EXHIBIT BB

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

http://hackmii.com/

Comment: Re:Wow... (Score 1) Comments: 532 **Comments: 532**

by bushing on Wednesday December 29, @05:04PM (#34703922)
Attached to: Playstation 3 Code Signing Cracked For Good

How did Sony fuck that one up? It was my(admittedly layman's) understanding that a public/private key crypto implementation, assuming it isn't deeply flawed, using key lengths suited to the computational capacities of PDP-8s, or otherwise totally fucked, was mathematically secure against anything other than a profound breakthrough in prime factorization algorithms, an unbelievable advance in computational power, or an insider leaking your private key.

Close. These algorithms only work correctly if implemented correctly. There are various known pitfalls with each of these algorithms; for example, the original iPhone was unlocked using an RSA implementation error (Bleichenbacher attack against an RSA implementation that does not correctly validate padding and uses exponent 3). ECDSA happens to have a "pitfall" that leaks information inside the signatures it makes.

This doesn't make it a bad algorithm -- it can achieve the same security of RSA using smaller keys and in less time -- but the "pitfall" here is particularly bad.

Read More...

---

bushing
Firehose
Comments
Submissions
Friends
Tags
Achievements

bushing's Achievements

Days Metamoderated in a Row
Got a Score:5 Comment
The Contradictor

bushing's Comments

Re:Wow...
Re:How did they get the private key, if they did?
Re:Amusing video but...
Re:Well, is this a good thing? (Score:2, Interesting)
Re:Well, is this a good thing?

bushing's Friends

jo_ham
Guy Harris
tepples
daviddennis
MattBurke

bushing's Tags

interesting (submissions)
stale (stories)
kickstarter (submissions)
usb (submissions)
insightful (comments)

bushing's Submissions

Nintendo charges extra fee to repair "hacked&#
XFree86 project releases 4.7.0

Comment: Re:How did they get the private key, if they did? (Score 2) Comments: 532

by bushing on Wednesday December 29, @04:49PM (#34703782)
Attached to: Playstation 3 Code Signing Cracked For Good

They don't have Sony's signing key, from what I've read. What they have is a flaw in the key generation process, which allows them to generate valid signed packages without the

private key. In fact, here's the video from the conference itself: http://www.youtube.com/watch?v=GPjd6gHY6A4

No, GP was right. The exact signing key used by Sony may be derived from the public components of their ECDSA signatures. Not something close; not something equivalent.

Games: Playstation 3 Code Signing Cracked For Good **Comments: 532**

Posted by samzenpus on Wednesday December 29, @04:19PM
from the forever-is-a-long-time dept.
ReportedlyWorking writes

> *"It appears that Sony's PS3 has been fatally compromised. At the Chaos Communication Congress in Berlin, a team named 'fail0verflow' revealed that they had calculated the Private Keys, which would let them or anyone else generate signed software for the PS3. Additionally, they also claim to have a method of jailbreaking the PS3 without the use of a Dongle, which is the current method. If all these statements are true, this opens the door to custom firmware, and homebrew software. Assuming that Sony doesn't take radical action and invalidate their private keys, this could mean that Jailbreaking is viable on all PS3, regardless of their firmware! From the article: 'Approximately a half hour in, the team revealed their new PS3 secrets, the moment we all were waiting for. One of the major highlights here was, dongle-less jailbreaking by overflowing the bootup NOR flash, giving complete control over the system. The other major feat, was calculating the public private keys (due to botched security), giving users the ability to sign their own SELFs. Following this, the team declared Sony's security to be EPIC FAIL!'"*

Playstation 3 code signing cracked for good!-> F-3582 **Comments: 1**

Submitted by F-3582 on Wednesday December 29, @01:33PM
F-3582 writes

> *"The PS3 has finally been cracked wide open! The secret code signing key has finally been discovered. Or as Marcan42 tweets:*
>
> *"FWIW lightning talks tomorrow are at 11:30-13:45. PS3 demo will be 4 minutes _somewhere_ within that range (to be determined). They can try to whitelist every existing piece of official PS3 code... but good luck with that. IOW they CANNOT change keys or fix this in a new firmware, because stuff we sign is every bit as good as existing official software. Wii fakesigning vs. PS3 epic fail: Wii issue is a BUG in console code (fixable), PS3 issue is a FAIL in THEIR secret signer (not fixable)."*
>
> *Read more: http://www.ps3news.com/PS3-Hacks/Fail0verflow-27C3-PS3-Exploit-Hacker-Conference-2010-Highlights/#ixzz19WiQ5llg"*

Link to Original Source

Sony's PS3 Jailbroken Forever-> ReportedlyWorking **Comments: 1**

Submitted by ReportedlyWorking on Wednesday December 29, @12:56PM
ReportedlyWorking writes

> *"It appears that Sony's PS3 has been fatally compromised. At the Chaos Communication Congress in Berlin, a team named "fail0verflow" revealed that they had calculated the Private Keys, which would let them or anyone else, generate signed software for the PS3. Additionally, they also claim to have a method of jailbreaking the PS3 without the use of a Dongle, which is the current method. If all these statements are true, this opens the door to custom firmware, homebrew software, and OtherOS! Assuming that Sony doesn't take radical action and invalidate their private keys, this could mean that Jailbreaking is viable on all PS3, regardless of their firmware!*
>
> *"Approximately a half hour in, the team revealed their new PS3 secrets, the moment we all were waiting for. One of the major highlights here was, dongle-less jailbreaking by overflowing the bootup NOR flash, giving complete control over the system. The other major feat, was calculating the public private keys (due to botched security), giving users the ability to sign their own SELFs Following this, the team declared Sony's security to be EPIC FAIL!""*

Link to Original Source

December 2010
November 2010

Comment: Re:Amusing video but... (Score 1) **Comments: 126**

by bushing on Friday November 26, @04:48PM (#34353200)
Attached to: Stephen Fry and DVD Jon Back USB Sniffer Project

Having worked with several commercial USB protocol analyzers over the years I have yet to see one was anything more than an FPGA connected to an off the shelf USB PHY chip. As much as I like cute dog videos these guys need to post proper requirements and design specifications if they seriously want funding from me.

Click through the links to the actual Kickstarter project description. We did some handwaving to keep it accessible for J. Random (Software) Hacker, but I think we gave enough details to answer your questions.

(tl;dr: yes, you're right, and that's more or less what we're doing. Haven't decided on which PHY to use, looking at some SMSC and NXP parts.)

> OpenVizsla will be a completely open design of a device that can capture USB 1.1/2.0 (high-speed, full-speed and low-speed) traffic passively between a target USB device and the connected host (usually a PC, but potentially anything that has a USB host port -- think Xbox 360 and PS3). It will be controlled by any computer using open-source client software or potentially in standalone mode (where captured traffic is stored onto an on-board SD card).
>
> As is proper for any open and hackable design, unused I/Os on the FPGA will be exposed (via 0.1" header) for use as a primitive logic analyzer. We hope to eventually support additional sniffing interfaces (SPI, I2C RS232, SD card etc) that connect to a high-speed Mictor connector that can act as 'man-in-the-middle' and extend the device capability limitlessly.
>
> The OpenVizsla device is built around a multi-layer PCB with around 180 surface-mount components that allow the target USB packets to be captured, buffered and delivered to the PC (or stored on SD card in standalone mode).
>
> An XMOS event-driven processor will handle the huge amount of USB data (these little chips are fast!) and it will handle the overall communications with the host (which will be a fully published protocol!) and will provide on-board system programming, housekeeping and of course flash the status LEDs! In standalone mode, the XMOS chip will handle data acquisition and SD card storage; this processor is fully reconfigurable and can be modified and reprogrammed to improve the features or adapt to new requirements.
>
> For the high-speed USB signals a Xilinx Spartan3E FPGA (with attached, expandable RAM) will capture, process and buffer the USB traffic from an attached USB transceiver that we use to deserialize the USB signals from the target link.

Stephen Fry and DVD Jon back USB Sniffer Project-> Anonymous Coward

Submitted by Anonymous Coward on Friday November 26, @03:52AM
An anonymous reader writes

> *"bushing and pytey of the iPhone DevTeam and Team Twiizers have created a Kickstarter project to fund the build of an open-source/open-hardware high-speed USB protocol analyzer. The board features a high-speed USB 2.0 sniffer that will help with the reverse engineering of proprietary USB hardware, the project has gained the backing from two high-profile individuals Jon Lech Johansen (DVD Jon) and Actor and Comedian Stephen Fry"*

Link to Original Source

The Openvizsla USB sniffer board-> godofpumpkins **Comments: 1**

Submitted by godofpumpkins on Tuesday November 23, @07:06PM
godofpumpkins writes

> *"bushing and pytey of the iPhone DevTeam have started a kickstarter project to fund the build of a open-source/open-hardware high-speed USB protocol analyzer. The board features a high-speed USB 2.0 sniffer that will help with the reverse engineering of proprietary USB hardware."*

Link to Original Source

Apple: Old Apple 1 Up For Auction, Expected To Go For $160,000+ **Comments: 156**

Posted by Soulskill on Friday November 12, @02:48PM
from the doesn't-run-flash dept.
vanstinator was one of several readers to point out that Christie's is holding an auction for one of the original Apple 1 machines, complete with a manual, the original shipping box, and the letter from Steve Jobs to the owner. The invoice says the computer was purchased on December 7th, 1976, with an Apple cassette interface card, for a total price of $741.66. The auction house expects it to sell for over $160,000.

November 2010
September 2010

Comment: Re:Well, is this a good thing? (Score 2, Interesting) **Comments: 169**

by bushing on Sunday September 19, @09:50PM (#33631906)
Attached to: Emulation Arrives On the PS3

Yup, similarly to the DS homebrew scene. IIRC the libdns homebrew library had parts which were ripped of the original nintendo SDK... of course people just turned a blind eye on that

It's a subject of some debate. The Xbox homebrew scene, as I understand it, used files directly copied from a leaked Xbox SDK. libnds uses some code that is more or less directly translated from disassembled DS SDK code (though you can get most of the same code from dumped games anyway); some feel that this is morally / legally equivalent to just copying the files.

Comment: Re:Well, is this a good thing? (Score 1) **Comments: 169**

by bushing on Sunday September 19, @09:39PM (#33631870)
Attached to: Emulation Arrives On the PS3

I fail to see your logic, there is no independent group in charge of banning people from the PSN. If Sony decides to ban you, there is absolutely nothing you can do about it, regardless of the reason they ban you.

Sure -- if Sony decides to ban you, you've already messed up. Sony can't "decide to ban you" if they can't tell you've done anything naughty, so it's better to avoid permanent changes to the console that can be detected by their software.

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