Home

DTrace vs. System Integrity Protection

The Problem

As you may now Apple released their new OS X revision 10.11 this year with a great security feature built-in: System Integrity Protection. In a nutshell, this mechanism protects any system data and important filesystem components (like `/System` or `/usr`) from being modified by user; even if they are *root*. SIP also disables any use of code-injection and debugging techniques for third-party software, so some of your favorite hacks may not work anymore.

> Here's an example: if you've been using TotalFinder extension — which basically injects some code inside Finder in order to make it better — you'll no longer be able to use it on OS X 10.11 with SIP enabled.

I'm not going to discuss all the pros and cons of this «integrity» thing, but what especially freaks me out is that you aren't supposed to use DTrace at all because:

1. You can no longer attach DTrace to «restricted» processes on your Mac [1]. And by «restricted» I mean every single built-in utility, daemon or application:

```
$ sudo dtruss echo "demo"
# > dtrace: failed to execute echo: dtrace cannot control executables
 signed with restricted entitlements
```

2. Some of DTrace provides just won't work (e.g. `fbt`);
3. Your .d scripts are prohibited from using any destructive actions:

```
# -w flag stands for «destructive»
$ sudo dtrace -w -q -n 'BEGIN {printf("It works!\n")}' -c ./demo
# > dtrace: could not enable tracing: Permission denied
$ sudo dtrace -q -n 'BEGIN {printf("It works!\n")}' -c ./demo
# > It works!
```

The Solutions

Completely disable SIP

Although not recommended by Apple, you can entirely disable System Integrity Protection on you Mac. Here's how:

1. Boot your Mac into Recovery Mode: reboot it and hold cmd+R until a progress bar appears.
2. Choose the language and go to Utilities menu. Choose Terminal there.
3. Enter this command to disable System Integrity Protection:

```
$ csrutil disable
```

4. It will ask you to reboot — do so and you're free from SIP!

The Good

You're able to do anything you want with the OS, yay! ٩(⁄⁄⁄◕ั ω ◕ั⁄⁄⁄)و

The Bad

You're not safe: there're plenty of rootkits in a wild which can infect your system. Actually, you're as safe as on OS X 10.10 or 10.9, so judge for yourself.

Partially disable SIP

Fortunately, SIP is not monolithic: it's built from many different modules we can disable/enable separately. Let's take a look at a typical `csrutil status` output:

```
$ csrutil status
System Integrity Protection status: enabled

Configuration:
    Apple Internal: enabled
    Kext Signing: enabled
    Filesystem Protections: enabled
    Debugging Restrictions: enabled
    DTrace Restrictions: enabled
    NVRAm Protections: enabled
```

I can count 6 different subsystems out here. Here's the way to selectively disable any of them:

1. Repeat steps 1 and 2 from «Completely disable SIP» section above.
2. Now in Terminal enter these commands:

```
$ csrutil clear # restore the default configuration first
$ csrutil enable --without dtrace # disable dtrace restrictions *only*
```

That's it: use `csrutil enable` + `--without` flag with a name of a module you want to disable:

```
$ csrutil enable --without kext
$ csrutil enable --without fs
$ csrutil enable --without debug
$ csrutil enable --without dtrace
$ csrutil enable --without nvram
# this one below is different, not sure why. Don't encourage you to disable it anyways…
$ csrutil enable --no-internal
```

3. Reboot and enjoy your OS again.

The Good

If you only disable `dtace` module you're still quite safe: SIP will keep an eye on your filesystem and kernel extensions as well as on any software trying to inject code.

The Bad

You're *still unable* to attach dtrace to restricted processes (ᡣ¤ᡣ):

```
$ sudo dtruss echo "demo"
dtrace: failed to execute echo: dtrace cannot control executables signed with restricted entitlements
```

(Bonus): a win-win solution

If you ask me, here's my advice: only disable `dtrace` restrictions on your Mac and use a virtual machine (such as VirtualBox or Parallels) where SIP is disabled entirely for deep analysis.

This way your main OS will remain quite secure and you don't actually care about what happens in a guest virtual machine OS since you may restore it to the initial state any time. (๑˃ᴗ˂)و

October 12, 2015

1. Well, actually Apple have been using PT_DENY_ATTACH `ptrace()` flag for iTunes&co. for a while now (since 10.5, IIRC) which also prevents debuggers and DTrace from attaching to these programs. But it was quite easy to bypass.↩