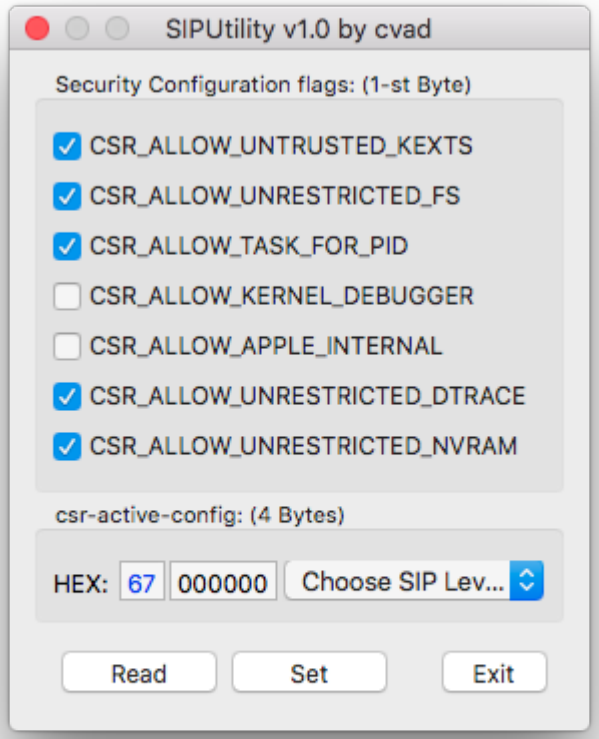
Erledigt SIP Tool für Rechner mit beschreibbaren NVRAM und echte MAC´s

Beitrag von „Griven“ vom 15. August 2015, 20:31

Im Zusammenhang mit dem bevorstehenden Release von El Capitan und IOS9 hat Apple noch einmal gewaltig an der Systemsicherheit gearbeitet und etabliert mit El Capitan eine Technik namens "System integrity Protection" (vgl. rootless) die das System weitestgehend vor Eingriffen von außen abschottet. Neben den bereits aus Yosemite bekannten Restriktionen beim laden von nicht signierten Extensions verhindert Apple mit der System Integrity Protection nun auch das verändern systemkritischer Verzeichnisse im Dateisystem sowie jegliche Manipulationen am NVRAM durch den User. Mit anderen Worten selbst mit Root Rechten sei es durch SUDO erworben oder im SingleUserMode ist der Inhalt bestimmter Verzeichnisse nicht mehr veränderbar (/S/L/E, /S/E, /bin usw...) ebenso lässt sich der NVRAM nicht mehr beliebig verändern oder Extensions patchen.

Alles in allem ist SIP eine gute und lange überfällige Technik denn viel effektiver kann man ein System nicht von Ausseneinflüssen abschotten trotzdem ist es natürlich insbesondere für die Hackintosh Community ein weiterer Stolperstein auf dem Weg zum Hacki denn mit aktiver SIP wird man nicht mal mehr die notwendige FakeSMC mehr geladen bekommen geschweige denn andere notwendige Extensions installieren können. Glücklicherweise haben findige Member der Community (dank an dieser Stelle an pikeralpha) längst herausgefunden wie die SIP funktioniert und wie man sie passend zum eigenen Gusto einstellen kann. Neben einer Fülle an NVRAM Befehlen für OZ basierte Systeme und einiger config.plist hacks für Clover basierte Systeme gibt es jetzt auch ein GUI Tool aus der Feder von cvad das es erlaubt die nötigen Änderungen bei allen Systemen, die einen beschreibbaren NVRAM haben bequem aus der GUI eines laufenden Yosemite Systems auf dem Rechner vorzunehmen.



Hierbei werden einfach die gewünschten Änderungen angehakt und anschließend gespeichert. Nach der Installation Eurer benötigten Extensions könnt Ihr die SIP wieder vollständig aktivieren denn was einmal im Cache ist wird trotz aktiver SIP geladen.
SIPUtility.zip

Beitrag von „MacGrummel“ vom 15. August 2015, 22:02

Ich schätze mal, da bleibt uns noch Einiges zu tun! Mein EX-58 läuft auf dem neusten Clover 3256, dass ja die SIP abschalten soll. Eben. Soll. Tut es bei mir jedenfalls nicht! Meine Experimental-Platten schmieren bei Neuinstallationen wie zuvor ab- Was aber hilft, ist die notwendigen Kexte entweder schon vor dem Update im System zu haben (also weg mit Clean Install !!!) oder von Yosemite aus die Kexte mit Multibeast auf die El Capitan - Partition installieren, incl. geänderter AppleHDA..

Beitrag von „Griven“ vom 15. August 2015, 22:05

Du musst die NVRAM Emulation zusätzlich installieren sonst wird das nix mit dem Abschalten.

Beitrag von „MacGrummel“ vom 15. August 2015, 23:02

Wenn ich mich recht entsinne, hab ich das mit viel Mühen im Januar aus allen Systemen operiert, damit iMessage und Facetime laufen können..

Beitrag von „Griven“ vom 15. August 2015, 23:09

Zum aber das iMessage Zeug braucht doch die NVRAM Emulation eigentlich auch??
Sonst einfach in der config.plist unter RT-Variables folgendes einfügen:

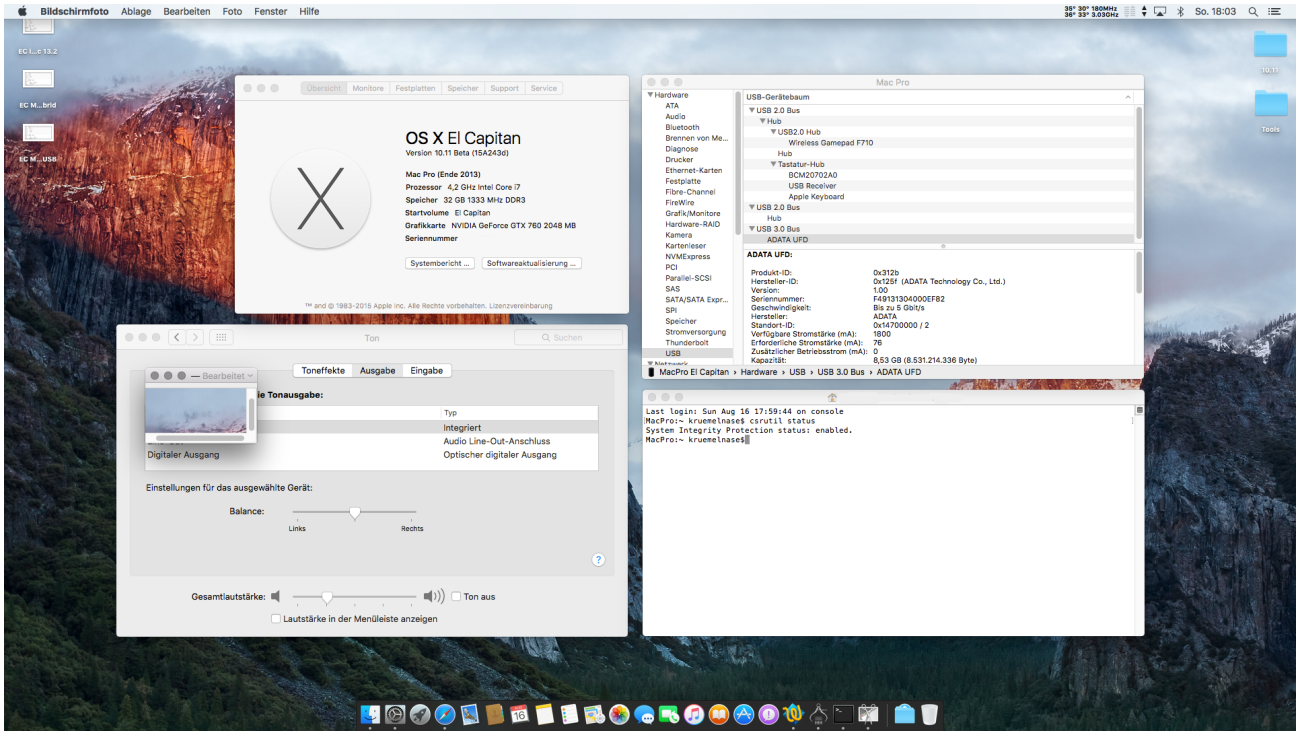
Code

```
1. <key>CsrActiveConfig</key>
2. <string>0x67</string>
3. <key>BooterConfig</key>
4. <string>0x28</string>
```

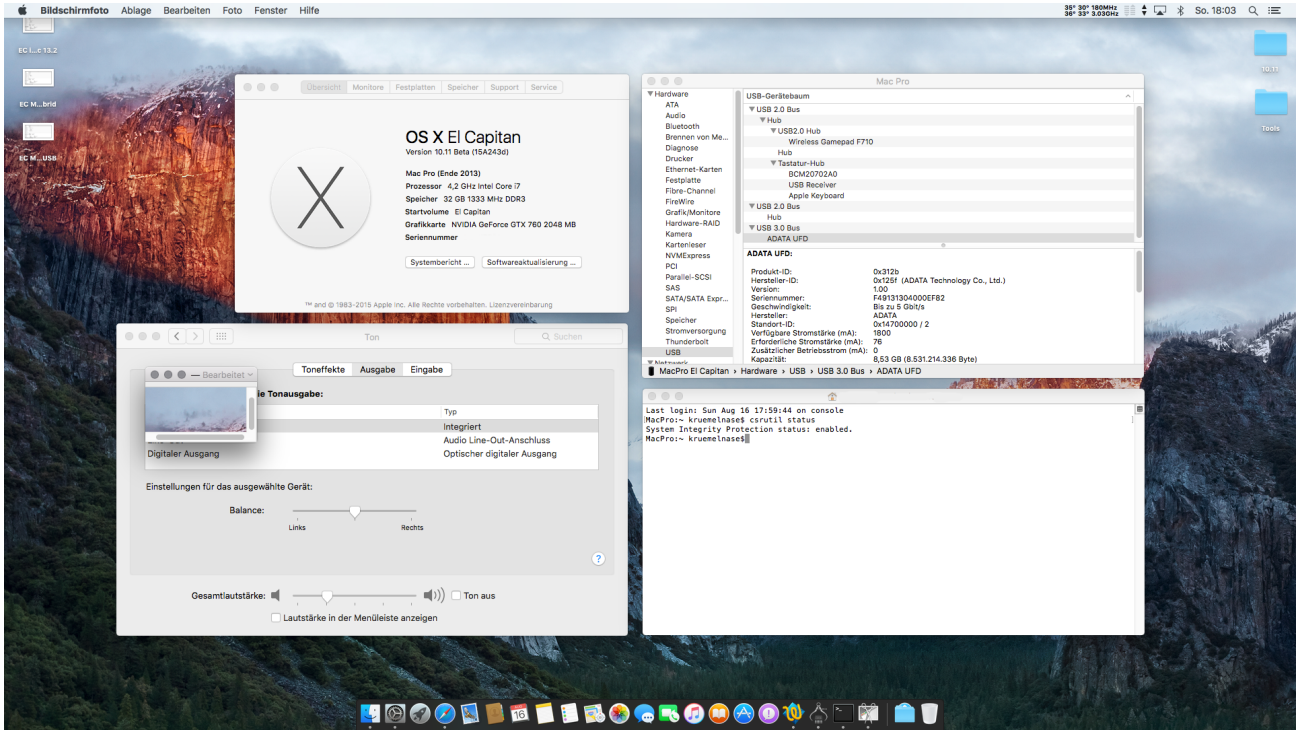
Das sollte SIP ebenfalls abschalten.

Beitrag von „kruemelnase“ vom 16. August 2015, 18:31

Mit Clover 3259 funktioniert das Kext injecten wieder wie vorher, auch wenn SIP auf enabled steht.
Hab getestet, alle Zusatz Kexte aus L/E entfernt Cache neu aufgebaut, Systeme booten normal, Yosemite sowie El Kapitän (DEV6 und PB4).



Nur um die AppleHDA zu patchen musste ich SIP nochmal deaktivieren und nach dem Patch wieder reaktivieren.



Beitrag von „Griven“ vom 16. August 2015, 18:46

Gut zu wissen

Beitrag von „thommel“ vom 13. Oktober 2015, 20:31

griven,

hätte mal zwei Fragen , eine zu SIP und eine zum Festplattendienstprogramm. Auf meinem X58 läuft El Capitan mit Clover 3280 sehr gut. Wenn jetzt alls läuft könnte ich doch die RT Variable 0x67 herausnehmen oder habe ich da was falsch verstanden? Sind dann aber nach einem Cache Rebuild die Einstellungen gelöscht?
Gibt es eine Alternative zur Reparatur der Rechte da im Festplattendienstprogramm die Option nicht mehr vorhanden ist. Habe im Netz was gefunden aber wollte Deine Meinung dazu hören.
http://ifreaky.net/os-x-10-11-…echte-manuell-reparieren/

thommel

Beitrag von „Griven“ vom 13. Oktober 2015, 20:53

Hi thommel wenn alles eingerichtet ist kannst Du die SIP ohne weiteres wieder aktivieren. Bei aktivierter SIP wird OS-X den Cache nicht wieder neu aufbauen sprich es wird sich daran bis zum nächsten Update nichts mehr verändern. Eine Reperatur der Rechte ist demnach eigentlich auch nicht mehr notwendig denn es kann sich hier an den Systemrelevanten Ordnern nichts mehr ändern oder anders einmal im Cache immer im Cache

---

Beitrag von „thommel“ vom 13. Oktober 2015, 21:02

Hallo Griven,

Danke für die Info. Also werde ich den Zugewinn an Sicherheit auch nutzen.

thommel