

# Staying Safely Connected: The Challenges of Securing Endpoint Devices

By Zvi Gutterman

## Introduction

Endpoint devices are everywhere and create a high-productivity environment. Laptops have become a priceless<sup>1</sup> working tool, making the world your office. From the moment your flight touches the ground and during your cab ride, you can download and answer emails on your smart phone. You can navigate as you drive with your PDA featuring an internal GPS while making a VoIP call from your handheld device; and this is just the beginning!

While enhancing productivity, a CSO's task is also to keep these devices and the enterprise data secure. PCs must remain protected from new attacks, data leakage must be prevented, and the enterprise security policy must be enforced. Mobility demands that security enforcement is conducted even while the end device is far away and disconnected from the office LAN.

Security, and endpoint security specifically, has a myriad of different requirements and solutions. Anti-virus and personal firewalls appear to be the main tools in use today for protecting PCs and other endpoint devices.

The anti-virus's unit of protection is the file. Viruses are identified when new files are created or when a program tries to change another file in a malicious way. At this stage the anti-virus program halts the file operation and quarantines or deletes the malicious code. In recent years, when viruses and Trojans spread mainly through e-mail attachments, anti-virus software also evolved to scan emails. Yet, the logic is similar to file scanning.

While viruses and anti-viruses have been in existence since the early 1980s, personal firewalls flourished during the late 1990s following the Internet boom. A personal firewall protects each individual endpoint from TCP/IP attacks and defines the access level of each program to the Internet. A personal firewall blocks network intrusions as well as propagation of worms and Trojans.

The emergence of communication protocols presents many new potential security threats, which neither Anti-Virus nor Personal Firewalls address well enough. These protocols include both wired protocols such as USB and Firewire (IEEE 1394), but the more frightening protocols are the wireless ones such as IrDA and Bluetooth. Additional emerging standards such as WUSB present even more potential vulnerabilities.

Recent incidents presented here will exhibit how evolving technology can leave enterprise networks exposed. Solutions for addressing these new security challenges will be presented, specifically stressing the protocol analysis approach utilized by Safend, followed by future direction predictions.

## Understanding the Threat

Security vulnerabilities range from simple policy evasion to buffer overflows or identifiable protocol holes. No one wants to be a victim. Thus, few

cases of endpoint exploitation have been published. The following two published incidents are offered as examples.

Historically, it has been common for an employee to keep a list of business contacts when changing jobs. Today, many employees keep their email files and contacts using Disk-On-Key and other similar storage devices. In March 2005 one such incident was reported when a former Jacada employee downloaded thousands of files just prior to exiting his position. A similar publicized occurrence took place in Columbia bank in September 2005.

In Haifa, Israel, the Postal bank was robbed when a wireless card was plugged into one of the machines, actually creating an additional Wi-Fi network. The hacked computer was used as a bridge to the bank's internal network.

Information was stolen from Sumitomo bank in London using a USB hardware key logger that was connected between the USB port and various USB keyboards. The amazing fact is that one can buy one of these devices for less than \$150 and record a year's worth of keystrokes from a typical PC.<sup>2</sup>

Abe Usher in his blog Sharp-Ideas<sup>3</sup> was the first to coin the term "iPod slurping" to describe the process of using an iPod to download data. The process entails running a program on an iPod which enables the device to extract megabytes of data from a PC. This can be done in seconds over the Firewire or USB with no evidence left on the PC.

At BlackHat 2005, Barrall and Dewey<sup>4</sup> demonstrated a buffer overflow for Windows USB stack which would enable an adversary to gain full control over the Windows machine. It is interesting to note that, at this writing, no Windows patch has been released for this vulnerability<sup>5</sup> and unless you are using specialized protection, you are exposed to similar attacks.

Events similar to the ones described have pushed research groups such as Gartner to warn clients against such potential threats and encourage companies to implement appropriate security measures for their physical ports, wireless channels and removable storage devices.<sup>6</sup>

## Solutions

The most secure<sup>7</sup> way to stop invasions via your physical and wireless ports is to disable the hardware. However, it is not possible to buy a PC today without USB ports, nor is it easy to find a laptop without a wireless adaptor. I met a security officer of one of the largest banks on the east coast who claimed that they are not using any wireless networks in the bank. I asked him if they bought any new laptops within the two years and of course the answer was yes. Since it was an Intel Centrino laptop it had a Wi-Fi adapter, and hence this laptop was able to connect to insecure wireless networks.

Physical ports can be disabled with glue, but such a tactic is hardly practical. What about USB printers? Scanners? PDA Synchronization? Backup tapes? Other peripherals?

Plus, will the seal hold for the next three years? The other answer is disabling USB, which can be difficult to reverse. In addition, even if it is disabled, it may still be impossible to hardware disable your Wi-Fi embedded chip inside a laptop.

Another option is to use the Operating System security controls. In Windows, these are the different registry attributes you can set. Using registry attributes has three main disadvantages, beginning with granularity. Windows includes very limited granularity over these protocols. For example, setting a policy where Bluetooth printers are enabled while allowing Bluetooth phone synchronization is simply not a possibility within the registry flags. A second issue is anti-tampering. Windows is lacking a strong protection between admin tasks. Any system process which gets admin right can actually change these registry values. A third issue is the fact that you probably also want security from bugs or a security hole in the operating system but attempting this within the operating system is not very efficient.

Some common questions are: "What will Microsoft do? Aren't they about to solve all the security issues in the coming months? Isn't Windows Vista ("Longhorn") about to solve all our security issues?"

Well, in short—no. Why? Because security is a very complex issue and when presented with an operating system with more than 50 million lines of code, the security mission is immensely difficult. A complete change of focus is necessary to even begin. Progress is being made, but no significant changes are expected in the coming years. Expect to see continued exposure of vulnerabilities on a regular basis. release.

A third option to control endpoint security vulnerabilities is through the protocols stack. The USB disk-on-key stack of device drivers within Windows, which is presented in Figure 1, can be used as an example. Similar stacks of protocols and device drivers exist for each application and protocol used.

The Figure illustrates how disk-on-key actually operates. While an application (e.g., a word processor) is writing data to a file on a storage device, each layer handles a few elements of data, performing buffering, data correction, segmentations and finely passing the datagram to the layer below until the data safely arrives at the hardware layer.

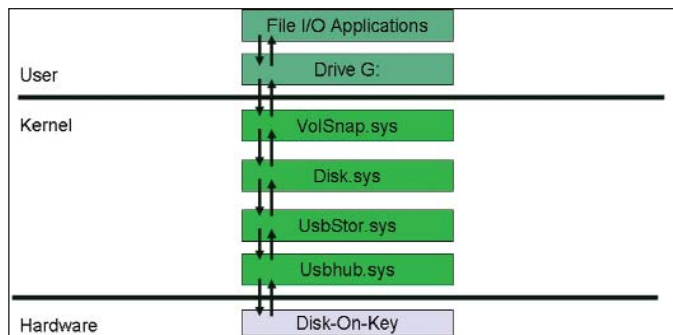
A similar flow works in reverse, transferring USB packets from the hardware token into the operating systems. Each level is handling a few actions and builds the right data representation to the layer above.

Security holes can occur in each layer of the protocols stack. A buffer overflow (like the one found by Barrall and Dewey) can take place in each of the four device drivers inside the kernel. Protocol violation can also be present at any of these stages and a hacker will seek the point where the least enforcement exists.

Using the protocol diagram in Figure 1, one can develop a security scheme which is an application-level filter controlling all application access to the lower level. This will stop invasions in the higher protocol levels but not ones which are targeted on the lower ones.

The strongest solution is to reside as low as possible such as just above the *USBHub.sys* device driver and handle all its traffic. Set the policy rules at this level and avoid any unauthorized files coming to the PC or those attempting to violate outgoing traffic rules.

It is not an easy task to implement such a deep protocol analysis solution, but this is the right way to control security. Such a design (developed by Safend) was presented at BlackHat 2005 as the only solution to prevent the zero day attack presented at the conference.



**Figure 1: Disk-On-Key device driver protocol stack in Windows 2K/XP/2003**

## Summary and Future Directions


Here, the importance of securing endpoint communication channels—USB, Firewire, serial, parallel, PCMCIA, IrDA, Bluetooth and storage devices such as DVD-RW, Backup Tapes, Disk-On-Keys, has been described

Hardware developers are taking the endpoint security challenge seriously and many new protocols are arriving next year. Ultra Wide Band (UWB) presents a great layer for moving wired protocols into wireless ones in short ranges. Next year printers will be seen working in Wireless USB (WUSB)<sup>9</sup> and the Wireless Firewire<sup>10</sup> standard is not far behind. Watch also for WiMax<sup>11</sup> which will provide broadband options for rural areas.

All these new standards present serious security issues such as those already described. New standards are always the Achilles' heel for IT professionals. It is not an easy task to write a new standard and make it secure in the first release (the move from WEP to WPA and lastly WPA2 is a great example).

The solutions alternatives discussed, from hardware glue to deep protocol inspection, have been around for the last decade. In the firewalls world, the state full packet inspection became the de facto standard for protection through deep TCP/IP protocol analysis. The seven-layer analysis and protection for the communication channel should be the new standard. Any other path is weak and can be easily bypassed.

It is important to note that while most of today's publicized security breaches (and devices), use Microsoft Windows, the same rules hold true for other operating systems from Linux, to Symbian, PalmOS and Windows Mobile.

While it is probable that most IT managers already have some kind of policy for some of the issues raised here, removable communications and storage devices will continue to pose security challenges as technology advances. Security professionals must constantly update their abilities to understand the risks, study the different solutions available and implement appropriate strategies. 

---

*Zvi Gutterman is CTO and co-founder of Safend, a leading endpoint security firm headquartered in Israel and with offices in Philadelphia.*

<sup>1</sup> Actually this May was the first month where the number of Laptop sales exceeded desktops.

<sup>2</sup> <http://www.keyghost.com/>

<sup>3</sup> [http://www.sharp-ideas.net/archives/2005/06/pod\\_slurping.html](http://www.sharp-ideas.net/archives/2005/06/pod_slurping.html)

<sup>4</sup> [http://www.blackhat.com/presentations/bh-usa-05/BH\\_US\\_05-Barrall-Dewey.pdf](http://www.blackhat.com/presentations/bh-usa-05/BH_US_05-Barrall-Dewey.pdf)

<sup>5</sup> <http://www.eweek.com/article2/0,1759,1840131,00.asp>

<sup>6</sup> <http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2005-2388>

<sup>7</sup> Gartner Research Advisories:

Ruggero Contu & John Girard: "Put Security Policies in Place for Portable Storage Devices"

Ruggero Contu: "How to Tackle the Threat From Portable Storage Devices"

<sup>8</sup> Only not using a computer can be more secure ...

<sup>9</sup> <http://www.usb.org/developers/wusb/>

<sup>10</sup> <http://www.1394ta.org/>

<sup>11</sup> <http://www.wimaxforum.org/home>