UNATECH

Protecting What Matters

SecureUSB™ White Paper

The Ubiquity of USB

Universal Serial Bus (USB) is the most successful computer interface ever invented. As of 2011, there were more than 3.5 billion USB devices shipped to date. New In-Stat research forecasts the total USB-enabled device shipments will approach 6 billion in 2015. These shipments are comprised of USB 1.1, USB 2.0 and USB 3.0 variants. Although USB 3.0 (SuperSpeed) has been expected to be dominant, its market share is still only 2% of the total USB device shipments to date. The In-Stat research report expects USB 1.1 (Low/full-speed) to still remain the interface of choice in HIDs, and USB 2.0 (high-speed) to still remain in many PC peripheral and consumer electronic (CE) applications through 2015 (www.in-stat.com).

The USB interface is found in keyboards, mice, webcams, flash drives, cameras, phones, printers, scanners and many, many other types of device. It is even found in non-data applications such as reading lamps and portable device chargers.

Perhaps the greatest innovation introduced by USB is now forgotten since it has come to be just expected. USB is a plug-and-play technology. The software drivers for most common devices are pre-installed in the majority of operating systems. Even if the software is not present, the system is able to identify the new hardware (USB device) that has been connected and then go and find the required driver, either from a local (CDROM) or remote (Internet) source. The user is not required to set any jumpers, choose connection speeds or type in identification information. It just works!

The vulnerability of USB

The ubiquity and ease of use of USB leads to its greatest danger. It is just too easy for the unwary or the unscrupulous to connect a USB device to a computer and enable an unauthorised transfer of information – from device to computer or from computer to device – to take place. A personnel file can be copied from a computer to a flash drive. A virus can be copied from a flash drive to a computer. The interior of a research laboratory can be captured and broadcast by a webcam. These and many similar breaches of security can occur within seconds and can be very difficult to detect physically due to the very small size of many USB devices.

Reported Security Breaches

A small sample of actual security breaches attributable to USB devices is included below:

- The Finance Department at Rochdale Metropolitan Borough Council, UK lost an unencrypted USB stick containing the personal data of several thousand constituents.
- A thief broke into a doctor's car and stole a brief case containing a flash drive that held personal data on patients of the University of Miami Miller School of Medicine.
- Personal information about Regions Financial Corp. current and former employees was lost in November (2011) when a flash drive with the data came up missing after being mailed by external auditor Ernst & Young in the same envelope as the decryption code.

Further examples can be found online. A key resource is the Identity Theft Resource Center (www.idtheftcenter.org).

Existing Solutions

The existing solutions can be separated into software and hardware based systems

Software solutions

Software security solutions are available from a wide range of sources. They provide an increasingly complex suite of services that provide functions such as configuration management, license management, disaster recovery, and asset management. Additional features such as geo-fencing and theft recovery assistance are starting to appear. Software encryption of sensitive data files is readily available.

Although software solutions are common, most suffer from a series of drawbacks. Software, by its very nature, is vulnerable to hackers. The more challenging software is to crack, the more appealing it becomes to the hacker community. Software requires continual upgrades to protect it from new attacks from viruses and malware. Furthermore, software solutions are based on a particular operating system platform and must be reinvented when a new platform, such as a mobile OS, is added to the network. Finally, software solutions add cost – they increase the initial capital cost, increase the maintenance cost and degrade system performance.

According to the Security for Business innovation Council, in 2010 the majority of IT leaders believed that their organizations had policies regarding connection of personal devices on the network, yet close to 60% reported unauthorized device connections still occurred.

In 2011, the Ponemon Institute of IT published a survey of professionals who report to chief information officers (CIOs) or chief information security officers (CISOs). The survey showed

40% believe employees of their organisations routinely turned off their laptops' security protection, despite 68% of their organisations having policies in place that do not allow this.

Hardware solutions

Hardware solutions are far less common than software solutions and tend to provide a much higher level of security, but support a much lower range of resources. For example, some systems may limit the type of devices that can be connected to a computer to a simple keyboard and mouse. Other systems may be equipped with self-encrypted drives (SEDs) to prevent data theft in the event of a laptop being lost or stolen. Although these systems may present powerful point solutions to a particular problem, they cannot protect a computer from the wide range of device interactions that are prevalent in today's rich device ecosystem.

SecureUSB™ Technology

SecureUSB™ provides a hardware solution to computer security threats that is reliable, simple and cost-effective. SecureUSB™ is configurable to obtain the desired security profile and is agnostic to the installed operating system.

How it works

Secure USB operates at the bus level of a USB system to allow or deny the operation of specific USB devices. It can also control the direction in which data is allowed to travel, i.e. from host to device or from device to host. Once configured, SecureUSB detects every USB device that may be connected to a system and monitors the traffic generated by that device. If a particular device or interaction is prohibited then SecureUSB eliminates the unwanted transmissions while permitting all other operations to occur normally. Since SecureUSB operates at the hardware level, system performance is unaffected by the security monitoring.

Restriction rules

The restriction rules provided by SecureUSB enable the level of security and the range of permitted USB devices to be selected and enforced. A typical set of rules might include the following:

1. Restrict all USB video interfaces. This prevents all webcams from being operated.
2. Restrict all USB devices manufactured by <Vendor>. This prevents any device manufactured by the specified vendor from being operated.

3. Restrict all USB mass storage interfaces. This prevents the operation of all USB flash drives, USB hard drives, USB DVD drives and similar devices. It also prevents the operation of any USB mass storage interface that might attempt to masquerade as another device – for example, a flash drive hidden inside a USB mouse.
4. Allow USB device with serial number <XXXXXX>. This overrides the general restrictions specified previously and permits the specified device to operate.

Additional rules that may be selected include restrictions based on product type, USB transfer type and data direction.

Configuration interface

The restriction rules may be set through a variety of interfaces depending on the manner in which SecureUSB is deployed. In its simplest form, SecureUSB™ may be configured by hardwiring a set of chip I/O pins at board assembly time. If more flexibility is required then the desired configuration may be programmed into a serial ROM or flash chip. If it is thought that the restriction rules may change frequently, then a networked interface can be provided but the network connection must itself be secured by alternative means.

Deployment options

SecureUSB™ is a hardware (gate-level) solution that can be deployed in a variety of ways. In discrete form, it can be implemented as an integrated circuit or FPGA inserted at the I/O bus level in a processor architecture. A typical example would be as an IC inserted between a USB host controller and an embedded USB hub. As a more integrated solution, SecureUSB™ can be combined with the USB host controller silicon or the USB hub silicon. Additional options may be available for custom applications.

Contact

Una Tech Corp.
#1805 - 1238 Seymour St.
Vancouver, BC, Canada, V6B 3N9
Phone: 1.604.715.4184
E-Mail: info@unatech.com