The amazing life & achievements of...

TASBot
THE PERFECTIONIST

Twitch.tv/dwangoAC  @MrTASBot

 dwangoAC  DEFCON
Presented and written by...

Allan 'dwangoAC' Cecil

http://acbit.net
Presented and written by...

President of the North Bay Linux Users’ Group

http://nblug.org

http://acbit.net
Presented and written by...

President of the North Bay Linux Users’ Group
Senior Engineer at Cyan Ciena


http://acbit.net
Presented and written by...

President of the North Bay Linux Users’ Group

Senior Engineer at Cyan Ciena


Speedrunning
Human limits
Playing games fast

http://speedemosarchive.com/
Playing games fast

- Inspiration: in-game completion timers
Playing games fast

- Inspiration: in-game completion timers
- Many categories, ranging from "any%" to "low% no major glitches"
- and others track fastest completion times
- Strict rules + peer review: no cheats, no macros
- Typically highly entertaining
Games Done Quick
Games Done Quick

Speedrunning marathons for charity streamed live on Twitch

Classic GDQ (2010), Awesome GDQ (2011-), Summer GDQ (2011-)
Abusing games

https://youtu.be/kIizE_H7D2g?t=5m27s  AGDQ 2014
Abusing games
Even 1-handed, blindfolded...
TAS verb / noun  ~

TASer noun

"I'm a TASer working on Tetris." / "I'm TASing Tetris."

"I TAS'ed Tetris." / "They made a TAS of Tetris."
Tool-Assisted Superplays

From human limits
To hardware limits
Tool-Assisted Superplays

From human limits
To hardware limits

TAS verb / noun ~ TASer noun

“I’m a TASer working on Tetris.” / “I’m TASing Tetris.”

“I TAS’ed Tetris.” / “They made a TAS of Tetris.”
Harder Faster Better Stronger
Harder Faster Better Stronger

- Early PC game TAS’s: Savestates, slow motion, and recording tools
Harder Faster Better Stronger

- Early PC game TAS’s: Savestates, slow motion, and recording tools
- ~1999: Doom Done Quick in 19:41
Inhuman skill on display

- Tools meant hardware limits became the only limits
Inhuman skill on display

- Tools meant hardware limits became the **only** limits
- TASing looked like the Doped Olympics
  - Competitors should admit to doping
  - Videos made with TAS tools should be labeled

http://tasvideos.org/WelcomeToTASVideos.html
Inhuman skill on display

- Tools meant hardware limits became the **only** limits
- TASing looked like the Doped Olympics
  - Competitors should admit to doping
  - Videos made with TAS tools should be labeled
- NESVideos created by Bisqwit in 2004

http://tasvideos.org/WelcomeToTASVideos.html
Inhuman skill on display

- Tools meant hardware limits became the *only* limits
- TASing looked like the Doped Olympics
  - Competitors should admit to doping
  - Videos made with TAS tools should be labeled
- NESVideos created by Bisqwit in 2004
  - Now at TASVideos.org with runs for many platforms

http://tasvideos.org/WelcomeToTASVideos.html
Console verified

Pushing hardware limits
Console verified
Pushing hardware limits

FAKE VIDEO. TAS is cheating...
Emulator used, not console!
Just kidding!
Ha ha ha. Bye!!
Console emulators

http://tasvideos.org/Lsnes.html

lsnes

http://tasvideos.org/BizHawk.html

BizHawk
Rerecording frameworks

Hourglass

NetHack specific tools

http://tasvideos.org/EmulatorResources/Hourglass.html

http://tasvideos.org/GameResources/DOS/Nethack.html
Emulation accuracy evolution
Emulation accuracy evolution

- Early emulators: highly inaccurate
- Clean room reverse engineering
  - or stolen manuals
Emulation accuracy evolution

- Early emulators: highly inaccurate
- Clean room reverse engineering
  - or stolen manuals
- *bsnes*: extreme accuracy, poor usability
Emulation accuracy evolution

- Early emulators: highly inaccurate
- Clean room reverse engineering
  - or stolen manuals
- bsnes: extreme accuracy, poor usability

http://byuu.org/emulation/higan/
Emulation accuracy evolution

- Early emulators: highly inaccurate
- Clean room reverse engineering
  - or stolen manuals
- higan: extreme accuracy, poor usability

⇒ match actual hardware, frame for frame
Memory searching, Lua scripting, disassembly

https://www.lua.org/
Memory searching, Lua scripting, disassembly

- More than just frame advance and savestates

https://www.lua.org/
https://www.youtube.com/watch?v=RtaS4KE4Qc
Memory searching, Lua scripting, disassembly

- More than just frame advance and savestates
- Find a specific value: save, reset memory search, run
  - Search based on conditions, repeat

https://www.youtube.com/watch?v=RtaS4KEE4Qc
https://www.lua.org/
Memory searching, Lua scripting, disassembly

- More than just frame advance and savestates
- Find a specific value: save, reset memory search, run
  - Search based on conditions, repeat
- Disassembly of RAM or ROM for complete understanding
Abusing handwriting recognition

https://youtu.be/mSFHKAvTGNk?t=29m53s AGDQ 2016
Abusing handwriting recognition

Editing memory live directly in the game

https://youtu.be/EHfw-BEuRO8?t=12m28s

https://youtu.be/mSFHKAVTNk?t=29m53s

SGDQ 2016

https://youtu.be/mSFHKAVTNk?t=29m53s

AGDQ 2016
TAS ↔ Infosec equivalents

- Savestate = VM snapshot
- Frame advance = VM CPU step / tick
- Glitch = Vulnerability
- Arbitrary Code Execution = Exploit
- Console verification = Evil maid attack

⇒ TAS = fun, technical, educational
SMB3 Total Control
Glitchfest by Lord Tom
TASBot
TASBot plays
TASBot plays Super Mario World
Early console verification devices
Early console verification devices

- 2009
  - a PIC to press NES buttons [true]
Early console verification devices

- **2009**
  - a PIC to press NES buttons [true]

- **2011**
  - NESBot [micro500]: first replay of SMB1
    - Used at SGDQ 2011 on SMB2 and W&W 3

https://www.youtube.com/watch?v=KQXVgMKJEDY
Early console verification devices

- **2009**
  - a PIC to press NES buttons [true]

- **2011**
  - NESBot [micro500]: first replay of SMB1
    - Used at SGDQ 2011 on SMB2 and W&W 3
  - Droid64 [SoulCal]

- **2012**
  - N64 [micro500]
- 2013
  - SNES and Genesis Arduino bot [GhostSonic]
  - NES/SNES replay device [true]
    - Streaming capable and inexpensive but limited datarates
The birth of TASBot

- 2013
  - SNES and Genesis Arduino bot [GhostSonic]
  - NES/SNES replay device [true]
    - Streaming capable and inexpensive but limited datarates
- 2014
  - Nintendo R.O.B + board + legos: "TASBot"
The birth of TASBot

- **2013**
  - SNES and Genesis Arduino bot [GhostSonic]
  - NES/SNES replay device [true]
    - Streaming capable and inexpensive but limited datarates
- **2014**
  - Nintendo R.O.B + board + legos: "TASBot"
- **2015**
  - Multireplay device [true]: self-contained ⇒ faster datarates
The birth of TASBot

- 2013
  - SNES and Genesis Arduino bot [GhostSonic]
  - NES/SNES replay device [true]
    - Streaming capable and inexpensive but limited datarates
- 2014
  - Nintendo R.O.B + board + legos: "TASBot"
- 2015
  - Multireplay device [true]: self-contained ⇒ faster datarates
  - Game Boy Player Player [endrift] (GBA on GameCube)
TASBot
THE PERFECTIONIST
TASBot
TASBot
plays
TASBot plays

SUPER MARIO WORLD
TASBot plays in Super Mario World.
TASBot plays in SMB in SMW by p4plus2 and Masterjun
TASBot plays the SNES classic...

https://www.youtube.com/watch?v=YHyaTCuZRZM

credits: p4plus2, Masterjun
TASBot plays the SNES classic...

Exploits it via input...

credits: p4plus2, Masterjun
TASBot plays the SNES classic...  
Exploits it via input...  
A homemade port of the NES classic is sent as payload...  

credits: p4plus2, Masterjun
TASBot plays the SNES classic...

Exploits it via input...

A homemade port of the NES classic is sent as payload...

A 8-bit game, on a 16-bit system!

credits: p4plus2, Masterjun

https://www.youtube.com/watch?v=YHyaTCuZRZM
You can write specific sequences in the **Object Attribute Memory** by using specific objects at specific coordinates,
Since CPU instructions are made of specific binary sequences...
Since CPU instructions are made of specific binary sequences... we can take over execution the way we want.
Since CPU instructions are made of specific binary sequences... we can take over execution the way we want. So, just via input...
Since CPU instructions are made of specific binary sequences...
...we can take over execution the way we want.

So, just via input...
...you can directly trigger the credits sequence!
TASLink

~184 Kbps was too limiting
32Mhz FPGA

Papilio Pro's Spartan 6 LX

max poll rate of the serial port (2Mb/s)

SMB1+2+3+Lost Levels played simultaneously during SGDQ 2016

https://youtu.be/EHfw-BEuRO8?t=58m29s
Anatomy of an Arbitrary Code Execution
Anatomy of an Arbitrary Code Execution

Pokemon Red

1. Input exploit
Anatomy of an Arbitrary Code Execution

Pokemon Red

1. Input exploit
2. Take over the Super GameBoy
Anatomy of an Arbitrary Code Execution

Pokemon Red

1. Input exploit
2. Take over the Super GameBoy
3. Gain full access to the Super Nintendo
Anatomy of an Arbitrary Code Execution

Pokemon Red

1. Input exploit
2. Take over the Super GameBoy
3. Gain full access to the Super Nintendo
4. Anything is possible
that the team put into it. Pokemon Plays Twitch Credits;
and Presenter, Primary Tester,
Emulator coder (l/snes),
tester, game mechanic researcher,
encoding scheme creator, SNES
expert, general stage 3-x help
idea and research, SNES advice
Python IRC to bot streaming.
true Creator of NES/SNES
Replay
TheSnek
Python script support
Nacho SGB docs, site desfacement
Tom: On-site hardware support
Vulajin: Camera serial interface
initial IRC Python script
full article in next Poc|GTFO.

TASVIDEOS
Pokémon Plays Twitch - How a Robot Got IRC Running on an Unmodified SNES

Credits: micro500, Ilari, p4plus2
abuses rival name & corrupts save file
swaps Pokemon

RIVAL’s NAME:

A B C D E F G H I
J K L M N O P Q R
S T U V W X Y Z

( ) ; [ ] P K

- ? ! @ # $ % ^ & *
.

Choose a POKÉMON.

Lower case

a a a a a a

v a a a a
Credits: micro500, Ilari, p4plus2
Pokémon Plays Twitch

- Abuses rival name & corrupts save file
- Swaps Pokémon and tosses items to craft a Twitch chat client

Rival's Name?

Choose a Pokémon.

-Threw away
-CANCEL
Pokémon Plays Twitch

RIVAL's NAME?

A B C D E F G H
I J K L M N O P Q
R S T U V W X Y Z

lower case

Choose a POKÉMON.

Threw away
CANCEL.

moltener: WHAT
asdyuu: startg
gadwin100: rekt
andykarate: fdg
tovargent: HI
soulpom: WHAT?
lukeskywars: UP
kiddsmirk: helloooool!
lovestruck: HULLO
HI MOM!
"anthécaiu: 🎉🎉🎉

credits: micro500, llari, p4plus2

https://archive.org/stream/pocorgtfo10#page/n5/mode/2up
CALL TO ACTION

join the chat for Q&A at http://twitch.tv/dwangoAC
From boot...
From boot...

...to ending, in 16 frames!
From boot...

...to ending, in 16 frames!

6000 buttons per second!
From boot... Some glitches are expected!

...to ending, in 16 frames!

6000 buttons per second!
DPCM memory

Conflict

Game controller

Flood weak controller code to abuse raster interrupt and take over execution

http://www.qmtpro.com/~nes/chipimages/#rp2a03
TAS'ers lethal weapon

- More flexible than IDA
- Graph view, low level IL and annotation support
- Python scripting
- NES support: ability to add new mappers
Am I cheating?
Am I... cheating?

No
Am I... cheating?

No, I'm just looking for technical challenge & visual entertainment!
Am I cheating?

No, I'm just looking for... technical challenge & visual entertainment!

I'm not the only one... ;)
But more importantly...
But more importantly...

over $200k USD

Raised for charity!

MEDECINS SANS FRONTIERES
DOCTORS WITHOUT BORDERS

prevent cancer FOUNDATION

http://tasvideos.org/forum/viewtopic.php?p=437688#437688
Thanks to:
micro500 Ilari
Thanks to:
micro500 Ilari
p4plus2 Masterjun true
total_ psifertext rust
Thanks to:

micro500 Ilari
p4plus2 Masterjun true
total_ psifertex rusty
TheAxeMan ange_ greenfly
ais523 and many, many others
In collaboration with Ange Albertini

Twitch.tv/dwangoAC

@MrTASBot

join the chat for Q&A at http://twitch.tv/dwangoAC