Reed Electronics Group

MICROPROCESSOR REPORT

www.MPRonline.com

THE INSIDER'S GUIDE TO MICROPROCESSOR HARDWARE

THE EDITORIAL VIEW

More Computers, Less Security

By Tom R. Halfhill {1/26/09-02}

In the 1970s, industry pioneers like Bill Gates and Steve Jobs envisioned a future with a personal computer in every home and office. At the time, their dream was revolutionary. Thirty years later, it seems quaintly limited. Many a home today has two or more personal computers, and many business people have both a desktop PC and a laptop PC.

Indeed, traditional PCs are beginning to seem archaic. There is an explosion of what I call second-generation personal computers—compact netbooks, smartphones, and multifunction cellphones. These personal computers are truly personal, because they accompany a person everywhere.

In addition, a growing number of personal computers are dedicated to specific tasks—"embedded personal computers," if you will. This broad category encompasses videogame consoles (both set-top and handheld), automobile entertainment systems, portable media players, digital cameras, digital picture frames, and other smart appliances.

All these things, fundamentally, are computers. All have microprocessors that run software. Most have some provision for adding new software or modifying the existing software. And therein lies the catch that threatens to ruin the dream of personal computing. Unlike the typical microwave oven or similar embedded system with fixed firmware, programmable devices require proactive user management and protection from increasingly devious malware attacks.

Managing a conventional PC is bothersome enough. There are software updates to download, software subscriptions to renew, software conflicts to resolve, security precautions to observe, and risky behaviors to avoid. Now multiply those responsibilities by the burgeoning number of computing devices entering our lives. Some fairly ordinary households are administering as many computers as a department IT manager does.

Moreover, these devices are very different from one other. They run a variety of operating systems, have different connectivity options, and are vulnerable to different kinds of threats. Some are easy targets for malicious email attachments and booby-trapped websites. Others can be bricked by a buggy firmware update from their maker. A few products are even sabotaged before leaving the factory, such as the digital picture frames recently found to infect PCs with spyware as they download photos over a USB cable. That was never a problem with wooden picture frames. What's a harried user to do?

Security Is an Afterthought

Unfortunately, there aren't many solutions to this problem, and it grows worse as people accumulate more devices. One solution is to emulate the Amish and reject all, some, or most new technology. Another is to outsource the system maintenance to someone else, usually a friend or family member who is the nearest alpha geek.

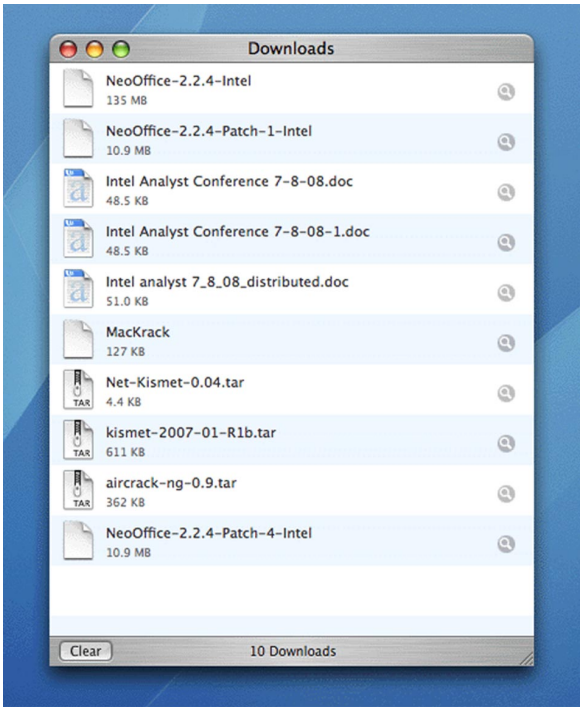

Figure 1. This window displays a log of files downloaded with the Apple Safari web browser. Clicking the "Clear" button in the lower-left corner would have erased the log.

The best solution is for the makers of these systems to stop regarding security as an afterthought or as someone else's problem. Security should be an integral part of the hardware and software design. Although making security the top priority requires more effort and hikes development costs, eventually it will become a selling point that supports higher retail prices.

Years ago, automakers resisted mandatory seatbelts, airbags, and crash testing. Over time, however, safety became a desirable feature. Today, motorists pay extra money for options like side-curtain airbags, antilock brakes, and collision-warning systems.

But even the best-designed system isn't foolproof or bulletproof. Security threats can blindside users from completely unexpected directions. It recently happened to me.

A Shocking Breach of Trust

I had a Macintosh with a minor hardware problem I couldn't fix. I brought it to a long-established local repair shop that specializes in Macs. Their repair technicians couldn't fix the problem, either, so I resigned myself to living with it. Later, while downloading a routine update for the open-source NeoOffice suite, I found something strange in Safari's download log. Someone had downloaded four files unfamiliar to me. (See Figure 1.)

The files were suspiciously named "MacKrack," "Net-Kismet," "kismet," and "aircrack." A quick Google search revealed that they are password-cracking programs, mainly for use against password-protected Wi-Fi networks. Someone had downloaded hacker tools onto my computer!

I searched the hard drive but couldn't find the programs. Perhaps they had been downloaded and copied to a flash drive without being installed. Or maybe they had been installed, used for a while, then removed. Or maybe they were hidden on the hard drive too cleverly for me to find. In any case, I was alarmed. What had my computer been used for? And what else might be lurking on the hard drive? Could there be viruses, spyware, a keylogger, child porn, or a program that surreptitiously seized control of my computer for a botnet?

One thing I didn't worry about was that any personal files had been rummaged. All those files were safely stored on an external drive, which hadn't accompanied the computer to the repair shop. Nevertheless, my Mac was now untrustworthy. After grabbing a screen shot of the download log, I shut down the machine and unplugged the Internet connection. Better safe than sorry.

My phone call to the repair shop reached a peculiarly nonchalant manager. He asked me to return the Mac so he could examine it and make any needed repairs. He declined my offer to send him the screen shot of the download log.

After consulting friends and colleagues, I decided to call the police instead. I had read about criminals hacking into wireless networks of stores and other businesses to steal credit-card numbers. If my computer had been used to commit a similar crime, perhaps this was exactly the break the police were looking for.

Not the Keystone Kops

So I phoned the police department located in the same city as the repair shop. Frankly, I wasn't expecting much help. To my surprise, I immediately reached a police detective on the fraud squad who was very knowledgeable about computer crime and interested in my story. He asked me all the right questions. He agreed with my concerns. He requested an email summary of the incident (including the screen shot), asked me not to delete anything on the hard drive, and explained that he would quietly investigate the matter.

Downloading hacker tools isn't a crime, he told me, unless they're used for a criminal purpose. I already knew that. But discovering that these programs had been downloaded onto my computer was like finding evidence that burglary tools had been stored in the trunk of a car left at a repair garage. Definitely suspicious.

The police investigation took a few weeks. Meanwhile, I didn't return the Mac to the shop or use it for anything.

When I talked again with the detective, he said the results of his investigation were inconclusive. He couldn't be certain my computer hadn't been used for wrongdoing, but he found no evidence of same. He advised me to return the computer to the shop, request an explanation, and settle the matter as I saw fit. He asked me to report any additional

information I might learn and let him know when the matter was resolved to my satisfaction. Afterward, he and his partner on the fraud squad planned to invite the shop manager for a cup of coffee and explain the importance of supervising employees more carefully.

Restoring a Clean Machine

When I returned my Mac to the repair shop, the formerly nonchalant manager was now very apologetic. He said he had conducted his own investigation and found the culprit. The repair tech who had worked on my machine admitted to downloading the hacker tools, claiming he was merely learning to use the Unix Terminal program, which is part of the command-line shell beneath Mac OS X.

That's a lame excuse, I said. Why download those particular files, instead of something more benevolent? And why would programs downloaded with Terminal appear in the Safari log? The manager shrugged and said it was the employee's only explanation. He added that the guilty party had been suspended. (Apparently, though, not fired.)

The manager offered to completely wipe the hard drive and do a clean install of the system software for me. Thanks, I said, but under the circumstances, I'd rather do it myself. We worked out a deal. The manager gave me some tips for securely wiping the drive and handed me a sealed copy of "Leopard," the latest version of Mac OS X (retail value $129). I went home and spent several hours wiping the drive, reinstalling the software, and downloading all the latest patches and updates from the Apple website. Finally, the machine was trustworthy again.

(Incidentally, I'm not naming the repair shop for several reasons. It's not relevant to people outside Silicon Valley; the transgression was probably the work of a rogue employee; I think the manager dealt with me honestly, and our settlement was more or less satisfactory; and the police visit should be sufficient to impress the shop with the gravity of the matter.)

A few lessons can be drawn from my experience. First, not all security threats sneak into a victim's computer over the Internet. We're so bombarded with warnings about anonymous attacks from afar that it's easy to overlook the potential threats closer to home. Consider the physical security of a personal computer—whether it's a desktop PC, laptop PC, mobile phone, or other device. Can everyone who handles it be trusted?

Second, think about the safety of your personal information. Consider storing important data on an external drive, on a removable memory card, in an encrypted file, or somewhere in the network cloud. All these alternatives have drawbacks, but they can protect valuable data if the computer is lost, stolen, or ransacked.

Finally, think about the millions of ordinary users who wouldn't notice a few odd files listed in a download log or realize the danger of using a computer whose security has been compromised. Consider the rapidly growing numbers of personal computers in various incarnations those people are accumulating. When designers treat security as an afterthought, users must think ahead.