

# Mac OS X Security

Alissa Miller

December 10, 2007

## Executive Summary

Mac OS X has for the most part, compared to other operating systems, enjoyed a carefree history when it comes to security. There are certainly some vulnerabilities, but relatively few known exploits for them. There are also almost no examples of attacks in the wild. The few attacks that researchers have noted in the wild, although highly publicized, are mostly harmless. This however should not be taken as evidence that OS X is difficult or impossible to attack.

Two reasonable explanations for the lack of any large-scale security threats facing OS X are its small market share and superior approach to security. OS X is based in BSD UNIX and uses time tested open source software for its security foundation. It was designed to be a multiuser operating system and has strong built-in file based permission system. OS X is also very secure out of the box and includes many easily accessible additional features. By default the root user in OS X is disabled, and most normal users should never even need to use it. Network services are also disabled by default. OS X provides a unique combination of good security by default and ease of use, making it a relatively secure system for normal users.

The first virus for OS X, OSX.Leap.A was discovered in the wild in February of 2006. Although this particular virus was innocuous, it should demonstrate that OS X is certainly not immune to security threats. While the OS X market share is small, it is steadily increasing. As it becomes a more popular operating system, security threats are likely to increase and become more severe. OS X is not by any means a bulletproof operating system and Apple will have to continue to be vigilant about security in order to stay ahead of hackers.

# Mac OS X Security

In a recent television commercial, two men are shown against a completely white background. The younger and ‘hipper’ man introduces himself as Mac, while the more nerdy one wearing glasses and a suit introduces himself as PC. PC barely makes it through his introduction before beginning to cough and sneeze. When Mac asks what’s wrong, PC explains that he is coming down with the new virus that is going around. PC also politely tells Mac to stay away, to which Mac responds, “that’s okay, I’ll be fine.”<sup>1</sup>

This ad, known as “Virus”, is from the “Get a Mac” advertising campaign created by Apple. It highlights the very intriguing fact that, most viruses don’t affect the Mac OS X operating system. This begs the question: is OS X really more secure? To fully answer this question, many more questions have to first be examined.

There is no straightforward answer as to why there haven’t been more successful attacks on OS X, but there are two primary explanations. The first explanation is that OS X really is more secure and that attackers have had problems figuring out how to successfully exploit the operating system. The second explanation is that the market share of OS X is so low that attackers do not think it is worthwhile to spend their time developing exploits for it. While there are a fair range of estimates of the actual market share for OS X, almost all estimates put it well below 10%, and sometimes even below 5%.<sup>2</sup>

It is reasonable that both of these explanations share some truth. One thing that is clear about the OS X market share is that it is growing. As more and more people buy Macs, OS X will likely become more of a target for hackers. Ad campaigns like Apple’s “Get a Mac” campaign are also likely to trigger the curiosity of hackers who are looking to make a name for themselves by putting the first huge dent in OS X’s armor.

My goal in this paper is to examine the main question of how secure OS X really is. I will examine several key areas of the operating system in relation to security. First I will examine the origin of the operating system and its roots in UNIX. Second I will examine the security record of OS X, a few of its vulnerabilities and the recent history of malware affecting it. Lastly I will take a look at the built-in user level security settings with a focus on out of the box settings and simple hardening measures. Once we’ve taken a closer look at these things, we will be better

---

<sup>1</sup> Apple. "Apple Get a Mac Ad Campaign-Virus."

<sup>2</sup> Kennedy, M.R. "Apple U.S. market share hits 5 percent."

equipped to answer the question “is OS X really more secure?”

My primary analysis in this paper is restricted to the client versions of Mac OS X and Apple-specific software. It is however important to note that security is only as strong as its weakest link. Because of its roots in UNIX and open source software, OS X employs many third-party tools, such as Apache, Samba, and MySQL. Even though OS X itself has yet to become a serious target of hackers, these third-party tools are all widely used and have their own vulnerabilities. To gain a greater perspective on OS X security, these vulnerabilities must be examined as well. That however, is out of the scope of this paper.

## **OS X Background**

Apple released the first public beta of its client version of OS X in September of 2000. Since this initial release of the beta version, there have been six major upgrades: Cheetah (10.0), Puma (10.1), Jaguar (10.2), Panther (10.3), Tiger (10.4) and most recently, Leopard (10.5) in October of 2007.<sup>3</sup> From this release schedule, it is clear that Apple has been upgrading their system at an unprecedented pace. For comparison, Microsoft Windows XP was released in October of 2001. The only major upgrade to the system was Service Pack 2, which was released in 2004. The next client version of Windows, Vista, was released in the end of 2006. Each OS X upgrade has included substantial feature additions and changes in security, showing a clear commitment on the behalf of Apple towards bettering its product.

Much of the success in terms of security in OS X can be traced back to its roots in UNIX, from which it was based. OS X was designed from the start to be a multiuser system and borrows heavily from time-tested UNIX traditions. The core of the OS X system is built on a combination of Berkeley Software Distribution (BSD) UNIX and the Mach kernel.<sup>4</sup> Many of the most important underlying security features, like the file system security policy, networking services, and memory management are based on these two things. On top of BSD and Mach, OS X also implements a layer of the Common Data Security Architecture (CDSA), to which Apple has developed its own security API's to better integrate with the rest of the technology. Apple documentation explains that CDSA provides a “wider array of security services, including finer-grained access permissions, authentication of users’ identities, encryption, and secure data storage.”<sup>5</sup> This underlying architecture of OS X is key to its security prowess.

---

<sup>3</sup> Adams, Aaron. "The Mac OS X Threat Landscape: An Overview." 3.

<sup>4</sup> Apple Developer Connection. "Security Overview." 14.

<sup>5</sup> Apple Developer Connection. "Security Overview." 13.

As described above, the core of the OS X system is UNIX. In fact, the most recent iteration of OS X (Leopard) has been officially certified as a UNIX system for the first time.<sup>6</sup> In addition to its UNIX background, OS X has also borrowed heavily from the tradition of open source software. This allows Apple to use services that have proven security over a longer course of time through open public scrutiny. In the company's Leopard security technology brief, Apple makes a point of mentioning the benefits of this approach:

Apple built the foundation of Mac OS X and many of its integrated services with open source software...that has been made secure through years of public scrutiny by developers and security experts around the world. Strong security is a benefit of open source software because anyone can freely inspect the source code, identify theoretical vulnerabilities, and take steps to strengthen the software.<sup>7</sup>

A potential weakness in using open source software is that it can arguably open an operating system up to security vulnerabilities, since the source code is freely available. While this may be true, it is also true that by allowing more people, security researchers in specific, access to source code also provides better security in the end

In Mac OS X, Apple enjoys a feature that almost no other current major operating systems can claim. It's new. Apple completely expunged its previous operating system, OS 9, in favor of starting over with OS X. This puts OS X in the unique vantage point of not having to rework an operating system that was designed and widely distributed before computer security became a common concern. This is a clear benefit when compared with the massive amount of effort that Microsoft has had to put into developing Windows Vista, all while attempting to maintain its compatibility with older applications and hardware.<sup>8</sup> Many of the security features implemented in Vista, such as User Account Control, are features that UNIX, and by extension OS X, have had some form of for years and are built into the foundation of the operating system. The relatively short history of OS X has allowed the system's development cycle to be quite agile, and adding new security features and responding new vulnerabilities at a rapid pace.

### **Examining the OS X Security Record**

One of the most obvious ways to gauge the effective security of an operating system is to take a close look at its security record. No software, no matter how good it is, can be completely free of bugs and security vulnerabilities. It is usually only a matter of time before specific vulnerabilities become public knowledge and exploits eventually written. It is therefore very important to note

---

<sup>6</sup> Apple. "Apple - Mac OS X Leopard - Technology - UNIX."

<sup>7</sup> Apple. "Mac OS X Security." 13.

<sup>8</sup> Thurrott, Paul. "Windows Vista Beta 1 vs. Mac OS X 'Tiger' (Part 2)."

how responsive a company is in responding to security threats and also how effectively they disseminate information regarding security threats.

Apple has released six versions of OS X in just six years.<sup>9</sup> In addition to the major upgrades, Apple also regularly releases security updates, although not on any set schedule. Since the first release of OS X, Apple has issued over 100 security-related updates, which sometimes fix as many as 25 separate vulnerabilities each.<sup>10</sup> Based upon this rather aggressive release schedule, it is clear that Apple is at least aware and actively engaged the betterment of security in OS X.

One of the biggest criticisms that can be leveled on Apple, as a company that develops an operating system, is their lack of transparency when it comes to their communication about security issues. They have been heavily criticized for slow responses to vulnerabilities and also very vague descriptions of what exactly security updates fix.<sup>11</sup> From Apple's own website, it is made clear that the company has no interest in sharing this information: "For the protection of our customers, Apple does not disclose, discuss or confirm security issues until a full investigation has occurred and any necessary patches or releases are available."<sup>12</sup> A quick look at the release notes of any recent security update from Apple will convince anyone that it is clear that they take this policy seriously.

Unfortunately, secrecy in security is not a good policy. The head of the security firm Secunia, Niels Henrik Rasmussen explains "Microsoft and most Linux distributions have learned the lesson and properly describe the nature and the impact of (most) vulnerabilities, allowing their customers to properly estimate the severity of a fixed issue. This is not possible when reading an Apple update."<sup>13</sup> Apple has yet to learn this lesson despite being frequently criticized. Although the developers at Apple have been faithfully churning out update after update, Apple's communication with security professionals and its customers has a lot of room for improvement.

As previously mentioned, all software contains vulnerabilities and bugs that must be patched. The report, *The Mac OS X Threat Landscape: An Overview*, published by Symantec gleans some interesting information by analyzing the security updates from 1999 to 2006. There is a clear trend in the types of applications addressed in the security updates released by Apple. Early in the OS X life cycle, most security updates focused on vulnerabilities in third-party applications.

---

<sup>9</sup> Apple. "Mac OS X Security."

<sup>10</sup> Adams, Aaron. "The Mac OS X Threat Landscape: An Overview." 4.

<sup>11</sup> Gruber, John. "Security Cannot Be Spun."

<sup>12</sup> Apple. "Apple Product Security."

<sup>13</sup> McCarthy, Kieren. "Techworld.com - Apple releases latest Mac version - with holes left in."

However, in recent years the focus has shifted to Apple-specific issues.<sup>14</sup> This shift has also coincided with an increase in research papers, released vulnerabilities and media attention on the security of OS X.

Most known vulnerabilities in OS X are of typical operating system varieties, including local privilege escalation, client-side code execution and remote code execution.<sup>15</sup> Based on data collected between 2003 and 2007, the security firm Secunia lists 109 security advisories for Mac OS X. Of the 109, only six have yet to be patched.<sup>16</sup> Considering that this data contains vulnerabilities, not necessarily exploits, it seems that there are surprisingly few for a five-year period. However, the Symantec report does claim that “exploiting these vulnerabilities on OS X is not notably more or less difficult than doing so on most other platforms.”<sup>17</sup>

*The Mac OS X Threat Landscape: An Overview* describes several of the more severe known vulnerabilities in depth. Particularly troubling are the five remote vulnerabilities listed because “remote hackers can exploit [them] without requiring authentication credentials or trust relationships with an affected target.”<sup>18</sup> One example of a significant remote vulnerability is the Apple Mac OS X AppleFileServer Remote Buffer Overflow Vulnerability. This can be triggered when authenticating to an AFP share. The password dialogue expects a string of a certain length, and when given a longer string will result in an exploitable stack buffer overflow.<sup>19</sup> The particularly troubling part about this vulnerability is that at least two exploits for it were published and freely available.

While much of the design of OS X can be considered very good in terms of security, there are a some severe weaknesses. One such weakness of OS X is how it has been designed to take advantage of both BSD and features of the Mach kernel. This type of “best of both worlds integration” has been largely touted by Apple. However, security researcher Nemo has pointed out that the design has created a weakness that allows Mach-specific calls with BSD-equivalent ones that would be otherwise rejected:

The securelevel feature of BSD is a rudimentary form of mandatory access control designed to prevent local users from carrying out specific actions when at specific securelevels. ...by careful use of Mach system calls, it’s possible to carry out what should be restricted activities, including lowering the securelevel value.<sup>20</sup>

---

<sup>14</sup> Adams, Aaron. "The Mac OS X Threat Landscape: An Overview." 4.

<sup>15</sup> Ibid. 4.

<sup>16</sup> Secunia. "Apple Macintosh OS X - Vulnerability Report - Secunia."

<sup>17</sup> Adams, Aaron. "The Mac OS X Threat Landscape: An Overview." 4.

<sup>18</sup> Ibid. 5.

<sup>19</sup> Security Focus. "Apple Mac OS X AppleFileServer Remote Buffer Overflow Vulnerability."

<sup>20</sup> Adams, Aaron. "The Mac OS X Threat Landscape: An Overview." 9.

This type of low level weakness in combining different architectures should be very alarming.

So far there have only been a couple of notable malicious code examples for OS X. Two examples of such code are OSX.Leap.A and OSX.Inqtana.A, both classified as worms by Symantec.<sup>21</sup> OSX.Leap.A was found in-the-wild while OSX.Inqtana.A was only demonstrated as a proof of concept.<sup>22</sup>

OSX.Leap.A is notable because it was declared the first ever virus for OS X.<sup>23</sup> The worm was discovered in February of 2006. It spreads via instant messaging programs, such as iChat, in a file called lastestpics.tgz, disguised as a picture file. The virus had to be manually executed, at which point it then attempted to attach itself to other applications. When the iChat application started, the worm would also try to send itself to all of the user's buddies in iChat.

A further inspection of the specific details of the virus reveals that it only spread on local networks through the Bonjour protocol. More importantly, the worm was so poorly written that, due to a bug in the code, it was unable to actually spread to other computers.<sup>24</sup>

The discovery of OSX.Leap.A was heralded by a blizzard of news stories from popular media about the end of OS X's carefree attitude towards security. A single Associated Press article ran on several major new outlets, with headlines ranging from "Viruses Catch Up to the Mac: Experts debate just how susceptible Apple is becoming" to "Macs No Longer Immune to Viruses, Experts Say" and even "Macs Invulnerable No More."<sup>25</sup> The security firm Sophos ran an opinion poll asking users if they now thought Macs would be more of a target in the future. The resulting story ran with the headline "79% believe Mac will be targeted more often in wake of Leap-A Mac OS X worm."<sup>26</sup>

Just a few days after the discovery of the OSX.Leap.A virus, the OSX.Inqtana.A was discovered as well. This particular virus used the Apple Mac OS X BlueTooth Directory Traversal Vulnerability to gain access and attempted to spread itself over BlueTooth to other devices. Oddly enough, this worm also had trouble spreading. A note on Symantec's description page explains that the "worm attempts to spread by using a time limited demo version of the Avetana library, which is bound to a bluetooth address. As a result of this the worm may not be

---

<sup>21</sup> Symantec. "OSX.Leap.A - Symantec.com."

Symantec. "OSX.Inqtana.A - Symantec.com."

<sup>22</sup> Adams, Aaron. "The Mac OS X Threat Landscape: An Overview." 11.

<sup>23</sup> Although both OSX.Leap.A and OSX.Inqtana.A are officially classified as worms by Symantec, there is a lot of debate among other sources as to whether it is a virus, worm or Trojan.

<sup>24</sup> Symantec. "OSX.Leap.A - Symantec.com."

<sup>25</sup> Gruber, John. "Good Journalism."

<sup>26</sup> Sophos. "79% believe Mac will be targeted more often in wake of Leap-A Mac OS X worm."

able to spread successfully.”<sup>27</sup> Although this worm was not established to have done any harm, something else did. Ironically, the update for the Sophos Anti-Virus software designed to catch instances of OSX.Inqtana.A ended up causing much more harm than the virus itself:

[Sopho's] update for the Inqtana-B virus identity file incorrectly flagged various Microsoft Office and Adobe Acrobat Reader files, to name just a few, which led to data loss for many of the program's users. Hundreds and in many cases thousands of files were erroneously flagged as being infected, and, depending on the settings of the users, were then deleted. In several cases the spread of the 'infected files' was so great that after the 'disinfection' the systems were left all but useless.<sup>28</sup>

Given the massive amount of media attention for both these worms, it can be hard to pick out the important details. Neither of them spread successfully or were sophisticated on any level. All that was really established was that it was indeed possible to write a virus for OS X. A claim that any serious security researcher has been making for years.

### **Out Of The Box Security and Additional Hardening Measures**

The out of the box security settings of OS X, in comparison to other popular operating systems, can only be described as conservative. A security technology brief from Apple explains the approach to security in OS X as “Secure from the start, easy to keep secure, and easy to make even more secure.”<sup>29</sup> As advertised, the default installation of OS X, with all relevant security updates applied is quite secure. There are several important factors that play into this.

The superuser of OS X, in tradition with other UNIX systems, is a user called root. However, in OS X, the root user plays somewhat of a phantom role. Although it is present in all OS X systems and plays a role behind the scenes, the account itself is disabled by default. Most users of OS X will never need to enable it or even know that it exists. This is a striking departure from systems like Windows, whose *default user* is in effect, root.<sup>30</sup>

In addition to the root user, OS X has also inherited a fully functional multiuser operating system. OS X is designed for use by multiple people, each sharing their own Home Directory, complete with application preferences. All files and folders in the system have built-in permissions settings and each user's Home Directory is designed so that no one but that user and root has access to it. New user accounts in OS X are always set to 'normal' unless otherwise specified, meaning the account only has basic privileges by default. This follows the security rule

---

<sup>27</sup> Symantec. "OSX.Inqtana.A - Symantec.com."

<sup>28</sup> Mihailescu, Victor. "Sophos Anti-Virus Software Causes More Damage Than All OS X Viruses, Trojans and Worms Put Together - Who will protect Mac users from the anti-virus companies? - Softpedia."

<sup>29</sup> Apple Developer Connection. "An Introduction to Mac OS X Security for Web Developers"

<sup>30</sup> Thurrott, Paul. "Windows Vista Beta 1 vs. Mac OS X 'Tiger' (Part 2)."

commonly known as the “principle of least privileges.”

One important aspect in host security is turning off all unnecessary network services. In the past some operating systems turned on many services by default to ease initial configurations; this is now considered bad practice because for each service enabled, a new attack vector is instantiated. In *Corporate Computer and Network Security*, Raymond Panko comments that “security experts now agree that a firm should turn off all unnecessary services because a large number of exploits take advantage of vulnerabilities in obscure and little used services...”<sup>31</sup> OS X goes one step further by disabling most of these services by default.

In a default OS X installation, only four network services are enabled by default: automounter, syslog, sunrpc and NetInfo.<sup>32</sup> These four services are essential parts of the operating system and cannot be turned off. Some of the important services included with OS X but disabled by default are SSH, FTP, File sharing over AFP and personal web sharing. These services can be easily turned on and off through a GUI dialogue in the System Preferences application. By including these features but disabling them by default, Apple has taken a very important step that sacrifices neither security nor ease of use.

No matter how secure any system is at its release, there will be inevitably be vulnerabilities and bugs. The reasonable approach to counteract this is to provide regular software and security updates. Similar to Windows, OS X also provides a method for automatic updating that is built in to the operating system. The update application, called Software Update, checks for updates weekly by default.<sup>33</sup> In addition to system-related updates, Software Update also checks for updates to all other Apple software installed on the operating system.

Lastly, OS X also includes a built-in system for logging all important system related events. The logs can be easily viewed in the Console application or at the command line interface for advanced users. OS X logs system events, crash reports and also all security related events, including any invocations of sudo.<sup>34</sup>

Despite the “secure from the start”, security motto for OS X, there are still some weak points in the default installation of OS X. Most of these weak points can be easily remedied, but they do require active intervention by the user and usually at least some knowledge of the features in general.

As previously mentioned, OS X is designed to be a multiuser system and each newly created

---

<sup>31</sup> Panko, Raymond R. *Corporate Computer and Network Security*. 228.

<sup>32</sup> Apple Developer Connection. "An Introduction to Mac OS X Security for Web Developers"

<sup>33</sup> Ibid.

<sup>34</sup> Ibid.

user is a normal user without administrative privileges. This is true, with one notable exception; upon installing OS X for the first time you are required to create a user account, which is actually an administrative account. After successfully creating the account the user is logged in to the system without any further notices regarding additional users.

While the admin group in OS X is not quite the equivalent of the root user, it does have the ability to escalate privileges for short periods of time in order to authenticate actions that would normally require root access. An example of this is the UNIX sudo command, which allows all users and groups listed in the sudoers file to perform root-level operations on the system. In layman's terms, this means they can do anything, including deleting the system.

The most unfortunate aspect of this is that the normal setup routine in the OS X installation does nothing to describe the security implications of this. There is no indication as to the fact that the user being created is an admin and more importantly, no indication that this should not be the primary user of the system. This is clearly a direct violation of the "principle of least privileges" rule.

Moving past the unfortunate design decisions regarding this first user, it is a relatively painless process to add an additional non-admin user for everyday use. If just starting out with a fresh installation, the user can simply proceed to make an additional non-admin account and use that one regularly. The design of OS X allows for a normal user to authenticate system changes (i.e. network settings and application installations) using an administrative account and password. There is no need to actually change accounts. Furthermore, there is nothing special about the *first user* of an OS X system. The user can always at a later point in time create a new admin account and then deescalate the privileges of the first account. This avoids the frustrating and time consuming operation of having to change a user accounts.

Modern security suggests that no operating system is complete without some sort of built-in firewall. OS X has included a firewall with the system since OS X 10.2. The interface for the firewall is somewhat primitive by design in an attempt to encourage normal users to make use of it. FJ de Kermadec elaborates on this by stating "some users may argue that the interface provided by Apple does not allow a lot of fine-tuning: this true, but is done on purpose to allow even newcomers to benefit from reliable security settings, without having to worry too much about settings."<sup>35</sup> Up until the release of Leopard, the built in firewall GUI interface was based entirely on services. Users select which network services, such as personal file sharing, remote

---

<sup>35</sup> Kermadec, FJ de. "A Security Primer for Mac OS X." 10.

login and printer sharing, they would like to allow or restrict.<sup>36</sup> Behind the basic GUI interface of the OS X firewall is the ipfw command line firewall tool. This allows a much more fine-grained customization for advanced OS X users.

While the simplification of the GUI interface for the OS X firewall can arguably be better or worse for security, and even perhaps both, there are some additional serious shortcomings. First and foremost is that the firewall is not enabled by default on any version of OS X. Furthermore, the interface to access it is buried deep in the System Preferences application. This is a real problem for most users; Kermadec notes, “few Mac OS X users know that their operating system of choice comes with a built-in, time-tested, industrial strength firewall that they can turn on by simply using the ‘Sharing’ preferences pane.” Looking past the issue of enabling the firewall, the technology itself has a few holes.

It was not until OS X 10.4 that the firewall enabled anything more than TCP filtering rules. Even in 10.4, UDP and ICMP filtering is only available through advanced configuration of the firewall.<sup>37</sup> Apple’s Bonjour service also proves to be somewhat problematic as well. Bonjour is Apple’s version of a local network discovery protocol for devices such as printers and computers and is known as mDNSResponder to the system. To enable it to work properly, “mDNSResponder listens by default on UDP port 5353.”<sup>38</sup> This is also true regardless of whether or not UDP has been disabled through the firewall.<sup>39</sup> Any service that listens by default on a port and cannot be disabled by the user is certainly problematic.

One last missing security detail to highlight involves the Software Update application. The application checks for system and security updates weekly by default. It can also be set to check for updates as frequently as daily and even download the updates automatically in the background. Bafflingly, it is not possible to automatically install updates. In his review of OS X Tiger, Paul Thurrott expounds upon this:

While you can check Software Update for new updates manually, you can also configure it to check for updates on a regular basis (say, daily) and download important updates in the background while your working [...]. However, Software Update cannot be configured to automatically install security updates, which I find somewhat confusing.<sup>40</sup>

This configuration may make sense in a large firm setting; there are other methods with which IT professionals can roll out the updates, allowing them to pick and choose which to apply and

---

<sup>36</sup> Apple. "Mac OS X Security Configuration For Version 10.4 or Later Second Edition." 117.

<sup>37</sup> Adams, Aaron. "The Mac OS X Threat Landscape: An Overview." 9.

<sup>38</sup> Ibid. 10.

<sup>39</sup> Ibid. 10.

<sup>40</sup> Thurrott, Paul. "Windows Vista Beta 1 vs. Mac OS X 'Tiger' (Part 2)." 5.

when. Unfortunately, for single users and small businesses, this decision seems to leave an unnecessary burden on users to manually apply each update.

The most recent release of OS X, 10.5 (Leopard) touts many new security features. Some of the major new features include application sandboxing, address space randomization, an application based firewall and input manager restrictions.

Both application sandboxing and address space randomization are important security additions to any operating system. Application sandboxing, also called mandatory access controls, provides kernel level control over what individual applications have access to and can do.<sup>41</sup> In the case of an exploit that might use a browser to arbitrarily execute code, a sandbox-type environment might prevent this.

Address space randomization goes a long ways towards preventing buffer overflow exploits. This feature randomizes important address references in the system, making it harder for hackers to anticipate where an overflow might occur. It also makes it much more difficult to write an exploit that will reliably work on a wide range of systems, since each system is randomized.<sup>42</sup>

While acknowledging that each of these features are important, some security experts have leveled criticism on their implementation. In the case of sandboxing, the default profiles don't seem to actually stop any of the most obvious threats. Important applications that have regular access to remote networks, such as Mail, Safari and iChat aren't actually sandboxed.<sup>43</sup> Apple's current implementation and documentation of the feature also make it difficult for responsible third-party developers to use it. Leopard's implementation of address space randomization has been criticized for not being *random enough*.<sup>44</sup>

The new application based firewall in Leopard switches from the previous service based model to an application based one. While this isn't necessarily a bad thing, it also hasn't made any inroads towards a more robust and configurable firewall. In fact, it seems to have taken a step backward. The firewall allows three basic settings: allow all incoming connections, block all incoming connections and set access for specific services and applications. Clearly the first two options are not practical, so we are left with the third option, which seems to have a rather odd and confusing interface as Rich Mogull explains in "Leopard Firewall Takes One Step Forward, Three Steps Back":

The first problem [...] is that it's difficult to tell what the Set Access option does. It starts the

---

<sup>41</sup> Ptacek, Thomas. "A Roundup Of Leopard Security Features."

<sup>42</sup> Adams, Aaron. "The Mac OS X Threat Landscape: An Overview." 25.

<sup>43</sup> Ptacek, Thomas. "A Roundup Of Leopard Security Features."

<sup>44</sup> Ibid.

new application-level firewall and lists in the Sharing pane any services you've opened, but it doesn't indicate if they are allowed or blocked. There's also no option for you to add your own open services or ports anymore. Instead, you can add or remove individual applications, but not network services. Stealth mode is still available in the Advanced settings, but the UDP blocking, useful to stop port scanning and some other attacks, is gone.<sup>45</sup>

Leopard has also changed the internal implementation of the firewall, replacing ipfw with an Apple developed firewall, which is less well known and possibly harder to do advanced configurations in.<sup>46</sup> Most importantly, Apple still has not changed the default firewall setting to be on rather than off.

The restrictions on input managers in Leopard are an important step in closing what was previously a major security risk in OS X. Security expert Thomas Ptacek describes input managers:

Input managers are terrifying. They're arbitrary blobs of code that get injected into almost every Mac application. They are a "UI extension interface" in the same way that Back Orifice 2k is a "remote system administration facility".<sup>47</sup>

Leopard puts serious restrictions on what input managers can do, effectively closing this security hole.

The new security features introduced in Leopard have a range in significance and quality of implementation. Considering that 10.5 is only a few months old, it is possible that they will be adjusted in future releases or updates.

The Mac OS X operating system does clearly demonstrate good out-of-the-box security, with only a few glaring weaknesses. Fortunately there are several easy steps that users can take to harden OS X. First and foremost, users should make sure to take the extra step at installation time to make an additional non-administrative account for every day use. Users can also choose from several other options via the Security panel in System Preferences to further harden the system. Users can disable automatic login, enable automatic logout, require a password to wake the computer from sleep or screen saver and require a password to unlock each secure system preference. The firewall can also be easily enabled and users can refrain from enabling unnecessary network services. Installing system and security updates does require active user participation, but is not an undo burden.

Other important, but more complex, options that the security panel provides are the options to use secure virtual memory and FileVault encryption. Choosing to use secure virtual memory

---

<sup>45</sup> Mogull, Rich. "Leopard Firewall Takes One Step Forward, Three Steps Back."

<sup>46</sup> Ibid.

<sup>47</sup> Ptacek, Thomas. "A Roundup Of Leopard Security Features."

allows the system to encrypt the memory's swap file, which can contain confidential data. While this is easy to implement, it is unlikely that most users understand what this does. FileVault is Apple's only implementation of file encryption for user data and can be easily enabled; however because of some serious shortcomings in the implementation and the drastic consequences of losing a decryption key, most professionals do not necessarily recommend this particular option.

Taking these few simple steps goes a long ways towards closing any security holes in the default OS X installation. While clearly not all attacks will be avoided using these methods, they do cut off many attack vectors. A considerable advantage of the approach taken with OS X, combining secure defaults and ease of use, is that it presents security in a way that is accessible to normal users. OS X makes implementing many fundamental security practices quite trivial.

## **Conclusion**

Mac OS X has for the most part, compared to other operating systems, enjoyed a carefree history when it comes to security. There are certainly many vulnerabilities, but relatively few known exploits for them. There are also almost no examples of attacks in the wild. The few attacks that researchers have noted in the wild, although highly publicized, are mostly harmless. This however should not be taken as evidence that OS X is difficult or impossible to attack.

One area where OS X clearly scores high marks is its out of the box security. The design decision to take a conservative approach to security is certainly a good one. There is room for improvement though. Most notably, the firewall should be enabled by default and it should be harder for users to run admin user accounts for day-to-day use. The security improvements in Leopard are a good step forward, but still need to be improved on as well.

What is undeniable about OS X security is that it has yet to be exploited on a large scale. When the OSX.Leap.A was discovered in February 2006, many people proclaimed that it would be a watershed event, and that Mac users were no longer safe from viruses. It has been nearly two years since then, and there are still no large-scale virus outbreaks for OS X. In fact, in a recent security report by Sophos, senior technology consultant Graham Cluley stated, "...hackers seem happy to primarily target Windows users and not spread their wings to other platforms. It seems likely that Macs will continue to be the safer place for computer users for some time to come - something that home users may wish to consider if they're deliberating about the next computer they should purchase."<sup>48</sup> Given the source, a senior consultant at a well-known security

---

<sup>48</sup> Sophos. "Sophos Security Report reveals Trojan domination in first half of 2006."

firm, this is a remarkable statement.

Even though OS X has an excellent security record, it is important to recognize that it has yet to stand up to the kind of security beating that operating systems like Windows XP have.

Windows holds somewhere around 90% of the PC market, making it an immense target for hackers. Microsoft did not have the benefit of obscurity working for it in the case of Windows, as OS X most certainly does.

It is important that Apple, and OS X users, not become complacent about security. As OS X becomes more popular, so will its attractiveness to hackers. Security is an ever changing and increasingly complex field, and Apple will have to continue to steadily improve its operating system to keep ahead. For the time being though, OS X does indeed seem to be 'more secure.'

## Citations

- Adams, Aaron. November 13, 2006. "The Mac OS X Threat Landscape: An Overview." Symantec DeepSight™ Threat Management System. [http://downloads.securityfocus.com/downloads/MacOSX\\_DeepSight\\_Report.pdf](http://downloads.securityfocus.com/downloads/MacOSX_DeepSight_Report.pdf)
- Apple. February 6, 2007. "Apple Get a Mac Ad Campaign-Virus." YouTube. <http://www.youtube.com/watch?v=nxjB9-klebU&mode=related&search=>
- Apple. 2007 "Apple - Mac OS X Leopard - Technology - UNIX." Apple Inc. <http://www.apple.com/macosx/technology/unix.html>
- Apple. 2007. "Apple Product Security." Apple Inc. <http://www.apple.com/support/security/>
- Apple. 2007 "Mac OS X Security." Apple Inc. [http://images.apple.com/macosx/pdf/MacOSX\\_Leopard\\_Security\\_TB.pdf](http://images.apple.com/macosx/pdf/MacOSX_Leopard_Security_TB.pdf)
- Apple. 2007. "Mac OS X Security Configuration For Version 10.4 or Later Second Edition." Apple Inc. [http://images.apple.com/server/pdfs/Tiger\\_Security\\_Config\\_021507.pdf](http://images.apple.com/server/pdfs/Tiger_Security_Config_021507.pdf)
- Apple Developer Connection. August 25, 2004. "An Introduction to Mac OS X Security for Web Developers" Apple Inc. <http://developer.apple.com/internet/security/securityintro.html>
- Apple Developer Connection. April 29, 2005. "Security Overview." Apple Inc. [http://developer.apple.com/documentation/Security/Conceptual/Security\\_Overview/index.html](http://developer.apple.com/documentation/Security/Conceptual/Security_Overview/index.html)
- Gruber, John. May 2, 2006. "Good Journalism." Daring Fireball. [http://daringfireball.net/2006/05/good\\_journalism](http://daringfireball.net/2006/05/good_journalism)
- Gruber, John. May 30, 2004. "Security Cannot Be Spun." Daring Fireball. [http://daringfireball.net/2004/05/security\\_cannot\\_be\\_spun](http://daringfireball.net/2004/05/security_cannot_be_spun)
- Kennedy, M.R. April 20, 2007. "Apple U.S. market share hits 5 percent." ZDNet. <http://talkback.zdnet.com/5208-10532-0.html?forumID=1&threadID=32795&messageID=603761&start=0>
- Kermadec, FJ de. February 2, 2004. "A Security Primer for Mac OS X." O'Reilly MacDevCenter. <http://www.macdevcenter.com/pub/a/mac/2004/02/20/security.html?page=1>
- McCarthy, Kieren. May 27, 2004. "Techworld.com - Apple releases latest Mac version - with holes left in." TechWorld. <http://www.techworld.com/security/news/index.cfm?NewsID=1636&Page=1&pagePos=4>
- Mihailescu, Victor. February 23, 2006. "Sophos Anti-Virus Software Causes More Damage Than All OS X Viruses, Trojans and Worms Put Together - Who will protect Mac users from the anti-virus companies? - Softpedia." Softpedia. <http://news.softpedia.com/news/Sophos-Anit-Virus-Software-Causes-More-Damage-Than-All-OS-X-Viruses-Trojans-and-Worms-Put-Together-18620.shtml>
- Mogull, Rich. November 5, 2007. "Leopard Firewall Takes One Step Forward, Three Steps Back." TidBits: Mac news for the rest of us. <http://db.tidbits.com/article/9294>
- Panko, Raymond R. 2004. \*Corporate Computer and Network Security\*. New Jersey: Pearson Education Inc.
- Ptacek, Thomas. October 29, 2007. "A Roundup Of Leopard Security Features." Matasano Chargen. <http://www.matasano.com/log/981/a-roundup-of-leopard-security-features/>
- Secunia. 2007. "Apple Macintosh OS X - Vulnerability Report - Secunia." Secunia. <http://secunia.com/product/96/?task=advisories>
- Security Focus. May 3, 2004. "Apple Mac OS X AppleFileServer Remote Buffer Overflow Vulnerability." Security Focus. <http://www.securityfocus.com/bid/10271/info>
- Sophos. February 17, 2006. "79% believe Mac will be targeted more often in wake of Leap-A Mac OS X worm." Sophos. <http://www.sophos.com/pressoffice/news/articles/2006/02/macpoll.html>
- Sophos. July 5, 2006. "Sophos Security Report reveals Trojan domination in first half of 2006." Sophos. <http://www.sophos.com/pressoffice/news/articles/2006/07/securityreportmid2006.html>
- Symantec. February 13, 2007. "OSX.Inqtana.A - Symantec.com." Symantec. [http://www.symantec.com/security\\_response/writeup.jsp?docid=2006-021715-3051-99&tabid=2](http://www.symantec.com/security_response/writeup.jsp?docid=2006-021715-3051-99&tabid=2)
- Symantec. February 13, 2007. "OSX.Leap.A - Symantec.com." Symantec.

[http://www.symantec.com/security\\_response/writeup.jsp?docid=2006-021614-4006-99&tabid=2](http://www.symantec.com/security_response/writeup.jsp?docid=2006-021614-4006-99&tabid=2)  
Thurrott, Paul. November 29, 2005. "Windows Vista Beta 1 vs. Mac OS X 'Tiger' (Part 2)." Paul Thurrott's SuperSite for Windows. [http://www.winsupersite.com/showcase/winvista\\_beta1\\_vs\\_tiger\\_02.asp](http://www.winsupersite.com/showcase/winvista_beta1_vs_tiger_02.asp)