GIAC
CERTIFICATIONS

Global Information Assurance Certification Paper

Copyright SANS Institute
Author Retains Full Rights

This paper is taken from the GIAC directory of certified professionals. Reposting is not permited without express written permission.

Interested in learning more?

Check out the list of upcoming events offering
"Security Essentials (Security 401)"
at http://www.giac.org/registration/gsec

USB – Ubiquitous Security Backdoor

GIAC (GSEC) Gold Certification

Author: Erik Couture, erikcouture@gmail.com
Advisor: Egan Hadsell

Accepted: August 25, 2009

Abstract

The Universal Serial Bus is an omnipresent data and peripheral communication port that poses a security threat in any modern computing environment. While there are many disparate guides and best-practices for their use in a secured computing environment, this paper will break down the issue into its base components and assist the reader in assessing his or her own organizational security needs. Proposed is a holistic approach to USB port-security, examining the problem from user requirements definition to organizational threat-risk assessment and finally technical and procedural-based risk mitigation.

© SANS Institute 2009, Author retains full rights.

1. Introduction

1.1. Aim

The Universal Serial Bus (USB) port is among the most prolific hardware computer ports in existence, with over 3 billion USB devices sold in 2008 (In-Stat, 2009). It provides the end-user a simple, universal connection conduit for a multitude of uses, eliminating much of the need for task or peripheral-specific ports of days gone by (parallel ports for printing, PS2 ports for mice and keyboards etc). It is this ubiquitousness, combined with a seemingly infinite number of uses that makes the port a concern to computer security experts. A port that can transfer data, provide power and allow connection of hardware peripherals, but also potentially pose a serious security vulnerability to personal and enterprise computing.

It is the aim of this paper to describe the possible threat, assess the implied risks in a given computing environment, and provide holistic mitigation strategies tailored to the user's requirements and risk tolerance.

1.2. Scope

While the USB specification is platform independent, this paper will focus primarily on USB port security in a typical Microsoft Windows network environment. USB v2.0-standard ports and devices will be assumed unless otherwise indicated.

2. Main

2.1. A Technical Introduction to the USB Port

The USB specification was originally designed by the USB Implementers Forum, an interest group which includes Compaq, Intel and Microsoft to address connectivity, ease of use and expandability issues (USB-IF, 2000). It was defined in 1994 and has since been revised several times, with a major upgrade in 2000 bringing the revision to v2.0. The latest updates have standardized higher data throughput rates (480Mb/s), while maintaining full backward compatibility with v1 standards. The USB v3.0 or 'SuperSpeed USB' standard was released in

© SANS Institute 2009, Author retains full rights.

2008, with additional performance increases (USB-IF, 2008), but has not been rolled out in great numbers by OEMs at the time of the publishing of this paper.

2.1.1. Electrical/Mechanical Specifications

USB v2.0 specifies several standard physical interfaces, which all provide robust connections for a broad range of external peripherals. Devices may be cascaded in series using hubs to a maximum of 127 devices, all which may operate concurrently. In addition to serial data, the USB specification provides for a 5V DC, 500mA power supply from which devices can draw power. This is a very notable feature, as few other standards provide power and data over a single port.

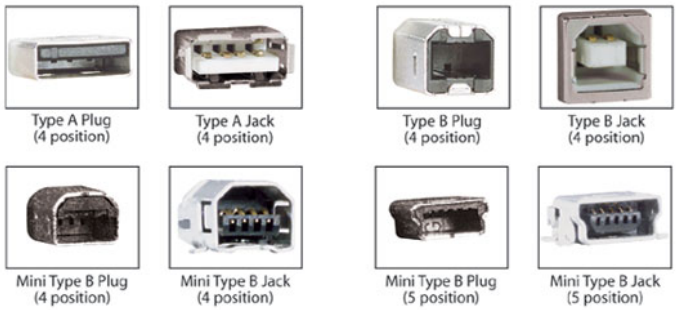


Figure 1 - USB Connector Types

2.1.2. Operating System Interaction

From a systems integration standpoint, the 'killer-app' of the USB standard is its ability to perform all the above tasks, while remaining hot-pluggable; insertable and removable while the system remains powered-up. This degree of plug-and-play provides tremendous advantage for a range of user applications, while foreshadowing the root of several of its security issues. When a USB device is connected to a system, it is enumerated by the host's bus and is assigned a unique address. The device presents itself as one of several Device Classes that include: Human Interface Devices (HID) such as a keyboard or mouse, printer, communications device or Mass Storage Class (MSC). It is the latter that is of greatest interest in terms of security implications. The MSC defines the way data storage devices, including flash drives, music players, and digital cameras shall communicate over the bus (USB-IF, 2003). While the precise low-level protocol

© SANS Institute 2009, Author retains full rights.

specifications are not critical to security, it is important to note that these device protocols are enabled at the core of the USB specification and, in keeping with backward compatibility requirements, will not likely be changed substantially in order to address security or other limitations.

2.2. User Requirements Definition

Before any security assessment takes place, user requirements must be captured and validated with organizational leadership. When acquiring USB requirements, the IT/security staff might find it useful to review ITIL Service Level Management or other standardized process for user requirements definition. The *Identification of Service Requirements* (Kempter, 2009) sub-process details best practices for gathering requirements in a large organization. Such requirements definition, however critical, is the same process carried out defining organizational needs for any other service, and thus will not be elaborated upon. At its simplest, users can be surveyed for their business-related requirements for USB devices and the resultant data set should be organized clearly and presented to senior management for vetting.

2.2.1. Typical business uses of USB

USB devices have many legitimate uses in the enterprise. Most common is the USB flash drive, which can easily transport data between computers within and outside the organization. Variations of the flash drive include external USB hard drives and memory card readers which all enable the same type of activity.

There are many devices on the market which are designed be connected to the USB port solely for its 5V DC power supply. Fans, vacuums and cup warmers are common and should also be identified and considered. Just because a device appears to be something as innocuous as a vacuum does not mean it cannot have internal data storage capabilities. Mobile phones and music players are contentious in the workplace as they are prolific and require frequent charging by USB port. These devices are clearly capable of carrying data onto and off of the network and the 'requirement' for their use in the workplace should be carefully assessed.

© SANS Institute 2009, Author retains full rights.

2.2.2. Defining User Requirements

The principal question to ask is: What are the valid business reasons to use USB devices? Users and managers need to come to an agreement on the minimum requirement for USB devices, primarily data storage devices, in order to fulfill business-driven processes. Annex A is a starting point to assist users and manager in validating their requirements. As with any business process which will likely later drive corporate IT policy, it is critical to get user and management buy-in at the ground floor. This will ensure full enumeration of business needs and enable security staff to conduct a comprehensive threat assessment.

2.3. Threat Vectors

USB devices pose a significant number of security challenges in the business environment. Many vulnerabilities may be exploited by several distinct groups: 1. Disgruntled workers, 2. Careless users, and 3. Malicious individuals. Exploitation by dissatisfied users is one of the most difficult threats to counter. Internal users have intimate knowledge of network resources while their physical right of entry and authenticated network privileges allow them access to critical business data. Imprudent users can unwittingly circumvent system defenses or be social engineered into installing malware. These users may lack the technical knowledge or security training to make smart security decisions, and inadvertently compromise the system. (Bowman, 2007) Malicious individuals are a definite threat, but due to USB access requiring physical access to the organization's IT infrastructure, this threat group is divided into two sub-groups; highly motivated and skilled social engineers, and criminals of opportunity.

For clarity, several USB-related vulnerabilities are organized below, grouped by core infosec principles (C.I.A).

2.3.1. Confidentiality

Data confidentiality is the most significant threat of USB devices in the corporate environment. A company's data; be it client personal information, future plans, financial data or intellectual property will form the electronic 'crown jewels' which should be the focus a multi-tiered network 'defense-in-depth'. While the spotlight is often on protecting data at rest or in transit within secured network segments or from external threats by the use of firewalls and

© SANS Institute 2009, Author retains full rights.

NIDS/NIPS, recent research has proven that user data loss comprises most data breaches (Ponemon, 2009). Whether maliciously or accidentally, vast quantities of data can be pulled off of internal systems via USB devices (and other means), completely circumventing network defenses.

Disgruntled users, particularly tech-savvy ones can cause massive damage to a corporation's data confidentiality. Their ability to pull key data from internal data stores and potentially understand how to cover their tracks can enable this small group to do a disproportionate amount of harm. Their motivation may be to sell the stolen data to competitors, blackmail the company or steal customers to their next employer.

Careless users are by far the most common source of confidentiality beaches. As the research data in the graphs below demonstrate, large numbers of users will admit to losing portable data devices (Fig 1), and the majority routinely copy sensitive data to data devices and admit to transferring it to non-enterprise systems (Fig 2). These statistics, while shocking, are in line with other similar surveys.

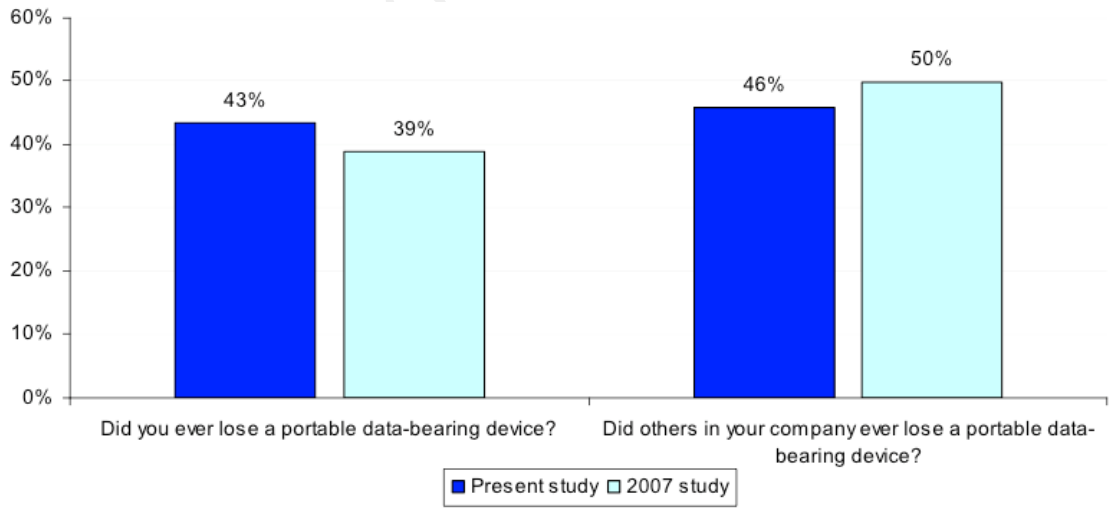


Figure 2 – Loss of Data Bearing device (Ponemon, 2009)

© SANS Institute 2009, Author retains full rights.

What is possibly most disturbing about the 'careless user' threat vector is that human nature and individual personality play a large part. The threat exists in any event, but it is the user's unwillingness to admit his or her error that magnifies the possible harm.

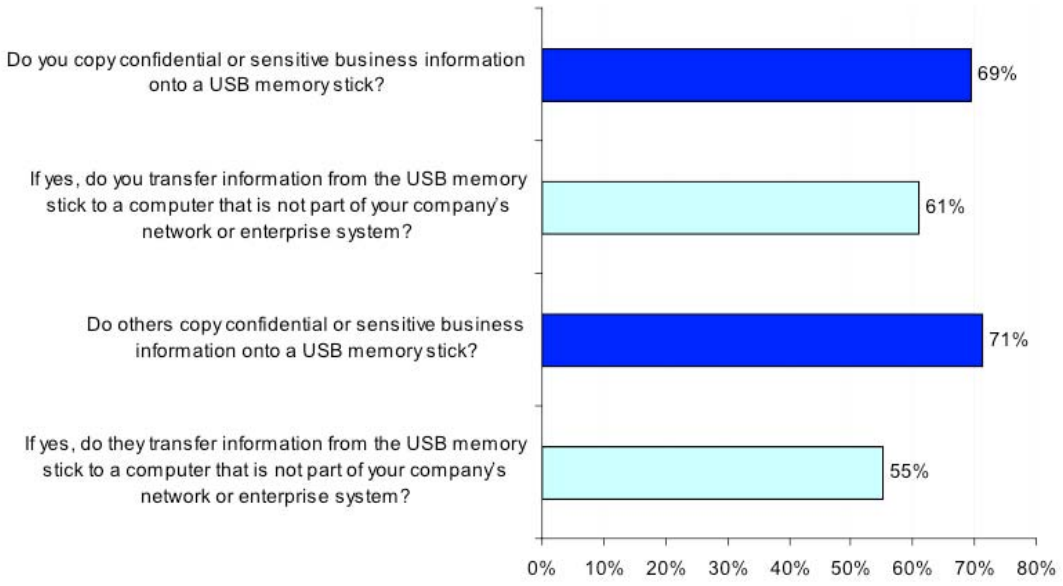


Figure 3 - Transferring confidential business data on insecure USB memory sticks (Ponemon, 2009)

Malicious individuals, external to organization, may use USB as an attack vector for a number of reasons. They may approach a semi-public workstation and covertly attach a custom USB device designed to 'suck' data from the local station or networked resource. Such software is freely available and easily installed on any USB flash drive. Googling "USB Switchblade" or "USB Hacksaw" gives examples of what is possible by anyone with even basic technical knowledge. Such a device can be created to look like a normal flash drive, or hidden within an innocuous looking device such as a mouse or other USB peripheral. Once connected, the device can autorun, installing itself and any other malware, copying system passwords and other critical data back to itself for later removal, or email them to an anonymous email address. While the Malicious threat is perhaps discouraged in certain scenarios due to the attacker having to put

© SANS Institute 2009, Author retains full rights.

himself at risk by physically entering the premises, a well planned distraction can allow the 5 seconds required to install the device. Alternatively, flash drives may be 'dropped' around the target premises with the hope that employees will find them and connect them to the network.

It has been demonstrated that the core USB protocol has serious security flaws that allows an attacker to design a device that can emulate a different USB Device Class. While masquerading as a 'read only' device like a keyboard, the malicious device can exploit the trust relationship it has with the OS and covertly retrieve or corrupt data. (Barrall & Dewey, 2005)

USB keyloggers are cheaply obtainable and undetectable to the untrained eye. Installing one on a semi-public computer such as in a hospital waiting room, store cash register or kiosk can be trivial, and can reveal user logins and passwords, in addition to personal and financial data. (Safend, 2007)

2.3.2. Availability

In most environments, the USB threat to system availability is somewhat lower then that of confidentiality. The most significant vector is the introduction of viruses/malware to the network through the connection of a device, circumventing network defenses. Malware can propagate through a corporate network, saturating network connections, email servers, and other network resources. Internal denial of service (DOS) attacks can be devastating to a layered defence focused solely on external threats. Depending on the industry and network segment affected, disruption of mission-critical services can have massive impacts. Control systems (SCADA) and other real-time services often have low tolerances to network resource exhaustion, with potential widespread impact. A high profile example of this occurred in 2006 when the Russian stock market (RTS) was taken down by internal DOS. (Stith, 2006)

Disgruntled or malicious users can potentially wreak havoc to system availability; a tech-savvy individual can introduce generic or custom malware into the environment via USB unleashing it immediately or at a later time.

2.3.3. Integrity

Data integrity is threatened when the introduction of a virus/malware deletes or makes changes to business data at rest on the secured network segment. Again, the introduction of this

© SANS Institute 2009, Author retains full rights.

type of malware by USB greatly increases the risk of its propagation if network defenses are focused on the external threat to internet/WAN border devices. Once a trojan/backdoor is introduced inside the network, an external hacker may have unrestricted access to internal resources, making changes to client accounts or defacing documents or websites. An inserted device may also contain code that may clandestinely make changes to data on the system, or perform an internal DOS or website defacement.

2.4. Organizational Risks

The 'risk' portion of a threat-risk assessment is often one of the most challenging to complete. Just what is the risk of a specified threat vector to a particular enterprise? Risk assessment can be very subjective, and even when thoroughly completed, is still subject to executive review, where organizational risk tolerance levels will dictate the appropriate countermeasures.

The risk of data breach to an organization is a combination of the value it places on its data, or conversely the cost of the loss of its data, multiplied by the possibility that this breach could occur. The possibility of a breach must be carefully assessed and initially, it is typical, although irrational, to hold a "it can't happen to me" attitude. Annex B has been included as a template to help identify the level and likelihood of various threats. Many recent examples of high-profile data breaches via USB devices highlight that it can in fact happen to any organization, and that when it does, the damage can be extensive; financially, legally, to corporate image and to personal and public safety. Additionally, recently introduced business regulations in the U.S (HIPAA, SOX, PCI) make compliance to data loss prevention mandatory,

A recent U.S Cost of Data Breach survey revealed that at $202 US per compromised record, the cost of a breach has risen by 40% since 2005. More the 88% of the incidents involved insider negligence. (Greiner, 2009) The high profile news stories abound: "60% of data breaches can be attributed to lost or stolen mobile devices", "Professor's lost flash drive contained 16,000 Social Security numbers", "Stolen flash drive affects more than 7,000", "Air Force Officer loses USB stick with Afghan mission data" (Centennial, 2008).

© SANS Institute 2009, Author retains full rights.

These examples all point to a rise in incidents of major data loss in corporations and government departments. It can, and will, happen to you.

2.5. Risk Mitigation Strategies

Faced with a comprehensive threat-risk assessment outlining the substantial costs associated with data loss or compromise to integrity, senior executives may be tempted to say, "Just shut all USB ports down and eliminate the problem". In certain environments this strategy may be part of the solution, but security experts are generally focused on risk mitigation; finding the right mix of creative technological solutions, user education, and meaningful, enforceable policy to *enable* business operations (Usher, 2006).

2.5.1. Technological Risk Mitigation

There are a number of technological options which may used individually or as part of a holistic risk-mitigation plan:

- Physical ports may be glued shut, making them inoperable
- Disable USB ports in BIOS
- Prevent installation of USB device drivers by denying permission on the files usbstor.pnf and usbstor.inf, located at %systemroot%\inf. Thus preventing users from installing a USB device. (Bragg, 2004)
- Make USB ports read-only by adding/modifying the following registry key in the Registry

```
Windows Registry Editor Version 5.00
[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\StorageDevicePolicies]
"WriteProtect"=dword:00000001
```

- Disable USB ports in Group Policy http://support.microsoft.com/default.aspx?scid=kb;en-us;555324
- Disable Autorun
- Update existing antivirus settings to ensure all attached USB devices are scanned immediately. (Labmice.net, 2003)

© SANS Institute 2009, Author retains full rights.

- Use endpoint Protection/Access Control software to regulate, track and audit what files get written and read from external storage devices
    - DeviceWall from Centennial Software
    - Sanctuary Device Control from SecureWave
    - GFI LANGuard from GFI Software
    - DeviceLock from SmartLine Inc.
    - SEP 11 by Symantec
- Make better use of existing file system/network permissions, maintaining the principle of least privilege
- Use software file encryption such as:
    - TrueCrypt
    - Microsoft BitLocker / Encrypted File System (EFS)
    - PGP / GPG
- Use hardware encrypted USB drives or file encryption, such as:
    - MXI Stealth
    - Ironkey
- Include return-to information printed on the flash drive or on an unencrypted file
- Use device tracking software, such as iHound, as a final resort to attempt to find lost USB devices (Fig 4)

© SANS Institute 2009, Author retains full rights.

© SANS Institute 2009, Author retains full rights.

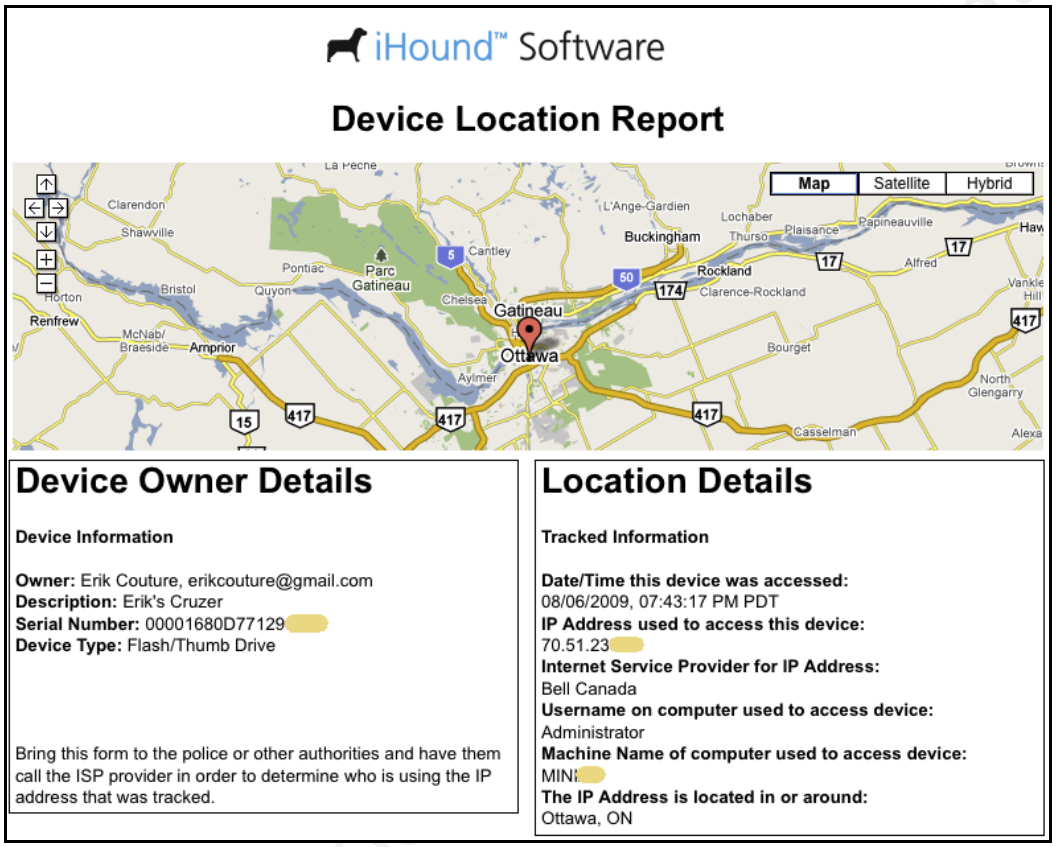


Figure 4 - iHound Device Location Report

Endpoint protection software may be a good choice for enterprise-wide risk mitigation. Major vendors in the field include Symantec, GFI, Safend and Centennial Software. Each package offers similar core endpoint protection features, but their methods for securing USB ports differ, as do their capabilities to audit data being transferred to removable media. Most packages offer comprehensive reporting of user compliance, allowing simple, graphical feedback to security staff and management. Audit data, often linked directly with the organization's Active Directory can add context and help assess the effectiveness of both technological and policy driven risk mitigation. When selecting an endpoint protection package, ensure the features offered line up with the highest/most critical risk areas, such that you are mitigating the correct risks. (Annex C) For example, some but not all packages offer the ability to detect hardware keyloggers. If such a threat is considered serious in your organization, due to public access to

© SANS Institute 2009, Author retains full rights.

workstations, it should be a priority on the feature list of the chosen endpoint security package, or a task-specific application could be sourced to meet the requirement.

2.5.2. Policy-Driven Risk Mitigation

Figure 5 graphically demonstrates the concept of policy management. When creating any issue-specific policy you first need to understand your acceptable risk. The threat-risk assessment is your friend in this regard and will guide management/data owners to make fair and responsible choices.

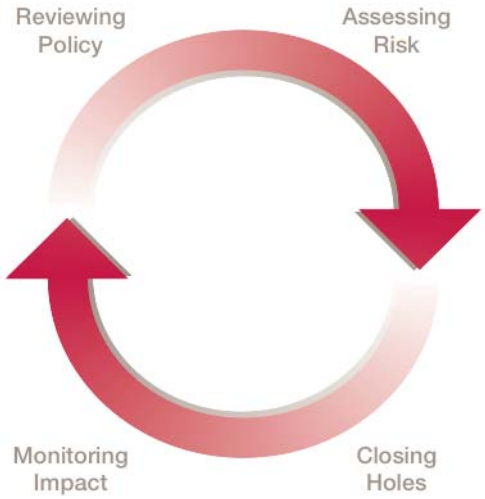


Figure 5 - The policy management cycle (Centennial, 2009)

The first step to mitigating risk is to fix the big holes first or 'picking the low-hanging fruit' to use an already tired metaphor. This step may include elements of technological solutions as well as policy but should focus on shoring up the most critical and easily/cheaply addressed issues. Depending on the risk assessment and your organization requirements, this may involve locking down non-essential USB ports via a GPO push, accompanied with a policy restricting the connecting of unauthorized USB devices for electrical charging.

Whatever the steps put in place, avoid unnecessary complexity and clearly communicate both the policy and the *intent* or *spirit* of the policy to the user base. It is critical to policy uptake

© SANS Institute 2009, Author retains full rights.

that the users understand why the policy has been put in place, what the risks are to the organization to breaking the policy and what the disciplinary action will be to non-conformers.

Finally, monitor the impact of the risk mitigation and routinely conduct audits to ensure the technological efforts and policy are having the desired impact. As time goes on the threat will also evolve, new devices and methods will be developed and will create new vulnerabilities. Review the policies and technological measures regularly and adjust as required to mitigate the evolving threat.

Policy approaches can attempt to impose any degree of the following:

- Total ban on USB devices in the environment,
- Ban on unauthorized devices (non-corporate issue),
- Ban on using USB ports for charging/power purposes (you may provide 5VDC power charging outlets for ipods/phones to reduce temptation),
- Restrictions from removing storage devices from the workplace,
- Enforcing desktop-lock timeout policy to minimize workstation vulnerabilities,
- Stronger physical security that prevents intruders from gaining physical access to USB ports,
- Mandatory paperwork to be completed each time data is to be moved off the system, forcing users to deliberately consider the risks; and
- Mandatory, regularly revisited, education of users and security personnel

The key parts of a policy include Asset Identification, Risk Assessment, Access Control and Incident Handling. (Kaleewoun, 2001) USB-security related policy is primarily focused on prevention. Once a breach has occurred an organization should follow its established incident-handling plan.

In a now infamous experiment conducted in 2006, a security audit firm scattered 20 USB flash drives around a financial group's building. Each was designed to collect passwords and other user information. All 15 of the drives that were picked up were plugged in to the corporate

© SANS Institute 2009, Author retains full rights.

system. (Lemos, 2006) This experiment has since been replicated many times, usually resulting in the same result. It makes a strong argument that even with policy and education in place, human curiosity will often blind users. For this reason policy must be accompanied with technology which, properly configured will make it difficult or impossible for users to make unwise choices.

One strategy put in place to a great degree of success by the London police force was for an Officer to file a formal request each time he needed to download data onto removable media. This extra step forced the user to go through a risk/benefit assessment and make an educated decision; based on the data's sensitivity and the consequences of its possible loss or compromise. (Wheatly, 2008)

Finally, only institute policy that you are set up to police and audit, and that senior management is prepared to levy consequences (particularly on breaches within senior management!) A policy without teeth is a waste of time and resources.

3. Conclusion

The following quotation brilliantly sums up the threat of a potent technology such as USB, when combined with fallible users.

"The twin lures of curiosity and utility, in the end, make USB drives a powerful trojan horse. Social engineering is always the easiest way to compromise a network, because people are typically very friendly and trusting." - Steve Stasiukonis, VP Secure Network Technologies, Inc. (DarkReading, 2006)

The aim of this paper was to raise knowledge of a ubiquitous, often overlooked security vulnerability. Through a discussion that began with the identification of user requirements, and progressed though threat and risk assessments, this paper helps prepare the technical manager or IT security professional to tackle a complex technological and policy issue. It is clear that as with all security issues, USB ports are delicately balanced between great simplicity and functionality for the user and great risks to the organization.

© SANS Institute 2009, Author retains full rights.

Instead of thinking "it won't happen to me", security professionals need to be constantly aware of the evolving threat and considering what they can do to ensure that their organization won't be the next.

© SANS Institute 2009, Author retains full rights.

© SANS Institute 2009, Author retains full rights.

4. References

4.1. Technical References

Barrall, D., & Dewey, D. (2005). *Plug and Root, the USB Key to the Kingdom*. Presentation at Black Hat Briefings.

Bowman, Michael. (2007) *Overcoming USB (In)Security* www.michaelboman.org.

Bragg, Roberta. (2004) *8 Ways to Protect USB Leakage*. MCP Magazine Security Watch http://tinyurl.com/7hxrt

Centennial Software. (2009) *Effective IT Policies*. www.centennial-software.com

Centennial Software. (2008) *Eight Reasons not to Stall on Endpoint Protection*. www.centennial-software.com

CSO Online. (2008) *Risk Assessment Tool: Application for Removable Device Media.* www.csoonline.com/article/print/329019

Checkpoint®. (2009) *The need for encryption: Keeping lost, stolen data protected.*

DarkReading. (2006) *Social Engineering, the USB Way* www.darkreading.com/story/showArticle.jhtml?articleID=208803634

Greiner, Lynn. (2009) *No Silver Bullet*. Security Matters Magazine, Vol 3 Iss 3, Summer 2009. KAP Publishing. Thornhill ON, Canada.

In-Stat. (2009) *Wired USB 2009: High-Speed Rules, SuperSpeed on the Way.* June 2009. www.InStat.com

Kaleewoun Philip J. (2001) *An Overview of Corporate User Policy*. SANS Reading Room

Kempter, Dr. Andrea. (2009) *ITIL Service Level Management* wiki.en.it-processmaps.com/index.php/Service_Level_Management

© SANS Institute 2009, Author retains full rights.

Labmice.net. (2003) *USB Flash Drives: Useful Device or Security Threat* labmice.techtarget.com/articles/usbflashdrives.htm

Lemos, Robert. (2006) *USB drives pose insider threat*. SecurityFocus.com

Ponemon Institute LLC. (2009) *Trends in Insider Compliance with Data Security Policies*.

Safend Ltd. (2007) Strengthening the bench. www.safend.com

Stith, John. (2006) *Virus infects Russian Stock Exchange.* SecurityProNews. www.securitypronews.com/news/securitynews/spn-45-20060206VirusInfectsRussianStockExchange.html

Tharp, Tom. (2007) *The Unique Benefits and Risks of USB Mass Storage Devices.* Information Systems Control Journal.

USB Implementers Forum, Inc. (2008) *Universal Serial Bus Specification*. Beaverton, OR

USB Implementers Forum, Inc. (2003) *Universal Serial Bus Mass Storage Class Specification Overview*. Beaverton, OR

Usher, Abe. (2006) *Podslurping*. http://www.sharp-ideas.net/pod_slurping.php

Wheatly, Malcolm. (2008) *How To Tell If That USB Download Is Really Worth the Security Risk.* www.csoonline.com/article/print/329014

© SANS Institute 2009, Author retains full rights.

4.2. Image References

Figure 1 – USB Connector Types www.l-com.com/images/usb_connectors.jpg

Figure 2 – Ponemon, 2009

Figure 3 – Ponemon, 2009

Figure 4 – iHound Device Location Report www.Ihoundsoftware.com

Figure 5 – Centennial Software, 2009

© SANS Institute 2009, Author retains full rights.

© SANS Institute 2009, Author retains full rights.

5. Annexes

5.1. Annex A – USB Requirements Definition Template

Possible uses for USB ports in the enterprise

1. USB Flash Drive
    a. For data transfer to other internal systems
    b. For data transfer to user's home systems
    c. For data carriage offsite to client's offices, presentations, meetings etc
2. External USB Hard-disk
3. Docking of legitimate business devices such as Blackberrys™ or PDAs
4. Direct file transfer between computers (desktop-laptop)
5. USB powered peripherals (lights, fans)
6. Charging USB devices such as MP3 players
7. Video cameras for business related video-conferencing
8. USB Networking devices (Ethernet-USB dongles)
9. Digital/video cameras and media card readers
10. USB Hubs
11. Authentication Tokens (Yubikey™)
12. Speakers
13. Local, non-networked printers
14. Keyboards, mice, human interface devices, smartcard readers
15. Custom or business specific instrumentation or data capture devices

© SANS Institute 2009, Author retains full rights.

5.2. Annex B – USB Security Threat-Risk Assessment*

Risk Assessment Scoring

Amount of information	Small <100kb Medium < 5Mb Large > 5Mb	35 40 50
Is the use of the device restricted to specific users?	Yes No	-5 10
Can transfers of information be audited?	Yes No	-10 10
Can the information be checked for malicious code?	Yes No	-10 20
What is the classification of the information involved?	Unclassified Restricted Confidential	0 20 40
Can the information be easily accessed if the device/media is lost?	Yes No	20 -30
What are the consequences of losing the device/media?	None Embarrassing Endangers business interests Endangers individuals	0 10 50 200
How easily can the information be transferred to other devices/media?	Easy Difficult Not possible	50 10 -50
Are there effective procedures in place that will reduce risk of misuse?	Yes No	0 50
Are there effective procedures in place that will reduce risk of accidental loss?	Yes No	0 50

Benefit Assessment Scoring

Does the proposed data transfer directly save money or generate income for the business?	Scale from 0-40
Does the proposed data transfer have a direct operational benefit?	Scale from 0-60
Does the proposed data transfer put people at risk?	Yes Scale -50 to 0 No = 0

© SANS Institute 2009, Author retains full rights.

Risk/Benefit Ratio

Benefit \ Risk	0 - 45	45 - 200	200 +
< 20	**Rejected** Insufficient Benefit	**Rejected** Insufficient Benefit	**Rejected** Unacceptable risk
20 - 40	**Low Risk & High Benefit** Acceptable risk-benefit ratio	**Rejected** Disproportionate risks to benefit	**Rejected** Unacceptable risk

The exact figures in the tables above should be tailored for the organization, based on business type and risk tolerance.

*Adapted from City of London Risk Assessment Scoring (CSO Online, 2008)

© SANS Institute 2009, Author retains full rights.

© SANS Institute 2009, Author retains full rights.

5.3. Annex C – Vendor List

AC to USB Power Adapter - http://www.thinkgeek.com/gadgets/travelpower/9124/?cpg=ab

Centennial Software DeviceWall® - http://www.centennial-software.com

Checkpoint Endpoint Security - http://www.checkpoint.com

DeviceLock Endpoint Protection (USB Keylogger detection) http://www.devicelock.com/dl/

GFI Endpoint Security - http://www.gfi.com/endpointsecurity

Hardware USB Key Loggers: http://www.keelog.com/

iHound USB Tracking Software – http://www.Ihoundsoftware.com

Ironkey – Secure flash drive - https://www.ironkey.com/

MXI Stealth - Secure flash drive - http://www.mxisecurity.com/

Safend Protector - port and device control- http://www.safend.com

Symantec Endpoint Protection - http://www.symantec.com/business/endpoint-protection

Yubikey: USB Authentication Device- http://www.yubico.com/products/yubikey/

© SANS Institute 2009, Author retains full rights.

© SANS Institute 2009, Author retains full rights.