

## Re: why microsoft choose mfc rather than wtl?

---

*Source:* <http://www.tech-archive.net/Archive/VC/microsoft.public.vc.mfc/2005-04/msg00896.html>

---

- *From:* Russ <[russk2@xxxxxxxxxxxx](mailto:russk2@xxxxxxxxxxxx)>
  - *Date:* Mon, 11 Apr 2005 19:42:12 -0400
- 

Daniel, thanks for your comments. It seems that your points hinge on the ability of someone to spoof my website and convince our customers to lower security settings, etc. I really think this is a matter of customer education. They must be taught to never accept any new server certificate(s), or change security settings beyond what is required for the initial installation.

But I am not at all convinced that spoofing our site and fooling anyone to accept a bad file would be that easy. The architecture of the site is such that the downloadable AX file only appears on a page that is several pages away from the start page. For a client to get there, he must traverse the pages and there must be data, specific to that client, that must be present and displayed on the page, or else the particular AX control is never accessed, shown, or downloaded. The data is stored on our back end server and is only accessible through two firewalls and via encrypted XML. I don't see the possibility that anyone will be able to spoof this data in a convincing manner.

So, to fool the client, the spoofer has to get him to accept a different client certificate, and get him to accept significantly different looking and performing web pages than he is used to. Then he also has to convince him to add that page to his trusted sites list, and/or lower his security settings to accept an unsigned control.

In my mind, anyone who is dumb enough to do all that, after being warned not to, is probably going to have a lot of other problems. He will probably be willing to download almost anything from anybody. I do not see that type of person to be our client. If it ever does happen, there is no way that the client's data that we hold will be compromised. If his computer is destroyed, and he blames us, I am willing to kiss the client goodbye and look for one with more smarts.

The bottom line though, for me, is that Microsoft has provided tools that allows us to deliver a business application to clients who only need a web browser and the ability to install a fairly simple piece of our software. The ability to update that software 'semi-automatically' during normal use of that product is a big

Re: why microsoft choose mfc rather than wtl?

advantage. I don't see the danger as anywhere near as threatening as what can happen to the buyer of an automobile if he does not heed safety warnings. I don't think many people would say that it is unethical to deliver an automobile to customers because it is possible for them to kill themselves with it.

You said:

>So, the question isn't whether you should design your site so that it  
>downloads a control over the wire, it's whether you ought to be using a  
>control for this \*at all\*. I don't know what your business application  
>is, but there are other ways of manipulating the browser display. Java  
>applets are much more secure than native executable code because the  
>JVM's sandbox has limited access to the machine, though they're still a  
>potential risk and should only be used when absolutely necessary...

There are some things that cannot be done with HTML. I don't know about Java, but I suspect the same thing is true. My Activex control is for the purpose of printing reports. It parses a downloaded reports file and sends the individual reports to the clients printer (s). It allows the client to specify which printer will be used for various types of reports, and saves that information in his registry so that he will not have to reselect printers every time. So it has to access the downloaded print file, his printers, and the system registry. The alternative is to deliver a full fledged application to do the same thing. The web solution, with Activex, is much more cost effective.

I have no quarrel with those who say an unsecured page with unsecured Activex controls is dangerous. But I do object to a blanket condemnation of the technology. On the other hand, maybe Microsoft should not be pushing the idea of IE based business solutions. Clearly some of the safeguards built into IE are at cross-purposes with business requirements. (For instance the inability to access system resources like printers & hard drives, or the inability to do something as simple as remove the "back" button and it's keyboard equivalents.) As I see it, using IE for this purpose (business apps) is just barely sufficient and operable. It could be a lot smoother if some of the restrictions were relaxed. Maybe Microsoft should come out with an alternative browser for business applications which would relax some of the prohibitions, but which could not be used in an unsecured environment.

Well, that's about all I have to say on the subject. Perhaps it gives you some things to think about. I know your comments made me think about it more.

Thanks, Russ

On Mon, 11 Apr 2005 11:41:24 +0100, Daniel James

Re: why microsoft choose mfc rather than wtl?

Re: why microsoft choose mfc rather than wtl?

<wastebasket@xxxxxxxxxxxxxxxx> wrote:

>In article news:<fhoi51p1k2ip4g56htn4rcnsloaee28834@xxxxxxx>, Russ

>wrote:

>> I respect both of your opinions, even though you have inadvertently  
>> called me 'unethical', but I would appreciate it if you could tell me  
>> good reasons for your blanket condemnation.

>

>My condemnation is of the introduction of technology into the browser  
>that enables executable code to be executed on the client PC. Executable  
>code can do anything – from formatting the hard drive to copying your  
>personal details to a criminal organization to EMailng death threats  
>from your account to the White House – so it's not something the user  
>innocently browsing the web wants to have arbitrary websites running  
>behind his back.

>

>As I'm sure you know: The browser can be configured to allow or prevent  
>the download of executable code, and can be configured to allow or  
>prevent the automatic running of the code. Furthermore code can be  
>digitally signed so that you know (in theory) who wrote it. The fact  
>that these controls can be set to insecure configurations makes  
>them a liability. Most users don't understand what the settings do and  
>will blindly follow instructions on a web page that tell them to lower  
>the security of their browser settings in order to get a page to "work".

>

>It was folly ever to allow the insecure settings to be supported ... but  
>ActiveX controls were supported in web pages because they were "cool",  
>with no thought to the fact that they were a security liability.

>

>> Now this is a business application ... It seems to me that there  
>> are sufficient safeguards built into the system to make this  
>> perfectly safe. In my case, all communication between the client  
>> and the server is done via SSL, and the identities of both the  
>> client and the server are confirmed by certificates.

>

>There are safeguards. Whether or not they are "sufficient" is moot.

>

>For example: What would the majority of users do if someone spoofed your  
>site with one that prompted the users to lower the security settings and  
>download a new control signed with a spoofed certificate ... perhaps a  
>self-signed certificate created with a subject ID that claims it belongs  
>to your company. The page might have some reassuring words telling the  
>users to check the certificate ID to ensure their security. How many of  
>your users would blindly go ahead and do what was asked, without  
>considering the security implications?

>

>By using a downloadable control you leave yourself open to this sort of  
>attack. Is it worth it?

>

>> This is a TON easier than having to distribute the new control to  
>> thousands of clients and expect that they will all install it without

Re: why microsoft choose mfc rather than wtl?

Re: why microsoft choose mfc rather than wtl?

>> problems!

>

>Oh, yes. Of course it is. It may even be more secure because it is  
>probably harder to spoof a website than it would be to send a CD in the  
>post to all your customers with a note saying "here is an update to the  
>browser plug-in for our web site, please install it at once". Most  
>people would do that without thinking, too.

>

>> So, tell me, what is so 'unethical' about the above scenario?

>

>It's not "unethical", it's naive. You have thought about the security  
>but you haven't looked hard enough. You haven't considered just how  
>security-unaware most users are.

>

>[Of course, even if \*you\* didn't use an ActiveX control there'd be  
>nothing to stop an attacker spoofing your site and getting the users to  
>download one ... but at least you could have a page in your  
>documentations saying "we don't use ActiveX controls and we strongly  
>advise you not to enable them in your browser for security reasons".  
>Then at least, if someone suffered a spoofing attack you could say "It's  
>not our fault. We told you not to do that".]

>

>You also haven't considered that some of your potential customers will  
>have knowledgeable security staff who will very sensibly tie down the  
>browsers on users' desktops so that they will be unable to access your  
>website. You'll lose customers if you rely on that control to make your  
>site work. You'll also lose customers who are using browsers that can't  
>run ActiveX controls -- which automatically includes any customers who  
>aren't using Windows.

>

>So, the question isn't whether you should design your site so that it  
>downloads a control over the wire, it's whether you ought to be using a  
>control for this \*at all\*. I don't know what your business application  
>is, but there are other ways of manipulating the browser display. Java  
>applets are much more secure than native executable code because the  
>JVM's sandbox has limited access to the machine, though they're still a  
>potential risk and should only be used when absolutely necessary (Java  
>also works in more browsers and on more platforms than ActiveX). Any  
>kind of server-side scripting will remove the risk from the client's PC  
>altogether, though at the cost of more load on the servers and probably  
>an increase in communications bandwidth. It depends what you're doing.

>

>What's wrong with HTML, for your application, anyway?

>

>Cheers,

> Daniel.

>

>

.

- **Follow-Ups:**

- ◆ **Re: why microsoft choose mfc rather than wtl?**  
◇ From: Daniel James

- **References:**

- ◆ **why microsoft choose mfc rather than wtl?**  
◇ From: Huang Shu Huai
- ◆ **Re: why microsoft choose mfc rather than wtl?**  
◇ From: Joseph M . Newcomer
- ◆ **Re: why microsoft choose mfc rather than wtl?**  
◇ From: Daniel James
- ◆ **Re: why microsoft choose mfc rather than wtl?**  
◇ From: Joseph M . Newcomer
- ◆ **Re: why microsoft choose mfc rather than wtl?**  
◇ From: Daniel James
- ◆ **Re: why microsoft choose mfc rather than wtl?**  
◇ From: Russ
- ◆ **Re: why microsoft choose mfc rather than wtl?**  
◇ From: Daniel James

- Prev by Date: **CString Function from DLL**

- Next by Date: **Re: Anybody in here do much with COM? Need to know what newsgroups...**

- Previous by thread: **Re: why microsoft choose mfc rather than wtl?**

- Next by thread: **Re: why microsoft choose mfc rather than wtl?**

- Index(es):

- ◆ **Date**
- ◆ **Thread**