

TECH

6G iPod nano hack just beginning of long road to nano apps

A secondary school student from Ireland has gotten developers interested in ...

CHRIS FORESMAN - JAN 3, 2011 6:44 AM | 18



➔ Credit: James Whelton



Eighteen-year-old James Whelton never imagined he'd become a minor Internet celebrity, nor did he plan to kickstart a race to hack Apple's sixth-generation touchscreen iPod nano. But the secondary student from Cork, Ireland found himself doing just that this week after winning a pink 8GB iPod nano in a student Web design contest. Now the teen is working with some well-known iOS developers and hackers to try and suss out a way to load and run custom software on the tiny device. While much progress has been made in the last few days, figuring out how to code software for the device could take significant time and resources to accomplish.

On a flight home from a conference where he won the iPod nano, Whelton decided to pass the time by attempting to hack his new prize. "It was just a product of boredom," he told Ars. "All the factory-installed stuff was seemingly boring to me, and I had time to kill, so I started playing with it."

The system-on-a-chip that powers the touch-based nano is in fact similar to the SoC used in both the fourth-gen iPod nano and the second-gen iPod touch. And while the device has a user interface that appears similar to that of iOS, it actually runs the same Pixo OS that has powered all iPod and iPod nanos since the original iPod was released in 2001. Whelton noted that plenty of work has been done to hack fourth-gen nanos, and he used knowledge of techniques used on that device to gain limited access to the system running on the touch-based nano.

ARS VIDEO

How Scientists Respond to Science Deniers



This led Whelton to discover a file called `IconState.plist`. This file controls what icons are displayed on the nano's tiny screen to access different functions. While the file itself doesn't make any reference to "SpringBoard," the visual UI and application launcher used on iOS devices, the app icons themselves are labelled "SBPhotos," "SBSongs," etc, leading Whelton and others to refer to the launcher UI on the nano as its "SpringBoard."

ADVERTISEMENT

What Whelton was able to do in his early hacking attempts was discover a way to bypass the nano's cache-checking feature, which allowed him to load a modified version of IconState.plist. By modifying this file, he was able to remove one of the icons on the nano's display, leaving a blank space on the SpringBoard.

"In terms of technical hacking it was nothing impressive," Whelton told Ars, but it did show that it was theoretically possible to get the device to load modified files, and even possibly display custom icons on the SpringBoard.

More importantly, his small hack attracted the attention of other developers. Developer Steven Troughton-Smith was able to find what he described as the nano's equivalent of the iOS DFU recovery mode, and modified a hacking tool called iRecovery to allow reading and writing files on the device.

Developers connected to the iOS jailbreak scene, including "DarkMalloc" and "Chronic" also began digging in to the firmware of the device. While no critical details have yet been uncovered, references to features including video playback and audio recording have been discovered in the devices firmware. The current hardware may be capable of much more than Apple has revealed so far, or those references may be features planned for a future iPod nano update.

"A few guys are hacking up the firmware at the moment," Whelton said. "We're working on it and making measurable progress. But it will take time before we know what the state of play is with us making our own apps."

"It's the same with everything—we'll have to play, hack, and learn, but the creation of our own apps is a top priority," Whelton explained.

ADVERTISEMENT



Tough nut to crack

While the progress so far is promising, and the existence of games for previous-generation nanos shows that running additional apps is possible, developing a custom app for the device won't be as easy as working with iOS. Apple provided a Pixo OS SDK to licensors like Electronic Arts and PopCap, both of which produce games for older iPods, but there isn't one for the latest nanos. "No 'normal' developer has ever had access to any of that stuff," Troughton-Smith told Ars.

"We have no idea what the internals look like—what the binary format is, how to make a toolchain to build apps," Troughton-Smith explained. "Apple may have a UI library on the device for their built in apps, or the apps may well be baked into the OS shell [SpringBoard] itself. We don't know anything about it."

Since the nano shares similar CPU and graphics resources as the second-gen iPod touch, however, it should be capable of some pretty impressive graphical applications. "Pixo uses OpenGL ES heavily, so if we were to ever build apps for it, games would be the easiest to port," Troughton-Smith said.

Both Whelton and Troughton-Smith were quick to point out that things are in the very early stages. "Suffice it to say, this all like what, a few days old?" Whelton said.

Troughton-Smith said that Whelton's work is the very first step in a long chain of events that have to happen before custom apps can be loaded. Pushing code, executing code, finding exploits, decrypting firmware, modifying firmware, and building a toolchain all come before writing apps is possible.

"We're at the push-and-execute stage," Troughton-Smith said. "To get anywhere further, an exploit will need to be found."



CHRIS FORESMAN

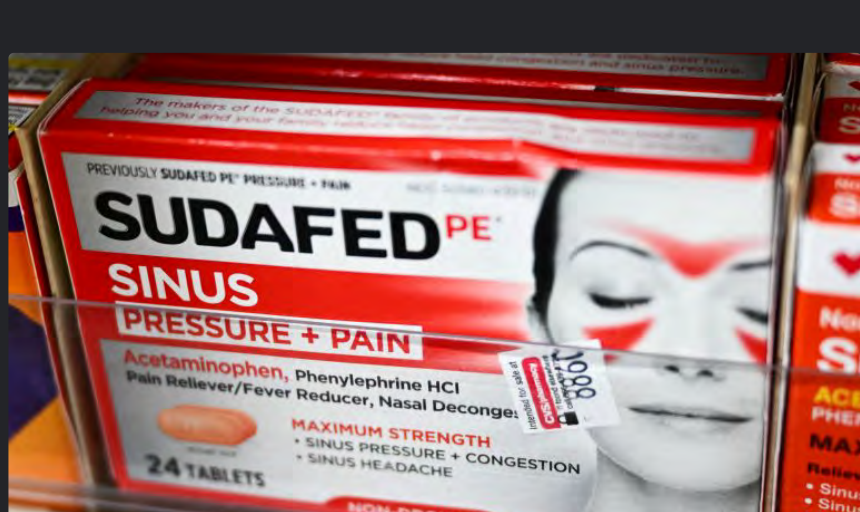
Chris is an Associate Writer at Ars Technica, where he has spent the last five years writing about Apple, smartphones, digital photography, and patent litigation, among other topics.

18 COMMENTS

➔ PREV STORY

NEXT STORY ➔

MOST READ



1. **After decades, FDA finally moves to pull ineffective decongestant off shelves**

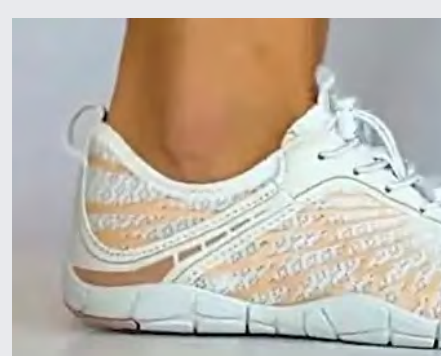
2. **Sega is delisting 60 classic games from Steam, so now's the time to grab them**

3. **Trump's likely FCC chair wrote Project 2025 chapter on how he'd run the agency**

4. **Review: M4 and M4 Pro Mac minis are probably Apple's best Mac minis ever**

5. **Secondhand EVs will flood the market in 2026, JD Power says**

Sponsored Links by Taboola



These Barefoot Shoes are Leaving Neuropathy Exper...

Barefoot Vitality



Wyoming: Big Changes Near Afton Leaves Drivers...

Comparisons | A... Learn More



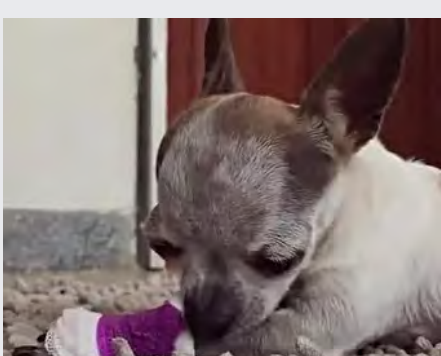
Surgeon Reveals: Don't Lotion Your Dark Spots! Use T...

Miami M.D.



Here Are 23 Of The Coolest Gifts For 2024

Best Tech Trend Learn More



Paw Licking Driving You Crazy? Top Vet Says To Make One...

Ultimate Pet Nutrition



25 Coolest Gadgets You Can Actually Buy

Cool Gadgets

Get Offer