

**Written Testimony of
Avadis “Avie” Tevanian, Jr. Ph.D.
on behalf of
Apple Computer, Inc.
before the
House Subcommittee on Technology, Information Policy,
Intergovernmental Relations and the Census
June 16, 2004**

Chairman Putnam and members of the Subcommittee, I am very pleased to be here today on behalf of Apple to participate in this hearing titled “*Locking Your Cyber Front Door – The Challenges Facing Home Users and Small Businesses.*” I am Avie Tevanian, the Chief Software Technology Officer for Apple, responsible for setting company-wide software technology direction. I joined Apple in 1997 as the leader of the team of software engineers that designed and developed Apple’s brand new operating system, Mac OS X. Mac OS X was first released to the public in 2001. Since its release, I am proud to say the migration of Mac users to Mac OS X has been viewed as one of the most successful operating system transitions in history. Mac OS X, with approximately 10 million active users and more than 10,000 native applications, is widely recognized as having been implemented with an effective, comprehensive approach to security for all users. Apple has an unwavering commitment to security based on our belief that effective, pro-active cyber security is essential to protect the economic health and welfare of our nation. I commend the Subcommittee for holding this series of hearings and appreciate the opportunity to contribute today.

Mr. Chairman, I can appreciate first hand the concerns of Congress in regard to the myriad of threats and challenges individuals face every day as they cope with attempting to manage computer security on their own. From computer companies and software developers, to government agencies, major corporations and small business owners, as well as to individual home users, we all must work together to thwart the growing threat of cyber attacks. Without a doubt, computer security begins with the design and development of secure hardware and software products from companies like Apple. However, it doesn’t stop there. Security is everyone’s responsibility. While all stakeholders are responsible in varying degrees for ensuring the security of their systems, home users and small business owners must remain vigilant by taking their own security seriously every day. Just as we are expected to lock our own front doors ourselves, we must also take basic steps to protect ourselves from unwarranted cyber intruders. An especially critical challenge for companies like Apple is making security tools as accessible, transparent and easy to use as locking your own front door.

Security Challenges and Threat

It seems that not a week goes by without news of another major software virus or computer worm having infected a host of computer systems. These attacks turn unknowing computer users into victims, sometimes with devastating effects. These victims are not only government agencies and major corporations running mission critical systems, but also include the many small businesses and home users with limited technology backgrounds.

Further, some very serious computer security attacks often come with much less public fanfare than a major virus outbreak, but the results are no less devastating – maybe even more so. For example, often we hear stories of a computer hacker that has commandeered another’s computer stealthily, initiating further attacks remotely, stealing important data and/or even that computer victim’s identity. Some of these victims never even knew they were being attacked until it was too late.

Why are small businesses and home users so vulnerable today? First, more and more small business owners and home users are accessing the Internet using always-on broadband connections. With these always-on high-speed connections, individuals are increasingly becoming prime targets from external cyber attacks. Second, the majority of individual computer users today are using one operating system, which makes it much easier for global cyber criminals to exploit. Third, just as common criminals tend to prey on the easiest targets, individual computer users are particularly at risk because they often lack the computer expertise, not to mention the information technology (IT) staff, necessary to monitor, assess and react to the constant bombardment of Internet threats. To make matters worse, these threats are constantly changing, morphing into new and increasingly sophisticated attacks, challenging even the most experienced IT professionals. Further compounding the problem, a number of security features available on many computer systems today were developed primarily for IT professionals working for large businesses. As a result, managing security effectively often remains beyond the ability of many average home users and small business owners.

It is important to keep in mind that just as is the case with physical security, information security is not always automatic. Individuals must remain security conscious and alert. At the same time however, we also believe that in order to make computer security more manageable for individual users, security software must be intuitive, easy to administer, and wherever possible, automatic. Otherwise, average computer users will either not know how to protect themselves appropriately or may implement security ineffectively. In the end, many inexperienced computer users often do too little to protect themselves, or worse – do nothing.

Apple’s Approach to meeting the Security Challenge

Just as building a computer securely in the first place is a priority for Apple, ensuring that security is easy to manage and maintain by the end user is equally critical. Since implementing the first commercial graphical user interface with the introduction of the Macintosh in 1984, Apple has prided itself on its “ease-of-use” operating system and software targeted originally for home users, small businesses and educators. As a result, Apple’s approach to security starts from the vantage point of the individual computer user. This overarching ease-of-use perspective still permeates the Apple culture today, and was the guiding force for me and my team of engineers as we set about to develop Mac OS X, including its built-in security features.

From the beginning, Apple implemented a security strategy approach that was central to designing Mac OS X. First, we developed an extremely robust security architectural plan. Then we applied that plan to securing the very core foundation of the operating system itself. Because security is built into the core, it remains integral to every part of the operating system. Further, understanding that security often would not be administered by a team of IT professionals but by average home users, we made it very easy to administer. This comprehensive approach to integrating security into every aspect of the operating system has also been given very positive reviews from NSA’s own security researchers. It is essential for operating system security to

provide a solid, virtually impermeable security foundation for all computer systems, whether intended for use in family rooms across the country or for hosting mission critical government systems. With a secure core in place appropriate layers of additional security can be added.

Let me explain this approach in a little more technical detail. First, at its foundation, Mac OS X is open sourced, based on UNIX, which has had its core components subjected to peer review for decades. We have found this approach has led to potential security problems being identified early and fixed before any vulnerability was exploited. Second, security is integrated directly into all software layers starting with the core foundation, using state-of-the-art standards based technologies (e.g., SSH, SSL, Kerberos, CDSA, AES Encryption). I would like to emphasize this point. We have built security directly into our operating system as an integral component, not simply added it on after the fact. Third, we placed administrative access to all of our security features inside a number of very intuitive applications that the average user can quickly grasp.

Knowing that new vulnerabilities can arise at any time, we built-in a software update tool that automatically alerts users when security updates are ready for download and installation. This feature is critically important. Simply building a secure system and then releasing periodic patches is of limited value if installing, or even finding those patches is confusing, complicated or simply inconvenient. At Apple, we believe that our software update approach ensures consistent secure software configurations, tested by Apple engineers, are readily available to our users. For the home user and small business owner, this approach makes keeping up-to-date as simple as clicking your mouse and authenticating a download – not to mention fast and effective.

We believe that an individual's computer experience can and should be protected from the start. Therefore, we ship all of our hardware and software products such that they are secure right out of the box. By starting out with a computer in a secure state, individuals are better protected when they first connect to a network or venture off onto the Internet. Later, they may choose for themselves those features and functions they want to implement on-the-fly without having security compromised unknowingly.

Knowing that more and more home users have always-on broadband connections, which increases vulnerability, is a significant reason why we built-in the capability of creating multiple user accounts on every computer. This feature enables the owner of a computer to designate himself as an "administrator" of that machine. An administrator is allowed to change important security and system settings. The administrator can also create additional user accounts and limit the degree to which other users of that computer can change important settings. Even those individuals with administrator privileges are required to re-authenticate before important system updates and changes are made, providing additional protection. As a further precaution, the administrator is kept from directly accessing the core of the operating system by default. In addition, to protect an unattended computer from unwarranted and unauthorized access, we configure our entire system to sleep when not being used and then to rapidly wake-up when the owner returns. When the system is asleep it is not accessible from the network nor is it susceptible to Internet attacks. We believe our implementation of these sleep and wake features is very robust and fast, reducing the desire of the user to disable them.

These highlighted security features are by no means intended to be exhaustive. In fact, although not the direct focus of today's hearing, Apple also provides advanced tools and technologies that allow system administrators to secure their enterprise desktops, servers and networks. As is our

approach to every software application we build, all of these security features and system controls are very configurable, extremely flexible, and highly intuitive, whether they are used by IT professionals protecting a cluster of 1,000 or more computers on a university campus, or by a home user managing an iMac with basic technical skills.

Providing security tools alone is not enough. To make educating our users about security convenient, Apple has created a public web page for customers to learn about all of the various Mac OS X security technologies and features (<http://www.apple.com/macosx/features/security/>). We also provide additional security resources and useful common sense security tips right on their desktop under a number of convenient help menus. Even with security settings easily managed on a Mac, we believe it is important to continually remind all home computer users and small business owners of the types of common sense steps they should be taking as they routinely go about working, communicating and surfing online. A sample of some basic security tips would include the following:

- Choose a password that is difficult to guess and change it often,
- Make sure your system software and security applications are up-to-date,
- Create multiple user accounts on your computer and limit those who are authorized to change system preferences and security settings,
- Be wary of unusual email attachments – even from friends,
- Only download applications and files from legitimate sources, and
- Backup your files regularly

Although these steps listed above seem very obvious, continuing to remind users of their importance can go a long way toward lessening the impact of a spreading virus or a malicious cyber attack.

Mac OS X Security Record

As we are all so well aware, tens of thousands of viruses and worms have been unleashed on the Internet in recent years. These attacks are unrelenting, interrupting Internet access, crippling large company networks, and even bringing down government agencies. The global costs from these disruptions to businesses alone were estimated by Trend Micro to be \$55 billion in 2003, up from \$30 billion in 2002, and \$13 billion in 2001. Not surprisingly, this steep upward trend is projected by Trend Micro to continue this year. Notwithstanding all of our collective efforts to mitigate this threat, it must be made clear that no company or its software can ever claim to be fully immune from viruses or guaranteed impenetrable from a cyber attack.

That said, since the debut of Mac OS X in 2001, and after three major updates, I am not aware of a single virus that has affected our operating system. Furthermore, we have been able to respond rapidly to any potential vulnerability in our operating system through 44 security updates delivered through our software update tool. Of those potential security problems, none were ever known to be exploited.

While Apple is very proud of our approach to security, we recognize the importance of being pro-active in anticipating new threats or security problems so that even potential risks are quickly mitigated and threats reduced. We all know that no security is 100% perfect. If managed improperly, or not at all, no amount of security can withstand a cyber attack. While we can provide secure systems and the tools to manage that security, we need to work with our

customers and partners, in government, industry and the consumer market to ensure preparedness and to ensure the use of best practices in protecting our information systems.

Beyond the Individual User – Employing Cyber-Diversity

Individuals within larger organizations often worry less about cyber security because they believe their internal IT/ Cyber Security departments will protect them. Although implementation of security updates can be administered at the network level, there is still an important role to be played by the individual user in understanding what security features should be enabled on their own desktop.

Moreover, I would urge the Committee to consider the significant vulnerability within many enterprises, including most government agencies, that results from having essentially a homogeneous operating environment. When security has been breached at the enterprise level, or a malicious virus has been unleashed inside an organization, it often propagates itself very rapidly because the organization is configured using one operating system and platform for many systems and applications. This homogenous configuration means that one worm could bring down an entire organization very rapidly, costing millions of dollars and hours, if not days, in productivity. While, with the strong leadership of this Subcommittee, most agencies have implemented redundant systems, disaster recovery plans and other forms of back up, if all the systems are the same, there is significant risk none will survive, even though they may be geographically isolated or have substantial external layers of security.

The Congress should approach this very real security vulnerability by encouraging agencies to achieve cyber-diversity. Organizations should consider adding a mix of interoperable computer systems to their networks such that when one system is attacked, another system will remain up and functioning within the organization on its network. Unfortunately, many organizations hold on to an obsolete belief that differing computer systems, such as Windows PCs and Macs cannot interoperate or are costly to administer when used together. Our implementation of Mac OS X has focused on open industry standards and formats. When possible, we provide direct compatibility with Windows-based PCs and servers. As a result, a Macintosh fits in quite easily with Windows and UNIX networks. We firmly believe that any perceived short term administrative efficiencies and/or cost savings identified by standardizing on one platform is more than offset by the security risk and productivity losses associated with having a thoroughly homogeneous environment that is vulnerable to attack.

Summary

Mr. Chairman, as I said at the beginning of my testimony, computer security is everyone's responsibility. For our part, Apple is committed not only to providing all users with a secure operating system, but also with the easy to use security tools they need to protect themselves, their businesses, and their families, while enjoying all the benefits from surfing online or connecting to others on a network. We remain committed to a computer security approach that is robust and effective, while at the same time easy to use and administer.

We appreciate the Subcommittee's interest in the computer security of small business owners and home users. We look forward to working with you on this very important issue. I'm prepared to answer any questions you may have at this time.