kill Bit

http://support.microsoft.com/support/kb/articles/q240/7/97.asp

Monitoring tools

http://www.sysinternals.com

Microsoft debugging tools

http://www.microsoft.com/whdc/ddk/debugging/default.mspx



Questions? Thanks for coming