EXHIBIT C

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

guardian.co.uk

GAMES BLOG

PlayStation 3 hack – how it happened and what it means

A group of coders claims the PS3 has been hacked, opening the doors to software piracy. We look into the implications

The PS3 has been hacked. But how – and why? Photograph: Kevork Djansezian/AP

In December, a group of coders operating under the name Failoverflow stood up at the Chaos Communications hackers conference in Berlin and proclaimed that the Sony PS3 security system was an epic fail. Through the use of what they termed "simple algebra" they had managed to exploit a weakness in the PlayStation 3's encryption system, thereby gaining the public key required to run any software on the machine.

Legitimate games and movies will only play on the console because the discs provide a password or signature to the encryption system, which recognises them as authorised products. But with the key – essentially a long sequence of numbers – Failoverflow coders would be able to compile their own custom firmware and then build applications that could run on any system. (You can view their presentation here)

Like many members of the hacker community, Failoverflow is resolutely anti-piracy – its members bypass console security systems merely as an intellectual challenge, or to run their own operating systems and applications. Consequently, the group didn't itself reveal the key. However, days later hacker, George Hotz (also known as Geohot), previously responsible for opening the iPhone system to so-called "jailbreak" hacks, *did* released the required firmware package decrypter on his website. Although the current hack requires users to modify their PS3 to run homebrew apps (or use a PS3 'Jailbreak' dongle, which bypasses the security system on machines with older versions of the firmware), further developments may ensure that anyone with the relevant software tools and technical knowledge could produce applications that will run on any PS3. It would then effectively be an open system. And naturally, the floodgates that have prevented widescale piracy on the console for the last few years could be smashed to

pieces.

Console hacking of this sort has been a part of the games industry for over a decade. Sega's Dreamcast console, launched in 1999, was one of the first major targets, favoured by homebrew coders for its powerful hardware, online functionality, and ease of access. The original Xbox also proved to be an easy machine to hack, thanks in part to a leaked SDK, which gave coders low-level access to the hardware.

Both the Nintendo DS and PSP have been comprehensively hacked, too, opening the doors not only to homebrew apps but to rampant piracy. There are products available for Nintendo's handheld that allow gamers to download pirated titles from the web and store dozens on a single cartridge. According to a report published by Japan's Computer Entertainment Supplier's Association last year, piracy on the Nintendo DS and Sony PSP has cost the industry $41bn (£26.5bn) since June 2004. It has also seen dozens of third-party developers and publishers abandoning the platforms. In 2009, Peter Dille of Sony Computer Entertainment Amerrica told Gamasutra, "We can look at data from BitTorrent sites from the day Resistance: Retribution goes on sale and see how many copies are being downloaded illegally, and it's frankly sickening. We are spending a lot of time talking about how we can deal with that problem."

Usually, what happens in these situations is an arms race with the hacker community. An exploit will be devised and distributed and the console manufacturer will release a firmware update that plugs the gap. This repeats, and with popular systems like the PSP, the hackers just keep coming back. As Dark Saviour of the UK-based homebrew news site, DC EMU, explains, "Sony released new firmware to close exploits on the PSP, but you would only need the new firmware for newer games, being on a older firmware did not taint the PSP experience, because it's mosly an offline console. Also with such a great homebrew scene, coders kept finding ways to get round the firmware fixes, and even released firmware downgraders so you could use the new firmware to play the new games and then downgrade your firmware to play your homebrew apps (and unfortunately warez games). It's quite a powerful system, has a huge homebrew library, and getting homebrew running is not that hard. There are many that argue that the PSP would never have sold as well as is has without the great homebrew scene."

Predictably, the manufacturers don't see it that way. Last year, Microsoft took the extra step of banning gamers from Xbox Live if they were found to be running pirated or back-up copies of games on their systems. That may be a possibility for Sony, but updating the firmware is no longer an option: the PS3 hack affects the core of the whole encryption system; the only way to close the door is to launch new hardware with an entirely fresh security setup.

Was this hack always an inevitability? Perhaps not. Failoverflow claims it only started to work on the PS3 system when Sony made the decision to disable the machine's Other OS functionality. This feature allowed owners to install their own Linux OS onto the console, giving them the ability to create and run their own applications, and to load apps developed by other users. It was an interesting invitation to the programming community, harking back to the 1997 launch of the Net Yaroze, a special programmable version of the original PlayStation console, which was widely used by home coders and by universities setting up games develoment courses at the time.

However, at the end of 2009, George Hotz announced via his blog that he was attempting to hack the PS3. His way in was through Other OS. The PS3's security "Hypervisor" allowed homemade Linux to run, but in a supervised mode with no access to lower level system functionality. Geohot bypassed the hypervisor, and published elements of the exploit online leaving the rest of the work to other hackers.

Sony's response was to issue Firmware update v3.21, which disabled Other OS, removing the Linux fuctionality and closing the system to home coders. The move was a red rag to the homebrew community. "[PS3] became a valid target," pytey, a member of Failoverflow told BBC News. "That was the motivation for us to hack it."

But did Sony really have much of a choice? When Other OS was effectively removed, Patrick Seybold, SCEA's director of communications and social media stated in a blog post that "disabling the Other OS feature will help ensure that PS3 owners will continue to have access to the broad range of gaming and entertainment content from SCE and its content partners on a more secure system". And that's the heart of it – the manufacturer's "entertainment partners" rely on the company to ensure their products aren't vulnerable to piracy. As Gamesindustry.biz points out in an editorial today:

> The hackers who follow in Failoverflow's footsteps and create custom firmware to run pirated games, emulators and so on will be targeting Sony's hardware, but it's third-party publishers and developers who have the most right to be outraged. The license fee they pay to Sony for every piece of software they sell is, in many respects, a fee for security – the price of selling software on a platform where piracy is difficult or damn-near impossible. Now that has been taken away from them, with the PS3 looking set to become the easiest platform to pirate software for – easier even than the Wii, DS or PSP, all notorious piracy targets but all of which require some degree of technical knowledge to get pirated software working.

In other words, Sony owes it to the games publishers and movie studios who create products for its machine to maintain a safe, secure platform. As soon as Geohot revealed that exploits were possible via OtherOS, the whole concept was compromised. Sony has already seen game publishers evacuating the PSP platform, it may have felt that there was little choice here.

In the future, is there a way that hobbyist coders could be appeased by console manufacturers? Generally, it's the anti-piracy programmers who have the ability to create hacks and exploits of closed systems – the producers of "jailbreak" cartridges and pirated warez tend to come along afterwards, taking advantage of coders who maintain, perhaps rather idealistically, that they're just interested in the hardware as a development platform.

With this in mind, Space Rogue of the Hacker News Network reckons it's time for console producers to stop viewing homebrew coders as the enemy. "Basically manufacturers really need to start taking advantage of the possibility that their hardware will be modified," he argues. "Doing so should be seen as a profit centre and not loss of sales. Take a look at the Linksys WRT series of routers. A large number of those have been sold specifically because people could mod them and run their own software.

"Sony and other companies are still trying lock down the hardware in an effort to protect their content. The solution here is to open up the hardware, welcome tinkerers and create loyalty to your brand. Another example is the Microsoft Kinect: Micosoft originally tried to lock it down but after people opened it up anyway, MS realised they couldn't keep it closed and opened up the platform resulting in more sales. Unfortunately, based on past moves by Sony I doubt they will take the same approach and the cat and mouse game will continue."

The central problem remains however: once the platform is open to hobbyists, it's open to pirates. Plus, many members of the coding community are unlikely to be appeased by a walled garden approach to hardware access, such as Microsoft's XNA architecture which allow home coders to create Xbox 360 games for distrubution via the Xbox Live

Indie Community. As Dark Saviour suggests, "I think they have some interest, but because they are normally limited in some way, either by licenses or how much of the consoles 'power', they can use, they don't have the same appeal as homebrew. At one stage someone was porting a Mega Drive emu to the Xbox 360 via XNA but they stopped because they released that MS would never let them release it, and XNA will not let you load a DVD – for example, a disc with your Mega Drive roms on it. I would say that Apple has done the best with engaging homebrew coders with the App Store which is far easier to get things released on it – even though Apple still blocks a lot of releases."

Interestingly though, Apple itself is in a similar situation to Sony. The new Mac App store has been hacked within 24 hours of its launch, allowing pirated software to be placed on the platform. Once again, the method has involved replacing signature files on illegitimate apps so that the security system sees them as official releases.

This is a war of attrition between manufacturers and hackers, but it is one in which the resources are utterly asynchronous. Console companies have the money to fund ever more intricate security systems, but they have to ship hardware at some point, and customers will only put up with so many firmware updates and featureset changes. Home coders, meanwhile, lack financial might, but have the time, perseverance and guile to keep chipping away for years on end. Sony has yet to comment on the PS3 hack, but is surely looking into its legal options, which are likely to be complex and limited. In 2007, the AACS encyprition key protecting the HD DVD format was cracked and distributed online; the Motion Picture Association of America sent out cease and desist letters to websites publishing the numbers, but bloggers responded by replicating the code on hundreds of thousands of sites. No cases were brought to court – indeed the American Bar Association issued a report which questioned the illegality of distributing encyrption keys.

For PS3, the future is uncertain. It's possible that hacks will become available, allowing console owners to download game ROMs onto hard drives, USB sticks or Blu-ray discs – these may run without modifications to the console hardware. It puts Sony Computer Entertainment in the same camp as the music and movie industries. Perhaps all that the company can now do is learn a very expensive lesson about the creation of encryption systems, a lesson that must then apply to the production of either the next iteration of PS3, or to any future consoles. For now, it has an open platform on its hands and, very probably, some extremely pressing questions from game publishers.

UPDATE: Sony has claimed to Edge magazine, that it WILL be able to fix the security breach: "We are aware of this, and are currently looking into it," Sony said in a short statement. "We will fix the issues through network updates, but because this is a security issue, we are not able to provide you with any more details."

Next
Previous
Blog home