

EXHIBIT I

DECLARATION OF RYAN BRICKER IN SUPPORT OF
PLAINTIFF SONY COMPUTER ENTERTAINMENT AMERICA
LLC'S OPPOSITION TO DEFENDANT GEORGE HOTZ'S
MOTION TO DISMISS FOR LACK OF PERSONAL
JURISDICTION AND IMPROPER VENUE



Original URL:

http://www.theregister.co.uk/2010/01/25/playstation_cracked_wide_open/

Once impenetrable PS3 cracked wide open iPhone hacker: 'I have great power'

By [Dan Goodin in San Francisco](#)

Posted in [Security](#), 25th January 2010 19:51 GMT

[Free whitepaper – The Register Guide to Enterprise Virtualization](#)

The first hacker to successfully jailbreak the iPhone says he has pulled off yet another modding marvel, this time penetrating the previously impervious PlayStation 3 gaming console.

The hack by 20-year-old George Hotz, aka geohot, is significant because the PS3 was the only game console that hadn't been hacked, despite being on the market for more than three years. The feat greatly expands the functionality of the box by allowing it to run unrestricted versions of Linux and a wide range of games that are currently forbidden. The hardware and software designer told *El Reg* it took him five weeks to develop the hack using a combination of modifications to the console's hardware and software.

"Basically, I used hardware to open a small hole and then used software to make the hole the size of the system to get full read/write access," he said in an interview. "Right now, although the system is broken, I have great power. I can make they system do whatever I want."

The first three weeks were spent trying attacks to directly access memory of the console. He eventually settled on his current approach after realizing software approaches alone were insufficient.

A dropout of the Rochester Institute of Technology, geohot said he is declining to provide details to prevent Sony from introducing changes that would stymie the modifications. But a [blog post](#) [1] announcing the accomplishment makes clear the hack gives users unprecedented control over their systems.

"I have read/write access to the entire system memory, and HV level access to the processor," geohot wrote. "In other words, I have hacked the PS3."

The hack will allow PS3 users for the first time to run unrestricted versions of Linux that have full access to the system's central processing unit and graphical processing unit. That will greatly expand the kinds of things users can do with the console. For starters, they could use the mod to run emulators that will play PS2 games on the

machine, something Sony strictly forbids. It could also allow programs like the VLC media player to run much more robustly. The hack also opens the door to pirated games on the console, although geohot said that's an activity he's not interested in pursuing.

Geohot said he doesn't plan to release the software used to unlock the box until he can make it more reliable. It currently takes about 15 minutes to run and frequently fails to work properly. "If I posted what I have now, people would get fed up with it," he said.

He praised the PS3 as a "pretty secure system," that was harder to hack than many hardware systems he has penetrated.

"One of the main things Sony did right was put all the security on at once," he explained. "From day 1, the PS3 was secure."

By contrast, anti-hacking protections in the iPhone were rolled out over time, allowing him to gain important insights into the overall design that helped him defeat changes that were introduced later.

"If the iPhone right now was released as is, it would be much harder for people to crack," he said. "With the iPhone, when a new version comes out, we can decrypt it right away because we have exploits for the old version."

A native of Glen Rock, New Jersey, geohot rose to prominence in 2007, at the age of 17, when he developed the first hack to allow the iPhone to work on networks other than AT&T's. Even after Apple introduced changes designed to reestablish Apple's iron-fisted grasp of the device, geohot devised ways [jailbreak newer versions](#) [2], unleashing a never-ending cycle of hacks and counterhacks.

While hacks of the Xbox and the iPhone have led to thriving developer communities that release custom applications for the modded devices, geohot said the challenge of overcoming the security overshadows those more practical outcomes.

"Personally, it's a win for me just to do it," he said. "It's just cool to have it cracked." ®

Links

1. <http://geohotps3.blogspot.com/2010/01/hello-hypervisor-im-geohot.html>
2. http://www.theregister.co.uk/2008/02/11/latest_iphone_hack/

Related stories

[Console games 'hack' reseller gets community service order](#) (10 January 2011)
http://www.reghardware.com/2011/01/10/console_modder_sentencing/

[PlayStation site hacker avoids jail](#) (11 May 2010)
http://www.theregister.co.uk/2010/05/11/playstation_hacker_sentencing/

[Hacker pledges to re-enable Linux on PS3](#) (31 March 2010)
http://www.reghardware.com/2010/03/31/ps3_hacker_fights_back/

[Sony: PS3 leap year glitch caused network lockout](#) (2 March 2010)
http://www.reghardware.com/2010/03/02/ps3_psn_access_bug_bypassed/

[Old PS3s locked out of PlayStation Network](http://www.reghardware.com/2010/03/01/chubby_ps3_psn_lockout/) (1 March 2010)
http://www.reghardware.com/2010/03/01/chubby_ps3_psn_lockout/

[Everything you ever wanted to know about Xbox hacking](http://www.theregister.co.uk/2010/02/21/xbox_hacking_phishing_analysis/) (21 February 2010)
http://www.theregister.co.uk/2010/02/21/xbox_hacking_phishing_analysis/

[Microsoft hit with cash-for-Points lawsuit](http://www.reghardware.com/2010/01/27/ms_points_lawsuit/) (27 January 2010)
http://www.reghardware.com/2010/01/27/ms_points_lawsuit/

[Prolific hacker releases PlayStation exploit](http://www.theregister.co.uk/2010/01/27/playstation_exploit_released/) (27 January 2010)
http://www.theregister.co.uk/2010/01/27/playstation_exploit_released/

[Hacker brings multitouch to Google's Nexus One](http://www.theregister.co.uk/2010/01/22/nexus_one_multitouch_hack/) (22 January 2010)
http://www.theregister.co.uk/2010/01/22/nexus_one_multitouch_hack/

[Console modders attempt to bypass Xbox Live ban](http://www.reghardware.com/2009/11/16/xbox_live_unblock_guide/) (16 November 2009)
http://www.reghardware.com/2009/11/16/xbox_live_unblock_guide/

[Hacker frees iPhone from Jobsian tyranny \(again\)](http://www.theregister.co.uk/2009/11/04/blacksn0w_and_blackra1n/) (4 November 2009)
http://www.theregister.co.uk/2009/11/04/blacksn0w_and_blackra1n/

[Hacker springs latest iPhone OS from Jobsian jail](http://www.theregister.co.uk/2009/10/12/latest_iphone_jailbreak/) (12 October 2009)
http://www.theregister.co.uk/2009/10/12/latest_iphone_jailbreak/

[Open sourcers strike back at Google cease-and-desist](http://www.theregister.co.uk/2009/09/28/google_android_developers_reaction/) (28 September 2009)
http://www.theregister.co.uk/2009/09/28/google_android_developers_reaction/

[Google hits Android dev with cease-and-desist letter](http://www.theregister.co.uk/2009/09/25/google_android_take_down_demand/) (25 September 2009)
http://www.theregister.co.uk/2009/09/25/google_android_take_down_demand/

[iPhone Dev Team player breaks ranks to release 3GS hack tool](http://www.reghardware.com/2009/07/03/iphone_3gs_jailbreak/) (3 July 2009)
http://www.reghardware.com/2009/07/03/iphone_3gs_jailbreak/

[Linux goes Wii](http://www.theregister.co.uk/2008/02/27/wii_linux/) (27 February 2008)
http://www.theregister.co.uk/2008/02/27/wii_linux/

[Teen hacker re-unlocks Apple's iPhone](http://www.theregister.co.uk/2008/02/11/latest_iphone_hack/) (11 February 2008)
http://www.theregister.co.uk/2008/02/11/latest_iphone_hack/

[Nintendo Wii hack opens door to homebrew games](http://www.reghardware.com/2007/12/31/nintendo_wii_hack/) (31 December 2007)
http://www.reghardware.com/2007/12/31/nintendo_wii_hack/

[Xbox 360 cracked](http://www.theregister.co.uk/2007/03/01/xbox_hack/) (1 March 2007)
http://www.theregister.co.uk/2007/03/01/xbox_hack/

© Copyright 1998–2011