EXHIBIT Z

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

BBC NEWS

TECHNOLOGY

5 January 2011 Last updated at 20:17 ET

iPhone hacker publishes secret Sony PlayStation 3 key

By Jonathan Fildes
Technology reporter, BBC News

The PlayStation 3's security has been broken by hackers, potentially allowing anyone to run any software - including pirated games - on the console.

A collective of hackers recently showed off a method that could force the system to reveal secret keys used to load software on to the machine.

A US hacker, who gained notoriety for unlocking Apple's iPhone, has now used a similar method to extract the PS3's master key and publish it online.

Sony declined to comment on the hack.

"The complete console is compromised - there is no recovery from this," said pytey, a member of the fail0verflow group of hackers, who **revealed the initial exploit at the Chaos Communication Congress in Berlin in December**.

"This is as bad as it gets - someone is getting into serious trouble at Sony right now."

The group, which has previously hacked Nintendo's Wii and says it is vehemently against

games piracy, said that it had developed the hack so that it could install other operating systems and community-written software - known as homebrew - on the powerful machine.

"The details we provided and information and techniques we disclosed would have been enough to install Linux," he said. "We have no interest in piracy."

Following the presentation, US hacker George Hotz, who has previously hacked parts of the console, used a similar technique to extract the master key. He has now published it on his blog.

This formerly secret number is used to "sign" all games and software that run on the system, to authenticate that it is genuine and approved by Sony.

However, once the key is known it can be used to sign any software - including unofficial software and games.

"I hate that it enables piracy," said Mr Hotz. "The publication of the key is more academic than anything else."

The number also works for Sony's handheld console the PlayStation Portable, said Mr Hotz.

Developers have already started **releasing tools** to develop new software for the PS3 using the hacks.

'Valid target'

The PS3 - once regarded as the most secure of the game's consoles, and the only one not to have been permanently cracked - has in the last 12 months come under increasingly scrutiny from hackers.

In January 2010, Mr Hotz claimed to have cracked the console.

Following his initial announcement, Sony released an update disabling a function, called OtherOS, that allowed gamers to install a version of Linux on their machines, thought to have been exploited by Mr Hotz.

Many saw it as a pre-emptive strike to guard against games piracy.

Mr Hotz never released the exploit and publicly said that he had stopped work on the console.

But Sony's removal of OtherOS prompted other hackers to begin to look at the system more closely.

"It became a valid target," pytey told BBC News. "That was the motivation for us to hack it."

He said the team had spent "months" trying to find their way into the system.

"It was not trivial to do this," he said.

In the end, the flaw that allowed them to crack the system was a basic cryptographic error that allowed them to compute the private key, held by Sony, he said.

"Sony uses a private key, usually stored in a vault at the company's HQ, to mark firmware as valid and unmodified, and the PS3 only needs a public key to verify that the signature came from Sony.

"Applied correctly, it would take billions of years to derive the private key from the public key, or to make a signature without knowing the private key, even when you have all the computational power in the world at your disposal."

But the team found that Sony had made a "critical mistake" in how it implemented the security.

"The signing recipe requires that a random number be used as part of the calculation, with the caveat that that number must be truly random and not predictable in any way," the team said.

"However, Sony wrote their own signing software, which used a constant number for each signature."

This allowed the team to use "simple algebra" to uncover Sony's secret key, without access to it.

"This is supposed to be the most secret of secret of secrets - it's the Crown jewels," said pytey.

The team decided to publish its method but not the keys.

After the team revealed their hack, Mr Hotz said that he was prompted to renew his work on the system.

"What fun is a race if no-one else is running," he said. "fail0verflow did great work - they took it up a level."

Using a similar technique he was able to extract the entire master key for the system, which he subsequently published online along with a demonstration of it in action.

However, he has not released the method he used to extract the key.

"There is no reason to," he said.

However, he said that he may release a piece of software that will allow people to easily sign their own pieces of software and homemade games - also known as homebrew - on to the console.

"I have a program running but am thinking of a good way to release it," he said.

Like fail0verflow, he said that he does not condone games piracy.

"I do not want it to be able to sign official Sony programs. I'd like it just to be able to sign homebrew."

fail0verflow said it "disagrees" with Mr Hotz's decision to release the key, saying that it expects them "to make piracy easier without accomplishing anything intrinsically useful".

Legal worry

Sony takes a dim view of people hacking its system.

Last year, a team released a USB dongle called PSjailbreak that contained software that allowed gamers to play homemade and pirated games on the PlayStation 3.

Sony updated its consoles to block the software and took legal action against distributors in many countries.

However, according to pytey, it may not be so easy to fix the problem this time.

"The only way to fix this is to issue new hardware," he said. "Sony will have to accept this."

He said that he thought his group was on safe legal ground with its work.

"I haven't stolen anything," he said. "It's my own hardware, I can run whatever I like on it.

Mr Hotz also defends his actions, although admits he is "scared of being hit with a lawsuit".

"I am confident I would win since what I released was just a number obtained by running software on the PS3 I purchased".

More Technology stories

Legal gamble for Facebook fortune [/news/technology-12155352]
Three Harvard graduates are to gamble a $65m settlement they made with Facebook over who came up with the idea for the site, in an effort to get more money.

Boss of chipmaker AMD stands down [/news/business-12158080]

Global dip in spam 'short lived' [/news/technology-12154118]
