

Browser Wars

By Bill Hely

There are a lot of conflicting stories floating around the World Wide Web about the relative "safety" of different web browsers. In reality things aren't quite as cut and dried as many of the story-tellers would have you believe.

If you ever take the trouble to read the warnings and alerts issued by watchdog services such as US-CERT you'll notice certain phrases appearing with monotonous regularity. One such description goes something like:

"... could allow a remote attacker to execute arbitrary code on an affected system".

Every time such a warning appears related to a Microsoft product, the press and pundits start screaming about *"Microsoft's failure to provide adequate security"*.

Let's face it, Microsoft is the big target so they get the most press attention. What the same press and pundits rarely mention is that the exact same phrase is not uncommonly used in reference to highly respected commercial heavyweights such as, for example, Oracle¹ Database Server. But, since 90% of the computer-using population don't know what Oracle is, such disclosures only get a mention in narrowly targeted specialist publications.

OK, yes, its true ... you don't see Oracle or any other major application appearing in the warnings nearly as often as do Microsoft's products. But, again, although Oracle products are used extensively by many of the world's largest organizations, Microsoft has many more products on many millions more PCs than any other player, regardless of size.

Perspective, my friend ... we must always strive to keep things in perspective.

Your best and safest and most workable option is to secure your PC with the help of a reliable reference source such as *The Hacker's Nightmare*TM and forget about chopping and changing to find "more secure" alternatives to your various Office programs.

If you want a computing environment that is inherently more secure by default, give Windows away altogether. Install UNIX on your PC, spend a year or two learning how to use it, and get used to being significantly incompatible with just about everyone else you need to interact with.

And then keep a watch out for the warnings about how *"...vulnerabilities could allow a remote attacker to execute arbitrary code on an affected **UNIX** system"*. They're rarer, but far from absent.

Since it is the Microsoft Internet Explorer web browser that attracts the most criticism and is the target of most recommendations to *"use something else"*, let's try to take an unemotional look at that situation.

All versions of Microsoft Windows come with the Internet Explorer web browser pre-installed. While there are many other browsers you can choose to use instead—many of them free—Internet Explorer's tight integration with the Windows Operating System

¹ Oracle is both a company—the second largest software manufacturer in the world after Microsoft—and a product. The Californian company claims to be the world's leading supplier of software for information management. Its Oracle relational database products run on high-end workstations, personal computers, minicomputers and mainframes, and are used in many Fortune 1000 corporations.

Browser Wars

means that its installed base outnumbers any other brand of browser by a ratio of literally millions to one.

It stands to reason, then, that when the cyber-grubs hatch their poisonous schemes against you and other Internet surfers, they aren't going to choose to target a browser that, by comparison, is used by an insignificant number of people.

Over the years there have been many thousands of attacks against Internet Explorer, and it has to be admitted that these attacks are, for the most part, made possible by vulnerabilities in the program code that makes Internet Explorer what it is.

Predictably, the next thing that happens is that the press and various gurus start publicly declaring Internet Explorer to be "unsafe" and recommending that you abandon it and start using some other browser instead.

And so we get to the two most important questions I want to deal with in this section:

1. Is Internet Explorer unsafe?
2. Should you change to some other browser?

OK, no beating about the bush. The one-word answer to question #1 is "Yes". Internet Explorer unarguably had (and has) many vulnerabilities—weaknesses that can be exploited by a programmer of the cyber-grub variety. Undoubtedly many more flaws will be discovered as time goes by, despite continued development, updates and patches.

You see, there is no such thing as a computer program of any significant degree of complexity that is immune to attack. Any computer code can be manipulated by a programmer who is clever enough and has the will to do so.

So why do we hear so much about the problems associated with Internet Explorer and very little about vulnerabilities in its competitors?

In large part it gets back to the popularity thing again. Insiders have a term for it: "security by obscurity". In other words, if the miscreants don't know about you, or if you are too insignificant to worry about, they won't beat you up.

That's not the whole story by any means. I frequently see writers proclaiming how weary they are of the "excuse" that Internet Explorer is only a target because it is the most popular. Well, the universe doesn't give much of a damn just how fed up they are—a fact is still a fact.

But reasonable people must acknowledge that it isn't *all* of the story.

I'm not making excuses for Microsoft. They have made a lot of mistakes and have a lot to answer for in many areas of their operations. Some of their policies have been morally, even legally, indefensible. But there's no such thing as non-trivial software that can't be compromised.

As unbelievable as it may sound, many of the program's inherent weaknesses were actually placed there *by design*. Microsoft's programmers intentionally provided many avenues for third-party programmers to add extra functionality to Internet Explorer. In the simpler and less paranoid early days of Windows development, that may have seemed like a reasonable, even commendable, thing to do.

Browser Wars

Of course, it backfired—badly. With the benefit of hindsight we can say that it was doubtless naive of those Microsoft programmers to think that all those lovely openings would only be used by the good guys to enhance the product and the user experience.

But back to the present.

Microsoft gets most attention from the cyber-vermin because it is the biggest and it has more software "out there" than probably all the rest put together. As stated, the grubs are not likely to try to make a name for themselves by attacking software from a startup with just a handful of installations in the marketplace.

The Apple comparison

I don't want to delve into this in any depth, but in all fairness there are a couple of things I should say about the relative vulnerability status between PCs and the Apple platforms.

The concept of "security by obscurity" that I mentioned earlier certainly plays a part in Apple's favor. The cyber-grubs want the biggest bang for their buck, the maximum exposure for their destructive output, so it's only natural they'll focus their efforts on the biggest player, which is Microsoft by a gargantuan margin.

But it must be said that it is more difficult to write malware (such as a virus) for the Apple Operating System. There are several reasons for this, the main one being that Apple Operating Systems are based on the Unix Operating System*, which first appeared as far back as 1969.

However, while Unix is inherently more secure than Windows, neither it nor its offspring are bullet-proof—far from it—and only foolish Apple users will ignore any opportunity to be proactive with security measures.

* Few users of Apple Computers ever realize that it is still possible to get "under the covers" and work directly with the Unix subsystem and Unix tools.

Second question: *"Should you change to some other browser?"*

Well, that depends on why you are changing. If you simply prefer the "look 'n feel" of another browser, or you like the way it does certain things, or you are hooked on some specific feature, then why not? By all means use whatever takes your fancy.

But before changing do give some thought to the matter of compatibility. Not all websites work equally well in all browsers. For example, if your work, profession or interests require that you interact with sites built around Microsoft's SharePoint technologies, then you'll be left out in the cold if you abandon Internet Explorer.

Also, many useful browser add-ons, extensions and toolbars only support one brand of web browser.

Still, by all means go with whatever attracts you.

But if your decision to change is prompted by the belief that Internet Explorer is "unsafe" and Brand-X is "safe", then your decision may be based on a false premise.

One of the most frequent reports we see in the popular press is worded something like: *"...a threat that targets a known flaw in Microsoft's Internet Explorer"*.

Now here's the question you should be asking yourself when you see such a report: Why should any **known** flaw be a vulnerability?

Browser Wars

Contrary to claims by rabid Microsoft-bashers, important vulnerability discoveries that threaten security are usually (but, unfortunately, not always) addressed by Microsoft in an expeditious manner. That's a general observation, and by no means does it exonerate Microsoft from some puzzling failures and omissions.

The main reason so many people succumb to *known* vulnerabilities is that the majority of computer users haven't got a clue about even elementary security precautions!

In most cases known flaws have been quickly addressed by *readily available* and *free* fixes, yet how many people apply them, or even know or care about them.

Of all the major virus/worm/trojan attacks that have circled the globe over the past few years—in some cases almost bringing the Internet to its knees—I can't recall one instance that just *had* to happen. Every such threat exploits the fact that millions of people are not taking responsibility for their own welfare and keeping their PCs secure with free and readily available resources.

There are those who will respond with: *"Why should we have to? Our computers should just automatically be safe and secure"*.

Well, that would certainly be nice, but as far as the likelihood of our software technology reaching that happy state in the near future, dream on. Maybe in another few decades—about when road transport is 100% safe and fatal accidents unheard of.

If we are going to use any complex appliance—be it car, computer, microwave oven or whatever—it is our own responsibility to keep informed as to elementary safety issues at the very least. While millions of people refuse to do that, or can't be bothered, or don't know how, they are going to be subject to violation in one form or another, no matter what Internet browser they decide to use.

None of this is new, as a little research would soon reveal. Which raises the old quandary: conflicting advice abounds, so who do you listen to? Who can you trust?

I'm not necessarily asking you to trust my word alone, and obviously you are unlikely to get fair, impartial and informed advice from any entity with a vested interest for or against a particular product, such as a manufacturer/publisher.

You have to find agencies with an established reputation for impartiality coupled with the technical expertise to unravel all the intricacies, and who will report in terms you can understand.

One of the most highly regarded organizations researching virus/worm/trojan and other vulnerabilities in a wide cross section of products and operating systems is Danish security firm Secunia:

<http://HackersNightmare.com/Secunia>

Their website provides lots of very relevant information.

If you are reasonably fluent in techno-speak, a good source of personal experiences and informed opinions from people of above-average technical competence is SlashDot, which covers a broad spectrum of topics, including security matters:

<http://HackersNightmare.com/SlashDot>

SlashDot is a community populated mostly by tech-types.

Browser Wars

Spend some time on either of those websites and you'll soon appreciate that every browser has its problems. It is thus not unreasonable to assume that every browser harbors other, as-yet undiscovered, potential problems that will surface in time.

Here's a very apt quote from Thomas Kristensen, Secunia's Chief Technical Officer:

"A product is not necessarily more secure because fewer vulnerabilities are discovered".

That statement reinforces the "security by obscurity" position I presented earlier. Given the complex nature of large and convoluted software code, potential problems almost certainly exist in all big programs. Until a particular program attracts a user base big enough to get the attention of a cyber-grub, those vulnerabilities are not probed and will most likely remain undiscovered.

One possible compromise is to run more than one browser on your system. It is an eminently sensible option because you don't need to risk deprivation just to mostly use the browser of your choice, no matter how big or small a following it may have.

I keep my own systems patched, scanned, fire-walled, backed-up and up-to-date and I have no more concerns about Internet Explorer than I would about any software program. Even so, I have long had several different browsers installed.

This is not from any dissatisfaction with Internet Explorer, but so I can see how a website will look and perform in the different browsers. And believe me, there can be some significant differences.

Some complex websites that use proprietary technologies to improve the user experience just won't work at all in some browsers. But you can bet that if there's one browser that's going to be "more supported" than others by website developers, it will be the one with the greatest number of users—Internet Explorer.

Danger! Do not uninstall Internet Explorer

Anyone considering a change should not attempt to uninstall Internet Explorer v6.0 or earlier. You can uninstall Internet Explorer 7.0, which will see your system revert back to the previously installed Internet Explorer version, but do not attempt to uninstall Internet Explorer completely.

Whether or not it is even possible to uninstall depends on your Windows version. Internet Explorer v6.0 and earlier are so tightly integrated with the Windows Operating System that removal attempts could well have some very undesirable side effects. Just leave it alone and install your preferred browser separately. Multiple browsers can happily coexist side-by-side.

Non-use of IE doesn't mean unaffected by IE problems

I've seen a number of people proclaim that they switched from Internet Explorer to Brand-X "for security reasons". Most then say they still have Internet Explorer installed but only use it when they have to. OK, they can use what they like, but it's quite clear that the real issue is not at all understood, so let's look a little deeper at that philosophy. Don't worry overmuch about understanding the fine detail of the next few paragraphs. Just try to see the big picture.

Internet Explorer is a "container" that brings together a number of different code segments, or modules, each designed to perform a particular task that contributes to

Browser Wars

browsing functionality. One of those modules is called the *HTML Rendering Engine*, which in turn is made up of other sub-components.

Just to give you an insight into the complexity, the components that form the HTML Rendering Engine are:

- DOM (Document Object Model)
- Screen Renderer
- Parser
- DOM Builder
- Print Renderer
- CSS Parser
- HTML DOM Fixer
- Layout Engine
- Document Type Definition Validator

As you can imagine, this is complex stuff for programmers to create and merge into a working whole.

Now, if another (non-Microsoft) developer working on a HTML software product could use some or all of the complex code of IE's Rendering Engine for his own product, he could save a lot of development time.

And that's exactly what happens.

Because Internet Explorer is universally present on Windows computers, other developers can and do use program code that is already available in Internet Explorer, without having to "reinvent the wheel", as it were.

For example, IE's Rendering Engine is used by the Outlook and Outlook Express eMail clients (both from Microsoft), by Windows Help files of the compiled HTML type (no matter who produces them), by some non-Microsoft eMail clients, plus other applications as well. If the Rendering Engine is not available then those dependant programs won't be properly presented.

There's even a third-party add-on called *IETab* available for Internet Explorer's main competitor that allows users of Mozilla Firefox to switch between its own rendering engine and that of Internet Explorer.

So whether you decide to use Internet Explorer as your browser or not, there is always a possibility that you are using some component part of it anyway, by virtue of some other program's reliance on its presence.

Thus hopefully you can see that, depending on what part of Internet Explorer's code a threat targets, simply not using IE as your browser doesn't necessarily mean you are not exposed to the same threat, because you *will* have Internet Explorer installed on your system. This is a good illustration of how taking action without really understanding the problem can lead to a false sense of security.

I'm not paid to be an Internet Explorer evangelist, and I have no problem with you using whatever browser you prefer and feel most comfortable with. But there were some points which needed to be made in the interests of accuracy and hopefully to the benefit of less experienced people who may have been swayed by false claims. However let me offer a provocative suggestion:

Whether or not you "feel" unsafe using Internet Explorer is beside the point. Whatever makes you feel good is OK by me. But...

If you REALLY ARE unsafe using Internet Explorer, then you have more problems that need addressing than just which browser you use.

Browser Wars

Here's a quote from an article by freelance technology writer Paul Boutin, who himself uses the popular *Firefox* browser:

Will Firefox make your computer hack-proof? Even Mozilla [the developers of Firefox] stress that no software can be guaranteed to be safe, and that Firefox's XPInstall system could conceivably be tricked into installing a keystroke logger instead of Sun's Java engine. But for now, there's safety in numbers—the lack of them, that is. Internet Explorer is used by 95 percent of the world. Firefox's fan base adds up to 2 or 3 percent at most. Which browser do you think the Russian hackers are busily trying to break into again?

Since the début of Mozilla Firefox there have been numerous alerts from US-CERT announcing "*Multiple vulnerabilities in Mozilla products*". One of the Mozilla products frequently mentioned has been Firefox, the browser so many people claim to have switched to "*for security reasons*".

Commendably, the Mozilla developers have had the necessary patches out and freely available very quickly. Just as Microsoft usually does with Internet Explorer.

Have a good look around the Secunia website and you'll see that all browsers have vulnerabilities that need to be addressed in the interests of security, and past discoveries are very unlikely to be the end of the story with any of them.

As I have repeated numerous times: Whatever Internet browser you decide to use is fine by me. Just be sure you are making your decision for the right reasons and not under any delusion that security will cease to be an issue. It won't.

And much the same goes for the never ending Microsoft Outlook vs. Brand-X eMail client debate.

Both Outlook and Internet Explorer can be used quite safely within the protective envelope of a comprehensive security strategy, which is what *The Hacker's Nightmare*™ teaches you to develop. Once again...

If you don't have a comprehensive and effective security strategy in place, you have more problems than just what browser or eMail program to use.

-oOOo-

Bill Hely is a technologist, consultant and author living in Brisbane, Australia. For most of the last two decades his professional focus has been on advising and supporting small business operators in Information Technology and Office Productivity issues. He is the author of several books and numerous articles on technology for the business operator, including the Bible of Internet and computer security *The Hacker's Nightmare*™.

To comment on this article please use the "Support" link at the bottom of the <http://HackersNightmare.com> main page.

Comments, suggestions, expressions of appreciation
— and especially testimonials —
are most welcome.