Wiping SSDs

by
Aaron Grothe
NEbraskaCERT - September 2016

Disclaimer

We're talking about wiping data from drives. This will remove (hopefully) the data from your drives. It will hopefully be unrecoverable after these actions.

So please be careful.

Upfront

Questions are welcome any time during the talk :-)

If you have experiences / information to share with the group. Please do so. I am still on the learning side of SDDs myself

If I start to mumble please let me know

How Do We Normally "Retire" a Hard Drive

Physical Destruction
Software Overwriting / E.g. DBAN (used by a lot of people)

Why are SSDs different? (Physical)

In the case of physical destruction classic methods like putting a drill through a drive won't necessarily destroy all parts of the drive

Built in redundancy, Load-levelling

Why are SSDs different (Software)

Load levelling means that sometimes instead of writing over a sector it will write the data to another sector, mark the old sector unused and continue.
This can leave a trail of old sectors of data

Even overwriting over and over again might not clear all the sectors

SATA Commands

There are SATA commands for wiping a hard drive that are available in almost every SSD of over 15gb manufactured in the last 15 years.

The quality of the overwriting the data varies by manufacturer, but is about the best you can do :-) except of course nuking it from orbit, just to be sure.

Tools to Wipe SSDs

Secure Erase (HDDErase.exe)
Parted Magic - iso
HDParm - done via the command line

Secure Erase

Works pretty well
Requires DOS boot media / works with FreeDos
Stopped being developed in 2008
Doesn't work with a lot of more recent chipsets

Parted Magic

Custom Linux distribution
Used to be free (beer), now requires a donation to download it
$9.00 / release - $49.00 / year subscription
Last free version from 2013 is still available at various sites

HDParm

HDParm is a Linux utility that is able to send ATA commands to your hard drive

It is available for almost every Linux distribution

It is used for things like tuning the hard drive. It also exposes the ability to talk directly to the drive's firmware and tell it to erase itself

Which is Best?

Parted Magic works very well and paying for it helps them continue development. They are adding new features all the time to it. Erasure over NVMe is new in the latest ISOs. Old version is still available if you're trying it out or just cheap :-)

Doing it through the HDParm commands is the "man's way" of doing it. It is also a way fraught with peril.

HDParm Demo

No Demo.

Managed to fry my Patriot 120gb drive playing around with these commands :-(Which may be almost totally secure

So we're going to run through the basics on how it works

Disclaimer: this can lead to bad things, be careful

HDParm Rules

Drive has to be plugged into the SATA bus directly, few if any work with USB/firewire/thunderbolt adapters, esata does work for most

Linux doesn't actually wipe the drive. It sends the commands to the drive firmware itself which actually wipes the drive

HDParm Non-Demo

Works out to be pretty much the following steps

hdparm -I /dev/sdx where /dev/sdx is the device

Look for a bit of relevant info

hdparm -I /dev/sdx | grep -i erase

HDParm Non-Demo (cont'd)

Make sure drive isn't frozen

hdparm -I /dev/sdx | grep frozen

If drive is frozen, sleep/wake computer to unfreeze may take several attempts

HDParm Non-Demo (cont'd)

Set a password for the drive (required for secure erase, don't reuse passwords)

hdparm --user-master user --security-set-pass password /dev/sdx

Try to remember this, losing it makes life more interesting

HDParm Non-Demo (cont'd)

Erasing the actual drive

hdparm --user-master user --security-erase password /dev/sdx

May want to use security-erase-enhanced instead if it is available

Difference between the two security-erase options are on the next slide

HDParm Non-Demo (cont'd)

Difference between the two

security-erase writes zeros to all user data

security-erase-enhanced secure writes predetermined data patterns from manufacturer to all user data areas including sectors not being used any longer because of reallocation

HDParm Non-Demo (cont'd)

Difference Between the Two (cont'd)

Does this wipe everything??? Once again manufacturer dependent, some wipe everything, some don't. There are options to set so it wipe non-user data.

HDParm Non-Demo (cont'd)

Non-user data

Two areas on the drive: Host Protected Area (HPA) and Drive Configuration Overlay (DCO). Are these wiped by secure erase. Depends on manufacturer

Hdparm allows you to reset the DCO. Has one of my new favorite flags. To use it the command is as follows:

hdparm --yes-i-know-what-i-am-doing --dco-restore /dev/sdx

HDParm Non-Demo (cont'd)

Post Erase

The drive should be set to not enabled (security off), not locked, and not frozen.

If not you may have run into a known problem that some older hdparm versions had issues if it took over two hours to wipe the drive

HDParm Notes

HDParm secure erase also works on most spinning rust drives in the last 5 years as well.

So you can use one tool for all data cleansing needs :-)

What is the best way to handle an SSD?

Just like a regular HDD

Encrypt everything on it to begin with using a tool like bitlocker, Versacrypt, or DM-crypt and just through away the encryption keys when you're done with it :-)

What is the best way to handle an SSD?

How you handle the retirement of SSDs are an issue and are going to increasingly be one as more and more people flip to them. Load levelling and other technologies are also making it into spinning rust drives as well.

Wiping an SSD will still take hours. So if you're in a high-risk situation encryption is still your best bet :-)

Summary

Success is rarely total, fortunately so is failure

Do I use hdparm to wipe my SSDs? Yes I do. Then I save them in a fireproof safe I have in my parent's basement, along with all my hard drives going back to my Atari ST MFM 20mb drive :-)

Thanks for listening

Q & A

Links

Secure Erase

http://cmrr.ucsd.edu/people/Hughes/secure-erase.html

Parted Magic

https://partedmagic.com

Links

Secure Erase

http://cmrr.ucsd.edu/people/Hughes/secure-erase.html

Parted Magic

https://partedmagic.com

Links

Wei's Paper - Reliably Erasing Data from Flash-Based Solid State Drives

https://www.usenix.org/legacy/events/fast11/tech/full_papers/Wei.pdf

Links

Tiny Apps guide to ATA Secure Erase - Excellent guide, goes into some
Edge cases (Hidden Data Areas like Host Protected Area (HPA) an Device Configuration Overlay (DCO)

https://tinyapps.org/docs/wipe_drives_hdparm.html

Links

Kernel.org - ATA_SECURE_ERASE Wiki Page

https://ata.wiki.kernel.org/index.php/ATA_Secure_Erase

Tiny Apps guide to ATA Secure Erase - Good guide, goes into some
Edge cases

https://tinyapps.org/docs/wipe_drive_hdparm.html