Back to my other projects

Hacking U3 Smart USB Drives

Wesley McGrew wesleymcgrew@gmail.com

Updates! (latest ones first)

October 27th, 2006:

Since most of you are coming to my pages through this writeup, I'll go ahead and link you to my blog that i just remembered that I had from here too. If you liked this writeup or my other projects, you might enjoy other things I have to say.

New for July 20th from an anonymous source:

> U3 and the hardware sellers are trying to agree on how to keep the users' data safe during manipulation, like perhaps enable locking of at least one partition from being messed with. Once agreed, they consider giving away a tool that will enable a limited set of smarter manipulations on the device. The tools for full repartitioning are going to be kept in house for security reasons (so a plugged key cannot be scratched by malware on the host). Such tools are still only made available to vendors. (My personal opinion as a computer guy has always been the same - security by obscurity never holds for too long...)

I have another report that after running U3-Uninstaller.exe, the drive was no longer recognized by LPInstaller.exe. So please don't attempt this unless you've got a quick and easy way of getting a replacement, or if you're just experimenting before wiping out U3 anyway, or if you're feeling particularly adventurous. GrangerX verified that he was still able to install after uninstalling and provided the following notes (also note the URL for the official U3 uninstaller, http://www.u3.com/uninstall):

```
The U3 Drive i'm using is:
SanDisk Cruzer(R) Micro USB Flash Drive
SDCZ6-512-A10
UPC: 6 19659 02536 6
(serial number censored)

My OS is WinXP SP2, with all but the latest Windows Updates.  The PC
is a Via Chipset Athlon (Sempron?) Socket462 freebie from the weekly
Fry's "buy a CPU, get a motherboard effectively free" deal.

The utilities I used had the following MD5s:

352bca7784d8dc68503379ff8cf46700 *u3_uninstall.exe #u3 branded, from
http://www.u3.com/uninstall

3f8ea63524f0c8339c34c6851f6ae8a6 *U3_Uninstaller.exe
#geeksquad-branded, from ... someplace on the internet

bc7c03b841864bb9ce30dd5429359cdd *cruzer-autorun.iso

36b872f94e88d9bbf266200c193e50f4 *LPInstaller.exe

After running the uninstaller (and removal, reinsertion of the drive),
the CD drive portion disappeared.  The RemovableDisk partition size
increased by the 6MB.
After running the installer, which didn't seem to require re-insertion
of the drive, the U3-CD-Partition reappeared, and the RemovableDisk
was the normal (-6MB) Size.
```

GrangerX, grangerx@gmail.com, wrote in with the following very helpful information:

> **...**
>
> **The utility "LPInstaller.exe" seems to be able to download two different ISOs, one with autorun, one without (at least the URLs were in the file, so I went ahead and grabbed both). *Also, if you put the ISOs in the same directory as the LPInstaller.exe, it seems to use them from there instead of trying to download them, which is faster, and doesn't require apache usage.***
>
> **There also exists a much harder to find executable, called "U3-Uninstaller.exe", that disables the CD "domain" (i think is U3's internal terminology for the different areas on the drive (I *wish* they'd release the darn HDK)) by (apparently, at least) burning the "dummy.iso" file into that domain, and then hiding/disabling the domain entirely (free space before was: 506,683,392 ; free space after was: 513,310,720). [Yes, several of their internal (debugging?) messages in the EXE files and their SDK docs mention "Burning" the CD ISO, so I guess it really *is* a burner, of sorts. :-p]**
>
> **My end goal is to be able to use a larger-than-6MB iso, which currently, I haven't been able to do. But, I have verified that the two utilities ("LPInstaller.exe" and "U3-Uninstaller.exe" are repeatably usable to remove/re-add the U3 functionality, so it should be safe for people to experiment with, if they have both utils *(Note: I've heard from others that this does not work, so be cautious)*. If you try to trick it into using a larger ISO, both utilities fail, but it doesn't seem to cause trouble once you run the utility as they intended. I can add or get rid of the U3 functionality as needed now, at least.**
>
> **My hope is that there's an offset in the LPInstaller.exe that one could patch and it would create a differently-sized ISO area, which could allow more clever things to be done with the devices.**
>
> **Anyway, thanks for getting things started. Hopefully they'll release at least the oft-referenced "U3 Tool" to allow users to modify their drives, but until then, it's fun to hack on.**

So a lot of the steps I've outlined below are actually a bit more complicated than you really need to do. The Sandisk installer looks in the local directory for ISOs first, so you won't have to spoof their website anymore ;)

A spy came in from the cold to write this (completely unverified, of course, but feels right):

> ***:snip snip:*...new controller at the hardware level, where it supports 24 more USB commands than the regular controllers, etc. apperently dividing it up to "memory domains" is dynamic and there are tools out there (windows only) for the manufacturers to resize the virtual CD and the main partition.*:snip:***

Thank you Agent Hanks :)

~~ATTENTION GEEKSQAUD~~

~~Someone on the geeksquad forums needs to either let me register an account or paste me the contents of this thread that's linking here:~~

~~http://forum.geeksquadforums.com/viewtopic.php?t=22998~~

~~I'd like to know what the geeks are saying about me ;)~~

HELLO FRIENDS FROM SANDISK

```
[Tue Jun 13 20:32:01 BST 2006] xx.xx.xx.xx
/~rwm8/hackingU3/
https://owa.sandisk.com/exchweb/bin/redir.asp?URL=http://cse.msstate.edu/~rwm8/hackingU
Mozilla/5.0 (Macintosh; U; PPC Mac OS X; en) AppleWebKit/418 (KHTML, like Gecko) Safari
```

Mac users even! Must be the legal department ;)

Introduction

U3 is a platform for developing applications that install to and execute from USB flash drives. It provides these applications a means to execute, read, write and clean up after themselves once the drive is removed. I haven't actually used any U3 apps yet, but having bought a "U3 Smart" drive at OfficeMax (the SanDisk Cruzer Micro 512M), I became interested in the unique way these U3 drives present themselves as two separate disks, so that the U3 software is write-protect and can auto-run on Windows machines. This page documents my attempts at changing the U3 drive to modify the write-protected partition and control the autorun feature.

Disclaimer

This information is based on the U3 Smart SanDisk Cruzer Micro 512M, and while I've taken a lot of care in my procedures here (I don't want to buy another drive if I brick this one either!), I can't guarantee that it'll work out so well for you. This information is immediately applicable to the Cruzer Micro 512M, and probably works for other Cruzer disks, but probably does not work on other U3 Smart disks. It should get you looking in the right direction though.

Two Drives in One!

The first thing you'll notice when you plug in one of these drives is that it shows up as two different disks: A USB CDROM with the title "U3 System" that takes the first available drive letter (E: in my case), and a USB Removable Disk that takes the next drive letter (F:).

More detailed information can be found when you plug it in under Linux and take a look at dmesg:

```
usb 1-1: new full speed USB device using uhci_hcd and address 6
usb 1-1: configuration #1 chosen from 1 choice
scsi7 : SCSI emulation for USB Mass Storage devices
usb-storage: device found at 6
usb-storage: waiting for device to settle before scanning
  Vendor: SanDisk   Model: U3 Cruzer Micro   Rev: 2.15
  Type:   Direct-Access                      ANSI SCSI revision: 02
SCSI device sdb: 990865 512-byte hdwr sectors (507 MB)
sdb: Write Protect is off
sdb: Mode Sense: 03 00 00 00
sdb: assuming drive cache: write through
SCSI device sdb: 990865 512-byte hdwr sectors (507 MB)
sdb: Write Protect is off
sdb: Mode Sense: 03 00 00 00
sdb: assuming drive cache: write through
 sdb: sdb1
sd 7:0:0:0: Attached scsi removable disk sdb
sd 7:0:0:0: Attached scsi generic sg1 type 0
```

```
  Vendor: SanDisk   Model: U3 Cruzer Micro   Rev: 2.15
  Type:   CD-ROM                             ANSI SCSI revision: 02
sr0: scsi3-mmc drive: 8x/40x writer xa/form2 cdda tray
sr 7:0:0:1: Attached scsi CD-ROM sr0
sr 7:0:0:1: Attached scsi generic sg2 type 5
usb-storage: device scan complete
```

Note that Linux seems to think the CD drive is a writer. Working on the side of caution against hosing the drive, I have not attempted to "burn" to this drive with cdrecord or k3b or anything. This is doubly true now that I have found a safe way of changing what's on this part of the disk, but if you want to give it a shot (and have a spare Cruzer to try it out on), email me and let me know what happens ;). There's a pretty good possibility that it's not identifying the drive correctly.

The CDROM that isn't

When you mount the CD drive, there's three files waiting for you: LaunchPad.zip and LaunchU3.exe (containing the U3 software), and an autorun.inf that executes LaunchU3.exe whenever you plug in the drive. Here's the contents of the autorun.inf after running the latest updates from SanDisk (More on this later):

```
[AutoRun]
open=LaunchU3.exe -a
icon=LaunchU3.exe,0

[Definitions]
Launchpad=LaunchPad.exe
Vtype=1

[CopyFiles]
FileNumber=1
File1=LaunchPad.zip

[Update]
URL=http://u3.sandisk.com/download/lp_installer.asp?custom=1.1.0.2&brand=cruzer


[Comment]
brand=cruzer
```

So, we see that it automatically runs LaunchU3.exe. There's a few other bits of information in this file that are handy too, especially the [Update] section, which wasn't there before the built-in updating feature of U3 was executed...

Updating means that *something* can write to it at least

Let's visit the SanDisk updating URL in Firefox:

Welcome to the SanDisk U3 Launchpad Installer

The SanDisk U3 Launchpad ActiveX Installer requires Microsoft Internet Explorer 5.0 or higher.

Whups, heh, let's view the source...

```
<OBJECT id="InstallLPCtrl"
        classid="CLSID:8BC53B3O-32E4-4ED3-BEF9-DB761DB77453"
        codebase="http://u3.sandisk.com/download/apps/LPInstaller.CAB#version=1,0,0,12"
        style="display: none"
        VIEWASTEXT>
        <span class="style2">The Launchpad Installer ActiveX Control did not SUCCESSFULLY
        <a HREF="http://u3.sandisk.com/download/apps/LPInstaller.exe"><img src="../img/u3
</OBJECT>
<script>
```

There we go. A URL for a stand-alone installer. When you download this installer, you'll notice that it's only a megabyte or so, while the CDROM drive is between 5 and 6 megabytes. This is because the LPInstaller.exe downloads the new ISO file for the CDROM from the SanDisk website. Let's fire up Ethereal, start sniffing, and run the installer to figure out where it's getting the ISO from:

```
⊟ Hypertext Transfer Protocol
  ⊞ GET /download/apps/lpinstaller/isofiles/cruzer-autorun.iso HTTP/1.1\r\n
    User-Agent: SanDisk HTTP Manager\r\n
    Host: u3.sandisk.com\r\n
    Connection: Keep-Alive\r\n
    \r\n
```

From here, you can download the ISO with wget or a web browser or anything. Mount the ISO and you'll see the same files (or potentially newer versions) as you would on the drive's CDROM.

The Sting

Make your own ISO, keeping within size limitations. Regarding this, although the ISO I downloaded from the SanDisk site was 5,752,832 bytes, the size of the CDROM images I get when I use dd straight from the block device is always 6,291,456 bytes. It appears the ISO is written into this 6,291,456 byte chunk, with the remainder padded out with zeros.

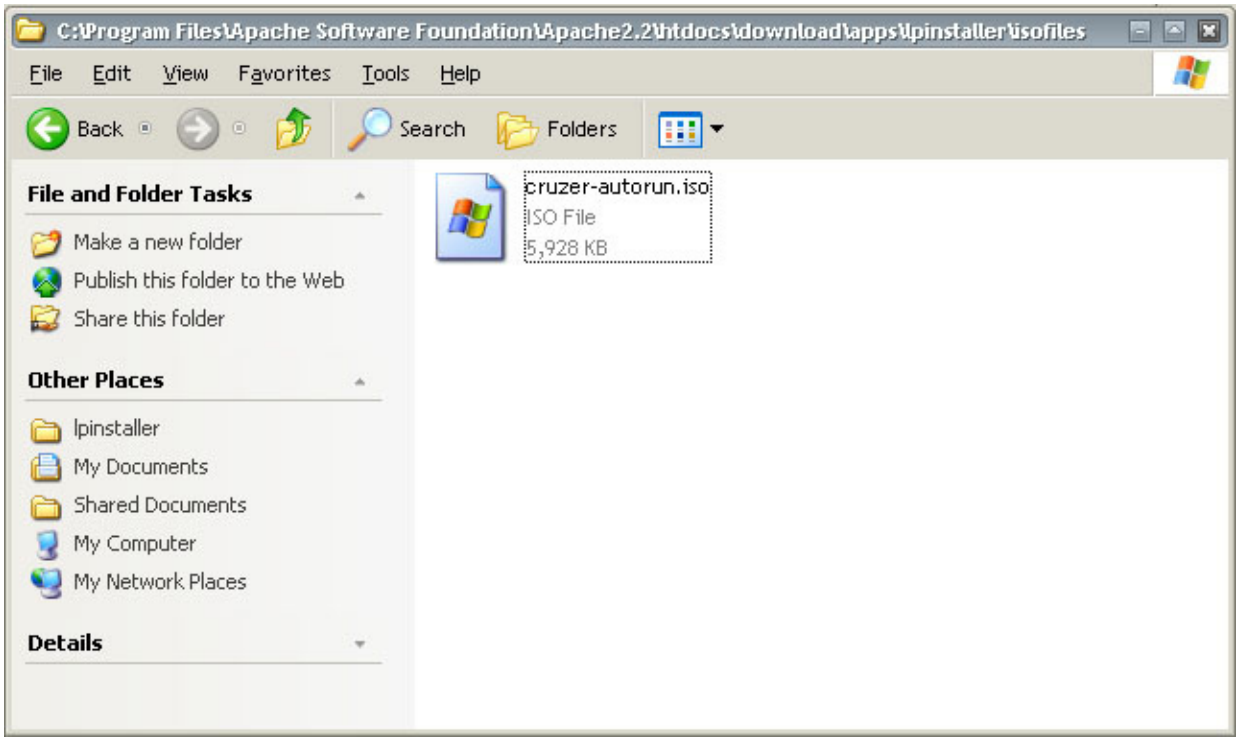
Double-plus-make-sure that the ISO you create is a bit less than 6,291,456 bytes. I don't know what will happen if you go over that amount, but there's a very good chance that it isn't pleasant.

Some good ideas for what you could do with the fake CDROM drive:

- **Do away with the U3 software entirely**
- **Auto-run your own programs/scripts**
- **iPod sneakiness without an iPod**
- **Store files that you want relatively strongly write-protected**

You can create ISO files using mkisofs from cdrtools, or any burning software you would like to use.

Once you have an ISO created, you'll need to set up a web server to mimic the update site. Here, I've installed Apache onto the windows machine running the installer, recreated the directory structure leading up to the ISO, and placed the custom ISO there with the correct name:



Next, change the c:\Windows\system32\drivers\etc\hosts file to point u3.sandisk.com to the correct ip address, in this case, the local host:

```
127.0.0.1       localhost  u3.sandisk.com
```

Now that everything's set up, you can run the LPInstaller.exe, and let it download and install the ISO you want to the disk. If everything goes well, the next time you mount the disk, it should be set up how you wanted it.

Taking it further

The above works for SanDisk Cruzers, so if you're feeling adventurous, you may be able to develop a similar procedure for other U3 Smart disks. It would also be nice to figure out how the installer is talking to the disk, so that a program could be created to let us more directly manipulate the disk, without having to spoof a web server.

Questions/Comments/Donations

If you have any questions or comments, email me at wesleymcgrew@gmail.com. Donations of broken/bricked/spare/extra USB keychains using U3 or similar technologies to tinker with are welcome ;).