Security Implications and Cost of Discontinued Support of Windows XP

Edward Simendinger
Mentor: Ming Chow

14 December 2016

Abstract

After a lengthy lifespan, Microsoft finally ended its extended support of the Windows XP operating system in April of 2014. However, it is still utilized in a number of different applications, ranging from typical consumers for personal use to ATMs to the U.S. military. While the latter of the three has purchased a special support plan for continued use, most users of Windows XP are now going without updates and technical assistance from Microsoft. This poses many issues, one of the most important being the security of the machines and the users' data. Since it is likely that the security features of these machines have not been updated in over two years, they are that much more susceptible to cyber attacks. This paper aims to examine the security vulnerabilities of Windows XP, and to offer some potential methods of preventing such attacks.

1 Introduction

1.1 Software Evolution

For as long as software has existed, there have always been ways to exploit it. Whenever a new piece of software is released to the public, it is only a matter of time before users find bugs and vulnerabilities within it. But software is living code, and it can be edited as needed to fix such faults. Maintenance of deployed code is a crucial part of the software development life cycle [5]. This stage lasts for as long as the software is supported, since its developers are constantly patching up new flaws that are being discovered. Throughout the software's life span, it evolves along with advances in its exploits. But eventually, support for the software must end, and anyone who choses to still use it must go at their own risk. This is known as end-of-life. At end-of-life, any flaws present in the program will remain unpatched, which could provide a great security risk to users' information. This is especially pertinent to zero-day vulnerabilities, which are pre-existing flaws in the software that the developers do not yet know about [2]. Additionally, cyber attacks continue to evolve and any unsupported software is completely susceptible to any newly-developed exploits.

1.2 The Windows XP Era

Windows XP is one of the most popular operating systems ever. Launched at the end of 2001, it arrived on the consumer market at a convenient time: users of its predecessors, Windows 95, 2000, and ME, were facing a number of bugs and inconveniences [6]. In addition to liking it for what it was not, users also greatly appreciated Windows XP for the features that it had. One main highlight of XP is its user-friendliness. It allowed for simple, intuitive web browsing, document editing with Microsoft Office, and some included games like the ever-popular Solitaire, among other attractive features [1]. Due to this ease of use, Windows XP was able to appeal to a new audience of less technologically proficient people. And it was a success: after five years of being on the market, Microsoft sold over 400 million copies of the operating system, and it took until 2011—ten years after its release—for its status as the most popular Windows OS to be taken by Windows 7 (although this is also due to consumer negativity regarding Windows Vista, released between the two) [6]. Between November 2007 and September 2008, Windows XP

accounted for 82% of all desktop computers in the world [3]. At the time of the Windows XP end-of-life in April 2014, this figure had decreased to around 30% [7].

2 To the Community

Why is Windows XP relevant two and a half years after Microsoft discontinued support for it? The truth is that an alarming amount of people and organizations are still using the outdated operating system. As of December 2016 (the time of the writing of this paper), 9% of all desktop computers in the world were running Windows XP [4]. While people are steadily transitioning to other operating systems, there are millions and millions of computers that are susceptible to all of the vulnerabilities associated with XP. The demographics of its users can show how serious this issue is. First of all, many of the people using Windows XP are older and less technologically proficient than others, and haven't switched to a newer OS because they don't have a need to or they don't know how to. This group of people likely does not know much about security, or how to protect their information from cyber attacks. Another portion of the operating system's users consists of companies running XP networks and servers. Without support from Microsoft, these companies are risking proprietary information and other material that should be under much greater protection. Windows XP is also still being used to a large extent in ATMs globally. As of October 2014, 95% of ATMs globally were running XP, and attackers were taking advantage of this [8]. In May 2015, a group of attackers in Europe hacked into a number of ATMs and were able to steal $1.32 million. All of these ATMs were running Windows XP. Finally, there are some exceptions where Microsoft has agreed to provide a special support plan for certain organizations, notably including the United States Army and Navy [8]. These special plans are not inexpensive, which will be discussed in detail later. Even though these support plans are able to prevent a significant amount of security threats to their respective systems, it is still obsolete software. To put it bluntly, a lot of people hear that using Windows XP in 2016 is dangerous, but they don't necessarily understand *why* it is so dangerous.

3 Vulnerabilities

3.1 Buffer Overflows

One of the most notable security issues of Windows XP (and newer versions of Windows, like Windows 7) is the buffer overflow vulnerability. A buffer overflow occurs when a user enters in more data than the program is expecting, causing other data to be overwritten. When a program is running, its active subroutines (i.e., functions that haven't yet returned to the origin from which they were called) are stored in a data structure known as the call stack [9].

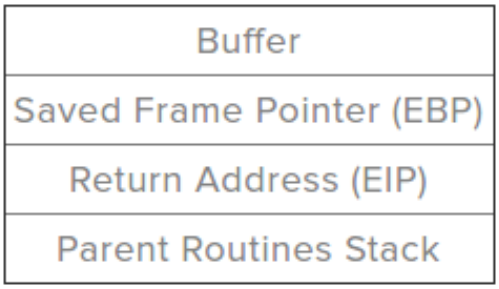

Figure 1: The internal structure of the call stack.

The Extended Base Pointer (EBP) points to a location within the stack that contains information needed by the program, and it moves around frequently. The Extended Instruction Pointer (EIP) holds the return address of the function. If a user enters a long enough string into the buffer, it will overwrite both the EBP and the EIP values, thus corrupting the return address of the function and potentially granting the user control over the system if done properly [9].

Figure 2: The construction of data to perform a buffer overflow.

By formatting the string inputted to the buffer in this manner, the contents of the EBP can be changed to hold malicious code and the contents of the EIP can be changed to hold the address of EBP, thus executing that malicious code [10]. This is extremely dangerous because it allows for users to do whatever they want on a system, possibly leading to the compromize of information and property.

In Windows XP Service Pack 2 (SP2), there is a feature called Data Execution Prevention (DEP), which can help combat this issue. DEP makes sure that programs are using the computer's memory safely by preventing any form of execulable code from running from certain locations [10]. DEP gives a warning message whenever a program attempts to run code from any of the specified protected memory locations. Microsoft recommends enabling this feature for all programs, and if necessary users can whitelist certain programs and services.

3.2 Malware

Windows XP has always been susceptible to security issues reagrding viruses, trojans, and other forms of malware, and this is even more of an issue after XP's end-of-life. Even though XP is inherently not much more prone to malware than other versions of Windows (studies actually indicate that—while it was still under Microsoft support—later versions of XP were better in this regard than its successor, Windows 7), Windows as a whole has a reputation for being an easy target for malware [11]. First, we will look at the security features added to Windows XP in Service Pack 2.

In terms of security, the original release of Windows XP was a disaster. Its firewall was disabled by default, it had an autorun feature that ran a device's programs as soon as it was connected to the system, and its network services were directly exposed to devices on the Internet [12]. A test was performed on an unpatched (i.e., without SP2) Windows XP system to see how quickly it would be infected by malware during the time of the Blaster worm, and its result was quite disturbing: within ten minutes of starting the system configuration process, the machine had already been found and infected with the worm [13]. A system running the unpatched version of Windows XP lasted only an average of four minutes after being connected to the Internet before getting infected [14]. Fortunately, Microsoft made steps

to correct these glaring issues with the release of XP SP2.

Even with the Service Pack 2 patch, Windows is more vulnerable to malware than many competing operating systems. An effective way of showing this is to compare Windows to a unix-based operating system, like Linux, and their construction and functionality. Windows began as a single-user design but eventually merged to a multi-user design, which will be discussed in more detail later. Additionally, Linux is built in a modular fashion whereas Windows is monolithic. This means that the entire Windows operating system is one singular unit with all its features tightly knit into every part, while Linux is built from a number of modules that are spread out on different layers [15]. So if one program is exploited in Windows, it is likely that other programs and features will also be compromised, where this is not the case with Linux. Finally, Windows uses the Remote Procedure Call (RPC) model, which allows for communication between programs over a network [15]. Programs in Windows are designed to listen to and perform instructions sent over a network, which can easily result in the execution of malicious code.

3.3 Internet Explorer

The nature of Microsoft Internet Explorer has allowed for a number of exploits and vulnerabilities to occur. Internet Explorer 6 was the version of the browser to originally come with Windows XP, but Internet Explorer 7 and 8 are also compatible with XP [16]. Microsoft has ended support for all three versions, with IE8 support for Windows XP ending along with the operating system's end-of-life in April 2014 [16]. Of course, the primary risk of using Internet Explorer on a Windows XP machine is the lack of support from Microsoft, there are some other fundamental flaws. Internet Explorer 6, the version of the browser that was released with the original version of Windows XP, is susceptible to many of the vulnerabilities associated with the unpatched operating system, such as buffer overflows due to the absence of DEP. With the release of XP SP2, dozens of vulnerabilities were patched in Internet Explorer 6 [17].

There have been a number of events that have compromised the security of all versions of Internet Explorer. For example, a vulnerability was discovered at the end of April 2014 that allowed for remote execution of code [18]. This was especially frightening for users of Windows XP, since Microsoft had

ended support for the operating system along with its compatible versions of Internet Explorer only a few weeks ago. Fortunately for its users, Microsoft decided to make an exception to the EOL policy and provide updates for XP and IE6-8 since it was such a severe issue and it was so soon after support was discontinued. Another group of severe vulnerabilities across all versions of Internet Explorer was identified in February of 2016, which also dealt with remote code execution [19]. However, this time Microsoft only fixed the flaws in Internet Explorer version 9 and up. Even though the vulnerability applies to all versions of Internet Explorer, the versions running on XP were ignored, making them that much easier to exploit.

3.4 Administrator Accounts

Because of the historically single-user design of Windows operating systems, despite the fact that Windows XP introduced a multi-user system most users of Windows XP did everything logged in as the Administrator [12]. This provided many conveniences to users, since they could control everything from the one account and didn't have to bother switching accounts when modifying system settings and installing new software. But this method had security drawbacks. If the Administrator account was logged in when the computer became infected with malware, the whole system would be compromised because the malware would have administrative access. If the user was logged into a different account, they might be able to log out and mitigate the issue from the unaffected administrator account. By using the administrator account for day-to-day activities, the whole computer is at risk.

4 Cost

At this point, we have talked about the privacy and security consequences of using Windows XP over two years after end-of-life. But we also should consider the monetary consequences. How much does it cost to maintain Windows XP? The first approach to estimating this figure is to consider the vast majority of users: people and organizations who are taking the risk of using XP without any form of support from Microsoft. These users aren't paying for any services to protect their information, but they could end up facing financial damage anyway. A study has shown that during 2014, mal-

ware attacks and information breaches costed the world $491 billion [20]. While it is difficult to assign an exact number, Windows XP was running on about 30% of computers in the world at this time, so that would equate to close to $150 billion. And because of the increased vulnerability due to the lack of support, this number could very well be higher.

The other alternative—only applying to certain organizations—was to pay Microsoft for a special Custom Support plan. Microsoft offered these plans to companies who were unable to move to another operating system before Windows XP's end-of-life. It is clear that Microsoft would prefer to not have to provide these: the plans cost millions of dollars per year (up to $200 per computer per year), and Microsoft even described these high prices as a sort of punishment for companies who took too long to transition to a newer operating system and couldn't make the April 2014 cutoff [21]. One such customer of the Custom Support plan is the British government, who paid £5.548 million for the first year [21]. Another organization using this service from Microsoft is the United States Navy, who was paying over $9 million per year and by June 2015 might have paid over $30 million, cumulatively [22]. Both of these contracts also include support for Microsoft Office 2003 and Exchange 2003, and the Navy's contract additionally includes support for Server 2003.

5 Action Items

So, what can be done about this issue? Well, the easy answer to that question is to just stop using Windows XP. New versions of Windows are better, faster, more powerful, and most importantly, more secure. If this can be easily done, it is far and away the best course of action to take. Your computer will be under Microsoft's wing, and in turn so will your privacy and security. But unfortunately, this isn't always an immediate option for every user of XP. Therefore, we will now go over some ways to practice effective security on Windows XP.

Make sure to utilize all of the security features included in Windows XP (particularly in the Service Packs). This includes the Data Execution Prevention feature, the built-in firewall, Internet Explorer download prompts, Windows Defender, and others. If you are still running Windows XP, this

should be the first thing you check after reading this. All of these features are built in already, and all that needs to be done is for them to be enabled.

Use an anti-virus software. Even though anti-virus software seems to be dying out in 2016, it is absolutely necessary for a non-supported operating system like Windows XP. Some anti-virus softwares like Norton still support XP, so they could be the only thing stopping new viruses and exploits from harming your machine [23].

Don't use Internet Explorer. There are so many browsers that are better and safer than Internet Explorer that are supported by Windows XP. Google Chrome and Mozilla Firefox come to mind. Since a significant portion of Windows XP's vulnerabilities have to do with the Internet, it is a good idea to make sure your browser is as secure as it can be.

Don't use the administrator account unless you are performing a task that needs administrative access. The administrator account isn't meant for basic computer use like browsing the Internet or working on a Word document. In fact, it is much worse to use the administrator account for mundane tasks such as these, due to potential malware infection affecting the entire system as opposed to just the user's account.

Finally, try to understand the specifics about XP's vulnerabilities and what exactly causes them. The best way to fix and prevent security issues is to think like an attacker would. Find out how to perform attacks on Windows XP and determine how to prevent them. This is perhaps the most valuable method of ensuring your security, and it could help others as well.

6 Conclusion

What was once the most popular operating system in the world has now been a zombie for close to three years. Despite its lack of support from Microsoft, it is not yet an uncommon sight to find both people and organizations still using it. Even though it was excellent while it lasted, it is now time to let go. The security vulnerabilities and expenses are too much to justify its use in 2016. I hope this paper has made you think about the repercussions of using such an antequated piece of software. But if you wish to continue using Windows XP, stay safe...and good luck out there.

7 References

https://www.netmarketshare.com/operating-system-market-share.aspx?qprid=10&qpcustomd=0&

1. Https://www.facebook.com/itproportal. "Here's Why Windows XP Was so Damn Good." IT Pro Portal. ITProPortal, 26 May 2015. Web. 14 Dec. 2016. ¡http://www.itproportal.com/2015/05/26/heres-why-windows-xp-was-so-damn-good/¿.

2. @FireEye. "Recent Zero-Day Exploits — FireEye." FireEye. N.p., n.d. Web. 14 Dec. 2016. ¡https://www.fireeye.com/current-threats/recent-zero-day-attacks.html¿.

3. "Operating System Market Share." Operating System Market Share. N.p., n.d. Web. 14 Dec. 2016. ¡https://www.netmarketshare.com/operating-system-market-share.aspx?qprid=10&qpcustomd=0&qptimeframe=M&qpsp=95&qpnp=11¿

4. "Market Share for Mobile, Browsers, Operating Systems and Search Engines — NetMarketShare." Market Share for Mobile, Browsers, Operating Systems and Search Engines — NetMarketShare. N.p., n.d. Web. 14 Dec. 2016. ¡https://www.netmarketshare.com/report.aspx?qprid=11%5C&qpaf=%

5. Hussung, Tricia. "What Is the Software Development Cycle?" Husson University. N.p., 05 Apr. 2016. Web. 14 Dec. 2016. ¡http://online.husson.edu/software-development-cycle/¿.

6. Https://www.facebook.com/TechRadar. "Windows XP End-of-life: Thanks for All the Fish!" TechRadar. TechRadar Pro IT Insights for Business, 06 Apr. 2014. Web. 14 Dec. 2016. ¡http://www.techradar.com/news/software/operating-systems/windows-xp-end-of-life-what-you-need-to-know-1240791¿.

7. N.p., n.d. Web. ¡http://www.extremetech.com/computing/180062-windows-xp-finally-put-to-sleep-by-microsoft-but-it-will-still-haunt-us-for-years-to-come¿.

8. Hein, Rich. "7 Places You'll Be Surprised to Learn Are Still Using Windows XP." CIO. CIO, 06 July 2015. Web. 14 Dec. 2016. ¡http://www.cio.com/article/2944673/security0/7-places-you-ll-be-surprised-to-learn-are-still-using-windows-xp.html¿.

9. "Windows Buffer Overflow Attacks Pt. 1 - Redscan." Redscan. N.p., 23 Sept. 2016. Web. 14 Dec. 2016. ¡https://www.redscan.com/news/windows-buffer-overflow-attacks-pt-1/¿.

10. https://support.microsoft.com/en-us/kb/889741

11. http://www.forbes.com/sites/gordonkelly/2014/05/12/windows-7-and-windows-vista-more-at-risk-to-viruses-than-windows-xp-says-microsoft/#6bd129d35a31

12. http://www.howtogeek.com/141944/htg-explains-why-windows-has-the-most-viruses/

13. http://blog.chron.com/techblog/2008/07/average-time-to-infection-4-minutes/

14. https://isc.sans.edu/diary/Survival+Time+on+the+Internet/4721

15. http://www.theregister.co.uk/2004/10/22/security_report_windows_vs_linux/

16. https://www.directionsonmicrosoft.com/roadmap/2013/09/supported-internet-explorer-versions-windows-os

17. https://support.microsoft.com/en-us/kb/326489

18. https://technet.microsoft.com/library/security/ms14-021

19. https://technet.microsoft.com/library/security/MS16-009

20. https://www.scmagazine.com/breaches-malware-to-cost-491-billion-in-2014-study-says/article/539302/

21. http://www.pcworld.com/article/2139929/windows-xp-support-will-be-available-after-april-8-just-not-for-you.html

22. http://www.defense.gov/News/Contracts/Contract-View/Article/606866

23. https://support.norton.com/sp/en/us/home/current/solutions/v95977279_EndUserProfile_e