Nintendo Entertainment Security

A Review of Nintendo Console Hacking

By: Chris Phifer

Introduction

Nintendo Facts

- Overall top seller of video game hardware, overtaking both Sony (PlayStation et al) and Microsoft (XBox et al)
- At one point had an NES in 33% of homes in the United States
- Infamously anti-homebrew, starting with the NES and the cheat devices for it released soon after

Consoles We'll See

For the purposes of this talk, we'll look at three Nintendo consoles:

- Nintendo Entertainment System
- Wii
- Switch

Nintendo Entertainment System

(Image taken from: https://images-na.ssl-images-amazon.com/images/I/61S2kp8sjoL._SL1200_.jpg)

- Released: 1983
- Units sold since release: ~62 million
- 8-bit architecture, reportedly saved the video game industry after the famous crash

Wii

(Image from https://upload.wikimedia.org/wikipedia/commons/1/14/Wii-console.jpg)

- Released: 2006
- Units sold since release: ~102 million
- Weak performance for generation, but popularized motion controls as a new paradigm for gaming

Switch

(Image from https://assets1.ignimgs.com/2017/01/20/nintendo-switch-button-2-1484875049952.jpg)

- Release: 2017
- Units sold since release: 42 million
- Weak performance for generation, but once more shifted the paradigm by blurring the lines between home console / handheld gaming

The Nintendo Entertainment System

Hardware Hacks: The Game Genie

- Game Genie was released as a third-party piece of hardware for the NES
- Allowed the user to input “patch codes” which were effectively game-code level cheats
- Exploit: An exposed data pathway between cartridge and console that, with no knowledge of the actual code, could be experimented with until useful results turned up (e.g. infinite health, infinite lives, otherwise inaccessible content)

Software Hacks: A PDF-ZIP-NES Game Quine

- Reverse engineers created an NES game that's also a valid PDF and valid ZIP archive, and even more it prints out its own MD5 hash when loaded on an NES

- How it works: Special sections in NES code layout that can be used to embed other file format headers, black magic to print out the MD5 hash of the program itself

- Demonstrates unique / outlandish uses of special-purpose hardware/software far outside of its intended use

The Nintendo Wii

Homebrew: Custom, Non-Licensed Software

- Homebrew: General term for firmware/software not officially supported by a developer or manufacturer; borrowed from the home brewing of beer and other alcoholic beverages

- Generally allows for greater system control, installation of third-party applications that aren’t licensed, possible use as a pathway to piracy and other illegal activities

WiiBrew: Homebrew for the Wii

- WiiBrew: A community of homebrewers who work on the Nintendo Wii
- Publish instructional information for newcomers, support a community of developers publishing both exploits enabling homebrew and new software that can be installed once custom firmware payloads are injected

Nintendo v Homebrew

- Nintendo traditionally averse to homebrew:
  - Concerns about damage to device hardware/software; can leave a console ‘bricked’
  - Concerns about piracy
- Work in recent years to combat homebrew, particularly in terms of piracy prevention. Patches to Nintendo eshop servers prevent 3DS, Wii, and (as we’ll see later) Switch from using workarounds to download legitimate copies of games for free

Wii Homebrew Basics

- Custom software written to be compatible with architecture, but blocked through licensure measures built in to the operating system
- Idea: Use exploits in various games / built-in applications to force execution of a carefully structured payload on an SD card in the console
- Do it once, change relevant security parameters, never have to do again & can safely keep receiving official Nintendo updates

The Nintendo Switch

Homebrew Redux

- The Switch is very new still, but has already been a target for exploitation, particularly via traditional homebrew techniques
- Similar community to WiiBrew; support for those new to console hacking, a number of developers producing custom apps, etc
- Problem: Crackdowns from Nintendo

Connectivity Focus: Homebrew Demise

- In 2006 with the Wii, connectivity was used (limited multiplayer in some games, browsing via console, some digital distribution) but since then digital distribution has become the norm

- The Switch relies heavily on its Internet-connectedness, and this provides a new attack vector for console hackers (both malicious and not)

- Nintendo cracks down on homebrew via physical device bans rather than accounts; harsh consequences for exercising freedom with one's personal property (e.g. can't install new games officially)

There’s lots of cool console hacking!

Applications

Is This Useful?

Some uses of console hacking we've seen / will see:

- Control of personal property
- Flipped: Nintendo uses knowledge to improve device security
- Cheating
- Speedrunning!

Control of Personal Property

- Console hacking is a straightforward example of exercising agency over one’s property: If I own a thing and want it to do more, I should in theory be able to make it do so
- This has legal consequences potentially, though, since gaining administrative control of a device often means being able to bypass piracy protection
- Difficult to balance control with legality

Improving Future Security

- All of this console hacking is advanced reverse engineering: Can be used by Nintendo directly to understand the types of exploits their hardware / software is vulnerable to, avoid it in the future

- Double-edged sword: How do they give users control of the devices they own without allowing for malicious use? Can lead to a “police state” mentality

- Nintendo hiring security experts for these purposes: https://careers.nintendo.com/job-openings/listing/190000002R.html?

Cheating

- Cheating in games can be fun! Overpowered behaviors, access to hidden content, messing around, etc
- Console hacking gives hardcore cheaters insight into how the console actually works, even if Nintendo et al don’t release full technical details
- Gives insight into the act of reverse engineering itself, given the complex nature of special-purpose hardware/software

Speedrunning

- Increasingly popular competitive video gaming: How fast can you beat X given some constraints (e.g. no major glitches)?
- Not just a competition: AGDQ / SGDQ are now large-scale annual charity events supporting Doctors Without Borders and the Prevent Cancer Foundation
- Console hacking helps speedrunners develop new techniques / gain more insight into games so they can hone their craft

Conclusion

Summary

- Console hacking has been going on with Nintendo devices since their flagship console, the NES, and has only gotten more sophisticated since
- Console hacking continues to happen despite attempts by Nintendo to curtail it
- There are many applications of console hacking, both on Nintendo's end and the user's end, ranging from preventive security measures to executing cheats at the game-code level

References

[1] (Various Sources and Authors) WePC 2019 Video Game Industry Statistics, Trends & Data,

https://www.wepc.com/news/video-game-statistics/

[2] Littrell, Drew. “That Time Atari Cracked the Nintendo Entertainment System”,

https://hackaday.com/2018/10/22/that-time-atari-cracked-the-nintendo-entertainment-system/

[3] Aclin, Justin and Garcia, Eddie. “Two Mario Games Continue Nintendo Switch and Nintendo 3DS Momentum Into 2019”,
https://www.businesswire.com/news/home/20190111005064/en/Mario-Games-Continue-Nintendo-Switch-Nintendo-3DS

[4] Welsh, Oli. “A complete history of Nintendo console launches”,

https://www.eurogamer.net/articles/2017-02-24-a-complete-history-of-nintendo-console-launches

[5] (Company collected statistics) “Dedicated Video Game Sales Units”,

https://www.nintendo.co.jp/ir/en/finance/hard soft/index.html

References (cont'd)

[6] Base System. "Nintendo Entertainment System/Famicom: Console Information",

https://www.consoledatabase.com/consoleinfo/nes/

[7] IGN. "IGN: Revolution's Horsepower",

http://wii.ign.com/articles/699/699118p1.html

[8] TechOn! "PS3 VS Wii, Comparisons of Core LSI Chip Areas",

http://techon.nikkeibp.co.jp/english/NEWS EN/20061127/124495/

[9] MITRE. "2019 CWE Top 25 Most Dangerous Software Errors",

https://cwe.mitre.org/top25/archive/2019/2019 cwe top25.html

[10] SethBling. "Super Mario World – Credits Warp in 5:59.6 (First Time Ever on Console)",

https://www.youtube.com/watch?v=14wqBA5Q1yc

References (cont’d)

[11] NESWorld. “Game Genie - The Video Game Enhancer”,

http://www.nesworld.com/gamegenie.php

[12] Sultanik, Evan & Teran, Evan. PoC —— GTFO. “This PDF is an NES ROM that prints its own MD5 hash!”,

https://www.alchemistowl.org/pocorgtfo/pocorgtfo14.pdf

[13] WiiBrew. “Brick”,

https://wiibrew.org/wiki/Brick

[14] Switch Homebrew Guide. “The Ultimate Noob Guide for Hacking your Nintendo Switch”,

https://switch.homebrew.guide/

[15] Andy. TorrentFreak. “Nintendo Plugs Leak That Provided Free 3DS Game Downloads”,
https://torrentfreak.com/nintendo-plugs-leak-that-provided-free-3ds-game-downloads-180823