Basic computer security

Les Hatton *

December 13, 2008

1 Overview

This is being written as a public service. Last week, three hospitals' IT systems were shut down because of viral invasion. In the last couple of months several close friends have had their machines invaded and mailing lists stolen. This may be the least of their problems so this short note is a basic guide to security for those people who really don't want to get into this kind of stuff but would like to have the benefit of using the web, e-mail and so on in a reasonably safe way.

2 Preparing your system

The main problem here is that Windows is so insecure that it might as well have a gigantic "Welcome" sign for anybody who wants to take over your machine. Nearly every other system - Mac OS X, Linux, Solaris, BSD Unix - is far more secure. However most of the world has to use Windows for all kinds of reasons so if you are a Windows user, please read this section carefully.

2.1 Windows

It doesn't matter which version of Windows you use, there are huge security holes in all of them. If you keep patching Windows systems they ultimately develop patch fatigue and give up the ghost. The following pieces of software help a lot. They are not produced by Microsoft who appear to be trying to make it as difficult as possible to run them until they can write their own second-rate equivalents but take no notice of this and load them anyway. They work very well indeed.

2.1.1 ZoneAlarm

You need to install this admirable free firewall. Don't panic and do the following:-

1. Go to http://www.zonelabs.com/ and choose Products and Services ⇒ Basic Firewall from the menu bar at the top.
2. Click on "Download Now" on the right

*Professor of Forensic Software Engineering, CISM, Kingston University, L.Hatton@kingston.ac.uk, lesh@oakcomp.co.uk

3. On the right hand side you will see a button for ZoneAlarm Firewall. Ignore all the stuff on the left hand side as you have to pay for that, (its very well worth it but small steps first). At some stage, I would upgrade to their full professional suite, (its easy as it will invite you to do it from time to time). Its only about 40 dollars and this product is good.

4. Click on the Button for ZoneAlarm Firewall. It will ask you if you wish to download something called zaSetup_en.exe. Click on "Save File". This will download this file onto your Windows desktop.

5. Find the file on your desktop and double click on it. This will take you through a set of instructions on how to install it.

6. The next time you reboot, it will be installed. Each time you go out to the web, you will see a dialog box appear on the right hand side asking you whether you want to allow or deny. Unless you recognise it as something belonging to Windows, or its Firefox or Internet Explorer or Exchange, say deny. ZoneAlarm will prevent other people getting in and taking over your machine although you should still follow a couple of procedures which I will mention later.

2.1.2 Firefox

Next you need to stop using the lamentable Internet Explorer and use the Firefox browser. Do the following:-

1. Go to http://www.mozilla-europe.org/en/firefox/ and click on Download Now.

2. This will invite you to download a file called "Firefox Setup 3.0.4.exe" (the numbers will change for the latest release). Download it.

3. Find the file on your desktop and double click on it. This will install Firefox. At some stage it will ask you if you want this to be your default browser. Say yes.

4. To browse the web, double click on the little Firefox icon, (a fox wrapped round the world). This will wake up ZoneAlarm which will ask you if that's OK. Say Allow and off you go.

5. You can protect yourself against various kinds of nasties using Firefox but the important ones are already set to be on for you. If you get really adventurous, go to Tools ⇒ Options and you can have your wicked way with it.

2.1.3 AVG anti-virus

Next you need to install this excellent piece of anti-virus software. Again the basic version is free for non-commercial use but you can upgrade if you wish. Anti-virus software will help keep your system clean. Do the following:-

1. Go to http://free.avg.com/download-avg-anti-virus-free-edition and click on Download for the left hand one (AVG Free). This will take you to another page. Click on the link "Download AVG Free 8.0 (AVG server)".

2. This will invite you to download a file called "avg_free_stf_en_8_176a1400.exe" (the numbers might change for the latest release). Download it.

3. Find the file on your desktop and double click on it. This will install AVG. You can default all the questions to install by saying Next all the time. At some stage, Zone Alarm will ask you if you want to allow AVG upgrade to access the Internet. Say yes. At the end, Zone Alarm will ask you if you want to allow Prevalence reporter to access the Internet. Again say yes.

4. That's it - you're done.

With these three bits of software, you have reasonable protection but you should read the next section for some tips on common-sense Internet use. It is very useful to burn a CD with the .exe files you downloaded for these three pieces of software in case you ever get compromised (see later).

2.2 Linux

Very little to do after installing any standard release.

2.3 OS X

Keep the machine up to date with the software updates particularly for security but otherwise very little to do.

3 Secure browsing habits

However well you protect your machine, no software on earth can stop us from doing silly things, so watch out for the following.

3.1 e-mail and spam

Although many people do not seem to realise this, when you send an e-mail, it is exactly the same as pouring out your heart on a postcard and then asking the nearest stranger to post it for you. In other words, it is completely open from end to end. During its travels it might well be analysed for keywords, perhaps for anti-spam purposes but other nefarious purposes are possible as society becomes rapidly more anal about this kind of thing. You simply would not believe the indiscretions I have seen in e-mails. You have been warned.

webmail If you use webmail to access your e-mail make sure that the web location you use starts with **https** and not **http**. If it starts with **http**, it is perfectly possible that your username and password could be read by an intruder in the middle. This isn't usually a big problem in office networks but might very well be if you use wireless in an airport for example.

e-mail identity hijacking Unless you have access to industrial strength e-mail filtering facilities, you will not only get spam but you might even have your identity hijacked. With very little effort, I could assume any of your identities and bombard the world with messages which look as though they have come from you. Its illegal and morally reprehensible but its painfully easy. The first you will know if somebody steals your identity is when you start getting "Message undeliverable" messages from people of whom you have never heard. If it gets really bad, you may even have to take out a new e-mail identity so be careful who you give it to and don't just put it in a web-page in plain form for anybody to see or somebody will read it, perhaps automatically and stick you on the spam lists. Once you are on, there is no escape.

unsubscribe If you start getting spam from somebody with an unsubscribe link, do not unsubscribe. Although some purveyors of bulk mail do the decent thing, many will simply take this as evidence that you exist and sell your e-mail address on to others. Its best just to block them using rules in your e-mail software if you know how to do this. (Its not too difficult as your confidence grows).

Google mail and other free mail In general these accounts are well protected from spam but I have heard numerous complaints of accounts just disappearing along with all your mail records. In addition, remember that Google, Microsoft or whoever can read everything you read or write and put that in the context that they know your browsing habits as well. It is better to use one search engine to host your free accounts and another to browse. Better still, don't use them for e-mail accounts.

e-mail and passing on warnings Every now and then you will get a mail from a well-meaning friend saying something like "New threat" or "New police camera" follows by "pass this onto 25 of your friends". **Don't**. A considerable percentage of PCs (some say around 25%) are infected to form part of robot networks which e-mail private data off to low-lifes who sell it on. Sending round these messages is just their way of milking their farm of PCs.

If you have followed the steps in the previous section, there is a much smaller risk that your machine will form part of one of these robot networks, unless you click on something silly and invite them in.

3.2 Phishing

Phishing quite simply is identity theft with criminal intent. The criminal community has proven to be very fertile inventors of ways of stealing your identity. At one end of the scale you get those morons from Nigeria who claim to have had a leg bitten off by a mad cheetah but who have managed to secrete many millions of dollars in the empty trouser leg which they would like to share with you, and at the other you get really sophisticated attempts to prise your bank details from you. In the middle you will get endless mails claiming you have won a lottery or a valuable prize, usually based in the Netherlands.

To put it succinctly, *they are ALL scams*. There is no such thing as a free lunch and if by some amazing chance you were ever the only surviving heir to the Burnley black pudding millions, the lawyers would send you a registered letter.

links in e-mail Do **NOT** click on links in e-mails unless you know where you are going. Depending on how good your e-mail software is, you might go off somewhere unpleasant which is masquerading as a valid site. Firefox can warn you of some of these but be careful. *No responsible bank will ever contact you by e-mail*. Note that some of these scams are particularly clever. A recent one invited the user to complete a questionnaire for the bank. At the end, it led you to an account confirmation site which was entirely bogus.

Some links in e-mail (if you wave your mouse over them in most e-mail software, you can see the real link), are very nasty and end in ".exe". Do **NOT** click on one of these.

zip files You will often see things like "Your shopping account" or some other such teaser accompanied by an attachment called a zip file, (because the names end in ".zip"). Do **NOT** click on one of these ever.

Do not use a machine if you think it has been compromised. It is possible that some low-life has infiltrated some keystroke eavesdropping software on it.

3.3 A little on passwords

The standard problem here is that they have to be long enough and unusual enough not to be guessed and, unfortunately, you have to remember them. Do not write them down unless its in a secure place. As a general guideline, try this:-

- Think of a nice tune you like. Alternatively think of one like "Hi-Ho Silver Lining".
- Take the first two characters of each word and separate them with punctuation or put numbers on one or both ends such as your housenumber to get something like 143Hi:Ho:Si:Li. You should have at least 8 characters (but I prefer 10) and it should have upper- and lower-case letters, some punctuation and some numbers. Above all, you should be able to remember how you constructed it so you don't have to write it down. This would be formidably difficult to guess and would be safe unless you inadvertently revealed it to some one. Don't just use words which appear in the dictionary.

3.4 Internet banking and online credit card use

The rules are pretty simple here. Type the name of your online banking into the location window at the top of your browser. If it doesn't begin with **https:**, its wrong, don't use it. If you are doing online credit card use, make sure that the page in which you put any personal details also begins with **https:** and it

is the payment site you are expecting. New threats are evolving here so I will update this bit also from time to time.

Larry Wagoner suggests getting a separate credit card for internet purchases and only using that one so you can see any strange entries quickly as you are more likely to remember them. Its also a good idea to get one that participates in the separate validation scheme. (With these, after entering all your details, the credit card company comes back to you for a validation password before proceeding).

4 What if my machine is compromised ?

Find a friend who knows what they are doing to clean the machine for you, or as a last resort, a reputable dealer who will probably charge you a fortune. This will involve re-writing the disc (re-formatting is safest). Back it up first. Windows should be restored locally and ZoneAlarm installed (see above) and any anti-viral software **before** any attempt to connect to the web and get Microsoft's innumerable patches downloaded. (I have had machines invaded by third-parties whilst updating patches from Microsoft's site, and if you put a naked (i.e. unprotected) Windows machine on the Internet, it will be compromised within a couple of minutes on average).

5 Conclusion

I will try and update this from time to time. If you do the above, you have a good chance of staying clean even in the high and increasing level of threat we currently face, but don't relax.

Best of luck.