EXHIBIT AA

DECLARATION OF RYAN BRICKER IN SUPPORT OF *EX PARTE* MOTION FOR TEMPORARY RESTRAINING ORDER AND ORDER TO SHOW CAUSE RE PRELIMINARY INUNCTION; ORDER OF IMPOUNDMENT

marcansoft (727665)

Slashdot News for nerds, stuff that matters

hector@@@marcansoft...com
http://marcansoft.com/
Jabber: marcan@marcansoft.com
If it works, I'll fix it anyway.

Comment: Re:Actually... green light. (Score 1) Comments: 598 Comments: 598

by marcansoft on Monday January 10, @01:35PM (#34825832)
Attached to: New Laser Makes Pirates Wish They Wore Eye-Patches

Expanded to 20cm, the power level is over 100 times lower, so it's pretty much guaranteed to be safe. I also typoed the "I'm going going to try pointing it into my eye". I meant "I'm *not* going to try pointing it into my eye", of course.

Read More...

---

marcansoft
Firehose
Comments
Submissions
Friends
Tags
Achievements

marcansoft's Achievements

Days Read in a Row
Got a Score:5 Comment
Had a Comment Modded Up

marcansoft's Comments

Re:Actually... green light.
Re:Actually... green light. (Score:5, Informative)
Re:Same private key?
Re:Same private key?
Re:Same private key?

marcansoft's Friends

bushing

marcansoft's Tags

interesting (submissions)
!eff (stories)
!hackers (stories)
worstheadlineever (stories)
dupe (stories)

marcansoft's Submissions

Apple Blocks Open Source Syncing (Again)
Apple Blocks Open Source Syncing (Again)
Wii Update 4.2 tries (and fails) to block homebrew
Scammers sell free Wii homebrew and make $8000/mo
The latest scam: selling homebrew software

Comment: Re:Actually... green light. (Score 5, Informative) Comments: 598

by marcansoft on Sunday January 09, @04:14PM (#34817242)
Attached to: New Laser Makes Pirates Wish They Wore Eye-Patches

To throw some numbers in: The glasses that the GP linked to are OD 4 for 532nm light (i.e. green Nd:YAG lasers, which are basically guaranteed to be the type used by this weapon). That means they block 99.99% of the beam at that wavelength. That's quickly going to turn any beam designed to be borderline non-permanently-damaging into barely a bother.

In fact, I just ran a quick test. I have a 30mW green pointer, which is definitely unsafe for direct eye exposure. I expanded the beam with a lens to about a 20cm radius, which is eye-safe at this power level. Looked at it thought my glasses (I actually have that same model), and it was just a very slight orange glow, about on par with an indicator LED. Took the goggles off and it was very annoying (I had an afterimage for a few minutes). I imagine the laser weapon will be closer to the damage threshold than my quick test, but still, the glasses will totally destroy any effect unless the laser runs at power levels much higher than eye-safe ones.

Or, testing with the (definitely eye unsafe) collimated 30mW, through the glasses, onto a wall: the green dot is barely visible. I'm going going to try pointing it into my eye (see below), but that mount of light is not going to bother anyone.

Note for anyone wanting to try this: don't unless you really know what you're doing. In particular, looking into the bare beam with glasses on is a very bad idea. You probably won't damage your eyes with the green light, but these cheap chinese pointers tend to lack IR filters, and **that** can screw you since the glasses won't block IR (worse, your blink response won't trigger and you'll slowly cook your retina). In fact, I can see a slight deep red glow around the projected green dot going through the glasses, which indicates there's a considerable amount of leaked IR, probably well above the damage threshold (if you can see IR, there's a lot of it).

Comment: Re:Same private key? (Score 1) Comments: 374

by marcansoft on Tuesday January 04, @02:42PM (#34757188)
Attached to: PS3 Root Key Found

Yes, but homebrew on the stock OS is something Sony is going to try to fight anyway. We're more interested in the (unpatchable) low level boot hacks.

Comment: Re:Same private key? (Score 1) Comments: 374

by marcansoft on Tuesday January 04, @02:39PM (#34757172)
Attached to: PS3 Root Key Found

The 360 has extremely well designed security, and the only exploits that there have been for it were quite contrived and difficult to pull off (and easily fixed). It's a great design.

However, it does fail in the drive security department, which is why there's all the warez firmware hacking going on. But the core system is very secure.

Comment: Re:Same private key? (Score 1) Comments: 374

by marcansoft on Tuesday January 04, @02:38PM (#34757154)
Attached to: PS3 Root Key Found

Hardware acceleration has been enabled ever since AsbestOS came out, and this also applies to native-boot AsbestOS. Of course, a driver needs to be written/ported. Getting nouveau integrated into the lv1 graphics framework is somewhere on my TODO for 2011.

Comment: Re:Same private key? (Score 4, Insightful) Comments: 374

by marcansoft on Monday January 03, @07:05PM (#34749242)
Attached to: PS3 Root Key Found

We published our exploits at the talk by explaining exactly how they works, and how anyone could use them. We said we'd release tools through the following month, and we already released two Git repositories containing most of the tools (that's 4 days after the talk). We didn't release keys due to fear of legal repercussions, but we told people exactly how to calculate them, and they did.

Geohot first released a useless signed loader to prove that he had the keys. Then he released the keys. He hasn't released information on how he got the metldr plaintext and apparently doesn't have plans to do so.

Personally, I think explaining things first, then a few days later releasing tools, is better than just dumping keys on the world and keeping how you got them a secret.

Comment: Re:Same private key? (Score 5, Informative) Comments: 374

by marcansoft on Monday January 03, @07:00PM (#34749208)
Attached to: PS3 Root Key Found

We (fail0verflow) discovered and released two things:

> An exploit in the revocation list parsing, enabling us to dump a bunch of loaders, and thus their decryption keys
> A humongous screwup by Sony, enabling us to calculate their private signing keys for all of those loaders, and thus sign anything to be loaded by those loaders

We used these techniques to obtain encryption, public, and private keys for lv2ldr, isoldr, the spp verifier, the pkg verifier, and the revocation lists themselves. We could've obtained appldr, (the loader used to load games and apps), but chose not to, since we are not interested in app-level stuff and that just helps piracy. We didn't have lv1ldr, but due to the way lv1 works, we could gain control of it early in the boot process through isoldr, so effectively we also had lv1 control.

With these keys we could decrypt firmware and sign our own firmware. And since the revocation is useless and the lame "anti-downgrade" protection is also easily bypassed, this already enables hardware-based hacks and downgrades forever. Basically, homebrew/Linux on every currently manufactured PS3, through software means now, and through hardware means (flasher/modchip) forever, regardless of what Sony tries to do with future firmwares.

The root of all of the aforementioned loaders is metldr, which remained elusive. Then Geohot announced that he had broken into metldr (with an exploit, analogous to the way we exploited lv2ldr to get its keys) and was thus able to apply our techniques one level higher in the loader chain. He has released the metldr keyset (with the private key calculated using our attack), but not the exploit method that he used.

The metldr key does break the console's security even more (especially with respect to newer, future firmwares - and thus also piracy of newer games), and also makes some things require less workarounds. Geohot clearly did a good job finding an exploit in it, but considering a) he used our key recovery attack verbatim, and b) he found his exploit right after our talk, so he was clearly inspired by something we said when we explained ours, I think we deserve a little more credit than we're getting for this latest bit of news.

There's still bootldr and lv0, which are used at the earliest point during the PS3 boot process. These remain secure, but likely mean little for the PS3 security at this stage.

Comment: Re:Exactly (Score 5, Informative) Comments: 374

by marcansoft on Monday January 03, @06:56PM (#34749184)
Attached to: PS3 Root Key Found

For the record, that wasn't there initially. We had to complain to him to get him to add that.

Last Week
Week of January 3

Comment: Re:Rich protecting themselves (Score 1) — Comments: 217

by marcansoft on Sunday January 02, @09:03PM (#34740728)
Attached to: Online Impersonations Now Illegal In California

Sad but true. No matter what the law says, getting protected as mere users is near impossible. Unless you're willing to go through a costly legal battle, no one cares.

A few days ago we presented ourselves as a hacker group at the 27th Chaos Communication Congress, presenting PS3 hacks, and now we have a YouTube account squater/scammer asking for donations in our name. I've tried YouTube impersonation reports, but apparently I'm "providing insufficient information" (duh, you get 300 characters to explain everything). I've tried YouTube Legal, received no response so far. I've tried getting people to flag the videos as a scam, but that doesn't work. I'm not even going to try PayPal; I've dealt with them before and they don't care.

This whole thing reminds me of my run-ins with scammers back when I was actively developing Wii homebrew stuff. The payment processors (ClickBank, Plimus, PayPal, and co.) don't care. They'll happily take people's money and hand it over to scammers, keeping a percentage, of course, even if what is being sold is a scam or illegal.

If you're a small consumer or producer, companies don't give a rat's ass about you. They'll only listen if they know you have the power and lawyers to actually file a lawsuit and win.

Comment: Re:Sigh (Score 1) — Comments: 532

by marcansoft on Thursday December 30, @10:28AM (#34710954)
Attached to: Playstation 3 Code Signing Cracked For Good

Everyone keeps forgetting that OtherOS was already removed / discontinued on new PS3s - the Slim - before Geohot started his work. That's what started it all. Removing OtherOS on the Fat made it a lot worse, of course, but it's the lack of OtherOS on the Slim (for a fishy - and, as it turned out, totally BS reason) that got people looking initially. We even gave it a quick look exactly one year ago, at 26c3, though we didn't try very hard (this was before OtherOS was pulled from the Fat).

Comment: Re:Sigh (Score 3, Interesting) Comments: 532

by marcansoft on Thursday December 30, @08:50AM (#34709880)
Attached to: Playstation 3 Code Signing Cracked For Good

Honestly, it's perfectly possible to engineer the signature randomization failure deliberately (it would certainly be very easy to botch a signer like this and make it look like a bug, see the Underhanded C Contest for similar examples), but I think it's extremely unlikely that something like this actually happened. Never attribute to malice that which can be adequately explained by stupidity. Especially considering the rest of the security is messed up in ways that clearly indicate they just didn't know what they were doing.

Humor in the Court: Q: Are you sexually active? A: No, I just lie there.