SanDisk Enterprise Secure USB Flash Drive Security Vulnerability

Device “CD-ROM” partition can be a host for malware and crimeware

February 2009

Introduction

After my recent experiences with the “Read Only” partition vulnerability of the MXI Stealth MXP secure flash drive, I decided to see if a similar vulnerability might exist with one of their competitors, the SanDisk Enterprise Cruzer secure USB flash drive. It turns out that the SanDisk device does in fact have a similar vulnerability that could allow the CD-ROM partition to be infected with malicious software. If this happens, a computer could be infected simply by inserting the SanDisk device into a USB port.

Comparing the MXI to the SanDisk

On the outside, the SanDisk Enterprise Cruzer device doesn’t look anywhere near as secure as the MXI device. The MXI has a large metal enclosure with a sliding mechanism. The SanDisk device has a simple small plastic housing and removable plastic cap. I was able to crack open the SanDisk device in a couple of seconds by inserting a screwdriver into the side of the case. The MXI device was more difficult to crack open, but it too yielded to a screwdriver in less than a minute.

The MXI device has a very complex interior, with two printed circuit boards housing eight computer chips and a fingerprint reader. That level of complexity concerns me, as each chip interconnect could expose a vulnerability in the circuitry or chip-to-chip communications protocols. Of particular concern is encryption key management and brute force password guessing prevention. If encryption keys or password counters are stored in the flash memory or in an external chip, it may be possible to defeat the protection mechanism by cutting wires or overwriting counters.

The SanDisk device is a much more simple device with only three chips. It uses two SanDisk NAND flash storage chips and an M-Systems S2 controller. The MXI device uses an FPGA chip and numerous off-the-shelf parts to do encryption and interface to storage, whereas the M-Systems chip inside the SanDisk device is a full custom ASIC with more functionality integrated into a single chip.

It appears that the SanDisk device stores its AES encryption keys in the flash memory itself, whereas the MXI device stores its encryption keys in a separate chip.
Figure 1a. MXI Stealth MXP
“Read Only” CD-ROM Partition

When you plug the SanDisk Enterprise Cruzer into your PC, it mounts up as if it were a CD-ROM drive. It then auto-runs the Enterprise_Launcher.exe, which requests your password and mounts the encrypted volume with your files. At first glance, this appears to be much more secure than the MXI Stealth MXP device, which mounts as a hard disk that emulates being read-only. As I discovered though, the SanDisk device has a vulnerability that allows the CD-ROM to be modified to contain any software or files that an attacker desires.

On Windows XP, I was able to temporarily write small files to the “read only” partition of the MXI device. I couldn’t do this on the SanDisk device, as it tells the operating system that it’s a read-only CD-ROM.

CD-ROM Updater

I found that despite their marketing, the SanDisk Enterprise Cruzer did not have support for the Macintosh OSX. I downloaded their updater application that would update the CD-ROM partition to add the Mac OSX support.
The updater executable is a self-extracting archive that unpacks a folder full of software, disk images and DLLs into a temporary folder on the PC. I copied this temporary folder and took a look into what’s in the updater.

What you can see in Figure 2 is that there is an Updater.exe application, a file that acts as a manifest that tells the Updater which files to write to the CD-ROM partition, and a number of files and DLLs.

I was impressed to see that many of the files had a .sig file, which contains a digital signature of the file. This, combined with a secure hash of the contents of the files, can prevent unauthorized or tampered files from being added to the CD-ROM partition.
I took a look into the UpdaterAuthFile.txt, and it lists the files that the Updater uses. It’s effectively a manifest of how to update the device and which files to load onto it. See Figure 3.
I decided to take a look at one of the signature .sig files. I looked at the text strings inside the file XKEYCD.ISO.sig. What you can see here is that the certificate used to sign the files in the updater folder appears to be issued in Israel. A collocation facility appears to be referenced Israel.emikolo.com/CertEnroll. It also appears that Seaside Software is mentioned, as an email address is referred to ittai@exchange.seasw.com
This appears to be a legacy from 2003, when M-Systems partnered with Seaside Software to build an “X-Key” product. From an October 14, 2003 press release, the X-Key is

“a key-sized appliance for Microsoft Exchange(R) users. The Xkey packages the mobility and computing power of the Smart DiskOnKey(R) platform with Seaside's Portable Web Services Software.”

Here a press release describing the X-Key partnership:


SEC filings indicate that M-Systems acquired Seaside Software in November of 2004.

http://www.secinfo.com/dRACe.11z.htm

In July 2006, SanDisk announced that they were acquiring M-Systems.
Missing Digital Signatures

After looking at the list of files, I realized that several of these files didn’t have .sig digital signature files. For example, none of the DLL files have .sig files that correspond to them, yet these files are listed in the UpdaterAuthFile.txt file.

This made me wonder if perhaps the Updater.exe didn’t actually check the digital signatures to ensure the correctness of all the files.

To test this, I decided to create my own CD-ROM disk image and see if I could update the “read only” CD-ROM on my device.

Creating My Own CD-ROM Image

What I decided to do was to copy the files from the CD-ROM image of the device into a folder on my computer. I then added some files that simulated malware on the device.
It took me a few minutes of googling around to figure out how to create an ISO image of the folder. ISO images are the format that you write to a CD-ROM. Once I created my ISO image, I decided to simply rename it to the ISO image that the Updater.exe loads onto the device (XKEYCD.ISO). To prevent the Updater.exe from detecting that the file had been changed, I simply deleted the XKEY.ISO.SIG file.

Loading My Own ISO Image Onto the “Read Only” CD-ROM

I then ran the Updater.exe program. It formatted my device, then loaded my ISO image onto the device. It did not issue any warnings that the CD-ROM image was not digitally signed, nor did it detect that the image had been modified. So, it was clear that the Updater does not check the digital signatures.
Format Warning

The formatting process erases all existing data on your Cruzer Enterprise. Please back up any important files to another storage device.

Format >  Cancel

Format Warning

Formatting your Cruzer Enterprise...
Now, the CD-ROM partition of my SanDisk Enterprise Cruzer secure flash drive contained the malware simulation files. When I plug in the device, it runs the files stored on my version of the ISO image, proving that the SanDisk hardware does not check for a digital signature of the software and files stored on the CD-ROM image. This is a pretty serious security hole, and allows malware or attackers to put whatever files or programs they want onto one of these devices.
SanDisk Installs Software On Your Computer Every Time The Device Is Used

During the course of this investigation, I noticed something very strange. It seems that the Enterprise_Launcher.exe application is actually an unpacker, which unpacks a file called Exmp.zip. This unpacks a set of software, images and DLLs into a temporary folder on the host computer. It then runs the actual unlocker application, which is called ExmpSrv.exe, from the temporary folder on the host computer. A quick google of ExmpSrv.exe shows that this is also the way that the Kingston Data Traveler Elite Privacy Edition secure flash drive uses this same process. That’s because the Kingston device is actually an OEM of the SanDisk Enterprise Cruzer device.

Figure 8. SanDisk Enterprise Cruzer Installs Software Every Time It’s Used

I’m a bit concerned that this device actually unpacks a .zip file of software, images and DLLs onto your device every time you plug it in. Firstly, this is pretty unhygienic for a security device. Secondly, it seems to open an attack vector whereby an attacker can modify the application and its DLLs, and re-create the Exmp.zip which could then be burned onto devices. If this happened, it would be extremely difficult to detect. A modified launcher could send a user’s device password over the Internet to a remote attacker when the user unlocks their device. Worse still, the application could be
modified to send private files from the unlocked device over the Internet to a remote attacker. Finally, it would also be possible for a modified application to install sophisticated Trojans and crimeware on the user’s computer.

Publicly Available Hacker Tools for Attacking SanDisk U3-based Flash Drives

The now-discontinued U3 software from SanDisk uses this same mechanism of unpacking and running the actual unlocker into a temporary folder on the host computer every time the device is plugged in and used. The Updater manifest file UpdaterAuthFile.txt does have a file called u3dapi10.dll, which lends evidence that the Enterprise Cruzer device family uses U3 technology. If the SanDisk Enterprise Cruzer is based on U3 technology, it is very concerning, as there are several tools for hacking U3 “smart flash drives” available on the Internet.


http://www.u3community.com/viewtopic.php?t=434

I have not tried these tools yet on the SanDisk Enterprise Cruzer device, but if it’s based on U3 technology, there could be a whole set of hacker tools readily available for any attacker or malware author. Here are links to several suites of USB malware tools.

http://www.usbhacks.com/2006/10/07/usb-switchblade/

http://wiki.hak5.org/wiki/USB_Hacksaw


Expired Certificates and Digital Signatures

It appears that the makers of the software attempted to protect their Enterprise_Launcher.exe program by digitally signing the application. It honestly appears to me though that the makers either don’t fully understand security, or the employees who did understand it have left the company. The certificate used in the digital signature was not issued by any known or trusted Certificate Authority. Furthermore, the certificate expired in September 27, 2007. The certificate was issued to einatm@m-systems.com
A recent development in the global security market is the emerging requirement for trusted supply chains. In the last year the FBI has investigated fake Cisco routers being manufactured by Chinese clone outfits. There are also concerns around back-doors and kill-switches being added into products during their manufacture, unbeknownst to the vendor.

A concern that I have with the SanDisk Enterprise Cruzer allowing any ISO image to be written to their “Read Only” CD-ROM partition is that there is no way to assure a secure supply chain from the factory to the customer. If an attacker were to work at a reseller, distributor or even at a package delivery service, they could modify the device software before it ever reached the customer. I was able to modify the software on my device’s “Read Only” CD-ROM partition, and I had never even set up the device. I could simply put it back in its package, and deliver it to a customer as a brand-new device.

**Trojan Devices**

A real world vulnerability that must be considered is that of Trojan devices. The attack goes like this: infect a USB flash drive with a self-installing Trojan that gives an attacker remote access into a company or government network once it’s installed on an internal computer. Then leave these drives in the parking lot of the company or agency that you wish to attack. Inevitably, some well meaning employee will find an infected device, and will insert it into the USB port of an internal computer, thus compromising internal security controls.

Steve Stasiukonis of Secure Network Technologies Inc. did exactly that in the parking lot of a credit union where his firm had been hired to perform a security audit. Of 20
infected USB flash drives that they planted in the company parking lot, 15 of them had been found and plugged into internal credit union computers within 3 days.

http://www.darkreading.com/security/perimeter/showArticle.jhtml?articleID=208803634

This attack vector has been seen in the wild in London UK, where infected USB flash drives were used to collect online banking usernames and passwords of consumers who found the devices on trains and in taxis.


If an enterprise or government agency were to standardize on the current version of the SanDisk Enterprise Cruzer device, they would still be vulnerable to Trojan devices. An attacker or disgruntled former employee could infect the “Read Only” CD-ROM partition of a device with Trojan malware, and leave the device in a parking lot, or even give it to the front desk receptionist claiming it was found in the parking lot. Once an employee or even internal IT security administrator plugged the device in, or ran a modified version of the Unlocker.exe software, their computer would be infected.

Summary

The SanDisk Enterprise Cruzer device is a hardware-encrypted USB flash drive originally developed by M-Systems and Seaside Software in Israel. It appears that there had been some thought put into protecting the CD-ROM partition from being infected with malware or other unauthorized software. Unfortunately it appears that the developers either didn’t understand security fully, or that the security developers have left the company. There are vulnerabilities regarding digital signatures that are not checked, use of expired certificates with no known chain of trust, and messy installation of software on every insertion of the device.