Why Windows is so Insecure

2008 February 9 by Anthony Glenn, http://www.netspeed.com.au/adglenn/

Windows is hopelessly insecure. It gets infected by malware amazingly easily. The major reason why that happens is the poor handling of executable files. Every time an executable file is started then the programmer who wrote the executable file can do anything he pleases to the computer. Windows allows the following scenario to happen:

1. The user of the computer foolishly downloads some executable file from some seedy place on the Internet. The deluded user may think he is getting “Picture of Hot Babe”, “Cool Screensaver”, “Latest Whizzy Game” or whatever. Somehow, somebody out there talks him into downloading the file. To download the file all he has to do is click on the link, then click “OK”.

2. Then the file is there in a directory on the user's hard disk, but one of the Very Foolish default settings for Windows is to “Hide Extensions for Known File Types”. The extension is the .exe part of the filename which tells Windows to execute the file. So instead of seeing “Picture of Hot Babe.exe” and being alerted that it is an executable file instead of a picture, all he sees is “Picture of Hot Babe”.

3. Thinking he is about to see “Picture of Hot Babe”, he double-clicks the file. The file is executed. No “Picture of Hot Babe” appears, instead there is a lot of hard disk activity. Uh oh. Our user is now doomed. The executable file can now engage in any amount of malevolence, such as infecting the computer with a virus or a whole suite of viruses. One thing the bad guys like to do is make the computer into a “bot” as part of a “botnet”. “Bot” is short for “robot”. The user's computer has become a slave computer, able to be controlled remotely by bad guys out there on the Internet. The botnet (namely all the computers in it) is controlled by a “bot herder”, a remote criminal in some place where law enforcement is weak. The bots can be used to send spam, or participate in other criminal exploits. So our foolish user now has his own computer sending out thousands of spam messages, which he pays for. Further, sending spam is a violation of the terms of use for nearly all ISPs, so our user can expect a hostile message from his own ISP accusing him of sending spam and cutting off his Internet mail access.

4. Now our unhappy user has to get his computer cleaned up. This is often beyond the ability of an average user. So he has to pay a computer consultant hundreds of dollars to save all his data, then wipe out all executable code on the computer (because any or all of it might be infected) then reload all of Windows, all drivers and all applications. Then reload all the data. Almost inevitably, some driver or application never gets reloaded (due to the install disk being hard to find), so there is a permanent loss of functionality.

Notice that all our unhappy user had to do was download a file, then double-click it. That is all. Windows offers no warning messages. Windows does not specially flag executable files as dangerous. Further, there are numerous file extensions which might have executable code in them, such as .exe, .com, .dll and now a new horror, .msi. Windows declines to allow a user to set “do not execute unknown applications”. Windows does not allow a user to require that an executable file can only be run by right clicking it and clicking “execute”. These are all deliberate and bad security decisions by Microsoft.

Linux does not have this problem. For a file on a Linux machine to be executable, it must have the execute bit set. Downloaded files do not have that bit set. Deliberate action must be taken to make a file executable. An ordinary user will not do it.

It suits Microsoft to have bad security on Windows. Why? Because it gets users used to continually upgrading. Upgrades are profitable for Microsoft. If there were not continual security scares, users might find that their computers “just work”. Then they might get reluctant to upgrade. We cannot have that, now can we? Continual upgrade mania must be encouraged at all times.

Office Suites

Upgrading applies not only to Windows, but applications as well, such as Microsoft Office. Have you used MS Office 97 and MS Office 2003? Quickly now, what used-by-you feature of Office 2003 was not there in Office 97? A lot of people have spent a great deal of money on MS Office upgrades, yet their actual output could have easily been produced in older versions of Office. For most people, the differences between the old Office 95 and the latest Office, were not worth the money. When you last upgraded MS Office, at expense, what exactly did you get for your money?

Do not waste your money, consider an alternative. There is a wonderful, functional office suite called Open Office, available for free from:

http://www.openoffice.org/

Open Office is supported by volunteers and various companies, who are competitors of Microsoft. All popular versions of Linux include Open Office, as standard. There are free versions for Windows, Macintosh and Solaris, as well. The users of Open Office do not have an upgrade cost problem – all their upgrades are free, because the whole office suite is free. Linux users get upgrades to major applications like Open Office as part of their standard system updates which they normally get for free over the Internet.

Do major Microsoft applications get upgraded for you for free? No, you have to pay. If you do not pay, then there are no upgrades for you. That leaves you vulnerable, because there exist Word and Excel macro viruses.

It Gets Worse

Sometimes our unhappy user does not even need to click to download the malevolent file. It just arrives as an attachment in a spam email. Alternatively, one of the pathetically insecure “features” of Internet Explorer is something called “Active X”. Active X “controls” can be written which will download a file, so our user needs only to visit a certain web page (controlled by the bad guys), then there is the malevolent file sitting on his hard disk waiting to be double-clicked on.

Then our user just has to double-click the file, then he is doomed.

There are even security holes in Windows being discovered, which mean that a user need only accidentally visit a web page controlled by the bad guys, do nothing else, then a file will be downloaded and automatically executed. Notice, that was “controlled” by the bad guys, not “owned” by them. If they can pervert somebody's web server, then they get control, even though somebody else is paying for the whole thing. So you might be visiting a website, owned by say the government, but due to the web server administrator not being completely on top of his game, it is bad, unknown to you. Your only defence is then your web browser. Alas, Internet Explorer has a dreadful security reputation, so IE is no defence. Use a secure web browser, such as Firefox. That is your only hope. IE is too dangerous to use.

Young teenagers are very inclined to consider themselves invulnerable, then to be careless. So, if there is a teenager in the house, it may not matter how careful the actual owner of the computer is, it only takes one mistake by the teenager, then the bad guys have their wicked way. Save yourself, use Linux instead.

Cost and More Cost

Of course, being a Windows user who is worried about computer security, you buy a security suite, plus an update service. That costs you typically something like $100 per year. Really, you have to regard that cost as a “bug fix” cost, which you would not have to pay if Windows was secure in the first place. Naturally, you have to pay that cost for every computer you own. People who own quite a few computers find themselves paying out rather a lot, once you add it all up.

Did you know, Linux users do not have to spend that money? They get updates for free, over the Internet. They can load any free version of Linux – of which there are a lot – on any and all computers, legally at no cost.

Why is Windows not written in a secure manner? Because what matters in Windows is flashy features, not security. Joe Average, visiting his computer shop, can see the flashy features and they might make him buy a new Windows computer. He does not see the security problems, at that time. So, at the critical time of the customer making his buying decision, security does not matter. So it gets little attention. Sometime later, when the computer gets a virus infection, then our typical buyer starts to realise that security is important, after all. Then, if he is smart, he becomes a more informed buyer next time.

Linux programmers are really careful about security. They have to be, Linux runs a lot of the biggest computers in the world, owned by big security-conscious companies. Those big computers have to run reliably, all day every day. Excuses will not be accepted. The system administrators really do not like being woken up in the small hours of the morning, by an alarm going off, because some bad guy is up to something.

Ordinary Linux computer users reap the benefit. They get a rock-solid secure system at no cost. It is a very pleasant arrangement. However, computer buyers need to be aware of the relative security reputations of Windows versus Linux. Then the buyers have to actually let that information change their buying decision. Just complaining, will not do.

The Cost of Anguish

Vast numbers of people have suffered the loss of their documents and pictures due to insecurity in Windows. The cost in distress has been incalculable. Billions of dollars have been spent cleaning up after malware infections. The total of losses worldwide, due to bad design decisions by Microsoft, is easily in excess of the total shareholder value of Microsoft. Were Microsoft to be somehow forced to pay for its own carelessness, Microsoft would be wiped out financially. It would be easy to argue that Microsoft is a company that the world does not need any more and would be better off without.

Why Are Linux Computers Hard To Find?

All the big computer manufacturers have to be able to ship computers with Windows pre-loaded. Linux-only computer manufacturers are still small. Manufacturers cannot afford to pay full retail price for Windows, it would wipe out their profit and effectively send the profit to Microsoft. They need the manufacturer price, which is typically only 20% of retail. (Yes, you the retail buyer are paying five times the price Microsoft charges to others. Nice, eh?) So each big manufacturer has to sign a contract with Microsoft. That contract contains all sorts of provisions designed to hurt Windows competitors, such as Linux and Macintosh. Check out your local computer store. Do you see Linux and Macintosh computers there right next to the Windows computers? No? Funny, that.

What to Do

So you are sick of Windows security problems. Now what? How do you get a Linux computer? There are two ways, (1) buy a computer with Linux already loaded, (2) load Linux on to an existing computer.

The safest way is to buy a computer with Linux already loaded at the factory. That way, you get full manufacturer support and no funny stuff with devices which do not support Linux properly. There are manufacturers of some devices (such as certain modems and printers), who have not yet done a good job of getting their Linux drivers sorted out. They have their Windows drivers done, but not Linux. It happens. That problem is going away as Linux gets more popular. You do not have to go to a large manufacturer. A Linux computer consultant could build a computer for you and load Linux. Your consultant would effectively be a one-person manufacturer. That arrangement works fine.

Many large manufacturers do offer Linux computers, but you normally have to do quite a bit of searching on their website, then order specially, then wait for your computer to arrive. Sales persons in computer shops are often not very helpful regarding Linux.

Loading Linux on an existing computer is not too difficult, if you know something about computers, but getting it all set up to your satisfaction may sometimes need advanced knowledge. Alternatively, hire a Linux computer consultant to do the job for you. Bear in mind that you might need to replace a device or two, due to the driver problem mentioned above, however, that should be unusual.

One advantage of loading Linux on to an existing Windows computer is that you may have the option of having “dual booting” set up. That lets you boot into Linux or Windows by making a simple selection in a “boot manager” when the computer is first turned on. Naturally, dual (or multiple) booting is more complicated to set up. If you are using a consultant, your consultant will charge more for all that. My advice is to stay away from dual booting unless you really need it. Say you had some Windows game you just could not do without. Alas, games in general, suffer from multiple incompatible platforms. Most Windows games do not have an equivalent Linux version, but there are many Linux games, though. The Windows game problem is gradually going away, too.

Another attractive possibility is to make your hard disk removable. Plug-socket devices to do that are known as “mobile racks”. It consists of a slot (which gets installed in a spare drive bay), and a plug-in drawer which holds a hard disk. You could buy two, one for Linux, one for Windows. The computer does not “know” that the hard disk has become removable, so your existing Windows hard disk will just keep on working when you make it removable. However, to change to Linux means simply shutting down the computer, swapping hard disks, then rebooting. Changing back is just as easy. You can change as often as you like.

You are Not Alone

You do not have to keep on suffering from high costs and poor security in Windows. Linux can save you. Linux computer consultants are available. I am one. Please feel free to call on (02) 6286 3903.