A Home User's Security Checklist for Windows

Andreas Lindqvist Stefan Pettersson
Linköpings universitet, Sweden
Email: {andli299, stepe955}@student.liu.se

Abstract

The user and her desktop are widely held to be one of the weaker links in the security chain. By letting the user secure their own workstation by following a set of steps put forth in a checklist it could be possible to cover both problems at the same time. An already existing checklist was revised to become more concise. Twelve users took this checklist concerning the security posture of them and their workstations. It turned out that the majority of users largely used the default settings provided by the operating system. This is also an obvious trend at Microsoft, to make the default settings secure. It is reasonable to believe that this will be even truer in Windows Vista. Checklists are especially good as inspiration for interested users seeking to increase their knowledge on the subject.

1. Introduction

When talking about security, professionals usually refer to the weakest link in the security chain. This link changes over time, but right now it seems to be the user and her workstation. This trend is apparent given that the number of vulnerabilities reported in client side software increases.

At a company, the user's desktops are monitored and managed by administrative staff. This type of support is obviously not available for home users. Even a very light-weight understanding of basic security configurations and concepts would probably go a long way.

Section 2 gives a background on the assignment and how it was solved. Results are presented in section 3 followed by user comments in section 4. Section 5 and 6 treat work done on similar topics and conclusions, respectively.

2. The checklist

By giving users a checklist that contains items concerning both configurations and behaviour it should be possible to improve the security of the desktop and the user's security awareness.

The assignment that was given was to critically review and revise the already existing "Home User's Security Checklist for Windows" [1].

The items in the list consist of a statement and a checkbox along with one or more links to pages that explain the topic in depth.

Checklists like this are quite powerful because of the ability to decide which items to include, the level of knowledge required and which knowledge is provided via the text and links, all depending on the audience.

The updated version of the checklist [2] was then used to evaluate the security settings of at least ten Internet users (family and friends). This can be found in Appendix B.

2.1 The revised checklist

One impression we got from reading the old checklist was that it was too big and hence the first goal became to shrink it without losing relevance. With the vision of a more user-friendly list the number of items was decreased from the original checklist's 40 items and eleven headings to the new checklist's 36 items and only eight headings.

2.1.1 Removed items

An example of an item that was removed is the item of virus hoaxes because it is nowadays not common according to the authors' view. The password text inputs were immediately wiped from the checklist. The authors' viewpoint is that if passwords are to be noted they should be written down on a paper that is kept private in the wallet instead of writing them down on the checklist which is bound to be lost. Not only were some items removed such as the ones above but several items were also merged. An example of this is that the number of items and text fields under the anti-virus and anti-spyware sections was successfully decreased.

Some items were outdated; not only because of links not functioning but also because new security vulnerabilities are discovered. For example, the item concerning the wireless networking standard scheme Wired Equivalent Privacy (WEP) was removed because of the its broken design.

When it comes to headings the latter impression of having a too big checklist grew to also fix illogical order. Eleven headings became eight. The "miscellaneous" headline was removed because of the authors' view that the item was ridiculous. The "Windows update" heading became "Keeping up to date" because of a broader focus in the new checklist. Anti-virus, Anti-spyware and Personal firewalls were grouped, because of the add-on software similarity. Last, the Windows headline became

"Windows configuration" and was placed at the bottom of the checklist. The motive for this was that administrator privileges are needed to do the proposed changes in the checklist, and to unburden the user to get back the rights every time a change is done.

2.1.2 Changed items

A lot of effort was given to search for good links for the new checklist. With good the meaning is that they should be relevant and not to difficult to the hypothetical target group which is neither power users nor aware of the subject. Easy "how to" guides were linked if they could be found. One item under the Anti-virus heading was changed to not only include instant messaging, but also email, file sharing and the web. The item "I've configured my Web browser securely." was split up into many items, because the need to explain the meaning of "securely".

2.1.3 Added items

Many important items were added to the checklist. First, the need to have an item concerning the importance of also keeping non windows software up to date was added.

Second, the email headline now includes an item about encrypted mail server connections.

Third, an "additional reading" link was added under a few headlines, giving the possibility to grip and cover more than one item in one link.

2.1.4 OS independence

One key idea was to change the checklist to be Desktop OS independent because of the authors' relationships with people running for example BSD or GNU/Linux. This was not implemented because of the problems this adds to the task. One example is the need to have different items, text and links depending on which OS the user run. Also the GNU/Linux operating system comes in so many flavours that it is harder to do a security checklist than on Windows, which much more comes in the "one size fits all" concept. We leave this task to other eager checklist constructors.

3. Results

The majority of the twelve users taking the survey were "casual computer users". They use the computer for work and entertainment, not because they enjoy working with computers. Only two or three could be considered "power users". Only one of the tested was not studying at the university, the rest were attending a variety of different programs, everything from computer science to health care.

The results are presented with the notations "everyone", "almost everyone", "almost no one", "no one" and "half".

A table displaying the results can be found in appendix A.

3.1 Keeping up to date.

Almost no one has switched to Microsoft update instead of Windows update, but almost everyone has automatic updates enabled.

Almost everyone is aware of the importance of keeping other software up to date, and everyone is aware that companies will not send software updates via email.

3.2 E-mail

Almost everyone has configured to not run scripts embedded in emails, but no one has disabled the preview pane.

Half of the users view emails in plain text format.

Everyone understands that emails can be forged.

No one runs attached executable files.

Everyone is aware of why not to respond to spam, or give up sensitive information upon request.

Almost everyone uses secure connections when communicating with their mail server.

3.3 Web

Almost no one has turned off scripting by default. Almost everyone respects warning messages concerning signed certificates. Everyone is aware of the dangers of ActiveX controls, fake warning dialogs telling you that your "computer can be hacked" and advertisements of free smileys, screensavers etc.

Everyone makes sure that they have a secure connection when doing online shopping.

3.4 Anti-virus and anti-spyware

Almost everyone has an anti-virus program running with automatic updates of virus definitions. Everyone is aware of the major virus infection vectors. Half of the users have anti-spyware programs installed.

3.5 Personal firewall and router

Almost everyone understands why it is important to have a personal firewall and run one.

Almost everyone understands when to allow software to access the Internet and when to be suspicious.

Half of the users have an external router or firewall and have their default passwords changed and remote access disabled.

3.6 Windows configuration

Half of the users have picked a good password for Windows log on. Almost everyone has configured Windows to show file extensions.

Almost no one makes regular backups of important data.

Almost no one has the Data Execution Prevention (DEP) feature enabled for all applications and almost no one runs Windows as an unprivilegied user.

3.7 Individual distribution

If every checkbox is weighted as one point each the maximum score possible is 36. The highest score achieved was 32, the lowest 14 and the average score was 26.

4. User reactions

This section will cover interesting questions and comments the users raised on specific items in the checklist. Any comments or questions regarding the checklist as a whole are treated in section 5.

While almost everyone uses automatic updates for applications where such technology was available, few bothered to update programs that required manual updating. One user had a Start menu that covered the entire screen and made the obvious statement that it would be completely impossible to keep track of updates manually. Said user later admitted that only a handful of these applications were ever used. Removing unused software is at least as important as keeping the ones in use updated since every application added to a system increases the attack surface.

Most of the users used a web based interface for sending and receiving mail. The fact that everyone claimed to understand that email can be completely forged was surprising. This is probably due to the outbreak of phishing mails that has gotten the mainstream media's attention lately. Few knew about web bugs [3] and when informed about them, very few cared.

The results for "I've turned off scripting by default, and enable it only when needed" are one of the more worrying as the web is becoming more important every year. This issue can easily be solved with an add-on like NoScript [4] for Firefox. It is reasonable to believe that similar functionality will become standard in browsers in the future. One enlightened user commented that most of the security measures you could apply when browsing the web was to *know* when to do what. This observation is of course just as spot on as it is unfortunate. Or, as the authors of *Protect your Windows Network* [5] put it in their version of the famous passage concerning the dancing pigs.

> *Given the choice of dancing pigs and security, users will choose dancing pigs every single time. Given the choice between pictures of naked people frolicking on the beach and security, roughly half the population will choose naked people frolicking on the beach. […] If a dialog asking the user to make a security decision is the only thing standing between the user and the naked people frolicking the beach, security does not stand a chance.*

The idea of an malicious applet with dancing pigs was originally put forth by Ed Felten in Securing Java [6].

Anti-virus programs are, alongside firewalls, many users' rationalised view of computer security. This is also evident from the survey where all but two participants use anti-virus software. None of the users had any comments regarding anti-virus software, most were of the opinion that every computer had it. The only surprise was that only two used Symantec's software and that fairly many used free alternatives as Avast! and AVG.

An interesting question raised by several users regarding anti-spyware applications was why anti-virus was not enough. There are probably several reasons but the one given was that anti-virus vendors historically have gotten in to trouble for calling certain software for malware when they clearly stated their function in the end user license agreement. Despite this uncertainty among the users, more than half of them used anti-spyware software.

According to the survey, only eight users were using personal firewalls while ten claimed to know *why* it was important. This result was expected to be the other way around since Service Pack 2 enables the Windows Firewall by default. There is unfortunately no clear reason for this result except perhaps the use of external firewalls.

One proud owner of a D-Link router was completely unaware of the existence of an administrative interface. The router worked right out of the box after plugging only three cables. There is obviously no need to stress the dangers of this, a router that works right out of the box with wireless and all *will* sell more than one requiring extensive configuration. Secure settings will require some configuration.

Unsurprisingly, the concept of good and bad passwords is known. However, some of the tested users had no password at all and were well aware of it. They argued that there was no other way in than via the local computer since a firewall was used. This well-known fact is illustrated as Microsoft's third "immutable law" of security. "If a bad guy has unrestricted physical access to your computer, it's not your computer anymore". [7] Before reading the checklist none of the users had heard about DEP.

5. Related work and improvements

The majority of the test persons requested some form of feedback at the end of the survey. A score, some graph, or pointers to what they should focus on. Another thing that was widely sought after was uniform instructions for each item instead of links to external pages.

One test person suggested that the format of the survey should be changed to make it less intimidating, for example by only showing one statement or section at the time. This would also help users to focus on the specific questions.

To make the analysis easier, special follow up questions are recommended ("If you answered yes to the previous question…").

Concerning the length; shortening the checklist will of course lead to less coverage. A partial solution could be to first let the user check a few boxes concerning the type of equipment he or she has and what activities he or she engages in, thus avoiding any sections that the user consider irrelevant.

One famous, and much more ambitious, example of related work is Bastille-Linux [8]. Bastille is a scripted security checklist that walks the user through a set of hardening configurations and calculates a final score. The program is available for a small range of Linux distributions, HP-UX and recently Mac OS X. One of the prime benefits of Bastille is that great effort has been put into explaining the configurations and reasons for them to the user.

6. Conclusions

Updating the checklist in order to make it clearer and easier to follow proved to be a step in the right direction. Users commented that it appeared too lengthy, that it would have been better to treat one question at a time. This wizard-like behaviour is obviously appreciated among users when they are required to follow complex instructions.

Providing feedback to the users after going through the checklist seems to be a very attractive functionality. A possible, and positive, side effect of implementing some form of scoring is that users will strive to improve their score and by that, hopefully their security posture.

With the improvised scoring system of one point for each checkbox checked, the maximum possible score was 36. The highest score achieved was 32, the lowest 14 and the average was 26.

Many of the users rely on the default settings provided with the products they use. Vendors are aware of this and some are going to great lengths in trying to make their products more secure by default. One example of this is Microsoft Windows that used to aim for "functionality by default" rather than "security by default". This approach has largely been abandoned since the release of Service Pack 2 for Windows XP. This is very evident in Microsoft's new operating system Windows Vista.

Security checklists like this one can be made easy for regular users to follow but without interest and willingness to change, they have little effect. When there is an interest though, they may well serve as a catalyst for pursuing further knowledge.

References

[1] Granneman, S. (2004). A Home User's Security Checklist for Windows. URL: http://www.securityfocus.com/columnists/220 (2007-04-27)

[2] A Home User's Security Checklist for Windows URL: http://www-und.ida.liu.se/~stepe955/checklist/checklist.html (2007-04-27)

[3] Web bug. URL: http://en.wikipedia.org/wiki/Webbug (2007-05-02)

[4] NoScript. URL: http://noscript.net/ (2007-05-02)

[5] Johansson, J & Riley S. (2005). Protect your Windows Network.

[6] McGraw, G & Felten. E. (1999). Securing Java.

[7] Microsoft TechNet, 10 Immutable Laws of Security. URL: http://www.microsoft.com/technet/archive/community/columns/security/essays/10imlaws.mspx (2007-05-03)

[8] Bastille-Linux. URL: http://www.bastille-linux.org/ (2007-04-27)

Appendix A

1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31	32	33	34	35	36	37	38	39	40	41	42	43	∑
1	1	1	1	1	0	0	1	1	1	1	0	1	1	1	1	1	1	1	Sophos	1	1	1	2009	1	0		0		1	1	Windows	1	0	0	0	0	1	1	1	30	1	1	28
0	0	1	1	1	0	0	1	1	1	1	1	0	0	1	1	1	1	1	AVG	1	2	0		1	1	Adaware	1	10	1	0		1	1	1	1	1	1	1	1	5	0	1	29
0	1	1	1	1	0	1	1	1	1	1	1	0	1	1	1	1	1	1	Symantec	1	3	1	2007	1	0		0		1	1	Windows	0	0	0	0	0	0	1	0		1	0	26
0	1	1	1	0	0	0	1	1	1	1	1	0	1	1	1	1	1	1	Avast!	1	1	0		1	1	Adaware	1	30	1	1	Windows	0	1	0	1	0	1	1	0		1	0	26
0	1	1	1	1	0	1	1	1	1	1	1	1	1	1	1	1	1	1	AVG	1	1	0		1	1	Adaware	1	30	1	1	Windows	1	1	1	1	1	0	1	0		1	0	31
1	1	1	1	0	0	1	1	1	1	1	0	1	0	1	1	1	1	1	Symantec	1	3	1	2009	1	1	Spybot	0	60	1	1	Symantec	1	0	0	0	0	0	0	0		0	0	25
0	1	1	1	1	0	1	1	1	1	1	1	1	1	1	1	1	1	1	Avast!	1	1	1	2007	1	1	Spybot	1	4-5	1	1	Kerio	1	1	1	1	1	0	1	1	7	0	0	32
0	1	1	1	0	0	0	1	1	1	1	1	0	1	1	1	1	1	1	NOD32	1	1	0		1	1	Spybot	1	50	1	0		1	1	1	1	1	0	1	0		0	0	26
0	1	1	1	0	0	0	1	1	1	1	1	0	1	1	1	1	1	1	Avast!	1	1	0		1	1	Adaware	1	30	1	1	Avast!	1	0	1	1	1	1	1	1	180	0	0	28
0	1	0	1	1	0	0	1	1	1	1	0	0	1	1	1	1	1	0		0		0		1	0		0		0	0		0	0	0	0	0	1	0	0		0	0	14
0	1	1	1	1	0	0	1	0	1	1	1	0	0	1	1	1	1	0		0		0		1	0		1	60	0	0		1	1	1	1	1	0	1	0		0	0	20
0	1	1	1	1	0	1	1	1	1	1	1	0	1	1	1	1	1	1	F-secure	1	0.3	0		1	0		0		1	1	Outpost	1	1	1	1	0	1	1	0		0	0	26
2	11	11	12	8	0	5	12	11	12	12	9	4	9	12	12	12	12	10		10		4		12	7		7		10	8		9	7	7	8	6	6	10	4		4	2	

Appendix B

The Home User's Security Checklist for Windows

Keeping up to date

I have switched to "Microsoft update" instead of "Windows update" to include Microsoft Office.

I have configured automatic updates.

I'm aware of the importance of keeping other software that I use up to date.

I'm aware that companies will not send me software updates via email and instead of trust links sent in these emails I will go directly to the company's homepage to confirm that there is a software update available.

Email

My email client is configured to not run scripts embedded in emails.

I keep the preview pane closed.

I have configured my email client to read all emails as plain text.

I understand that even if an email says it is from a person I know, the mail could have been forged.

I will never open attached executable files, for example that end with .bat, .com, .exe, .scr, .vbs, .pif, .cmd.

I never respond to spam, even to "unsubscribe".

I understand that my bank and other web sites related to money will never send out requests for me to login and or give up any sensitive information like PINs and passwords.

I have configured my email client or webmail to use a secure connection to the mail-server.

Additional reading: A quick guide to email security

Web

I've turned off scripting by default, and enable it only when needed.

I will take warning messages concerning untrusted signed certificates seriously and will not trust the certificate unless I really know what I'm doing.

When browsing I will not install ActiveX components when asked unless I really understand what it does.

I understand that advertisements on Web sites warning me that my computer can be hacked or fixed should be ignored.

I understand that advertisements concerning "toolbars", "wallpapers", "screensavers" and "smileys" often contain hidden malware.

When I shop online, I make sure that sensitive information is entered only on secure pages (https) and that the shop and the homepage is trustworthy.

Anti-virus

I have anti-virus software ___ installed and running.

New virus definitions are downloaded every ___ days.

My anti-virus software updates expire on ___.

I understand that viruses can arrive, for example, via (1) web downloads, (2) email attachments and (3) files sent via IM and file sharing applications.

Anti-spyware

I have anti-spyware software ___ installed and running.

I run my anti-spyware software manually every ___ days and make sure it is updated before I run it.

Personal firewalls

I understand why it is important to have a personal firewall installed on my computer.

I have the personal firewall ___ installed and running.

I understand when to allow software to access the Internet and when to be suspicious.

Router

I have an external router/firewall hardware installed and I use it.

I changed the default password on my router/firewall.

I have made sure that the router/firewall administration page is only set up for the wired LAN and not via the Internet (WAN) or wireless.

I've configured my wireless router to use good encryption. Don't use WEP, instead go for WPA or even better 802.11i (also known as RSN or WPA2).

Windows configuration

I picked a good password to log in to Windows.

I have configured Windows to show all file extensions.

I make backups of my important data every ___ days.

I have configured Windows to use DEP for all applications.

I am not running Windows as Administrator.