Global Information Assurance Certification Paper

Universal Serial Bus: Friend or Foe?
Mark Alabastro
02 August 2004

ABSTRACT: Does the availability of Universal Serial Bus (USB) ports on today's computers, in addition to the necessary operating system support, make this component a friend or foe to security? In the home environment, a computer's USB port is great for attaching a digital music player capable of holding 20 gigabytes (GBs) of music. However, the use of the same USB digital music player poses a potential security risk when attached to the USB port of an office computer, especially one containing sensitive files. In the office environment, that USB port is the physical connector for an authentication token, but in the home that same authentication token is useless when attached to a computer used by a child to type a school report. This paper examines both the security benefits and risks of USB devices, but will focus more intensively on the risks. However, before discussing the benefits and risks, summary information will be provided on the USB specification and a survey of the types of commercially available products will be presented. This paper will conclude by discussing methods for securing USB ports on today's computer systems from the risks introduced by storage and networking devices.

Summary of USB

In 1995, the Universal Serial Bus (USB) specification was developed jointly by Intel, Compaq, Microsoft, and NEC, with the overall goal being to provide an easy-to-use and inexpensive means to connect peripheral devices to a host computer. Intended to replace the various serial and parallel port connectors, one of the goals was to define a standard set of connectors and cables that would allow bi-directional communication between peripheral devices and the host computer.

Another goal of the specification was "plug-and-play," which would allow for the connecting and disconnecting of peripheral devices to the host computer without powering down. Additionally, the USB specification required the ability to distribute power to any peripheral device on a connection that could host up to 127 devices at once.

These goals formed the USB Revision 1.1 specification[1] that was implemented with devices with a throughput of 12 Mb/s for "full speed" devices and a throughput of 1.5 Mb/s for "low speed" devices, such as keyboards and mice. USB Revision 2.0 specified support for 480 Mb/s transfer rates while being backwards compatible with USB Revision 1.1.[2]

As a result, computer manufacturers have incorporated USB ports into their product lines, and some have started to remove legacy connections. However, a majority of computer manufacturers still offer legacy connections, such as serial, parallel, and PS/2 ports, along side USB ports.

The peripheral market has responded by offering devices such as USB keyboards, mice, printers, floppy drives, among others. Thus, it has become increasingly difficult to find a device with legacy connectors on the market today.

Survey of Commercially Available Products
The USB peripheral market can be segmented into hubs, human interface devices, output devices, storage devices, and networking equipment. Many vendors offer their products in various form factors, from key-sized devices to full-sized devices like computer hard drives.

Hubs are devices that allow the daisy chaining of peripheral devices to achieve the “127 devices at once” goal. Early adopters of USB provided only two USB ports on their products, while more recent products provide at least two USB ports.

Human Interface Devices (HIDs) include keyboards, mice, joysticks, game pads, digital cameras, card readers, authentication tokens, cryptographic modules, and optical scanners. Printers and speakers are categorized as output devices.

Storage devices cover a wide range of products, such as floppy drives, hard drives, digital music players, and CD/DVD reader-writers. More recent storage devices like flash drives can store anywhere from 16 megabytes (MBs) to one GB in the form-factor of a key fob or watch. Some digital music players not only store music, but can also function as hard drives.

Networking adapters provide Ethernet, Wireless Fidelity (WiFi), and Bluetooth connectivity. These adapters provide additional connectivity via any available USB port on a host computer or hub, in addition to the built-in network connector (usually Ethernet).

All these various devices connect to a host computer through a standardized connector that can provide power and high throughput. This was not the case prior to USB ports being available on a computer system: printers were connected via a parallel port, and sometimes a specific printer needed a bi-directional printer connection; keyboards and mice connected specifically to a serial connector or a PS/2 connector; and modems connected to a serial connector. In short, if someone wanted to plug a device to a host computer that did not have a USB port, a peripheral device’s specific port had to be present on the host computer. Sometimes a type of port, like a parallel port, had to support additional capabilities, such as bi-directional communications, in order for a specific device to work.

Security Benefits and Risks
With numerous vendors developing USB devices, each type of device brings about a security benefit or risk. In some cases, it can be both a benefit and risk,

depending on the use. HIDs and storage devices are the primary focus of this section's discussion, but networking equipment will be an additional focus when discussed in the section concerning the risks of USB devices.

Security Benefits – HIDs
Some of today's HIDs provide authentication and/or authorization capabilities. These USB devices are in the form of a USB token and provide the ability for two-factor authentication (something you know and something you have). In this scenario, the user knows a PIN that is stored in an encrypted format on something he/she has, namely a USB authentication token. The authentication process to access a host computer begins with the user attaching his/her USB token to the host computer. Secondly, the user must enter the appropriate PIN in order for the authentication process to proceed. Third, the host computer compares the entered PIN with the data securely stored in the USB token. Unfortunately, the above scenario is not that straightforward. This is because behind the scenes an infrastructure is deployed to every host computer on the corporate network.

Examples of such products are Entrust USB Tokens, RSA SecureID 6100 USB Tokens, Rainbow Technologies iKey USB Authentication Tokens, and Griffin Technologies' SecuriKey.

Entrust USB Tokens[3] require a software component that is installed on a host computer that provides two-factor authentication capabilities. When deployed with the Entrust Secure Data Solution authorization capabilities are additionally provided.[4] As a result, access to information (files) and resources (applications, web servers, databases, etc.) are controlled.

RSA SecureID 6100 USB Tokens[5] provide two-factor authentication similar to the Entrust USB Tokens. And like Entrust, RSA's solution requires the needed infrastructure to perform the necessary authentication functions. Rainbow Technologies' iKey[6] provides two-factor authentication. When used with additional infrastructure resources, it provides authorization to additional computing resources, like web applications, that are beyond the user's desktop.

Griffin Technologies' SecuriKey takes a different approach to two-factor authentication. Unlike the Entrust, RSA, and Rainbow Technologies' solutions, which require a user to provide "something you know," SecuriKey takes a different approach by having "something known" be something that is already part of the corporate infrastructure, like Windows Active Directory.[7] The "something you have" acts like an "ignition key" to use the host computer.

Overall, HIDs that perform authentication and/or authorization rely on some underlying infrastructure, whether it already exists as part of the corporate infrastructure or is a separate component that needs to be added.

Security Benefits – Storage
The main goal of USB storage devices is availability to data. USB storage devices take many form factors, from something small enough to fit on a key ring to a full-sized hard drive and CD/DVD reader-writer with a USB connector. These devices provide for the backup of large files that do not fit on three-and-half inch floppy diskettes.

USB storage devices that are small enough to fit on a key ring range in size from 16 MB (today's market makes it difficult to find something smaller than 64 MB) to one GB. These devices require no additional software or power connections, as power is drawn from the USB port (see Summary of USB).

Some USB storage devices provide the additional functionality of authorized access to the data stored on a USB storage device through password protection. Since authorization is not part of the USB specification, password protecting a USB storage device is achieved by additional software installed on a host computer.

Something along the lines of a hard drive can store one terabyte of data, like LaCie's USB 2.0/FireWire 800 Bigger Disk.[8] No additional software is required, since the operating system provides built-in support.

A CD/DVD reader-writer, while not capable of storing as much as up to a terabyte of data, still allows the user to copy large files to removable media that can be secured in an off-site storage facility. If the operating system does not support burning capabilities, additional software is required in order to burn a CD or DVD.

Most of the USB storage devices are already supported by the operating system and do not require any additional software installations. Some USB storage devices provide additional functionality requiring the installation of additional software. This requires the proper administrative privileges to perform, and a desktop user does not have the privilege to install new software.

Security Benefits Summary
Some of today's USB products provide functionality that allows us to achieve the goals of authentication, authorization, and availability. These products require the user to provide something known when accessing a computer system. Some of these products even provide access control to computing resources. A user's data is kept safe by making it available on another medium that is separate from his/her desktop computer.

Some products require no additional software because the operating system provides support for the USB specification. For those products that provide additional functionality beyond the USB specification, additional software needs to be installed by someone with the appropriate administrator privileges.

Security Risks – HIDs and Storage
Certain USB products are security risks because of their ability to provide unauthorized access. These devices can be small enough to fit in a pocket and often draw power from the USB port. In addition, with USB 2.0, high-bandwidth devices can be attached that allow for the quick transfer of large data files or the streaming of real-time data. Video conferencing cameras are a type of HID that pose a security risk. USB storage devices with various form factors also allow for the unauthorized movement of information to outside a security perimeter.

Video conferencing cameras potentially allow for the unauthorized transfer of audio and video to an external party. Depending on the design, some video conferencing cameras provide no indication that they are on. Other designs have no lens cap to prevent the inadvertent capture of images. Usually having a small form factor, these devices can be carried into an environment and installed. If the operating system has built-in video conferencing software, a user can eavesdrop on closed-door conversations easily without installing extra software.

Storage devices are the more common security risk because of the numerous products available, the various capacities, and the various form factors they can take. These devices can be used to allow for the unauthorized transfer of data outside a security perimeter. USB storage devices that fit on a key chain or in the form factor of a watch, such as LaCie's Data Watch[9], can be carried in and out of an area undetected. Today's small form factor devices are limited to carrying one GB of data. The unauthorized transfer of larger data sets beyond one GB usually requires a hard drive or a CD/DVD reader-writer. As noted earlier, a CD/DVD reader-writer, unless there is native support by the operating system, requires additional software. Hard drives require no additional software, as these are readily recognized by the operating system per the USB specification. An individual carrying a hard drive into a secure area would be noticed, but an individual with a digital music player probably would not.

Digital music players, along with shrinking hard drive technologies, have become a security risk. For example, Apple Computer's iPod (as of July 2004) has a maximum storage capacity of 40 GB contained within a shell measuring a 4.1 by 2.4 by 0.69 inches (a "deck of cards" form factor); the iPod Mini has a capacity of four GB in a 3.6 by 2.0 by 0.5 inches, a "credit card" form factor.[10] According to a July 13, 2004 Reuters report by Warner, these devices have been recognized as a security risk by the British military.[11] Therefore, one terabyte of storage is appropriate for legitimate backups, but four GB could be more than enough to copy all information pertaining to a particular business area.

Video conferencing cameras and USB storage devices (in their various form factors) are security risks in terms of unauthorized access to information. Once copied and carried out of a secure area, the organization is at a risk. However,

inspection of personal items might not be the solution, given the annoyance it might cause employees or the possible legal ramifications.

Security Risks – Network Adapters
It is possible that carrying information out of an area might not be ideal for an adversary because of established security checkpoints. USB-based network adapters are another type of device that can be used to gain unauthorized access to information. As presented by Ziller at the May 2000 USB.org conference, network adapters (communication) accounted for 19% of the tested products at USB.org's March 2000 compliance workshop; HIDs accounted for 23%, and storage devices accounted for 17%.[12]

USB networking equipment can support Ethernet, Wireless Fidelity (WiFi), and Bluetooth. An Ethernet adapter's form factor does not come in the size of a token, whereas some WiFi and Bluetooth adapters do come in a token form factor.

WiFi USB adapters are more predominant in the consumer market. However, only a small number of manufacturers, like Belkin[13] and D-Link[14], have a Bluetooth USB adapter.

Ethernet adapters won't be discussed here, since these require a physical medium to transmit (usually the corporate network). Instead, the focus will be on WiFi and Bluetooth adapters.

Network Adapters – Background
WiFi, in particular the 802.11b implementation, is predominant in the consumer market because of the low cost and its proliferation in coffee houses and airports, to name a few. What makes this technology appealing is that by attaching it to an access point, which is connected to the Internet or Intranet, consumers have ubiquitous availability. Ratified in 1999, updates to the 802.11 Standards have resulted in higher data rates as summarized by Melby (see **Table 1: Comparison of 802.11 Standards**).

Table 1: Comparison of 802.11 Standards

	802.11	802.11b	802.11a	802.11g
Frequency Spectrum	2.4 GHz	2.4 GHz	5 GHz	2.4 GHz
Max Data Rate	~2 Mbps	~11 Mbps	~54 Mbps	~54 Mbps
Range	50-100 m	50-100 m	50 m	50 m
Modulation	FHSS/DSSS	DSSS	DSSS	DSSS

Source: Melby. March 2002. LoopStart Consulting Group, Inc.[15]

In addition to its ability to connect to an access point, the 802.11 Standards allows for the creation of ad-hoc, peer-to-peer networks in which WiFi-enabled computers communicate with each other without an access point.

As summarized in a white paper by Melby, Bluetooth's range, unlike WiFi's, is limited to 10 meters. Like WiFi, Bluetooth operates at the unregulated frequency spectrum of 2.4 GHz at a rate of 720 Kb/s. Bluetooth can operate as a voice/data access point when a Bluetooth-enabled computer connects to a Bluetooth-enabled cellular phone. Thus, the cellular phone becomes an access point to the Internet. Bluetooth can also operate as a peripheral interconnect that merely provides computer peripheral connectivity without wires. Lastly, Bluetooth can operate as a Personal Area Network that allows for the creation of ad-hoc networks.[16]

Network Adapters – The Threat
With either technology (WiFi and Bluetooth), the security risks are the ability to create ad-hoc networks and for Bluetooth to operate as a voice/data access point. The ability to create ad-hoc networks allows for the creation of an unauthorized network connection that is outside the security perimeter of the corporate network.

With the range and throughput provided by WiFi, data can be copied, without notifying any of the network security measures in place, from an internal computer system to another computer system that could be located in an adjacent parking lot. In a simplified scenario, by inserting a WiFi USB adapter to a host computer and creating an ad-hoc network (peer-to-peer) with an external computer, an adversary can take critical information without carrying it past a security checkpoint.

Although it has a smaller range, Bluetooth technology allows for the same scenario. Rather than having an external computer located outside a given area, a cellular phone is used instead. Inserting a Bluetooth USB adapter to a host computer and creating an ad-hoc network with a cellular phone that an individual has carried into the office allows for the unauthorized transfer of data to a remote computer. By creating an ad-hoc network, data can also be transferred without authorization to a Bluetooth-enabled hand-held computer, which can then be easily carried out of the office.

Security Risks Summary
USB video conferencing cameras can provide unauthorized access to closed door conversations, but require more resources if the operating system does not have built-in video conferencing software. The higher risk devices identified in this paper are storage and networking, especially those devices that pass through a security checkpoint undetected because of their small form factors.

As USB storage devices provide availability to data, these same devices can provide availability to unauthorized parties. Some USB storage devices can be passed through a security perimeter undetected, but still require an individual to physically carry something.

Wireless networking devices only require an adversary to carry them into a security perimeter while the unauthorized recipient of the data is located elsewhere. With high transmission speeds, information can be copied without setting off any security alarms.

Securing the System
Securing all the desktops in an office environment can be a daunting task. How does one implement non-disruptive countermeasures? General solutions are provided, from software to Basic Input-Output System (BIOS) implementations.

Software
A software solution is one that is integrated with the operating system. Common among software-based solutions is the ability to provide user-based access control to the USB ports. Software-based solutions are deployed to every host computer in the corporate network and are centrally managed.

Enterprise software-based solutions integrate with a central user database, like Active Directory or Domain Controller. These software-based solutions then authorize user access to hardware components in real-time. This is particularly useful when host computers are shared among employees.

Some software-based solutions allow for the selective use of devices based on type. For example, the USB ports on a host computer could allow a USB keyboard and mouse to operate, but will deny access to those ports when a USB storage device is connected.

Additional features of software-based solutions are time of day and/or day of week access to the USB ports. This makes it possible for the USB ports to be available on an individual's host computer during core hours, and disabled afterwards when the cleaning staff makes the rounds. This does not allow for the ad-hoc access of a legitimate user after hours without any coordination with the Information Systems (IS) team.

A software-based solution allows for the use of a host computer's USB ports based on individuals or groups. For example, such measures would allow the marketing department staff to connect digital cameras to their desktops, but the administrative assistants in the engineering, legal, and human resource departments would not be permitted to do the same. Software-based solutions serve as an authorization, not an authentication, mechanism. Such solutions also serve as a second or third line of defense. Examples of software-based solutions for Microsoft Windows are SmartLine's DeviceLock[17] and Pixel Production's SecureNT.[18]

BIOS Settings
Disabling the USB ports on a computer by the BIOS is the most effective and simple solution. But do not forget to password protect the BIOS and lock the case

to prevent anyone from resetting the CMOS memory by removing the battery. As new hardware arrives, it needs to be configured for the deployed environment, so take the extra step to disable all USB ports. However, the assumption is made that the system has legacy ports for the keyboard and mouse. Despite the initial idea that USB ports will replace legacy ports, the PS/2 keyboard and mouse connector do have legitimate reasons to maintain on current hardware.

Modifying the BIOS to not allow additional devices to boot the system resolves the issue of anyone bypassing any installed software countermeasures. Additionally, this removes the possibility of any software countermeasure from being tampered with.

This is certainly an all-or-nothing solution. However, there is no need to access to the USB ports on a desktop system for the daily usage of e-mail, word processors, spreadsheets, and presentations.

In addition to computer systems deployed through the corporate network, disabling the USB ports via the BIOS settings is highly appropriate for a server. Usually found in a compute center, there is a low probability that a USB device would be appropriately attached to a server. Usually, the USB ports are located in the back, where access is difficult. However, some manufacturers have made a single USB port in the front of the machine available, where an attached device could be accidentally pulled off.

If a USB device were plugged into a server, it would most likely be a hardware-based, software-license key. In this instance, it would be appropriate to get the licensing mechanism migrated from a hardware implementation to a software implementation. If migrating away from a hardware implementation is not available from the software vendor, then installing a software-based solution with specific access to a hardware token is required.

Conclusion

USB devices, especially those that provide authentication, authorization, and availability of data, assist in securing the corporate network. However, do the benefits outweigh the risks? If the risks outweigh the benefits, then it might be better to not even introduce USB technology into the corporate network.

However, computer manufacturers dictate the core feature set for consumers. Therefore, avoiding USB technology in this environment is not an option. Thus, we are left with the task of securing every USB port on every desktop and server in the corporate network.

If USB technology were prohibited in the environment, then disabling the USB ports on each host computer would be appropriate. However, if USB technology is needed, then a software-based solution is called for because the majority of

the solutions authorize access to a USB port based on the user. But deploying a software-based solution could be cost or manpower prohibitive.

Unfortunately, “defense in-depth” for USB ports is not appropriate, since using a software-solution to provide authorized access to the ports is useless when the USB ports have been disabled in the BIOS. Assuming that organizations are segmented in the enterprise and if only a certain organization requires access to USB devices, then the problem space has gotten smaller. In such cases, a software-based solution could be affordable and would not be a burden on the IS team.

In rare instances, purchasing machines with only legacy ports would be an appropriate solution if it is not cost prohibitive. Since USB is prevalent in today’s deployments, the corporate security plan needs to explicitly address this technology in order to prevent unauthorized access to data.

References

[1] Compaq Computer Corporation, Intel Corporation, Microsoft Corporation, and NEC Corporation. Universal Serial Bus Specification. Revision 1.1 September 23, 1998 <http://www.usb.org/developers/docs>.
[2] Compaq Computer Corporation, Hewlett-Packard Company, Intel Corporation, Lucent Technologies Incorporated, Microsoft Corporation, NEC Corporation, and Koninklijke Philips Electronics N.V. Universal Serial Bus Specification. Revision 2.0 April 27, 2004 <http://www.usb.org/developers>.
[3] Entrust, Inc. “Entrust USB Solutions” <http://www.entrust.com/tokens/index.htm>.
[4] Entrust, Inc. “Entrust Secure Data Solution“ <http://www.entrust.com/data/index.htm>.
[5] RSA Security Inc. “RSA SecurID Authentication” <http://www.rsasecurity.com/node.asp?id=1156>.
[6] SafeNet, Inc. “iKey” <http://www.rainbow.com/products/ikey/index.asp>.
[7] Griffin Technologies, LLC. “SecuriKey” <http://www.securikey.com>.
[8] LaCie Limited. “LaCie Bigger Disk” <http://www.lacie.com/products/product.htm?id=10118>.
[9] LaCie Limited. “LaCie Data Watch” <http://www.lacie.com/products/product.htm?id=10128>.
[10] Apple Computer, Inc. “iPod and iPod mini Technical Specifications” <http://www.apple.com/ipod/specs.html>.
[11] Warner, Bernard. “British Military: iPods Pose Security Risk” Reuters 13 July 2004. 13 July 2004 <http://www.reuters.com/newsArticle.jhtml?type=technologyNews&storyID=5653399&section=news>.
[12] Ziller, Jason. “USB 2.0: An Evolution Underway” USB.org Conference 16 May 2000: 15.

[13] Belkin Corporation. “Bluetooth USB Adapter” <http://catalog.belkin.com/IWCatProductPage.process?Merchant_Id=&Section_Id=200583&pcount=&Product_Id=126336>.
[14] D-Link Corporation. “Wireless USB Bluetooth Adapter” <http://www.dlink.com/products/?pid=34>.
[15] Melby, Jason. “Wireless Local Area Network (WAN) White Paper” March 2002: 13. LoopStart Consulting Group, Inc. <http://www.loop-start.com/portfolio.html>.
[16] Melby, Jason. “Bluetooth White Paper” April 2002. LoopStart Consulting Group, Inc. <http://www.loop-start.com/portfolio.html>.
[17] SmartLine, Inc. “DeviceLock” <http://www.devicelock.com>.
[18] Pixel Productions Pty Ltd. “SecureNT Product Overview” <http://www.pixel.com.au/html/products/secure_nt/secure_nt.htm>.