Cyber Security and Video Game Speedrunning

Jordan

Mike

Quick Overview

- Basic Speedrunning
- Tool-Assisted Speedrunning (TAS)
- Emulation
- Reverse Engineering
- Fuzzing
- Hardware Hacking
- Arbitrary Code Execution

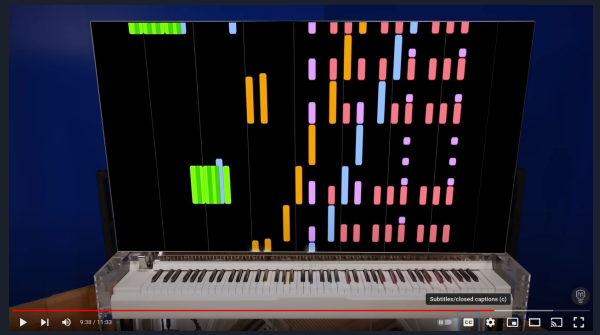
Speed Running

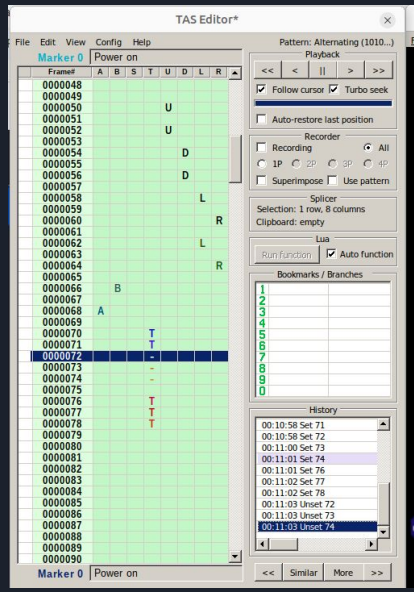
- Playing a video game as fast as possible
  - Any % - get to the ending as fast as possible
  - 100% - full completion of game (collect all items, play all levels)
  - Glitchless - can't use glitches during gameplay
- How fast can you play through Zelda BotW or TotK?
  - I'm 110 hrs into TotK, only have 3 heroes with me
  - BotW took me over 100 hrs…
- Some records from Speedrun.com
  - Zelda: Breath of the Wild takes < 24 min
  - Zelda: Tears of the Kingdom < 44 min
- 2 Big Speedrunning Marathons each year for charity
  - Jan - Awesome Games Done Quick (AGDQ)
  - Jun - Summer Games Done Quick (SGDQ)

Zelda BotW Speedrun Excerpt

Tool-Assisted Speedrunning (TAS)

- Precise manipulation of all controller inputs faster than humanly possible
- Typically Requires
  - Emulation
  - Save States
  - Frame by Frame Control inputs
- Doom Done Quick (1999)
- Contra - Konami Code





Emulators

- Software that enables a computer system (host) to behave like another (guest)
- Have a way to interact with guest (I/O)
  - Controller inputs
  - Networking
  - Keyboard / Mouse
  - Graphics
- Simulation CPU operation
  - Understand and implement all assembly instructions
  - Processor interrupts / exceptions
- Memory
  - ROM Chips
  - Virtual addressing modes
- Debugging
  - Stepping through code as it executes

Speedrunning vs Security Researcher

Feature	Speed Runner	Security Researcher
Save State	Rewind to improve each segment of speed run	Freeze malware before it starts malicious activity.
Crafting inputs	Precise controls / frame perfect inputs	Crafting the perfect set of bytes to trigger vulnerability or exploit
Memory Introspection via Debugger	How can I manipulate game state / PRNG	Examine memory contents after this virus deobfuscates itself
No original hardware required	Old consoles unreliable, analog video, expensive.	Real hardware may not be available, rare, too expensive.

Reverse Engineering

- What controller inputs make me go fastest?
- What attacks do the most damage?
- Live Split timing - inspects memory to detect run time / changes in game state
- Trainers (cheats)
- Cracking copy protection (not piracy)
    - Floppy disks with fuzzy bits / busted sectors
    - DRM that breaks games on newer operating systems
    - Does your PC still have a CD-ROM or floppy drive?
    - Rockstar games has repeatedly sold cracked copies of their own games on Steam
    - Old hardware that doesn't work

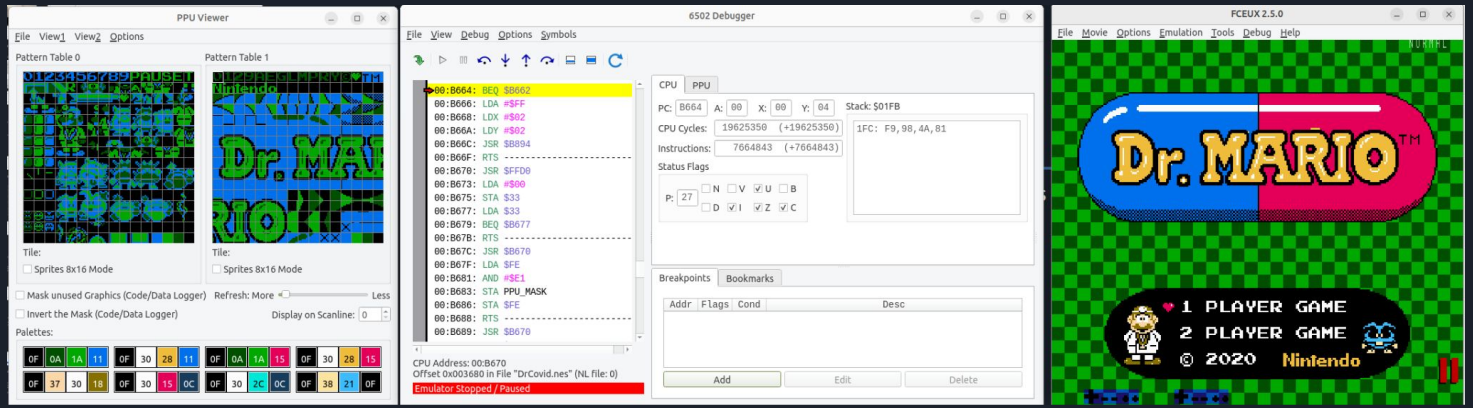
Rom Hacks / Patching

- Randomizer
  - Change item locations so game route has to change randomly
- Level Customizations:
  - Kaizo
- Relay Races
- Regular ROM Hacks
  - Language translations
  - Quality of life
  - Custom levels / Artwork
  - Extra Difficulty

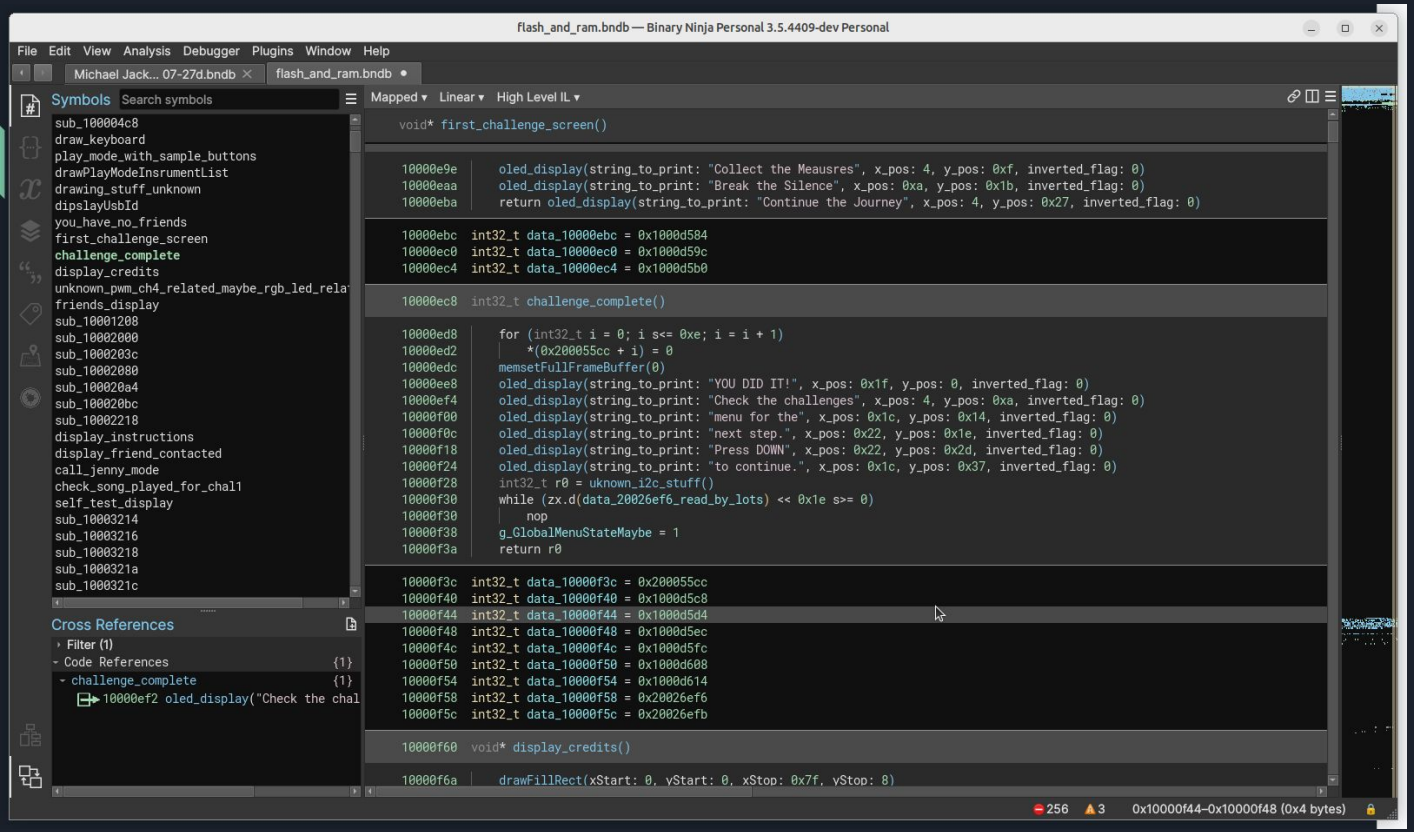
- Disable anti-debugging / security features
- Disable encryption on comms
- Add in secret features

Reverse Engineering Tools

- Convert binary data from ROM into assembly instructions / game data
- Convert assembly code into high-level code / C code
- Create data structures / further understand code
- Assign names to function / variables
- Go back and forth between debugging and static analysis

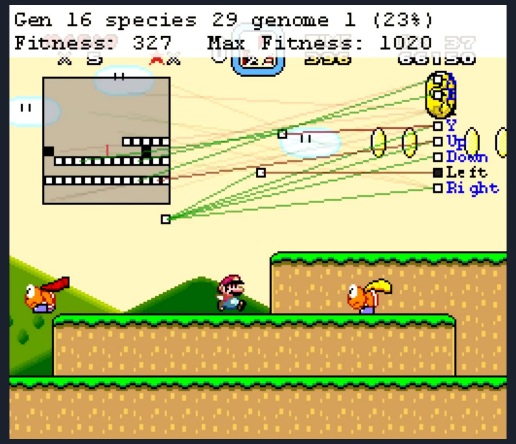


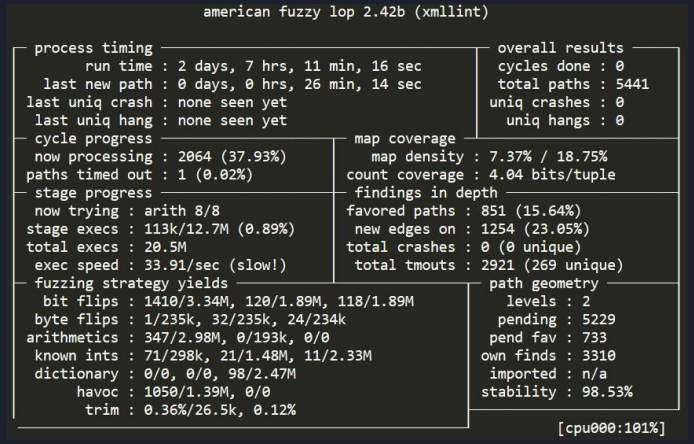
Reverse Engineering Tools



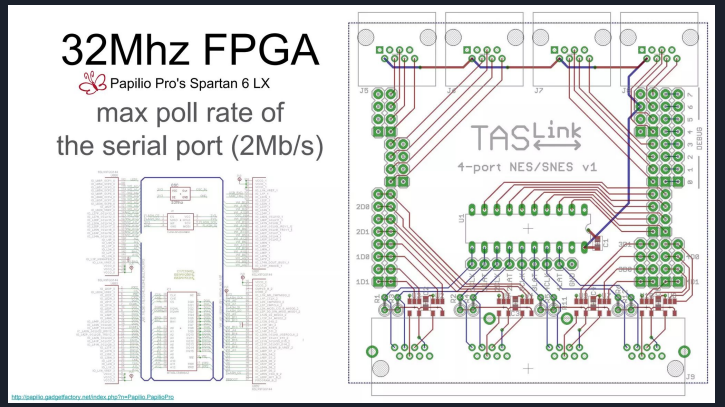
Fuzzing

- Send random data (or corrupt / randomize parts of good data) into a software system
- Monitor the system and check for anomalous outputs
- Repeat until things break, study the input, determine why the input breaks the system
- TAS: MarI/O, Mario FLOW (Mario Kart AI), PlayFun, Bizqwit TAS runs
- Fuzzers: AFL, AFL++, libFuzzer





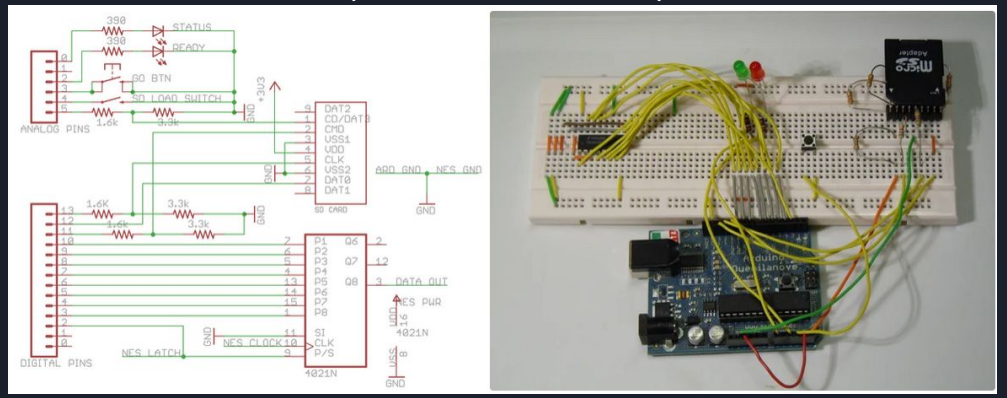
Hardware Hacking



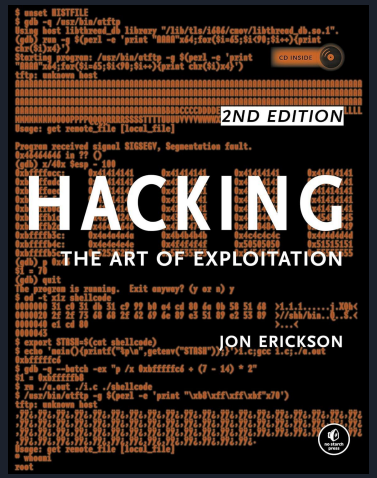
- Build custom circuits to get controller inputs Into the console
- Electrical Engineering skills
  - Digital circuit design
  - Custom FPGAs

Hacker Badges!

Micro500 - Early TAS hardware, ran script from SD card



Arbitrary Code Execution



- Using item manipulations / memory corruption bugs
  - Change the flow of code of a program
- Credits warp
- Adding whole new games / modes / code
  - Snake/Pong game in Super Mario World
  - Pokemon Red with Twitch Chat on SNES
  - Pokemon Yellow with Tetris, SMB, Portal music

Super Mario World TAS Excerpt

Hackable Games

More than just speedrunning, other reasons to hack games:

- For fun!
- For ~~profit~~!
- For learning

Hackable Games

PwnAdventure

- PwnAdventure2
- PwnAdventure3
- PwnAdventureZ (NES)
- SuperMonsterBall
- Sourcery (Online)

Squally

Education and Training

- 4 years of college recommended
  - Computer Science
  - Computer Engineering
  - Electrical Engineering
- Preferred Languages: C/C++, Python
- College 4 year degree not required, but it opens extra doors. It's a great ROI
- Cyber Security Clubs
  - West Shore Computer Science Club
  - FITSec (Florida Tech)
  - HackUCF (UCF)
- Coding contests / challenges
  - Advent of Code
  - Game Jams
- Capture the Flag
  - Online cybersecurity competitions

HACK UCF

CTF TIME

Security as a Field

- Defense (bigger!)
  - Malware Analysis
  - Incident Response
  - Forensics
  - Network Security
- Offense (more fun!)
  - Network Penetration Testing
  - Vulnerability Research
  - CNO Dev

Government vs Commercial

Government

- ❌Clearance usually required
- ✅More offensive opportunities
- ✅More stable
- ✅Patriotism / Make a difference
- ❌Less pay
- ❌More geographically restricted

Commercial

- ✅No clearance required
- ❌Defensive focused
- ❌Less Stable
- ❌Less impactful
- ✅Much higher pay opportunities
- ✅More flexible location/WFH

Salary and Compensation

- New Grads with 4 year degree
  - $90,000 - $100,000 ($42 - $48 per hour)
  - Benefits
    - Health Insurance
    - 401K matching 5-10%
    - Yearly Bonus 10%
- Lots of different types of Cyber Security - Ethical Hacking / Offensive Cyber
  - Reverse Engineer
  - Vulnerability Researcher
  - CNO developer
- Companies: Raytheon CODEX, Research Innovations, Red Lattice, Cromulence, STR
- Cyber Security has typically had better benefits, raises, work perks, training than typical engineering firms

Other Factors

- Fun / Interesting Work
  - You get to hack things, and get paid for it
- This stuff matters
  - ***NOT*** annoying people with ads / stealing customer data to resell
  - ***NOT*** writing backend middleware connecting web sites to the cloud
  - You are helping your country / war-fighters
- You will never stop learning
  - Work is challenging / constantly solving new problems
  - Constantly learning new things
  - Tools / techniques you learn for cyber will make you a better developer
- Impact / Reward
  - Great feeling to land your exploit / crush a new piece of HW / SW

Attributions

- Youtube: BotW Any% 23:42 [WR] by Player5
- Youtube: How to create the perfect speedrun by Bismuth
- Youtube: [TAS] Mario Kart 64 - All Cups -- 1P, GP, 150cc in 20:33:32 by weatherton
- Youtube: MarI/O - Machine Learning for Video Games by SethBling
- Book: Hacking: The Art of Exploitation by Jon Erickson
- Youtube: Super Mario World TAS Arbitrary Code Execution Demo by Masterjun3
- Micro500: https://www.instructables.com/NESBot-Arduino-Powered-Robot-beating-Super-Mario-/
- Youtube: TASBot at DEF CON 24 - Robot Hacks Video Games full talk by dwangoAC
- Youtube: SNES Code Injection - Flappy Bird in SMW by SethBling
-

Questions?!