# Cryptography failure leads to easy hacking for PlayStation Classic

Enlarge / The PlayStation Classic’s internal USB, removed and picked at as part of the hacking effort.

## reader comments

78 with 62 posters participating, including story author

## Share this story

In the days since the PlayStation Classic’s official release, hackers have already made great progress in loading other PlayStation games (and even non-PlayStation software) onto the plug-and-play device. What’s more, it seems some sloppy cryptography work on Sony’s part is key to unlocking the device for other uses.

Console hackers yifanlu and madmonkey1907 were among those who were able to dump the PlayStation Classic’s code via the system’s UART serial port in the days after its release. From there, as yifanlu laid out on Twitter, the hackers found that the most sensitive parts of the system are signed and encrypted solely using a key that’s embedded on the device itself, rather than with the aid of a private key held exclusively by Sony. In essence, Sony distributed the PlayStation Classic with the key to its own software lock hidden in the device itself.

Further examination by yifanlu during a series of marathon, Twitch-streamed hacking sessions found that the PlayStation Classic also doesn’t seem to perform any sort of signature

check at all for the sensitive bootrom code that’s loaded when the system starts up. That makes it relatively trivial to load any sort of payload to the hardware from a USB device at startup, as yifanlu demonstrated with a video of a *Crash Bandicoot* prototype running on the PlayStation Classic last week.

These revelations have already led to a couple of open source projects that let PlayStation Classic owners load a USB thumb drive with a correctly formatted payload that can get the hardware to temporarily recognize and run new sets of PlayStation games. The current tools require some decently onerous editing of database or INI files and may not work correctly on every regional variation of the system at the moment. There are also reports of improperly formatted payloads bricking systems, so please take care if experimenting with them yourself.

The relative ease of PlayStation Classic hacking stands in stark contrast to similar efforts on the NES and Super NES Classic Edition systems. Hacking those devices requires dumping the contents of that specific system to a computer over USB, then modifying those files and reflashing the system’s kernel using a hacker-coded tool.

In any case, the almost total lack of functional security on the PlayStation Classic itself probably means we’re only seeing the very beginnings of what hackers will be able to unlock on the ARM-based system. There is already video evidence of a Linux-based *Doom* port running on the hardware, which probably means getting non-PlayStation emulators running on the console is only a matter of time.

https://arstechnica.com/?p=1425895