

Forum:[Hack Forums](#)

Thread: [help w. cryptsetup blowfish HD decryption](#)

cocobongo - January 8, 2016, 8:36 am

Hi all,

a friend that owns a cafeteria had bought a pc running some mp3 jukebox software + many mp3 sorted in folders from a local company back in 2009. That company went bust some years after and soon enough the pc stopped working. Someone from the company was adding mp3s every few months under a subscription contract and I guess he also updated some "run until" software lock. I fiddled around with it and noticed that when I changed the BIOS time to sometime in December 2009 it was functional again. That was ok until the remote controller broke down and we had no way of changing the mp3 genre so it was rendered useless again (there's a custom-made serial port IR Receiver and I can't guess the frequency it's listening for).

The PC's HD has three partitions, one Linux Swap, one Linux EXT running the system (Gentoo), one large encrypted containing all the mp3. There's also a hasp usb (Aladdin HaspHL Pro) that is called at boot up. As the PC starts, there's two splash screens that completely hide all menus/interface so I can't do any key/mouse presses (maybe their drivers aren't even loaded?) and after the HaspHL usb stick lights up I hear music playing (can't control it though).

So, I started it up and tried the cold booting method, dumping the RAM on a stick many times and looking for any AES keys using findaes.exe and Elcomsoft Forensic Disk Decryptor but no keys were found. I noticed that the ram dumping program had written some of its stuff at the beginning so maybe it has overwritten the AES keys? Or is the AES key in the HaspHL and it never appears on the RAM (I'm guessing, have no idea how that hasp works or what it contains) so should I concentrate on how to dump and read that Hasp?

I have uploaded the second partition with the Gentoo Linux system here:

[sendspace.com/file/3go8et](#) (10MB)

PLS ADD DOT ABOVE

so someone can have a look at it if you're curious. I'm no Linux user so the only thing I found was that the Rush file in the root folder contains what looks like a Linux distribution that has the following init

```
Code #!/bin/sh
export PATH=/sbin:/bin:/usr/sbin
umask 000
/bin/mount -t proc proc /proc
/bin/mount -t sysfs sysfs /sys
/bin/mount -t tmpfs tmpfs /dev
echo /sbin/mdev > /proc/sys/kernel/hotplug
/sbin/mdev -s
/bin/cpucrc
/bin/mount -t usbfs usbfs /proc/bus/usb
/bin/akusbcd
sleep 1
cd /bin
/bin/rushasp
cryptsetup -c blowfish -h sha256 -d /dev/urandom create swap /dev/sda1
```

```
/usr/sbin/fbcondecor_ctl -c setcfg -t RUSH  
/usr/sbin/fbcondecor_ctl -c setpic -t RUSH  
/usr/sbin/fbcondecor_ctl -c on -t RUSH --tty=/dev/tty1  
#sleep 10  
mkswap /dev/mapper/swap  
echo > /proc/sys/kernel/hotplug  
killall -9 aksusbd  
umount -l /proc/bus/usb  
umount -l /proc /sys /dev  
exec switch_root /new /sbin/init
```

Since the AES key is auto loaded on startup I would be equally happy if I could modify some boot init configuration that allows me to bypass those splash screens, initialize mouse & keyboard (or activate them if they are deactivated), connect an empty usb drive and copy all files from the encrypted partition while it's playing.

Thanks