Securing Computing Resources from USB Borne Viruses and Malware

White Paper

By

Ray Dupont
Director of Engineering Desktop Solutions
ClearCube Technology
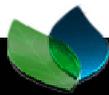
The Nature of the Problem

The USB dongle (also known as a disk-on-key or thumb drive) has become an integral part of our work environment, replacing the floppy disk of years ago. Floppy disk drives no longer appear on most computers sold today but these computers all have USB ports, so use of the USB dongle has become a major method for users to easily capture and transport data in many work environments.

As use of the ubiquitous USB dongle increases, transmission paths and security vulnerabilities have been created for increasingly sophisticated software malware, included worms and viruses. In many cases, the threat presented by these malicious software elements greatly outweighs the benefit to the users.

There have been multiple articles on the threat that USB Mass Storage Devices have had in spreading worms and viruses throughout the military and corporate world. Multiple documented cases of government espionage, illegal or unauthorized transfer of documents, and hacking could have all been avoided by a proven, secure solution thus preventing these kinds of malicious acts.

- *What are the potential ramifications of having an easily accessible, unguarded port to an organization's secrets?*

- *What is the impact of a breach in national security?*

- *Has your organization considered how to prevent such breaches with the right technology or do your current IT practices continue to make decisions around and source technology based on the existing status-quo?*
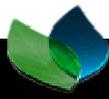
Links to Recent Articles

For more information about how these security threats are already effecting DoD installations, you can review some of the following articles:

"Under Worm Assault, Military Bans Disks, USB Drives" – November 19, 2008

Link: http://blog.wired.com/defense/2008/11/army-bans-usb-d.html

---

"USB Devices Containing Worms Threaten US Army, All Removable Devices Temporarily Banned" – November 20th, 2008

Link: http://cyberinsecure.com/usb-devices-containing-worms-threaten-us-army-all-removable-devices-temporarily-banned/

"Old worm infects Department of Defense computers" – November 22, 2008

Link: http://www.itworld.com/security/58270/old-worm-infects-department-defense-computers

---

*"Malware spread explains Pentagon USB ban" – December 1, 2008*

Link: http://www.theregister.co.uk/2008/12/01/malware_pentagon_usb_ban/
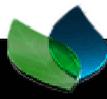

Methods to Address the Problem

The question for the IT management now is how to effectively block this security threat and still maintain a productive environment for users. There are several approaches to this problem:

1) **Brute Force** – this method imposes a personnel based policy ban on all USB dongles; they simply don't allow them in the environment. This is the approach that is being taken by IT management in many of the articles cited above. This however is going to have a stifling impact on the productivity of the employees and IT staff, and can be difficult to enforce. This is an ineffective solution with lots of negative impact.
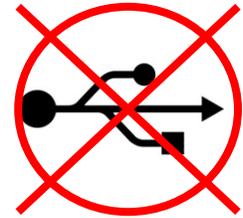
2) **Software Policy** – this method uses a software based policy manager to selectively allow registered or deny unregistered USB devices. These policy managers are typically available through the operating system, middleware or end user programs. The problem with this method is that whenever a software method is used to secure the USB ports, there will also be a way to subvert it through software hacking. This represents a more flexible solution, but is still not entirely effective.
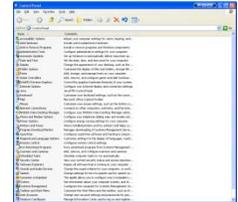
3) **Firmware Policy** – this method is more secure than the software method, and is usually a feature in embedded hardware that forms a client access device at the user desktop. Such client devices are normally part of a centralized computing architecture and provide user connectivity to computing resources in a secure data center. This method is more secure than a software policy, and certainly more difficult to hack, but still leaves the client device accessible to a malicious user. Therefore, this is also a flexible solution, but does not guarantee security - the ingenuity of hackers has been demonstrated over and over again.

4) **Hardware Mass Storage Lockout** – this method moves the enforcement of the USB policy against mass storage devices to the host computing resources inside a secure data center. This is the method that ClearCube uses and provides the most secure method of protecting the system. This method will be further explained in the following section.

The ClearCube Solution

The ClearCube concept is simple: condense the PC into an Intel-based "blade PC" form-factor, house it in a chassis and centralize it in a secure location. A small user port connects the monitor, keyboard, mouse and USB peripherals to the blade across a wired or wireless network. Users can also access their blades through a variety of industry standard access devices (e.g., thin clients, tablets, and PDAs) via a web browser. IT administrators remotely control the entire system from anywhere in the world using simple but powerful ClearCube management software (Sentral).

The ClearCube solution consists of Blade PCs, user ports, and management software:

Blade PC – an end user business computer that is rack-mounted in a secure location. ClearCube PC blades contain the latest Intel Pentium Dual-Core or Xeon processors, high-performance disk drives, DDR2 memory and PCI Express graphics cards.

Chassis – enclosure that provides all of the Ethernet connections, user port connections, airflow management and power input to the blades. Features are delivered through a modular architecture.

User port – a small solid state access device that connects the end user's computing peripherals (monitor, keyboard, mouse, speakers, and authorized USB devices) to a ClearCube blade PC across a wired or wireless network. About the size of a paperback book, the user port has no fans, emits no noise and produces very little heat.
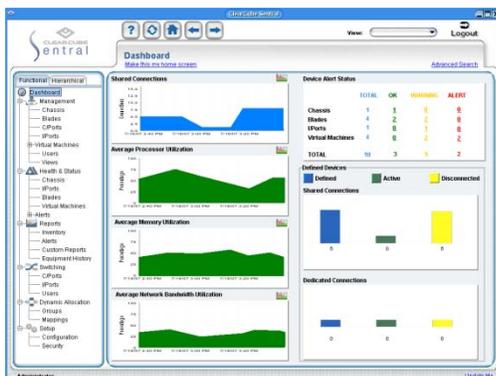
ClearCube Sentral Management Software – enables IT administrators to manage global centralized infrastructure deployments from a single onsite or remote console. Sentral includes unique features such as connection brokering, virtual machine integration, remote BIOS upgrades, active health monitoring, multi-level security configuration and customized views and reporting. The software can also be leveraged to support virtualized desktops or other vendors' blade systems.

ClearCube Technology   **www.clearcube.com**   **1-866-652-3500**
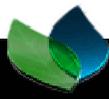
Introduction of the Hardware based Mass Storage Lockout feature

In 2001, ClearCube Technology announced the USB C/Port, a cutting edge enhancement to its highly-acclaimed *C3 Architecture* for centralized computing. The *C3 Architecture* revolutionized desktop PC management by centralizing computing assets while delivering full PC functionality to the user desktop. The USB C/Port delivers complete graphics and USB functionality to the desktop from a Blade PC in the data center. The USB C/Port and subsequent devices are ideal for clients that need to provide their users with the greatest amount of flexibility without sacrificing either network security or the quality of the user experience.

The *C3 Architecture* was originally designed for government and military customers including the DoD and DoE, and was specifically targeted to address demanding security requirements, and leverages the benefits of centralized computing, wherein blade PCs are secured in a controlled access environment. Because they are placed within controlled access, these Blade PCs can deliver a full PC user experience without exposing unwanted security risks.

To further improve the security of the USB functionality, a hardware mechanism was added to control access of USB mass storage devices. The Blade PC provides a hardware jumper that is set by the person who has access to the secured environment. This hardware jumper is virtually impossible to defeat by the usual software methods used by hackers. This **effectively reduces significant expense in time, effort and resources that organizations expend combating the problems and potential threats associated with unlocked USB ports.** Today, the ClearCube Mass Storage Lockout implementation is available in several different product lines, designed to address different user experience requirements:

In the original **C/Port solution**, USB security is assured by the unique ClearCube mass storage lockout feature on the blade side of the solution. By enabling the jumper on the blade the USB controller now monitors all of the traffic on the USB ports. Whenever it identifies a USB Mass Storage device is plugged into a USB port on the C/Port (or indirectly connected through a USB hub) downstream of the C/Port it will lock it out and send a message that the device is not allowed. There is no software method from the C/Port side to defeat this hardware lockout.

In the newer **PCoIP solutions**, the client firmware provides the capability to lockout USB devices by class or registered serial number through a very flexible policy management system – only specifically allowed devices can be used. For complete security, the ClearCube PCoIP solutions can also be combined with the same hardware method as the C/Port solutions. Whenever the PcoIP client device forms a session with a blade that has the jumper enabled it will automatically lock out all Mass Storage Devices, overriding any existing firmware/software policies.

Conclusion

ClearCube offers solutions with patented technology that enable host based Mass Storage Lockout which permits IT organizations to effectively allow USB access to only those that should have access while prohibiting access to those that do not. This feature has been an integral part of the ClearCube solution since its inception and does not require additional hardware and software to implement.

Organizations that are concerned about vulnerability to USB borne virus attacks need to evaluate the ClearCube solution as the only completely effective hardware based protection against this type of security threat.

www.clearcube.com

About ClearCube

ClearCube is the market leader of centralized computing and virtual desktop solutions. As the pioneer of centralized desktop computing, ClearCube provides solutions that span 1:1 power users to 1:many virtualized desktop environments, integrating connection broker software, blades, access devices and professional services to give organizations full control and flexibility over end-user computing. ClearCube's Sentral™ VDI Management System provides clients the ability to utilize any back-end hardware or user access device for desktop virtualization. Organizations deploying ClearCube gain improved manageability, 99.9 percent availability and hardened security while reducing support costs by more than 40 percent. For more information, visit its corporate website at www.clearcube.com.