Zoneloader 0.5 Source and Direct Boot Notes 2003.

As its 2 years old and PS2 is about dead, i thought id share the directboot notes plus the source code to Zoneloader so hopefully people can learn from it and improve on the methods.

So how are direct boot discs made?

The PS2 protection is based on EFM (eight to fourteen modulation) and is basicly invisible. The digital signiture is basicly a pit and land structure which is what is known as DSV values. DSV (Digital Sum Value) is an integer that is incremented by every pit and decremented by every land. Example:

P-P-P-P-L-L-P-P (Lands -2, Pits +6) so would give a DSV of +4 (just used for example)

Due to EFM and how it works, EFM encoders in PC readers/writers try to keep the DSV as low to 0 as possible, as to avoid errors on the disc, as if a too high DSV the CD/DVD drive cant track properly and report a read error.

Sony however found a very clever and interesting way of using a special EFM encoder to master the data in exactly the same way a PC would but use different EFM on the data in a certain area of the disc based off offsets of the Disc ID. For example say the byte pattern 05 05 05 05 on sector 25 the DSV output on a PS2 disc was +5 DSV if it was burned on a CDR the DSV would be +4 or maybe +2 for example (only used as an example).

So as you can see the protection is completely invisible and due to the hardware electronics of a PC burner, it would always be impossible to burn a PS2 format disc. An EFM burner that could do it would cost thousands and no drive manfacturer would ever make it anyway as it wouldnt appeal to the mass market.

So why cant datel press discs like sony?

Simple as Sony mastering encoder is lock and key and no one can gain access, datel need to make the discs using normal mastering equipement.

So how did Datel / Success make direct boot CD's?

Datel Discs (action replay ect) have errornous datas in the sector region 25 - 4000 (roughly) which you think is just there to stop newbies copying the disc. However this is not the case at all the data holds the protection data for the disc!

What Datel did was using some equipment is calculate the true DSV off an original ps2 game, maybe using some fine pit and land microscopes and then outputed the data back onto there disc, this would of took alot of time and maybe expensive equipment.

They then recreated the DSV off the disc just using the correct byte patterns to make the pit and land waveform identical to the master they used. The disc all Datels discs are based off is Time Splitters (irrelevant anyway). As an example say the original PS2 disc hade data 05 06 07 08 (DSV X amount) the output data would be 24242424 (DSV X amount) as long as datel matched the DSV waveform regardless of the output data the protection could be duplicated, again using monitoring equipment. They did all the hard work :p

So inside Sectors 25-4xxx there are just data patterns that match the DSV on the original disc, the patterns inside extremely high and low DSV repeative pattaerns which makes a wobble, basicly a pit and land waveform _____---------_____ for example.

So how is this data burned pressed?

Well due to hardware electronics the DSV patterns cant be burned or pressed as there either too high or too low, and the PC hardware electronics would read error or just recorrect the DSV using EFM to bring the DSV valus back down to 0 or nearest too.

So how datel do it?

Well this is what took me months to figure out, I figured out that datel had actually scrambled the data on the disc using a standard scrambling method, which is basicly just some simple XORing which basicly outputs the data randomly so that when its fed into the mastering EFM encoder it reduces the risc of error. This is extremely clever as all cd burners and mastering equipment scramble data before it gets fed into the EFM encoder, datels sectors 25-4xxx are already scrambled, so as its just some simple XORing and as data Xored twice will give the original output data.

This is actually how safedisc 2 sectors are also put on the disc for PC so it wasnt hard to find a sector scrambling code to actually scramble/descramble datels datas.

Data scrambling for all CD rom drives is the same, it is described in one of the ECMA documents and other yellow book / red book documents over the net, this information is open also and no secret.

What do the datas look like:

Here is part a datel DSV protection sector, sector 36:

A0659ADCA0659ADCA0659ADCA0659ADCA0659ADCA0659ADCA0659ADCA0659ADCA0659ADCA0659A
DCA0659ADCA0659ADCA0659ADCA0659ADCA0659ADCA0659ADCA0659ADCA0659ADCA0659ADCA065
9ADCA0659ADCA0659ADCA0659ADCDD4C46AF

As you can see its very clean and repeated data.

Here is the same data scrambled on the disc:

A0659ADCA0659ADCA0659ADCA1E59ABCA04D9AC2206DFADA0867645D2005FAF4887B0454C80334
765C1A9B3CA02D9AEA20737AD26861CC5FDE847A94E8532C4A568B5C10F2B06743A1CD9AA22045
FAC4886F045B88070475081B647C9D34768D

I have attached one sector (36) from action reply ar2 one is unscrambled to show you the actual DSV protection, the other is scrambled to show you how the data is laid on the datel disc.

Can you verify this?

Attached in the zip is a sector scrambler source and execuble which i have added with one sector, run the data through the scrambler and you will see the datas, it is a default EFM sector scrambler and the source was written by Spath of cdfreaks.com

So how do i get the protection datas?

There is no easy way to get the data, the only way to get the accurate data is by using a hacked PC firmware, you have to locate the sense codes and work back from the subroutines, turning ECC/EDC error checking off and various other things. I am not going to post my firmware or how i did it, as this will cause big problems with sony and im not really interested in giving a full how to so people can mass pirate discs.

Anyway with a simple firmware hack based on a plextor 708a drive i read all the data out, i looked at the patterns by adapting the basic scrambler code so out putted all to a file which was very simple.

So what about success-hk method?

after analysing all of datels discs i found the protection data is always the same for each region, for example all pal discs the same, all ntsc discs the same. I then got hold of memory max and other discs by success and ripped it out using the same method, after unscrambling i found the data is also 100% identical to the AR2 data datel had used, and that theres is only one way to do it. This is really when i found out this was the real protection data, as every disc need this to boot.

So what are the lines on the success discs?

they are nothing and not read, there just extra protection put in by themselves, maybe knowing that other people know how the discs are made and protecting there investment, the lines are just a decoy.

So can i have a full ISO?

No. The reason for this is that i wanted to release this doc to give an insight as to how the ps2 protection works, not a how to on direct boot warez. There is enough info to go make further stufy and analyze the sectors yourself and play with them.

So what is the CD key you mentioned earlier?

Every game has a disc id, i.e SLES_500 ect ect, this file name is used to as an offset to make the original discs, it is also checked by the PS2 when booting. This is why datels disc all have SLUS_200.90 for usa discs as this is the time splitters key. All datels discs are made off one discs which is timesplitters, as i guess it didnt make sense to make another disc, du e to the time it takes to calculate and reconstruct the DSV. This key is also used to check the ps2logo is intact and other shit on the disc but this can all be copied anyway.

What about DVD?

DVD is much simpler than CD, it works exactly the same way, its just data was put in the CPR-MAI,EDC of success swap magic 2 dvd disc so the protection sectors couldnt be read out. This can also be read out, but only mastered not burned.

So can it be burned?

No it cant be burned, mastering equipment has a special mode 7 SSM 7 which lets you output full data ignoring all errors. For DVD you can also master 2064 bytes complete using a special mode. The mastering documents can be obtain from www.dcainc.com there called DDP documents. There are confidential but if you are a company you can obtain them by faxing your company info and signing a NDA. The DDP format is very similar to ISO but has many modes a cd cant burn. No special encoders or equipment is required to press a direct boot disc due to new modes in the DDP ;)

Anyway tt is actually very simple once you got the firmware all hacked up, but did take 2 years to figure out at the time due to lack of resources and knowledge of how the CDVD mechacon worked.

Extra reading:

EFM
http://www.ee.washington.edu/conselec/CE/kuhn/cdaudio2/95x7.htm

Google keywords: EFM DSV, Digital sum value, weak sectors.

Also read the yellow book, redbook types and many ECMA docs.

Thanks:

Big thanks to filterX for releasing the zoneloader executable which entitles the source to be released. Thanks to spath for the sector scrambler and also X for helping me reverse the plextor firmware, you know who you are ;) also to datel for cracking the original ps2 format.

enjoy

fusion