Game Hacking, Speedrunning, and Cyber Security

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

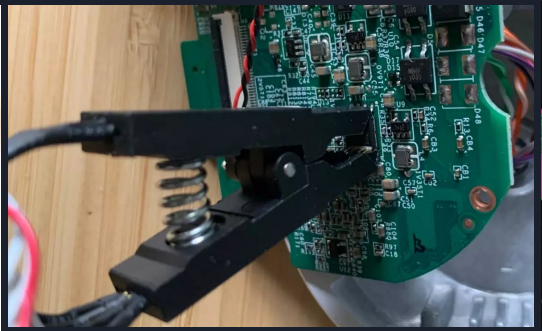
Speedrunner Goals

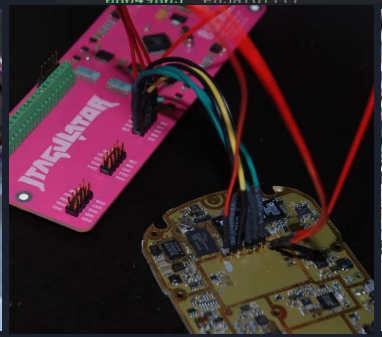
- Fastest paths
- What are the actual stats for items in game?
  - Damage a weapon does
  - Health of a monster
  - Weaknesses
  - Drop rate of items
- Undiscovered secrets
- RNG manipulation
- What controller inputs / mechanics make me go fastest?

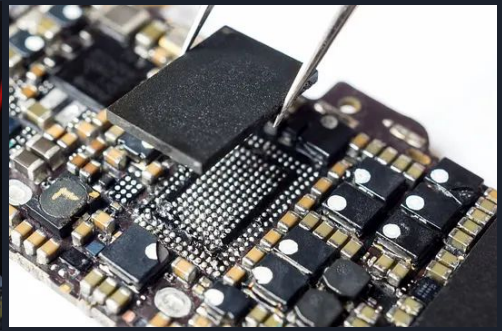
Static Analysis

- Acquire binaries
- Open disassembly in RE tool
  - Can “decompile” to C
- Label function names
- Label variables (global and local)
- Add comments
- Create structures
- Create classes (for OO programs)

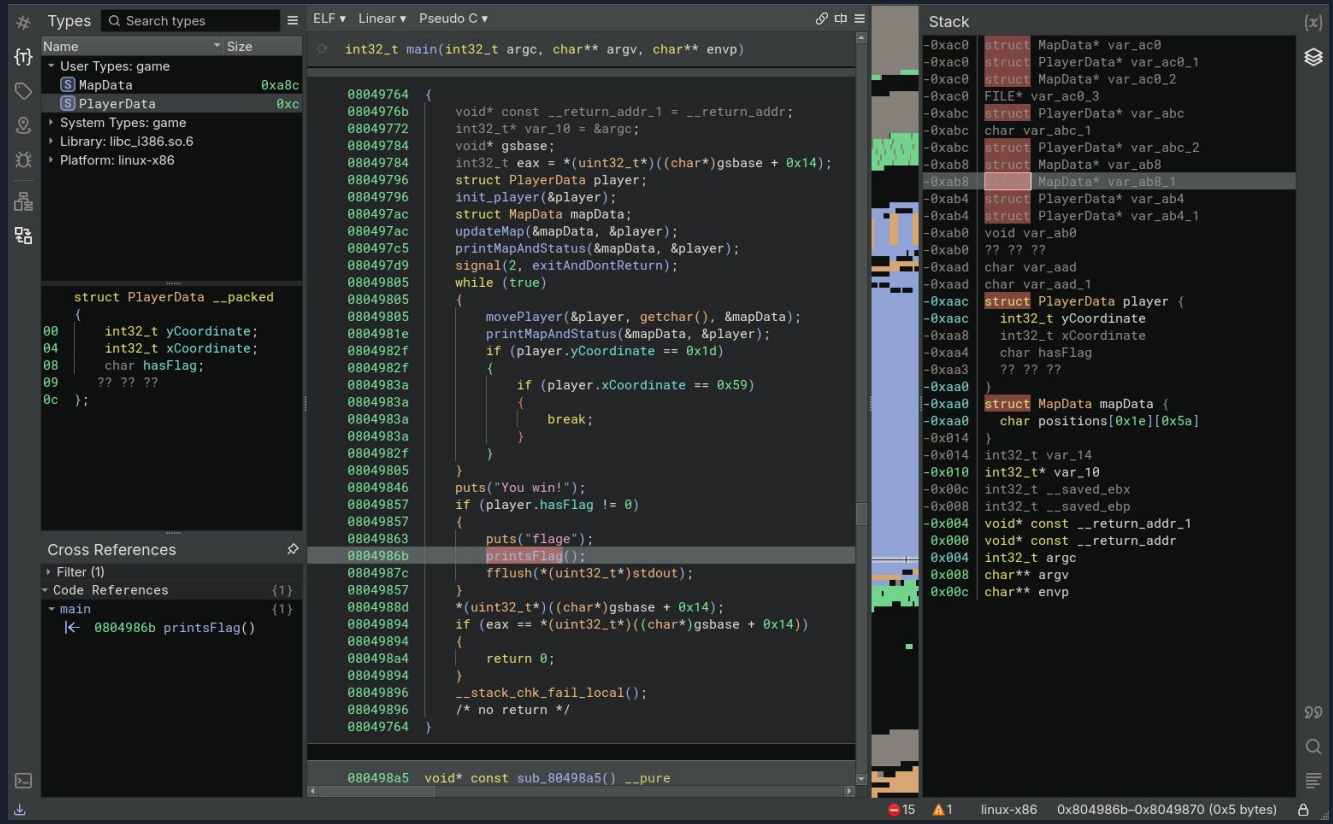
```
ELF ▾  Linear ▾  Disassembly ▾

int32_t main(int32_t argc, char** argv, char** envp)

080497ab  50              push    eax {var_aa0} {var_ab8}
080497ac  e817fbffff      call    sub_80492c8
080497b1  83c408          add     esp, 0x8
080497b4  83ec08          sub     esp, 0x8
080497b7  8d855cf5ffff    lea     eax, [ebp-0xaa4 {var_aac}]
080497bd  50              push    eax {var_aac} {var_abc}
080497be  8d8568f5ffff    lea     eax, [ebp-0xa98 {var_aa0}]
080497c4  50              push    eax {var_aa0} {var_ac0}
080497c5  e8c0fcffff      call    sub_804948a
080497ca  83c410          add     esp, 0x10
080497cd  83ec08          sub     esp, 0x8
080497d0  8d8316d2ffff    lea     eax, [ebx-0x2dea]  {sub_8049216}
080497d6  50              push    eax  {sub_8049216}
080497d7  6a02            push    0x2
080497d9  e8b2f8ffff      call    signal
080497de  83c410          add     esp, 0x10

080497e1  e88af8ffff      call    getchar
080497e6  88855bf5ffff    mov     byte [ebp-0xaa5 {var_aad_1}], al
080497ec  0fbe855bf5ffff  movsx   eax, byte [ebp-0xaa5 {var_aad_1}]
080497f3  83ec04          sub     esp, 0x4
080497f6  8d9568f5ffff    lea     edx, [ebp-0xa98 {var_aa0}]
080497fc  52              push    edx {var_aa0} {var_ab8_1}
080497fd  50              push    eax {var_abc_1}
080497fe  8d855cf5ffff    lea     eax, [ebp-0xaa4 {var_aac}]
08049804  50              push    eax {var_aac} {var_ac0_1}
08049805  e85afdffff      call    sub_8049564
```





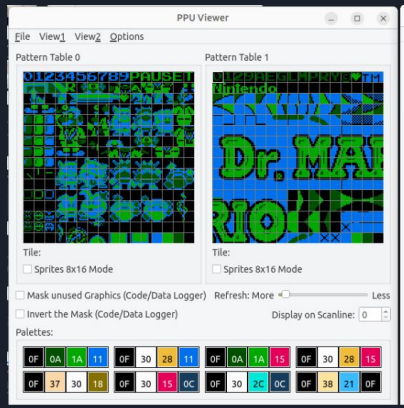


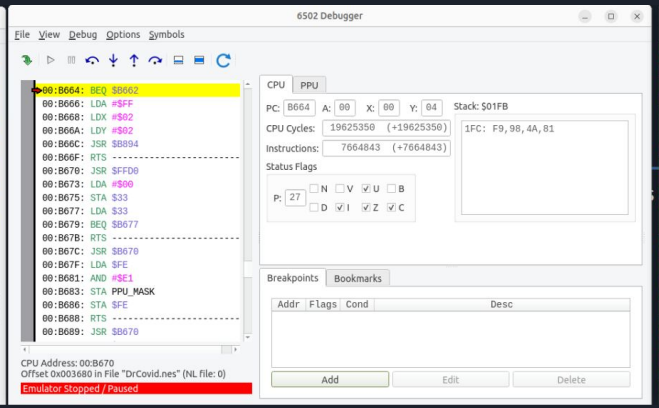
Now function is mostly readable

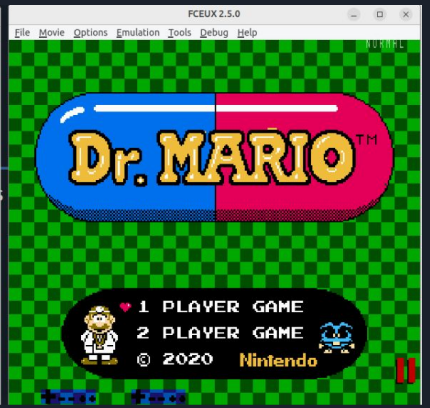


Emulators / Dynamic Analysis

- Simulate hardware running the game on your PC
- Emulator Duties
  - Simulate all CPU instructions
  - Simulate I/O: memory, disk drives, controllers, video output
- Inspect system / memory state while program runs
- Can single step through bugs / glitches
- Save / load game at any state. Replay





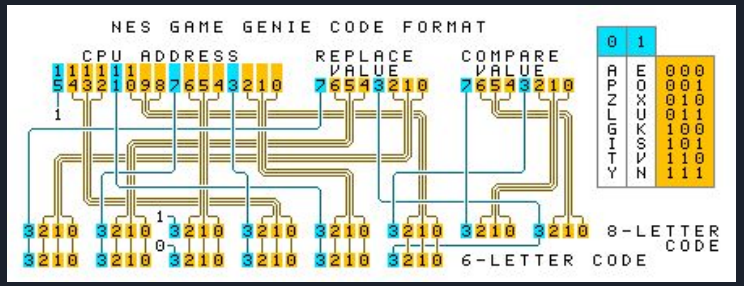


Reverse Engineering Benefits

- Live Split timing - inspects memory to detect run time / changes in game state
- Recompilation
  - Mario64 PC Port
  - Mario 64 60FPS N64 optimization
- Preservation projects
  - Cracking copy protection (not always 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

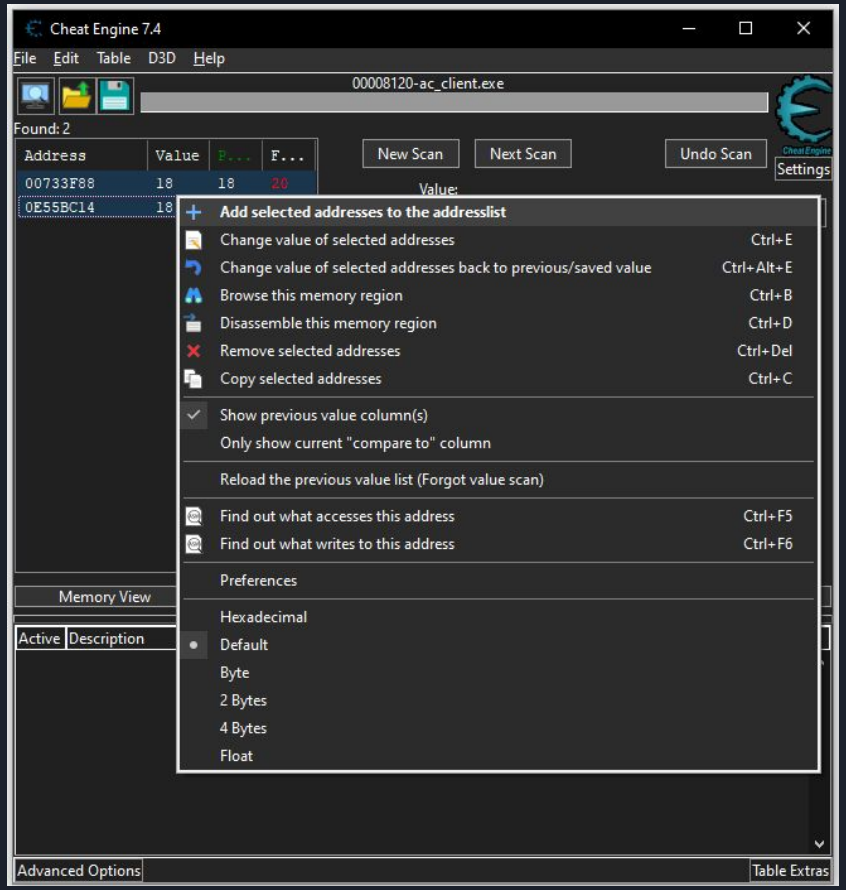
Cheating at Video Games

- Intercepts up to 3 addresses, and allows cheater to replace memory value read by system
  - Change number of lives you have
  - Delete the ammo decrement operation
  - Change damage value
  - Change start level
- Came with a giant book of codes
- Fairly limited, but very powerful



PC Cheating

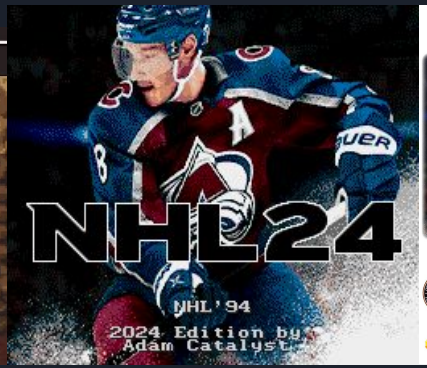
- Cheat Engine for PC Gaming
  - Attach to process
  - Scan / Inspect memory
  - Set memory values
    - Infinite Ammo
    - Life never decreases
- LD_PRELOAD on Linux
  - Make your own version of function that program calls instead of real function
- **Don't cheat in online games**
  - Account bans



Rom Hacks / Patching / Mods

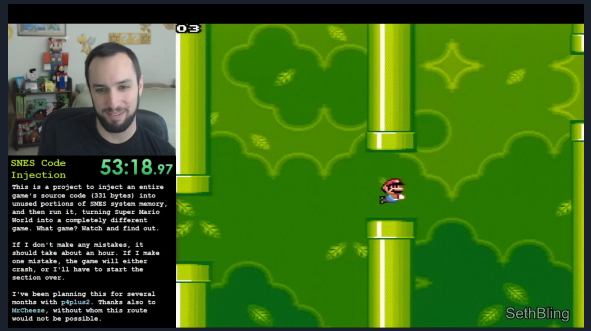
- Randomizer
  - Change item locations so game route has to change randomly
- Level Customizations:
  - Kaizo
- Relay Races
- Regular ROM Hacks
  - Language translations
  - Quality of life
  - Custom levels / Artwork
  - Extra Difficulty
  - Roster updates

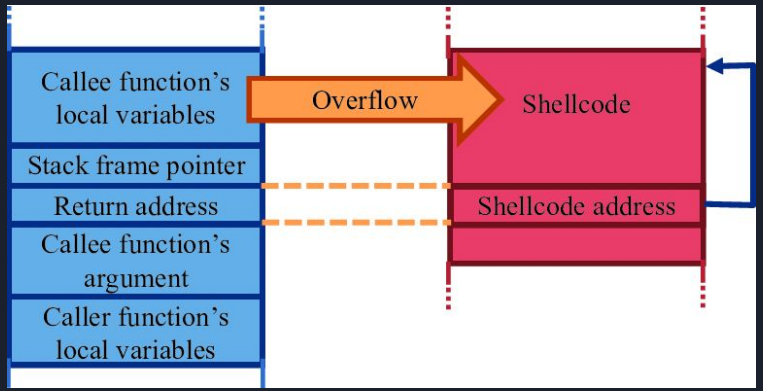
- Disable anti-debugging / security features
- Disable encryption on comms
- Add in secret features



Arbitrary Code Execution (ACE)

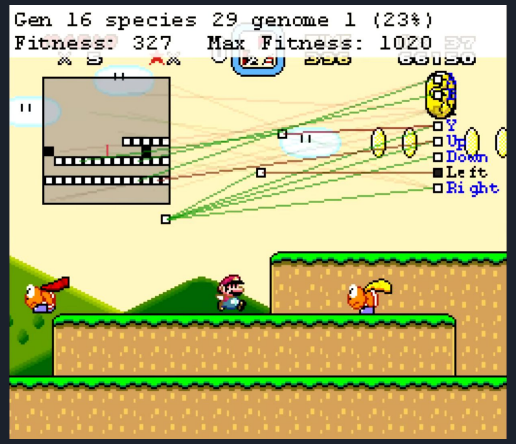
- THPS had a skate park editor
- Could name the gap between ramps
- Game reserves 32 bytes for the name in memory
- Hacked save file with never ending name will overwrite memory in the game
- Allows arbitrary code execution
- Could share your skate park over LAN

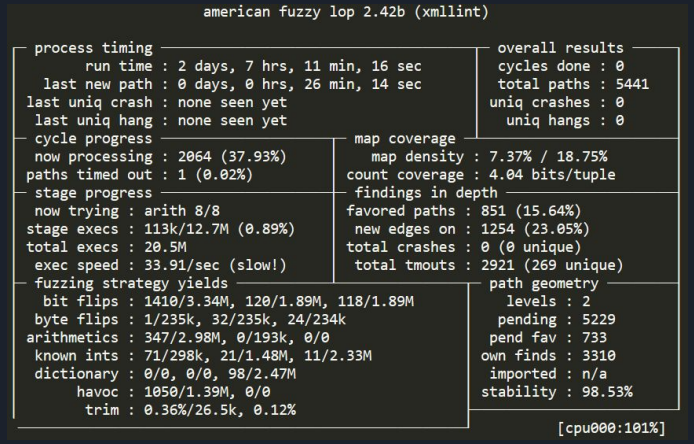




Fuzzing

- 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





Hackable Games

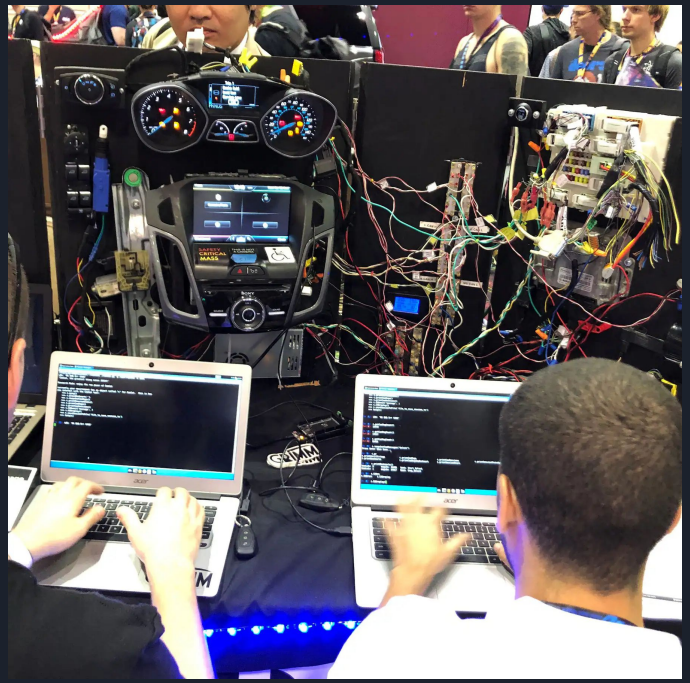
PwnAdventure

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

Squally

Hacking in real life / cyber-warfare

Hacking targets of concern...



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 Developer

- Cybersecurity support / auditing / asset security
- Network administration
- Cyber security architect
- Penetration tester
- Incident responder
- Offensive cyber / vulnerability researcher

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

- Interns: $20-$35 per hour
- New Grads with 4 year degree
  - Starting salaries are $90,000 - $110,000
  - Salaries grow to almost $200K, but high performers exceed that
  - Benefits
    - Health Insurance (very low or no premiums)
    - 401K matching 5-10%
    - Yearly Bonus 10%
    - 4 weeks vacation / year
    - Fun work culture. Gaming (Smash, D&D, Chess), NERF wars, DEFCON
- Local Companies: Nightwing CODEX, Research Innovations, Cromulence, Red Lattice, Vector 35, 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

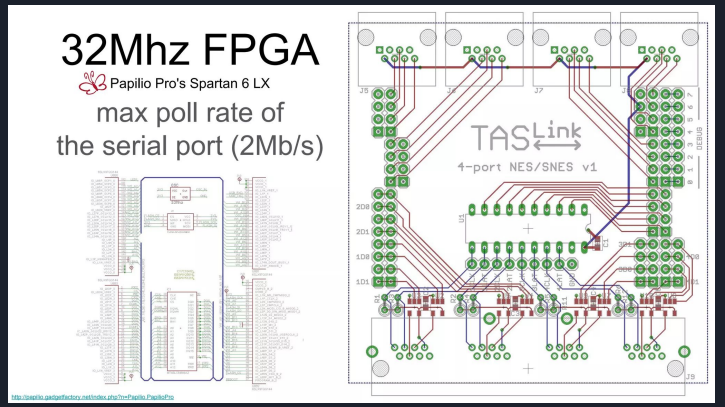
- Youtube: BotW Any% 23:42 [WR] by Player5
- Youtube: How to create the perfect speedrun by Bismuth
- Youtube: [TAS] Mario Kart 64 - All Cups -- 1P, GP, 150cc in 20:33:32 by weatherton
- Youtube: MarI/O - Machine Learning for Video Games by SethBling
- Book: Hacking: The Art of Exploitation by Jon Erickson
- 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
- Youtube: Game Console Security Playlist by ModernVintageGamer
- Extracting firmware: Every Method Explained by Slava Moskvin
- Crypto-Cat CTF Hacking Resources Guide
- Tony Hawk Pro Strcpy Github
- Hacking the XBox by Bunnie Huang

Links my coworkers wanted me to show you

- EA Won't Sell This Game - So I Hacked It
- Chef Stef NES Arkanoid TAS run and writeup
- Beating Minecraft in 30 seconds speedrun
- LiveOverflow’s Minecraft Hacking Playlist
- Super Mario 64 Parallel Universes
- Pokemon Yellow Arbitrary Code Execution TAS
- TAS Super Mario Bros 3 “Total Control” by Lord Tom

Questions?!

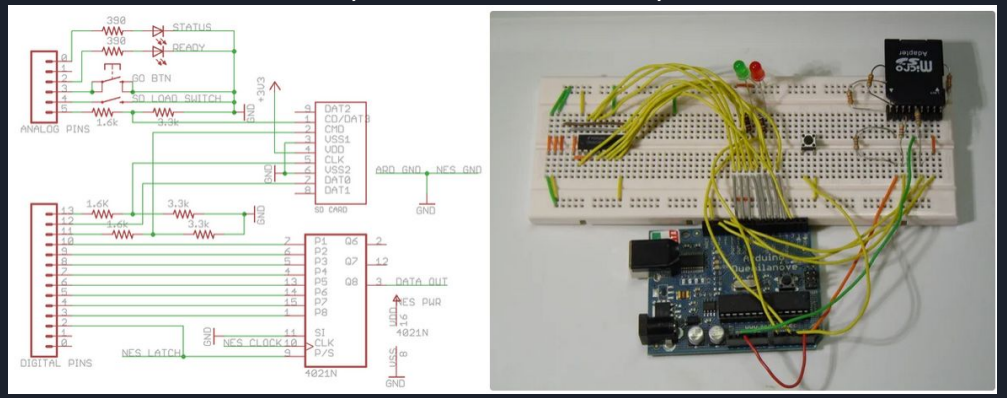
Hardware Hacking



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

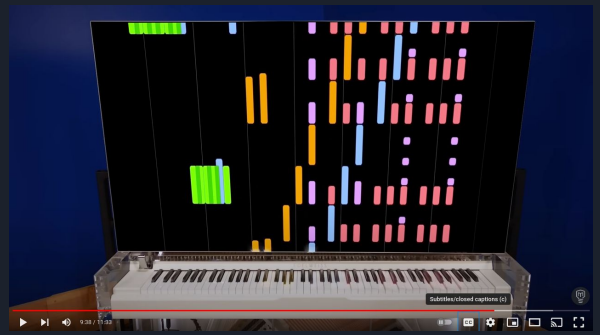
Hacker Badges!

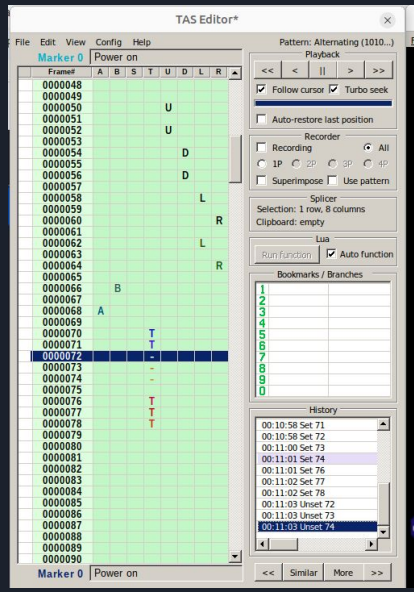
Micro500 - Early TAS hardware, ran script from SD card



Tool-Assisted Speedrunning (TAS)

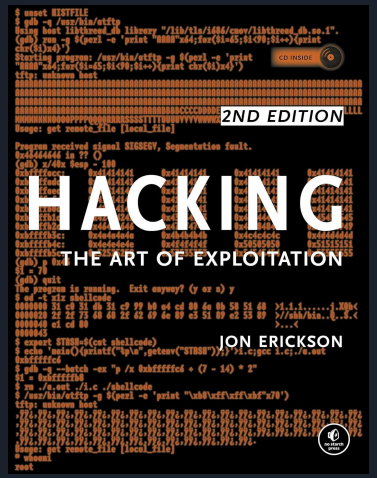
- Precise manipulation of all controller inputs faster than humanly possible
- Typically Requires
  - Emulation
  - Save States
  - Frame by Frame Control inputs
- Doom Done Quick (1999)
- Contra - Konami Code





Super Mario World TAS Excerpt

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

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.