CHAPTER

8

Don't Use Dinosaurs

They're Extinct for a Reason

Sue is an experienced marketing vice president at a Fortune 100 athletics gear merchandising firm with a nationwide distribution and retailing network. She left her laptop at home while on vacation with her family, visiting her parents in the mountains, and didn't realize it was gone until she arrived. Sue feels naked without her computer. She also doesn't like to use other people's machines for her work. However, she had a few remaining things to get off her plate before she could really relax.

Her parents' machine runs an old version of Microsoft Office (2007), has out-of-date antivirus protection, and is generally ill-equipped to effectively fend off any concerted "modern" attack; nonetheless, Sue used the old XP desktop to check her work e-mail, revise some work-related documents, and update the parameters of several ongoing provider contracts. In all, Sue spent no more than a few hours working on the machine, but it required that she connect to the company server and several sensitive databases. She crossed her fingers, and typed fast, hoping that no one up in the mountains was looking to hack her connection. She got everything done quickly and, for the rest of the much-needed long weekend with her family, was able to put work out of her mind.

Several weeks later, Sue found out that her parents' computer contained several forms of malware and that as a consequence, both her work credentials and several company databases may have been compromised. Following mandated protocol, Sue immediately contacted her IT director when she found out, changed all of her passwords, and locked down all of the accounts she supervises, but tremors of concern resounded throughout her office. This sort of breach could easily represent a major financial loss to her company in the form of forfeited revenues, compromised confidential information, loss of customer data, malware-related downtime, public relations setbacks, and more.

Software: It Has an Expiration Date

As we've established at multiple points throughout our discussion thus far, the always-on nature of the modern Internet is both a blessing and a curse to users enmeshed in its limitless possibilities and engrossed, emboldened, empowered, and enthralled by its endless capabilities. On the one hand, it is a truly wonderful thing to have the power to sit down at a computer and almost instantaneously look up sports scores, make reservations, buy tickets, dash off an e-mail, get a weather report, check movie times, talk to a friend, read a book, and buy a shirt, plane tickets, or anything else that Amazon or myriad vendors sell. We all well remember the not-too-distant past when we had to dial up to connect to the Internet and the screeching noises of the modem and the 30–60 second delay necessary to get connected. No one wants to return to the cumbersome, time-consuming bad old days. But the always-on Internet also comes with real risks to both our data and our identity.

This risk emerges from the fact that, as long as our computers and other devices are connected to the Internet, the potential is there that they can be found and compromised by thieves looking to steal everything important stored in our machines. In order to protect against this literally ever-present threat, it is critical that users today keep up-to-date the software architecture that allows these constantly aging devices to function "safely" in this information-porous environment. This wasn't always so.

The "Good Old Days" of Software

Fifteen years ago, it didn't really matter if a user's home computer was still running the Windows 95 operating system four or five years after its first release. The "old" OS still ran most current software, and the functionality users experienced wasn't substantially different than they enjoyed with its immediate successor, Windows 98. In fact, most users with conventional computing needs wouldn't even notice. Users commonly kept their desktop computers (few had laptops) for six, eight, or even ten years, running the originally installed operating system and applications. Viruses, though they existed, were primitive and were generally propagated via floppy disks, not e-mail or the Internet. Applications like Microsoft Word weren't generally exploitable, so updating them was not critical.

However, the pace of technological innovation has continued to advance in an essentially exponential way. With the ever-increasing sophistication of criminals seeking to breach system security, extended operating system utility and safety is a thing of the past. The shelf-life of current operating systems and a great deal of productivity software as well has shortened directly in conjunction with increased speed, capacity, functionality, and criminal viciousness. Today, an outdated operating system, particularly one that is no longer receiving manufacturer security patches, represents an extreme liability for anyone using that machine for modern, connected computing.

New Software for a New Era

As highlighted in our previous discussion, hackers are always developing more sophisticated malware variants along a wider and wider range of attack vectors. They are as a category relentless and primarily profit driven, and they do not sleep. This has led to a virtual arms race, where each side is constantly challenged to take the next offensive step in battles with shifting, complex, dynamic lines of encounter. When criminals come up with a new vehicle for attacking the most up-to-date security systems, software developers create new defenses, the attackers find ways around these defenses, and the cycle continues—until it stops. When this happens, when the build-up becomes one sided, the nature of the cycle changes in a fundamental way.

When a manufacturer stops producing new updates for an operating system, when the software developers are no longer defending the battle lines, attackers have free rein to exploit all of the vulnerabilities that they can find in that system. What’s more, because of the nature of modern information flow and unfettered, broad-scale dissemination, these vulnerabilities are publicized in an essentially viral way so other attackers can take advantage of them as well. Because gaps in the system’s security are no longer being filled with protective software previously offered by manufacturers, until users adopt the next iteration of their device’s operating system, criminals can gorge themselves on what they find on users’ machines.

Don’t Forget About Mobile Apps

As with computers 15 years ago, cell phones in the 1990s—even the first “smartphones” or PDA/phone combinations in the late 1990s and the early 2000s—were generally not upgradeable to more sophisticated operating platforms. Or, if these devices could be modified, upgrading them was an extremely tedious and complex process requiring that the phone be hard-connected to a computer. Wireless or “over-the-air” updates that are entirely taken for granted today were simply unheard of at the time—pure fantasy.

But, avoiding this cumbersome upgrading process didn't have any substantive impact on the safety of users' data or system security because hackers weren't pursuing mobile devices as a point of attack at this time. These devices also were not constantly connected to the Internet, so it was nearly impossible for an attacker to gain unauthorized access. Because these devices didn't use "apps" other than the preloaded stock functions that came on the phone from the factory, piggyback attacks also were not an option for cyber criminals. To a great extent, during this period mobile devices were all but immune from attack. However, this sepia-toned mobile exemption began to evaporate as the sophistication of modern devices increased their vulnerability. Modern smartphones are so powerful and also so Internet-connected that they have become for all intents and purposes minicomputers. In fact, many people increasingly use their smartphones for just this purpose in lieu of a traditional computer.[1] By extension, this also means that they have inherited some of the same kinds of risks (and benefits) as modern users of computers, tablets, and other "computing" devices. These risks can be great. Unquestionably, the broadest user-segment vulnerability today is found among users of the Windows XP operating system.

Windows XP

Windows XP, the fantastically successful operating system first released by Microsoft in 2001 and sold until 2010, is the best-selling operating system in history. Unofficial estimates place sales at nearly 1 billion copies.[2] However, in April 2014, support for the system was officially discontinued. Microsoft announced that it would produce no more security updates or patches for Windows XP. The cycle had come to an end.

In May 2014, Microsoft made a "single" exception to this official withdrawal and patched an exposed exploit to its Internet Explorer web browser. The software giant made this patch available for Windows XP despite official warnings. The Microsoft PR apparatus announced that this step was taken due to the exploit's "proximity to the end of support for Windows XP." Peter Bright, a regular contributor to the tech site Ars Technica, criticized Microsoft for this backpedal, writing "if Microsoft can blink once, who's to say it won't do so

[1] NJ.com, Allan Hoffman, "Seven Ways to Use Smartphone like a PC," www.nj.com/business/index.ssf/2013/01/hoffman_why_lug_a_laptop_when.html, January 18, 2013.

[2] ExtremeTech, Sebastian Anthony, "Windows XP Finally Put to Sleep by Microsoft—but It Will Still Haunt Us for Years to Come," www.extremetech.com/computing/180062-windows-xp-finally-put-to-sleep-by-microsoft-but-it-will-still-haunt-us-for-years-to-come, April 8, 2014.

again?"[3] Since making this one last patch publicly available, as of the writing of this book in July 2014, Microsoft had not yet "blinked" again. No further XP updates or security patches have since been released to the public. Perhaps Microsoft is really done with XP—time will tell.

The end of the XP era is quite ominous from a data security standpoint. As of April 2014 the market share owned by Windows XP was estimated to be hovering at just under a third of the entire market, with 28 percent of all Internet-connected computers utilizing the operating system. However, the actual percentage may be much higher, as significant numbers of XP machines are likely protected behind firewalls or not always connected to the Internet. This problem is not limited to users in the United States. For example, it is currently estimated that in China alone 50 percent of all desktop computers are still running Windows XP.[4] The scale of the problem is truly enormous. As of April 2014, an estimated 300 million computers worldwide were still running the depreciated XP operating system.[5] As we saw in the chapter opener, users like "Sue" may sometimes stumble across an older Windows XP computer while traveling or when in protracted transit and faced with lost baggage or other conventional setbacks (e.g., dead battery, no Wi-Fi).

Microsoft made a concerted public-relations effort in the several months leading up to the XP end date to communicate the impending vulnerability to users. This effort was intended to encourage private consumers, small businesses, and organizations with enterprise-level systems to upgrade or replace their XP computers altogether (see Figure 8-1). Toward this end, Microsoft retail stores actually offered a $100 credit to any consumers bringing in a Windows XP computer as a trade-in for newer, supported devices.[6]

[3] Ars Technica, Peter Bright, "Microsoft's Decision to Patch Windows XP Is a Mistake," `http://arstechnica.com/security/2014/05/microsofts-decision-to-patch-windows-xp-is-a-mistake/`, May 1, 2014.

[4] TechRepublic, Tony Bradley, "Windows XP Use Declining but Millions Still Willingly at Risk," `www.techrepublic.com/article/windows-xp-use-declining-but-millions-still-willingly-at-risk/`, April 16, 2014.

[5] Network World, "Twice as Many Desktops Still Running Windows XP than Windows 8, 8.1 Combined," `www.networkworld.com/article/2226663/microsoft-subnet/twice-as-many-desktops-still-running-windows-xp-than-windows-8--8-1-combined.html`, April 2, 2014.

[6] Daily Tech, Jason Mick, "Microsoft Will Give You $100 to Get Rid of Your Windows XP PC," `www.dailytech.com/Microsoft+Will+Give+You+100+to+Get+Rid+of+Your+Windows+XP+PC/article34567.htm`, March 21, 2014.

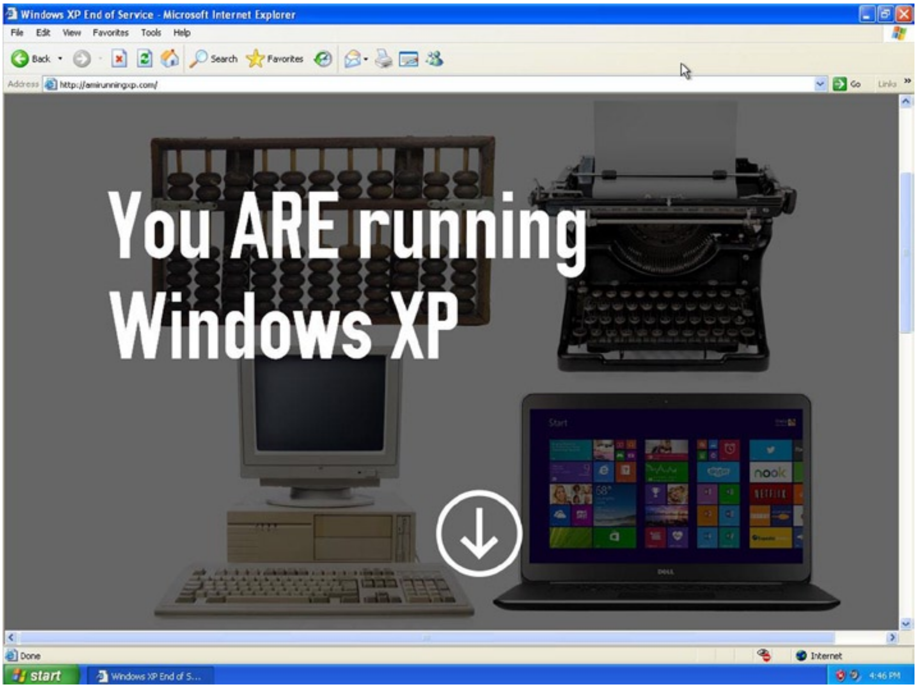
Windows XP End of Service - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back
Search
Favorites
Address
http://amirunningxp.com/
Go
Links
You ARE running Windows XP
Done
Internet
start
Windows XP End of S...
4:46 PM

Figure 8-1. Microsoft developed a customized web site in 2013 to tell end users if their PC was in fact running Windows XP and, if so, how to upgrade. (Microsoft, amirunningxp.com)

Some corporations and government entities made exclusive, specific arrangements with Microsoft to pay for extended support of the operating system for a limited period of time, being unwilling or unable to switch their computers away from XP before the deadline. For example, the government in the United Kingdom agreed to pay Microsoft 5.5 million pounds (approximately $9.2 million in US dollars) to extend XP support for a single additional year.[7] The Internal Revenue Service also paid the company approximately $500,000 (significantly less than the figure originally cited by some sources) to extend Microsoft’s support of its XP desktops for an additional year.[8] Big companies and government agencies with fear of being left unprotected can pay big money for a little more protection from Microsoft, for a short period of time.

[7] *Huffington Post*, Matthew Held, “If You’re Still Using Windows XP Your Company Is at Risk,” www.huffingtonpost.ca/matthew-held/windows-xp-no-support_b_5481600.html, June 10, 2014.

[8] *Computerworld*, Gregg Keizer, “Update: IRS Misses XP Deadline, Will Spend $30M to Upgrade Remaining PCs,” www.computerworld.com/s/article/9247634/Update_IRS_misses_XP_deadline_will_spend_30M_to_upgrade_remaining_PCs, April 11, 2014.

But, for the average private consumer or small-to-medium business without the kind of deep pockets of the Internal Revenue Service or Britain, spending vast sums of money for continued support of an outdated operating system is simply not a realistic option. As time passes and April 2014 continues to recede further into the past, the list of Windows XP's weaknesses and vulnerabilities will grow larger and larger. Hackers will continue to find new avenues of attack and to share these exploits with others who will be both informed and emboldened by them. This list of weaknesses will never shrink, because Microsoft is no longer closing these security "holes." Windows XP is truly a "dead end." Any individual or entity still using XP is advised to immediately upgrade any XP machines still in use anywhere in their physical plant—whether a large corporation with thousands of machines, a smaller business with hundreds, a family business with several, or a private user with one. It also is critical to avoid using for any purpose an XP machine that belongs to someone else, like Sue from our introduction did—these devices simply can no longer be secured or relied on.

Ultimately, of course, the same fate will eventually befall all of Microsoft's other post-XP operating systems as well. These schedules have already been published for public consumption and infrastructure planning purposes. It takes time to retool the physical plant and associated communications infrastructure that large corporations (and governments) rely on to complete core operating tasks. Without advance warning of such OS impending abandonment, larger firms and individuals alike would be caught unaware and their data left vulnerable to attack. These published schedules go out years in advance. For example, Windows Vista is scheduled to go out of support in 2017, Windows 7 will go out of support in 2020, and Windows 8 will be unsupported in 2023. No one should be surprised when software products and the support systems they rely on for continued functionality are retired, yet many are.

Not Just Windows

Although we've focused primarily here on emergent vulnerabilities in the PC operating system context, this isn't a problem exclusive to Microsoft's operating systems. Apple also has moved to a yearly release schedule for new versions of its desktop operating system, OS X. The most recently announced version, OS X Yosemite, will go into distribution sometime in late 2014. Currently (mid-2014) the shipping version is the OS X 10.9 Mavericks. Apple actively supports the current version of the OS as well as the two most immediately previous versions, Lion and Mountain Lion. As of mid-2014, then, versions 10.7, 10.8, and 10.9 (the current shipping version) were actively being supported with security updates and patches. In February 2014 OS X 10.6, Snow Leopard, was removed from active support. This planned and explicitly scheduled support pullback left approximately 20 percent of Mac users (an estimated 15 to 20 million people) vulnerable to active exploits.[9] Average OS X users have upgraded to the newest operating system substantially more promptly than have Windows users, however. Within five months of its release, OS X 10.9 had an approximate 40 percent market share, with its predecessor, OS X 10.8, making up another 20 percent.[10] From these data, it appears that nearly two-thirds of Mac users are running one of the two most recent versions of the OS. Apple's OS upgrades are now free (as of version 10.8), which certainly helps to encourage more punctual user upgrades!

Not Just Operating Systems

Of course, in addition to the operating system that allows the device to function, all other software loaded on the machine must be updated and kept at a secure level of modernity. Browser plug-ins, such as Flash and Java, often are used as convenient avenues of attack by criminal hackers. Security analysts note that Java, produced by Oracle, has become criminals' favorite channel into users' PCs for an attack. For example, in December 2013, IBM's X-Force Threat Intelligence Report found that at least half of all exploits were aimed at Java.[11] Adobe's Reader software was a distant second at 22 percent of recorded exploits. Productivity software such as Microsoft Office also can be exploited. In November 2013, McAfee Labs discovered a threat that exploited the graphics-handling abilities of Microsoft Word. This vulnerability potentially allows an attacker to take over a computer by tricking users into opening an infected Word file.[12] What is clear is that the system protections offered through active updating and patching have across-the-spectrum data security relevance, and further speak to the importance of remaining current in all aspects of device functionality. From our story at the beginning of the chapter, Sue's parents' computer could easily have been infected by malware via exploits in Windows XP, Office 2007, both, or from exposure to another piece of outdated software.

[9] *Computerworld*, Gregg Keizer, "Apple Retires Snow Leopard from Support, Leaves 1 in 5 Macs Vulnerable to Attacks," www.computerworld.com/s/article/9246609/Apple_retires_Snow_Leopard_from_support_leaves_1_in_5_Macs_vulnerable_to_attacks, February 26, 2014.

[10] MacRumors, Eric Slivka, "OS X Mavericks Adoption Pushing Toward 50%," www.macrumors.com/2014/03/27/os-x-mavericks-adoption-50/, March 27, 2014.

[11] JavaWorld, Tony Bradley, "Report: Half of All Exploits Target Java," www.javaworld.com/article/2104862/java-security/report-half-of-all-exploits-target-java.html, March 5, 2014.

[12] McAfee.com, Haifei Li, "McAfee Labs Detects Zero-Day Exploit Targeting Microsoft Office," http://blogs.mcafee.com/mcafee-labs/mcafee-labs-detects-zero-day-exploit-targeting-microsoft-office-2, November 5, 2013.

Java updates have been particularly problematic, as many large organizations use other applications (database, HR, finance, etc.) that rely on specific versions of Java. These organizations may have customized their applications, relying on features in a specific Java version. When Java is upgraded, these customizations may not function as expected. So these companies are stuck with two unappealing choices: upgrade Java, and break existing functionality that might be mission-critical, or don't upgrade Java, leaving existing security vulnerabilities as venues of attack. In 2013, Oracle ruffled some feathers by using an update to Java version 7 to silently and forcibly remove Java version 6 from users' computers. This caused widespread failures of many companies' applications that depended on the older version.[13]

Not Just Desktops and Laptops

Here, again, it's not just the operating systems and software on desktops and laptops that are at risk as a consequence of obsolescence. The ubiquitous, powerful smartphones and tablets that are almost always in use and connected to the Internet also depend on software and applications that must be kept up-to-date. In Chapter 7 we discussed in depth the malware threats prevalent on the Android mobile operating system. A substantive contributing factor underlying these threats is the considerable "fragmentation" of that operating system's market. Apple's iOS is sold exclusively on hardware manufactured by Apple, in a monogamous hardware-software pairing. In contrast, the Android OS is made by Google but is sold on a range of hardware platforms. What this means is that there are many more versions of the Android operating system "in the wild," and the environment is consequently fragmented.

This also has led to a substantial percentage of users running operating systems that are increasingly clunky and out-of-date—way out-of-date. As of July 2014, 53 percent of the Android devices that had recently connected to the Google App Store were running Android version 4.1 or earlier (see Figure 8-2), which are from 2012 and earlier. Presuming this sample of users is reflective of the population of Android users broadly (and this may be a conservative assumption in light of their purchases of new software), this means that more than half of Android users are currently using operating systems that are at least two years old. In late 2013, Google announced the activation of its one billionth Android device. Taking into account the retirement of old devices and

[13] *Register*, John Leyden, "'Silent but Deadly' Java Security Update Breaks Legacy Apps-Dev," www.theregister.co.uk/2013/01/31/java_security_update/, January 31, 2013.

the purchase of new devices (Google claims 1.5 million Android devices are activated each day[14]), a conservative estimate puts at least 500 million Android devices running out-of-date system software. This is a really big target.

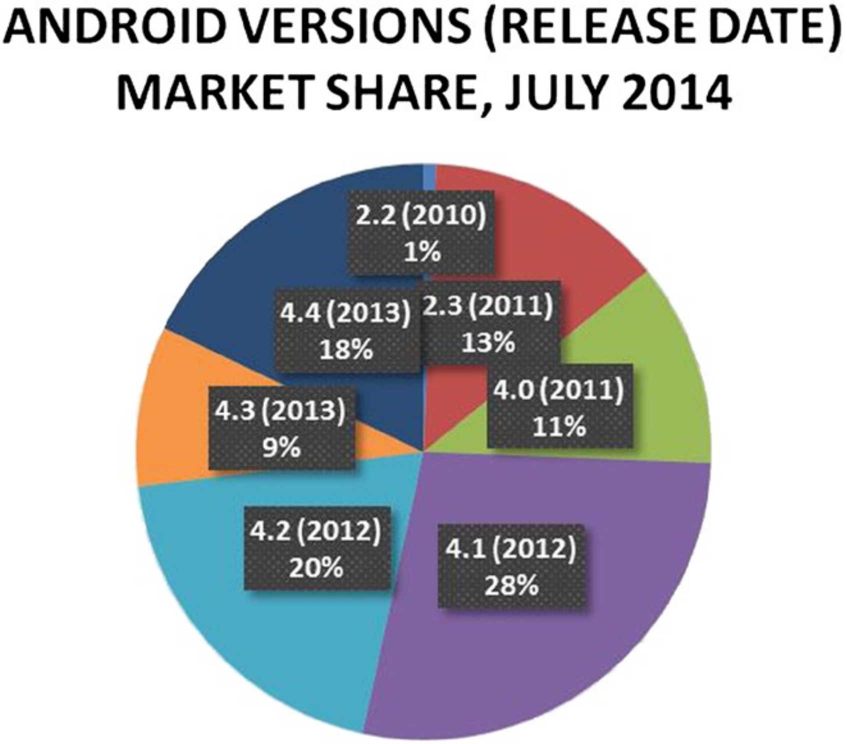

Figure 8-2. More than half of all Android devices, as of mid-2014, were still running operating systems from 2012 and earlier. (Data from http://developer.android.com/about/dashboards/index.html)

For all iOS devices, when a software or operating system update is released by Apple, the end user can decide when to install or make an upgrade. In contrast, on the Android platform, while the update is released by Google, the schedule is generally determined by the particular telecommunications provider (e.g., Sprint, Verizon, AT&T) supporting Internet access. The clear divide between these two approaches has led to essentially two classes of users:

[14] Pocket-lint, Elyse Betters, “1.5m Android Devices Activated Daily, 1 Billion Total Devices on Horizon,” www.pocket-lint.com/news/122459-1-5m-android-devices-activated-daily-1-billion-total-devices-on-horizon, July 19, 2013

broadly protected and broadly unprotected. This divide may be at least in part a consequence of big business economics. Writing for *PC Magazine*'s "Security Watch," analyst Fahmida Rashid noted that:

> *Android's open platform allows device manufacturers and carriers to tweak the operating system to bundle extra software and set certain configuration settings. Whenever Google releases an operating system update, both the vendor and carriers have to test the changes against their homebrew systems before rolling out the latest version. The carriers claim this is a slow process, but many security experts believe carriers are prioritizing profit over security.*[15]

But the situation isn't entirely rosy on the other side of this divide either. Apple users are not wholly immune from vagaries in corporate data protection policy. For example, in February 2014 the company was criticized when a security fix was made available only for the newest OS (iOS 7) and not for the previous version of the system, iOS 6.[16]

At the time, approximately 15 percent of iPhone users were running the older version of the operating system. These users had chosen not to upgrade their software, many in response to reports of poor battery life when iOS 7 was installed on older hardware. Interestingly, Apple made a patch for iOS 6 available for users who were unable to upgrade to iOS 7. This included users of the iPhone 3GS, for example, as that device is not compatible with iOS 7. Here, in a conspicuous effort at social engineering, Apple drew a clear policy distinction between those users who couldn't upgrade their OS due to system incompatibility issues and those who chose not to upgrade due to performance issues (e.g., battery life). Users in the former category were supported with a security patch. Users in the latter were not, unless they relented and upgraded to the new software. The unseen hand at work….

In general, however, the immediacy of Apple's OS updates, coupled with the total homogeneity of the hardware appears to encourage iOS users to upgrade faster relative to Android users as a body. As shown in Figure 8-3, as of July 2014, the Apple Developer Program reported that 90 percent of active iPhones were running iOS 7, the most recent version of the operating system.

[15] *PC Magazine*, Fahmida Rashid, "Android's Biggest Security Threat: OS Fragmentation," http://securitywatch.pcmag.com/android/308966-android-s-biggest-security-threat-os-fragmentation, March 8, 2013.

[16] NPR, Laura Sydell, "iOS 6 Users Left in the Lurch After Security Flaw Discovered," www.npr.org/blogs/alltechconsidered/2014/02/25/282671039/ios-6-users-left-in-the-lurch-after-security-flaw-discovered, February 26, 2014.

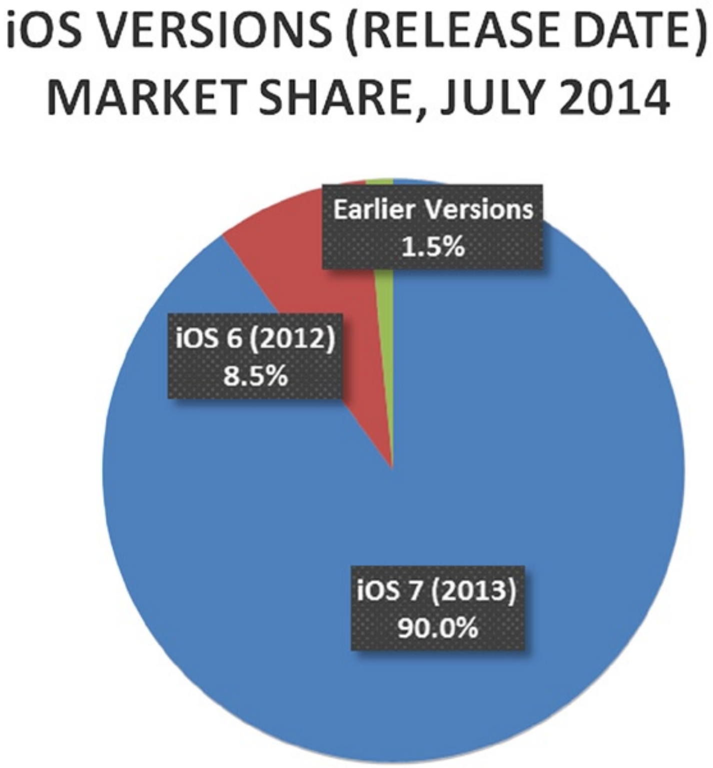

Figure 8-3. In general, iOS users upgrade their operating systems more regularly than Android users. (Data from https://developer.apple.com)

What Can You Do?

First, absolutely do not use Windows XP for anything. Period. Don't use a toaster in the bathtub…don't use Windows XP.

For all of your mobile devices, including phones and tablets, upgrade when new versions of the OS or a new patch are made available by the manufacturer. It is important to keep up with these upgrades serially as they're published. Adoption lags increase the potential that your devices will be vulnerable to attacks exploiting earlier system and software configurations. Often, however, as a result of emergent hardware insufficiencies, updates to the most current software or OS can no longer be made (e.g., iPhone 3GS ≠ iOS 7). If a device is old enough that it is no longer eligible for software updates, or is incompatible with the newest operating system, it may be worthwhile to consider investing in a new device.

This caution, of course, also applies to personal computers, be they Mac or Windows-based machines. Upgrade the operating system when a new version becomes public. Keeping operating systems and software current doesn’t have to involve a lot of steps or take a lot of time. Users can take advantage of the automatic update option standard in all modern operating systems to automatically download new updates when these are announced. Given their favored status among criminals seeking access to your devices, it is also important to update software like Microsoft Office and Adobe Reader and browser plug-ins like Flash and Java, when these become available. Using outdated products for any length of time, particularly online, is just an invitation to hackers looking for easy points of access.

The mechanics of this process are obviously likely to be very different for personal computers vs. those owned and maintained by an employer. While users have autonomous control over their personally owned devices, on company computers many of the upgrade decisions are simply out of the hands of end users, who likely do not have extensive administrative privileges. Corporate or company IT departments generally set the upgrade policies that define the configuration of users’ devices. Sometimes, there is a firm-level reason to stay with an older OS or software application. For example, a newer version of Java may not be compatible with an in-house database application or inventory management system, limiting the broad-scale options available for making an upgrade to current software. However, it is important that end users pay attention to upgrade e-mails and announcements from their corporate IT staff.

It is crucial that users try to actively collaborate with this process and adopt a regular, disciplined approach to keeping their devices up-to-date. Although tempting, because they can be annoying, don’t try to find ways around automatic updates. Everyone groans when the message “Windows has new updates available that will require a reboot” pops up on their machine. But don’t ignore these messages. Let the computer update itself ASAP. It is important not to wait if you believe your operating system, software application, or browser plug-in is out-of-date. Discuss these suspicions with your IT representative. It also is important not to connect any BYOD laptops, phones, or tablets to a corporate network or other resources if they are unpatched or at all out-of-date. Doing this has the potential to put the entire system or network at risk (and you won’t know if the computer is out-of-date if it isn’t yours). Increasingly, many corporate wireless networks will refuse to allow outdated computers or other devices (e.g., Windows XP computers) to connect to corporate resources.

Additional Reading

For more on keeping your systems up-to-date, see the following links and visit our web site at `www.10donts.com/dinosaurs`:

- Apple, "Updating OS X and Mac App Store Apps," a similar guide for Apple's operating system: `http://support.apple.com/kb/ht1338`
- Adobe, "Flash Player Help," a site that allows users to determine their current version of Flash and upgrade if necessary. It features comprehensive instructions for enabling it in your browser(s): `http://helpx.adobe.com/flash-player.html`
- Mashable, "Windows XP Isn't Safe to Use Anymore. Here's What to Do Next," a great guide helping users transition off of XP: `http://mashable.com/2014/04/08/windows-xp-upgrade-or-switch/`
- Microsoft, "What Is Windows Update?" a single point of reference for enabling automatic updates on each version of the Windows operating system: `http://windows.microsoft.com/en-us/windows/windows-update`
- Oracle, "Verify Java and Find Out-of-Date Versions," an easy way to determine if your computer uses an outdated version of Java: `http://java.com/en/download/installed.jsp`