Erledigt *Möglicher* kritischer Fehler bei Ozmosis FFS Integration

Beitrag von „Tuxuser“ vom 1. Juni 2014, 11:49

Moin Moin,

Es gibt interessante Neuigkeiten!
Momentan entwickele ich ein Programm, welches die Bearbeitung von AMI BIOSes ermöglicht. Unter diesem Umstand habe ich auch mit einem Entwickler gesprochen, der sehr tief in der Materie drin ist - der hat mich auf etwas interessantes hingewiesen.

Wenn man sich mal den Weg anschaut, wie *wir* zur Zeit Kexts in FFS umwandeln, könnte da ein Problem bestehen - welches zu einem instabilen BIOS führt:

Aktueller Weg

Code

```
1. dd if=/dev/zero of=NullTerminator bs=1 count=1 1>/dev/null 2>&1
2.
3.
4. # Hier wird zuerst die Info.plist, dann 1x NULLbyte und dann der eigentliche Treiber zu einer Datei zusammengefügt
5. cat /Sample.kext/Contents/Info.plist NullTerminator /Sample.kext/Contents/MacOS/Sample > binary.bin 2>/dev/null
6.
7. GenSec -s EFI_SECTION_PE32 -o pe32 binary.bin
8. GenSec -s EFI_SECTION_USER_INTERFACE -n versionstring -o userinterface
9.
10.
11. # Hier wird das entstandene Konstrukt als EFI_FV_FILETYPE_DRIVER deklariert !!!
12. GenFfs -t EFI_FV_FILETYPE_DRIVER -g 99F2839C-57C3-411E-ABC3-ADE5267D960D -o output.ffs -i pe32 -i userinterface
```

Alles anzeigen

Problem: Der Typ **EFI_FV_FILETYPE_DRIVER** steht für einen EFI-Treiber, d.h. das BIOS selbst

lädt diesen automatisch.
ABER: Das BIOS kann mit einer Kext-Binary nichts anfangen. Die Kexts können erst vom mach_kernel (OS X Kernel) verarbeitet werden
=> Es bringt nichts, das BIOS zu veranlassen eine Kext zu laden (versuchen).

Ergebnis: Das BIOS scheitert am Laden der Datei und wirft einen ERROR - das **kann** bei mehreren solcher FFS zur **Verlangsamung oder Instabilität des Systems** führen.

Was soll man also nun machen?

Einfach!

Code

1. GenFfs -t EFI_FV_FILETYPE_DRIVER -g 99F2839C-57C3-411E-ABC3-ADE5267D960D -o output.ffs -i pe32 -i userinterface

in

Code

1. GenFfs -t EFI_FV_FILETYPE_FREEFORM -g 99F2839C-57C3-411E-ABC3-ADE5267D960D -o output.ffs -i pe32 -i userinterface

umändern.

Das Layout der Datei bleibt das gleiche, das BIOS selbst ignoriert jedoch diese Datei und sie wird erst von OSX geladen

Vielleicht ist es hilfreich für den ein oder anderen.