Security Threats and Mitigating Risk for USB Devices

ANNETTE TETMEYER AND HOSSEIN SAIEDIAN

Digital Object Identifier 10.1109/MTS.2010.939228

Computer users have consistently sought out improvements to devices for removable storage to provide the quickest and most efficient means of transferring data from one computer to another. Cheap, convenient floppy disks with limited capacity gave way to optical discs, such as rewritable CDs, which significantly improved storage capacity. However, both floppy disks and CDs required the use of a drive in order to read and write to either and incompatibilities with both media were not uncommon. Email evolved as the next method for transfer of small or medium sized files. However, users still found the need for less cumbersome, higher-capacity portable media for the transfer of files.

In 2000, Universal Serial Bus (USB) devices emerged as a new form of portable storage media with even greater storage capacities, high data transfer speeds, and a desirable small size. With a height of around four inches and weighing under a few ounces, these devices were extremely portable and often marketed as personal storage devices. The "plug and play" capabilities required only a simple USB port to connect devices to a computer. Modestly priced when introduced, USB drives became increasingly popular as storage capability increased and prices decreased.

For a computer user, these devices make it possible to conveniently store, transfer or backup data. User knowledge and skill required to transfer files to and from a device is minimal, which has enhanced their appeal. While some organizations provided sanctioned devices for employee use, many other devices found their way into organizations because users personally purchased devices to meet additional needs.

Portable storage media have always been fraught with risk. Security considerations have always been a concern and organizations have tried to mitigate these threats using many controls. However, since threats are constantly evolving and changing, security controls must also evolve and change to keep up with these threats.

There are a variety of removable storage devices that can be connected via a USB port. Devices include memory cards (CompactFlash, Secure Digital, Memory Stick), removable USB flash drives, and iPods. Although other types of removable storage devices are available that may be connected via USB ports, we address here only removable USB flash drives and iPods. Due to the portable, removable nature and common use of these USB attachable devices, they may also be referred to as transient storage devices (TSDs) [13].

Popularity of Transient Storage Devices (TSDs)

As professionals become more "nomadic," remote access to computing systems is increasingly required [2]. While remote access typically conjures an image of accessing organizational systems from outside the organizational perimeter, remote access can also mean accessing data and accomplishing business needs from computers outside the organization's control. In an effort to balance productivity and convenience, personally owned and public computers may be used for business functions. Data may be accessed or transferred to these computers, processed, and stored back to the TSD.

TSDs are also being designed to allow users portable virtual access by allowing applications to be run directly from them. The "borrowed computer" could then be used to run the user's operating systems, personalized browsers, applications, and data. Portable storage-based personalization allows a computer to boot from the USB storage device, creating a personalized computing environment [12]. Personalized sessions may include virtualized operating systems, applications, and access to files. Web browsing settings, configurations, preferences, and bookmarks are envisioned for other personalized systems.

Other TSDs that are not purchased by the organization and are used for non-business functions may be present in an organization. A primary example would be the presence of iPods that are personally owned by employees or outsiders interacting with the organization. Generally seen as a mechanism for personal entertainment, the intended function of iPods is rapidly evolving. The capacity, functionality, and proliferation of iPods and their impact on organizations is also evolving. Regardless of the intended use of the TSD, understanding primary modes of access is necessary to identify risks pose by these devices.

User Interaction with TSDs

System connection for TSDs requires direct user interaction. Two areas will be explored: primary modes of access for TSDs and user perceived notions of threat models for TSDs.

Primary Modes of Access for TSDs

TSDs require some form of physical access to systems for interaction. Physical access can be further sub-classified as intentional or unintentional consented access. "Consented use of USB devices means that the USB device is used under supervision of the owner or user of the computer containing the USB port" [3]. Consented use can also be a form of "soft-hacking" where the technical skills of the attacker need not be strong since the user has allowed or invited the attacker to access the system [17].

From the viewpoint of the organization, an insider attack where social engineering is used to provide access to the USB port would

be unintentional consented access. A social engineering attack of this type might be from a person requesting to plug in and charge an iPod to the victim's computer. Because the victim's mental model does not include "access to USB ports to charge an iPod" as a threat, consented access may be readily given [18]. The attacker now has access to the system based on the user's authorization level. If the user happens to be logged in with administrative access, an attacker with malicious intent could pose an extreme threat to the organization.

Intentional consented use can also occur if an employee launches an attack. The employee may have malicious intent and could download organizational data or launch an attack. A malicious attack launched in this manner might negate "defense in depth" mechanisms [8]. Intrusion Detection Systems (IDSs) or antivirus software might be assumed to be "defense in depth" mechanisms that would alert the organization to massive downloading of data or another insider attacks that are launched from within the organizations system perimeter. However, if these devices are not configured to differentiate between authorized use and malicious activities by insiders, protection safeguards will be bypassed [9]. Additional threats exist if the insider downloads data to a TSD and transports it outside of the organization's perimeter.

If an attacker intends to steal and transport data outside of the organization, the wide variety of form factors available for TSDs can aid the attacker in concealing the device. Form factors for TSDs vary and can look as innocuous as a pen [7]. The savvy attacker may be able to avoid rousing suspicion even if physical security, such as inspection at a guard desk upon entering or leaving a facility, is enforced.

All of these modes of access point to the importance of "human factors" in relation to IT security [17]. Whether intentional or unintentional, "user behavior is a weak link in system security" [2], [17]. Understanding the human factors involved will aid in categorizing the risks TSDs pose to organizations.

User-Perceived Notions of Threat Models

Users have wildly inaccurate models of threat possibilities and the importance of security [2]. This situation is compounded by the fact that the physical appearance of a device does not provide an accurate picture of the true functionalities (and security threats) that a device poses [1], [7]. Most users would expect an iPod's function to be primarily for listening to music and watching videos. However, an iPod has much greater functionality that users generally do not appreciate. Current storage capacity of the iPod can be as much as 160GB. For an organization, this can pose a serious security threat to an attacker wanting to upload to or download files from the organization's network.

Personalized, bootable USB devices may be an intriguing option for highly mobile users. The capability of being able to transport an operating system, applications, browsers, data, and user settings to any computer would provide users with tremendous flexibility. Users of these systems might have a false sense of security in thinking that use of these devices is safe and data will be secure. However, booting a public PC from a USB device may be risky for the device owner. A compromised or corrupted Basic Input Output System (BIOS) could corrupt data, copy files or steal encryption secrets [12].

While specifically focusing on the issues of worms, cookie management, and phishing attacks, Yee [18] stresses that security and usability must be aligned in order to be effective. This underlying principle is applicable to security issues for transient storage devices. If devices are solely focused on security, usability will suffer. If they are solely focused on usability, security will suffer. "Fundamental changes to operating systems and applications" are required if strong security is to be in place for the use of transient storage devices [18]. Smith [15] also notes that users have varying interpretations about what to trust, and that security problems arise from bad interactions between users and systems. Finally, users may be blissfully unaware of the security risks that TSDs pose and can inadvertently put systems at risk by their actions [5].

Risks to Organizations

If robust security relies on both users and systems, how does the system determine if a TSD can be trusted? Arce [1] states that "the kernel code that manages and operates peripheral devices is a poor single line of defense for today's most popular operating systems." TSDs connecting to a host system may also mistakenly trust the system and could be at risk for BIOS or virtual machine (VM)-based attacks [12]. The Trusted Computing Group (www.trustedcomputing.org) seeks to address secure computing from all levels of hardware through operating systems (OS). Emerging standards and devices for secure system interaction of TSDs is addressed in later sections of this article. Finally, firmware-controlled resources may provide backdoor access to a system that can place the trust of a peripheral in jeopardy [16].

A number of researchers categorize the risks posed by mobile devices. When applied to TSDs, the risks will include:

- Theft of sensitive data.
- Loss or theft of device.
- Viruses, worms, or other malware.
- Data loss/leakage due to a small footprint and portability.
- Surreptitious interaction with systems.

For each of these risks, user and/or system interaction is needed to carry them out. Understanding how these attacks are carried out and the consequences to an organization will be useful in determining mitigation strategies.

Theft of Sensitive Data; Loss or Theft of Device

Security breaches occurring with loss or theft of organizational data are frequently in the news. Recent breaches include classified data being transported outside of secure facilities on a USB drive, and stolen U.S. military flash drives with confidential information being sold in Afghanistan. While these headlines are related to government organizations, loss or theft of data also can occur in any business.

Pod slurping is an example of an emerging threat in which massive amounts of data can be copied covertly and quickly. Originally, the Slurp.exe file was created as a scare tactic to demonstrate the risks that USB devices, in particular iPods, posed to systems. If used maliciously and with administrator-level access, significant risks are present [3].

The financial impact of the loss of information or harm to systems for a business can be severe. Heikkila [9] cites the 2006 Ponemon Institute survey rating data loss at $182 per record. Costs include recovering or repairing damage due to data loss, contacting customers, notifying the public, and complying with regulatory or legal requirements. The exact amount of these costs varies depending on the sensitivity of data, but costs can quickly rise.

Viruses, Worms, or Other Malware

TSDs may contain malicious code that can bypass layers of security and controls that an organization has in place [8]. While users may be aware that viruses can be easily spread by opening unknown files or email, there are current examples of actual breaches occurring. There have been many reports, for example, that a security test using USB devices was anonymously sprinkled throughout an organization. The devices contained malicious code disguised as an image file and all devices were found to have been plugged into the organization's system. These examples are not uncommon and demonstrate the ease with which malware can be spread and the damage that can be inflicted upon the systems.

Data Loss/Leakage Due to Small Footprint and Portability

As discussed, the small size and increasing capacity of TSDs make data loss/leakage easy to carry out. Trusted users who may be authorized to access sensitive data can copy large amounts of data to a TSD. Outsiders carrying out insider attacks can also access and transfer data to a TSD. In both cases, the very small size of the TSD makes it easy to conceal and remove data from an organization. In cases where there are security measures in place to mitigate transfer of data from the premises, the TSD may not be flagged as a threat. Small devices may go unnoticed or the innocuous nature of the TSD, such as an iPod, may not cause alarm.

Surreptitious Interaction with Systems

Malicious code may not only spread viruses or worms, but can surreptitiously interact with systems using auto-run capabilities available to TSDs. USB U3 technologies have been developed "to provide portability without violating copyright laws or end-user licenses" [3]. Additional marketing for U3 devices cites benefits such as "leaving no trace…on the host computer after the smart drive is removed" [4]. While additional research shows that traces for U3 devices are indeed left behind on the host computer [4], it is not clear if developers, regardless of intent, are working on trace-free solutions. Additional details on forensic traces from TSDs are provided later in this article.

In addition to understanding that loss of data, malware, fraud, and surreptitious interaction with systems are significant risks posed by TSDs, it is also necessary to understand the forensic evidence left behind by TSDs before moving on to risk mitigation strategies.

Forensic Evidence for TSD Devices

Forensic evidence is a necessary step in tracing TSD usage either after an attack or as a means to improving security controls. U3 USB devices are marketed based on the claim to being untraceable on the host computer. However, traces can be found in the Windows XP (SP2) operating system. Bosschert [4] demonstrates that the following traces can be found:

- U3 directory created in the users documents and settings folder.
- Recent file information from applications opened
- Registry changes to in multiple locations.
- Prefetch files for programs that run when the U3 device opens.
- Applications that were run from the U3 device may also leave additional traces, such as names of documents.

Data also can be left behind left by TSDs in Linux and Windows operating systems. Each time a TSD is connected to a system, the product name, serial number, manufacturer, and date inserted are left behind in the registry. Windows log files also can be used to trace TSD start, stop, and device installation [10]. However, Rich [13] points out that vendor and product IDs can be easily falsified by unscrupulous parties.

When implementing or monitoring security controls, forensic

evidence can be a useful tool for ongoing TSD risk mitigation.

Mitigating TSD Risk

Mitigating risks from TSDs requires a comprehensive approach that takes into account both user and system interaction. Table I outlines a variety of risk mitigation techniques and system interaction protection strategies [3], [7], [16].

Table I is not an exhaustive listing of risk mitigation strategies or techniques, but it is a comprehensive summary. Further analysis and explanation for selected strategies is as follows.

All peripherals connected via USB ports are not "bad" and may be necessary for system operations [1]. The example of superglue being used to disable ports may be extreme; decisions should be made based on the sensitivity of data accessible from a system or the security needs of a system, such as a server [3]. Logs are an important tool in detecting insider attacks. System logs may be the most likely means to uncover evidence of an attack. An emerging strategy is also the use of honeypots to detect security breaches.

Auto-run, auto-mounting features, and auto-installation of drivers will make TSDs easier to operate for users as well as the unscrupulous attacker. Auto-run can be blocked by holding down the SHIFT key when connecting a TSD to the USB port [3].

Access control can be used as a means to determining device trust. TSDs or other peripherals should be configured based on the type of device and intended operation. Access controls should include authentication options such as passwords, biometrics, and encryption [16]. To be effective, the balance between security and usability for authentication options should always be taken into consideration [2], [5], [15].

Encryption can be a difficult hurdle to overcome. Some have proposed a scheme to protect data from thieves who might access data that has left the organizations perimeter. Encrypting File System (EFS), PGPdisk, and TrueCrypt are among the alternatives. Encryption addresses the needs of individuals who routinely transport sensitive data via TSDs and may not necessarily provide for a larger organizational security framework.

Each of these strategies demonstrates that TSD security requires addressing elements of user and system interaction. Awareness and education address user interaction whereas disabling BIOS access to USB ports addresses system interaction. While geared more heavily to user interaction, Cranor and Garfinkel [5] reiterate this principle that systems need to be built that "just work" without user intervention. Systems also need to allow for the correct use of security tools. Cranor and Garfinkel also note that training is critical.

Emerging Standards

Unlike earlier storage devices, TSDs pose a greater security threat due to their capacity and capabilities. Host systems require authentication from the TSD before being allowed to mount to the system. Based on this need, the IEEE Computer Society's standards committees on information assurance and storage systems have developed the 1667 Standard Protocol for Authentication in Host Attachments for Transient Storage Devices. Published in June 2007,

Table I
Risk Mitigation Techniques and System Interaction Protection Strategies

	Source		
Technique or Strategy	Al-Zarouni	Halpert	Thibadeau
Physical access controls such as disabling USB ports	✓	✓	
Logical access controls such as disabling BIOS feature for USB ports	✓		
Group Policy to block and/or audit USB device use	✓		
Log data	✓		
Disable auto-run	✓	✓	
Disable auto-mounting features		✓	
Disable auto-installation of drivers		✓	
Limit administrator privileges, use least privileges	✓		
Use anti-virus and anti-hacker tools	✓		
Awareness and Education	✓		
Encryption	✓	✓	✓
Password authentication		✓	✓
Biometric authentication		✓	✓
Restrict user access to existing devices		✓	

the standard was designed to address the issue of an authentication method for TSDs [13].

The standard's architecture uses addressable command targets (ACT) with related silos to determine the device's functional capabilities. An initial probe silo allows for querying to determine the ACT functionality. Next, authentication silos use a variety of certificates which provide authentication of the host and ACT. Up to 256 silos are available per ACT.

If supported by operating systems, IEEE 1667 can improve TSD security by providing bi-directional TSD authentication between both host systems and TSDs. One downside to the standard is that it does not address authorization, only authentication [13].

An emerging area of security is through the use of USB devices that are intended to enhance security to systems. U-Key and I-Key are two different approaches that use bootable USB devices.

Shaunghe and Zhen [14] propose a scheme to provide boot integrity and to enforce access control. The U-Key combines a smart card with a USB interface to create a trusted computing environment. When a PC is booted with the U-Key inserted, the integrity of the operating system can be verified as well as the legitimacy of the user (the U-Key owner).

The I-Key model is also intended to enhance security by inserting a USB device during system boot. Users are authorized and allowed access to specific data based on defined access controls. Provisions are made for revoking or reassigning access to records as well as for revoking access due to lost keys [6].

Expanding Capabilities

The increasing capacity and expanding capabilities of USB devices will continue to make them popular for computer users. Security threats, both current and emerging, will need to be fully investigated and understood in order to mitigate the risks these devices pose. Threats from USB devices require some form of physical interaction by users whether consented or not. Next, system interaction is required for threats to materialize. Common threats include data loss/theft, fraud, and malicious attacks via worms, viruses, or malware.

Increased awareness of USB threats also has improved understanding of forensic tools available for tracing USB usage. Traces left behind and methods in which an attack can be carried out provide insight into the need for standards to mitigate USB risks. Therefore, the risk mitigation challenge is the need to provide a comprehensive strategy that takes into account both user and system interactions when considering security strategies for TSDs.

Risk mitigation controls need to be a combination of user and systems controls. Awareness, education, user authentication controls, and blocking physical access to USB ports will provide some level of risk mitigation for user interaction. Easy to use encryption and authentication controls also should be incorporated to provide additional security without negatively impacting the user. Systems controls such as disabling autorun features and policies to block access will provide additional layers of security. Finally, emerging standards such as IEEE 1667 appear to be a great start in further security improvements while maintaining usability for USB connected devices.

Author Information

Annette Tetmeyer is with the Department of Engineering Management, and Hossein Saiedian is with the Department of Electrical Engineering and Computer Science at the University of Kansas, Lawrence, KS 66049 U.S.A. Email: saiedian@ku.edu.

References

[1] I. Arce, "Bad peripherals, *IEEE Security & Privacy*, vol. 3, no. 1, pp. 70–73, 2005.

[2] A. Adams and M.A. Sasse, "Users are not the enemy," *Commun. ACM*, vol. 42, no. 12, pp. 40–46, 1999.

[3] M. Al-Zarouni, "The reality of risks from consented use of USB devices," in Proc. 4th Australian Information Security Conf., Perth, Western Australia, 2006; http://scissec.scis.ecu.edu.au/conference_proceedings/2006/aism/.

[4] T. Bosschert, "Battling anti-forensics: Beating the U.S. stick," J. Digital Forensic Practice, vol. 1, pp. 265–273, 2006.

[5] L.F. Cranor and S. Garfinkel, "Secure or usable?," *IEEE Security & Privacy*, vol. 2, no. 5, pp. 16–18, 2004.

[6] A. Dalley, J. Fulcher, D. Bomba, K. Lynch, and P. Feltham, "A technological model to define access to electronic clinical records," *IEEE Trans. Information Technology in Biomedicine*, vol. 9, no. 2, pp. 289–290, 2005.

[7] B. Halpert, "Mobile device security," in *Proc. 1st Ann. Conf. Information Security Curriculum Development* (Kennesaw, GA), 2004, pp. 99–101.

[8] J.V. Harrison, "Enhancing network security by preventing user-initiated malware execution," in *Proc. Int. Conf. Information Technology: Coding and Computing*, vol. 2, no. 4–6, pp. 597–602, 2005.

[9] F.M. Heikkila, "Encryption: Security considerations for portable media devices," *IEEE Security & Privacy*, vol. 5, no. 4, pp. 22–27, 2007.

[10] V.C. Luo, "Tracing USB device artefacts on Windows XP operating system for forensic purposes," in Proc. 5th Australian Digital Forensics Conf. (Perth, Western Australia), 2007; http://scissec.scis.ecu.edu.au/conference_proceedings/2007/forensics/00_Forensics2007_Complete_Proceedings.pdf#page=214.

[11] P.M. Milligan and Hutcheson, "Business risks and security assessment for mobile devices," in *Proc. 8th WSEAS Int. Conf. Mathematics and Computers in Business and Economics* (Vancouver, Canada), 2007, pp. 189–193.

[12] N. Ravi, C. Narayanaswami, M. Raghunath, M. Rosu, "Securing pocket hard drives," *IEEE Pervasive Computing*, vol. 6, no. 4, pp. 18–23, 2007.

[13] D. Rich, "Authentication in transient storage device attachments," *Computer*, vol. 40, no. 4, pp. 102–104, 2007.

[14] P. Shaunghe and H. Zhen, "Enhancing PC security with a U-Key," *IEEE Security & Privacy*, vol. 4, no. 5, pp. 34–39, 2006.

[15] S.W. Smith, "Humans in the loop: Human-computer interaction and security," *IEEE Security & Privacy*, vol. 1, no. 3, pp. 75–79, 2003.

[16] R. Thibadeau, "Trusted computing for disk drives and other peripherals," *IEEE Security & Privacy*, vol. 4, no. 5, pp. 26–33, 2006.

[17] C.S.M. van Baal and H.J.M. Winjenen, "Human factors on IT security," http://janus.cs.utwente.nl/~baal/docs/Human_Factors_on_IT_security_-_CSM_van_Baal_HJM_Wijnen.pdf.

[18] K. Yee, "Aligning security and usability," *IEEE Security & Privacy*, vol. 2, no. 5, pp. 48–55, 2004.