U3 USB Stick (In-)Security

Q2/2007 by Martin Suess, martin.suess@csnc.ch

USB Sticks with the U3 feature threaten the security of workstations and the enterprise infrastructure.

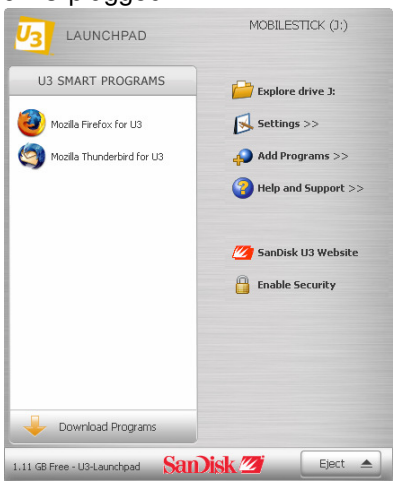
A technical analysis about the U3 technology on USB sticks and mitigation approaches for personal usage as well as enterprises.

Introduction

USB memory sticks can be found almost everywhere. Today, they can be seen as the replacement for floppy-disks, ZIP-drives and all that kind of media. Nearly unnoticed, many of todays memory sticks contain the two characters "U3" in a symbol on the backside. Where is the difference to the old fashioned USB sticks? Do they bear any risks?

The U3 Technology

A U3 USB Stick is a normal USB memory stick on first sight. Additionally it emulates a CD ROM drive with around 6MB of space. Any computer will recognize a USB disk drive and a USB CD ROM drive when this stick is plugged in.



The U3 technology was developed by U3 [1], a joint venture of SanDisk and other memory vendors. U3 was created to be able to have Windows applications and their configurations always ready to run from a USB stick. Applications which are enabled to run from a USB stick are called "Portable Applications".
The U3 capable USB sticks contain a LaunchPad.zip, a LaunchU3.exe and an autorun.inf file. When the stick is plugged in, the Windows autostart feature reads the autorun.inf file like on other CD/DVD ROMs and starts the U3 launcher application. The U3 Launchpad emulates a Windows-like start menu and controls the installation and program start of portable applications. The systems do not have to be modified and the autorun feature for CD/DVD drives is enabled by default on Windows systems. The application which is run by the autostart feature is executed with the current user.

Applications may access local files and registry information but they are removed when the stick is ejected properly.
Windows stores a few information bits in the registry for every USB device which is plugged in under the following registry key: *HKEY_LOCAL_MACHINE\System\CurrentControlSet\Enum\USB*

But wait a second, ...

...you can also use the Windows autostart feature with a normal USB stick, so what's the big deal?
To automatically start an application from a normal USB stick, the Windows registry has to be changed (described later in this article). By default, Windows only autostarts from CD/DVD ROMs. Since U3 sticks emulate a CD ROM, the application will be started by default.
In short, a Windows has to be changed to **allow** autostart from removable devices but has also to be changed to **deny** autostart from CD/DVD drives.
By the way: The autostart feature does not work on Windows XP/2k when the screen is locked.

Modifications

The Official Way

The vendors of the USB sticks offer updater applications which allow updating the firmware of the emulated CD ROM on the U3 Stick. In case of SanDisk, the updater is named LpInstaller.exe and fetches the most recent ISO file cruzer-autorun.iso from the SanDisk website. The content of the CD ROM space is then replaced with the files contained in the ISO file.

Pimp my USB Stick

Before the updater of SanDisk downloads the ISO file, it tries to find the ISO locally in the same folder as the updater is started from. A hacked ISO may be put on the stick when the desired content is put in an ISO named exactly like the official ISO. The ISO size must not exceed 6'291'456 bytes in order to work.

Another way is to set up a web server locally and redirect the request for u3.sandisk.com to the local web server using the hosts file.

The autostart feature automatically runs the application defined in the autorun.inf. This file may be adapted to run malicious code.

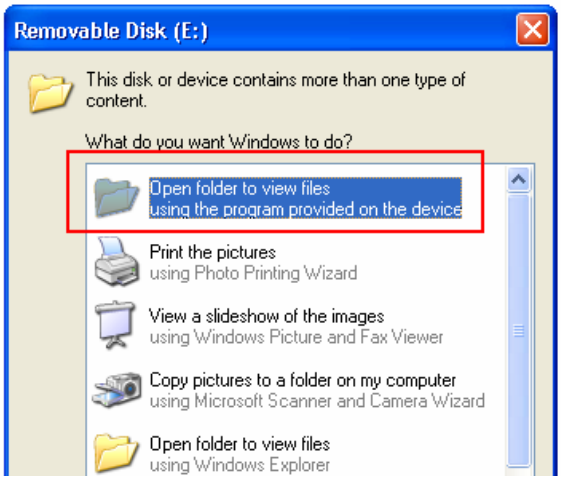
The stick may be changed in a way that the autorun starts the malicious code which then starts the official launcher application stored on the memory stick drive. This way it is hard for a user to determine the difference between a normal U3 stick and a modified one.

Since nearly no evidence is left on the machine, it is hard to track such malware. A virus scanner might detect known malware when the stick is plugged in through on-access scans. The virus scanner may also be started manually to search the drives.

When a USB stick drive it is plugged in, Windows will, by default, ask which action to execute. Such actions can be defined with an additional autorun.inf on the USB stick:

```
[autorun]
icon=folder.ico
open=evil_hack.bat
action=Open folder to view files
shell\open\command=evil_hack.bat
```

What happens when you plug in a stick prepared like this? Autorun starts the following dialog:



Please notice that the Windows default entry to view the folder content also appears further down in the list. Clicking on the injected command executes the batch file evil_hack.bat in this example. The last line of the autorun.inf file causes the evil_hack.bat to be executed when a user double-clicks on the drive in the drive overview (under "My Computer") and even works when autostart is disabled:

This technique clearly aims on social engineering but also works for normal, non-U3, USB sticks.

Small, Yet Powerful

Using the possibilities of this new technology, many scenarios come to mind. Let's have a quick thought on the options:

1. A memory stick which is prepared to gather information on every machine it is plugged in and executed. The information is packed and stored on the stick. The software could steal passwords, confidential documents and more. Nearly no evidence remains on the system - a forensic nightmare. This is also known as pod-slurping [5].

2. The stick could contain a program that installs itself on every system it is plugged in and executed. Once it is installed on the system it could monitor users, copy data from the system and memory sticks which are plugged in later. This stick could be plugged in at the Internet Café around the corner. The data could easily be packed and sent over the Internet.

3. Similar to the second scenario, a stick could be used to bring a trojan into a company which tries to open a tunnel to the attacker through various channels.

4. When an attacker wants to own a bot network. He visits various Internet Cafés with his U3 USB stick containing a self-

install bot and infects the PCs there. He is then able to control these machines.

These are only four out of dozen of possible scenarios.

Ready, Set, Go - Available Packages

The worst is yet to come: There are packages which are built exactly for the purposes named above. And they can be downloaded for free.

One of these packages is the so-called "USB Switchblade" developed by the group Hak.5 [4]. It is made to silently "recover" information from a target Windows computer, including password hashes, LSA secrets, IM passwords, IP information and more. It requires a Win2k/XP/2k3 system and a user with administrative privileges and physical access but its payload can run silently and without modifying the system or sending network traffic, making it near invisible.

Another package by Hak.5 is the "USB Hacksaw" which automatically infects Windows PCs. Once it is installed it will retrieve documents from USB drives plugged into the target machine and securely transmit them to an email account. Even automatic propagation to other USB devices is possible.

What happened so far?

More and more incidents involving USB sticks can be read in newspapers. In one case, a Dutch officer lost his USB stick in a rental car and then got into the hands of a Dutch newspaper. The USB stick contained confidential information like secret entrance codes to a diplomat's home and the names of bodyguards…
A security analyst posted an article [3] about one of his jobs. He got hired by a financial institute for a penetration test. He gathered promotional USB sticks and copied a self written trojan on each of the sticks. One day, early in the morning, he dropped 20 of those sticks around the financial institute. Within three days, 15 sticks were found and all plugged in and the trojans were executed…
In January 2007 the British security group NCC sent 500 modified USB sticks to financial directors of British companies [13]. The USB sticks where covered as invitations for an event and automatically started a website when they were plugged in. According to NCC, more than 47% of the managers plugged the sticks in and the website was opened…

Mitigation Approaches

So how can someone get rid of those risks? Most of us would not want to miss the ease of use that USB sticks provide, would we?

There are multiple approaches which should be combined:

- Policies
- Technical Solutions
- Education

Policies

A few basic rules may save a lot of trouble. Release rules in your IT Policy to restrict or forbid the usage of USB devices generally or USB sticks only.

Keep sensitive data strongly encrypted. This makes it a lot harder - if not impossible - for a data thief to gain anything from stolen information.

Be restrictive with giving away your USB stick and accepting sticks from other people.

Technical Solutions

Disabling USB Devices

If you do not need USB devices, disable the USB port generally. For some devices, this can be done in the BIOS settings. In Windows, USB mass storage devices can be disabled through the registry.
The following image shows the registry key *HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\USBSTOR*:

Name	Type	Data
(Default)	REG_SZ	(value not set)
DisplayName	REG_SZ	USB Mass Storage D
ErrorControl	REG_DWORD	0x00000001 (1)
ImagePath	REG_EXPAND_SZ	system32\DRIVERS
Start	REG_DWORD	0x00000004 (4)
Type	REG_DWORD	0x00000001 (1)

USB mass storage devices can be disabled by changing the DWORD value of *Start* from 3 (enabled) to 4 (disabled).

The permission of this key has to be changed. Deny Full Control to the System group. Otherwise, when adding new devices, Windows will change the DWORD to the default value (3) again. The permissions can be changed in the registry editor by right-clicking on the folder where the registry key is located and selecting "permissions".

Thirdparty Tools

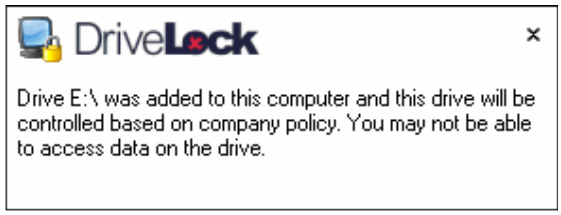
If some devices or whole device classes are needed, consider using specialized software to whitelist these trusted devices.
Such tools use fingerprints of USB devices (Device ID) to identify them. So far, no way to fake these device IDs is known to Compass. The programs allow a centralized device management (AD, MS SQL) and policies may be applied based on domains, groups or users.

There are various third party products available which allow tightening the endpoint security in an enterprise in different ways. Some of the tools are listed here:

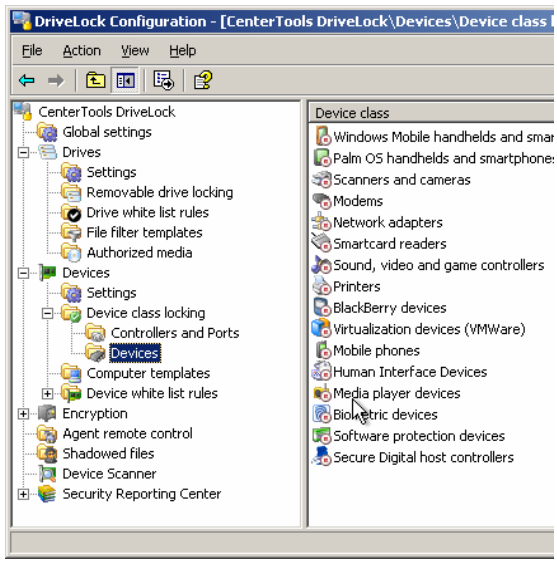
- GFI EndPointSecurity [10] can be embedded and configured through Active Directory and allows group-based permissions. It controls only whole device categories and not single devices.
- CenterTools DriveLock [12] can be embedded in Active Directory and allows an alternative configuration through configuration files. It allows various kinds of configurations based on users, groups, device identifiers or combinations.
- Smartline Device Lock also supports Active Directory and an optional Enterprise Server can be used to store audit logs and more on a MS SQL server.
- Safeend Protector [11] also integrates with Active Directory and allows policy definitions based on users, computers or groups.

DriveLock

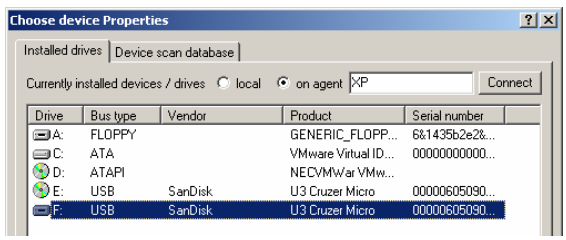
We installed an evaluation version of CenterTools DriveLock to show some features here. After installing and (very) basic configuration, plugging in a USB device causes this message to appear and the disk cannot be accessed:



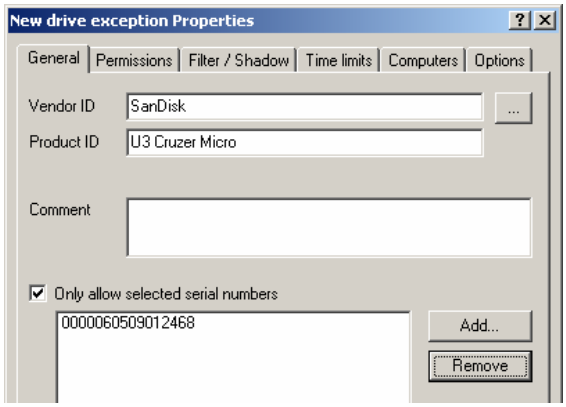
The following picture shows the administration interface of DriveLock. It contains not only options drive and device blocking but also for encryption, shadowed files and a device scanner.



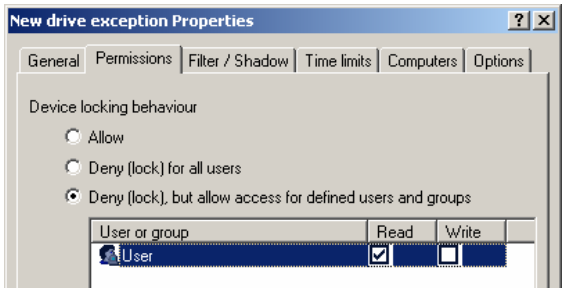
In an enterprise it might be necessary to allow certain USB sticks and it is still not desired that any stick may be used. DriveLock allows defining the allowed USB sticks very precisely.



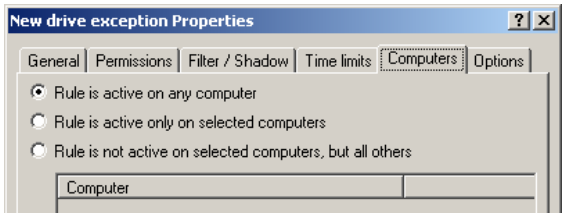
It is possible to allow a whole Vendor / Product ID group (e.g. SanDisk U3 Cruzer Micro) and/or only specific devices which are defined by their serial numbers:



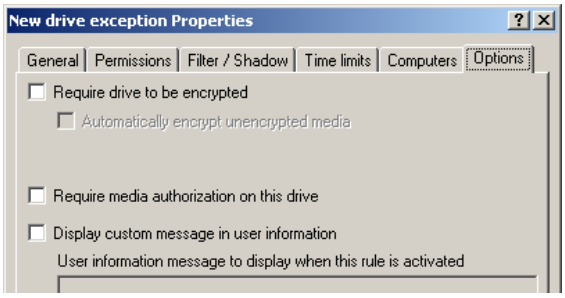
The permissions can be set for users or groups and read and write access can be specified.



Additionally, the configured settings can be distributed and applied to specific (or all) other computers.



Finally, it is also possible to require encrypted disks, show user messages and more.



To disable the U3 part of a USB stick but still be able to use the stick itself, an enterprise could use a third party software to disable all CD ROMs except a few whitelisted ones that are actually used.

Autostart Feature

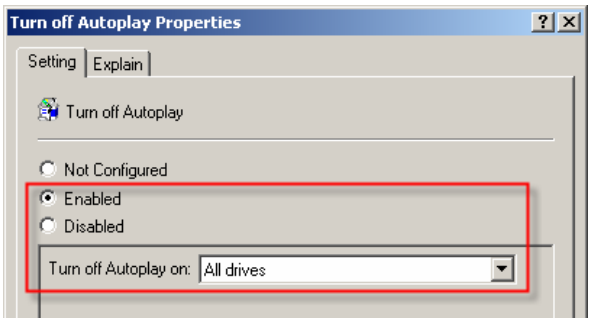
It is helpful to disable autostart feature for all devices and not only for CD ROMs. Please keep in mind that this does only prevent the autorun feature to start a program automatically. There is still a high risk since it takes the user only one wrong click to start some evil program.
The according registry for Windows XP is:
[HKCU or HKLM]\Software\Microsoft\Windows\CurrentVersion\Policies\Explorer\NoDriveTypeAutoRun

The following table explains the meaning of the bits of the DWORD value (bit set means disabled):

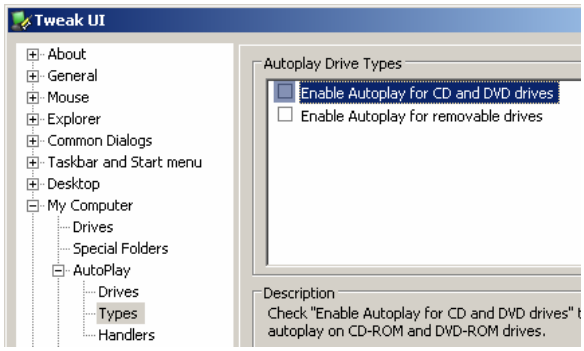
DRIVE_UNKNOWN	0x01
DRIVE_NO_ROOT_DIR	0x02
Removable Drives	0x04
Harddiscs	0x08
Network Drives	0x10
CD/DVD ROM	0x20
RAMDISK	0x40
Unknown drive type	0x80
All drive types	0xFF

When the key is set in HKLM, a similar key in HKCU is ignored. Also see the Microsoft website [9] to get more details.

This can be done through the Group Policy (GPO) and locally. The following picture shows the modified GPO setting (*Computer Configuration > Administrative Templates > System > Turn off Autoplay*):



Microsoft's TweakUI also supports this setting but only controls CD/DVD and removable drives.



Select *My Computer > AutoPlay > Types* and uncheck both entries. This will disable the autostart feature for both CD/DVD drives and removable drives.

Inherited from older operating systems, another registry key to enable and disable autostart from CD/DVD ROMs can be found here:
HKLM\System\CurrentControlSet\Services\CDRom\AutoRun

The value can be set to 0 (autostart disabled) or 1 (autostart enabled).

Manual Prevention

If you are not sure whether or not the autostart feature is disabled, press SHIFT while plugging in a (U3) USB device. This disables the autostart feature temporarily. From the security point of view it is a little bit risky to rely on a single button press though…

Getting Rid Of U3

U3 sticks also support removing the emulated CD ROM on the USB stick. If you use U3 sticks personally or in your enterprise and you want to get rid of the CD ROM part, use the removal program of the manufacturer or U3. The program can be found on the U3 website [1].

After the removal, you will have roughly 6MB of additional space on your memory stick to use.

Test the technical solutions applied to make sure they are working.

Education - Prevent Social Engineering

Along with releasing a policy and implementing a technical solution it might be helpful to tell the people concerned what the risks are and why those measures have been taken. A demonstration shows the risks and how an incident could affect the company.

Finally…

... there is one more threat which is not subject of this paper but shall be part of further research: USB driver exploits. They are even more threatening because they give access to local system privileges and are way harder to detect. Best solution for now: Update system regularly or even better, disable USB functionality on your system.

About the Author

Martin Suess completed his studies for BS in Computer Sciences in December 2004 with his diploma thesis in the fields of ZigBee networks in Singapore. During his studies he concentrated on IT security, as well as on network and Internet technologies. After his study, he worked on Bluetooth- and embedded-projects at the University for Applied Sciences in Rapperswil. At the same time he coached student projects as well as tutorials in "Algorithms and Datastructures in Java". He joined Compass Security AG as a full time security analyst in January 2006.

martin.suess@csnc.ch
http://www.csnc.ch/

About Compass Security

The Job of a security specialist is like searching in the fog. The more opaque the environment the harder it is to find traces and establish methods and tactics. A good compass can help to determine the direction and choose a path that will securely lead to the destination.

Compass Security Network Computing AG is an incorporated company based in Rapperswil (Lake of Zurich) Switzerland that specialises in security assessments and forensic investigations. We carry out penetration tests and security reviews for our clients, enabling them to assess the security of their IT systems against hacking attacks, as well as advising on suitable measures to improve their defences.

Compass Security has considerable experience in national and international projects. Close collaboration with the technical universities of Lucerne and Rapperswil enable Compass to carry out applied research so that our security specialists are always up-to-date.

Credits

Thanks to all Compass Security members who helped me writing this paper through reviews and coming up with new ideas.

References

[1] U3 Developers Homepage
http://www.u3.com/
http://www.u3.com/uninstall/

[2] SanDisk, USB Stick Manufacturer
http://www.sandisk.com/

[3] Social Engineering, the USB way
http://www.darkreading.com/document.asp?doc_id=95556&WT.svl=column1_1

[4] Hak.5 - Wiki
http://www.hak5.org/wiki/

[5] Pod Slurping
http://www.sharp-ideas.net/pod_slurping.php

[6] Hacking U3 Smart USB Drives
http://www.cse.msstate.edu/~rwm8/hackingU3/

[7] Deactivate USB Sticks through GPO
http://www.gruppenrichtlinien.de/HowTo/usb_sticks_deaktivieren.htm

[8] Microsoft TweakUI Autoplay Registry
http://www.microsoft.com/mspress/books/sampchap/6232a.aspx#140

[9] Microsoft Autostart Registry Key(s)
http://www.microsoft.com/technet/prodtechnol/windows2000serv/reskit/regentry/58886.mspx?mfr=true

[10] GFi Endpoint Security
http://www.gfi.com/

[11] Safeend Auditor and Safend Protector
http://www.safend.com/

[12] DriveLock
http://www.drivelock.com/

[13] NCC Group - Awareness Campaign
http://www.nccgroup.com/services/pen-testing/network-security-awareness-campaign.aspx