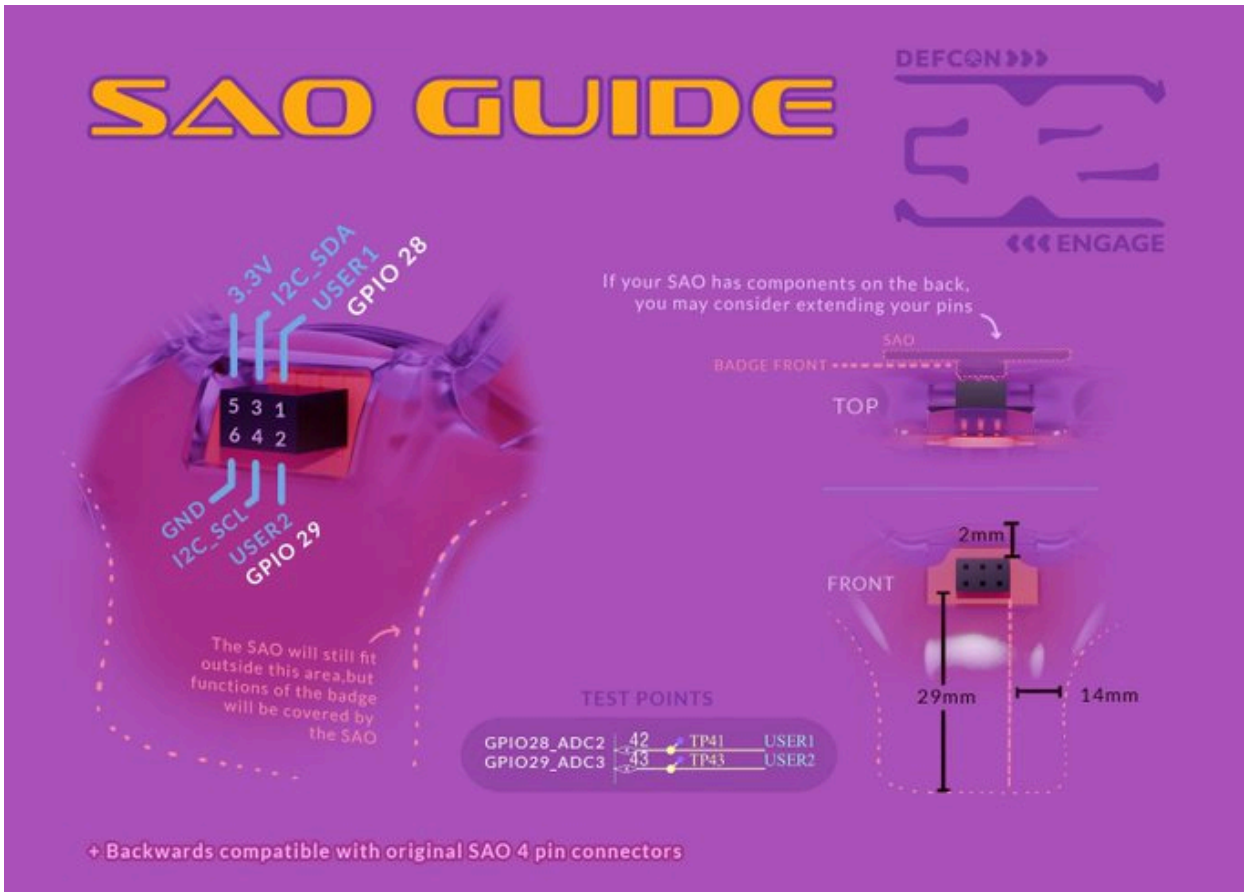
{DEFCON 32 Badge Hacking Challenge Notes

The purpose of this document is to be a collective note gathering location for the DC32 Badge Challenge.

What we know so far?

The badge has a redesigned SAO port wherein pins 3 and 4 are I2C ports that are live, meaning they should be able to interface with for an active serial connection. [1]



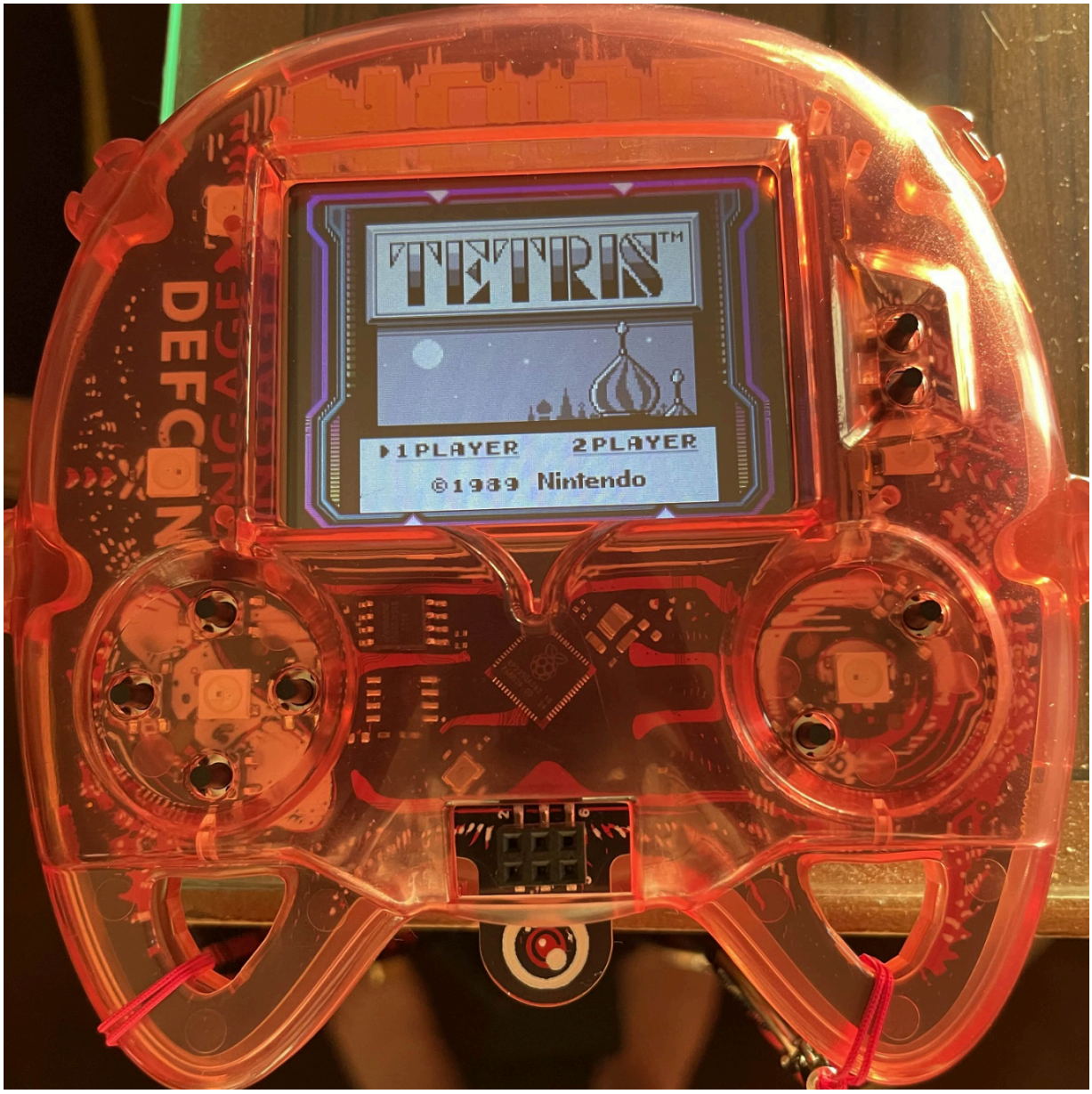
[1] Badge Sneak Peek https://x.com/defcon/status/1808279118477418640

Badge Design

The badge is designed to resemble a cat head when viewed from the front and a controller with a built-in screen when held by the wearer. The screen is a 2.4-in TFT resistive touchscreen display (https://displaysino.com/product_details/SCT024015-V01.html), though the game does not use the touchscreen. The processor is the new RP 2350 chip, which was announced/released on August 8, 2024 (https://forums.raspberrypi.com/viewtopic.php?t=371165).

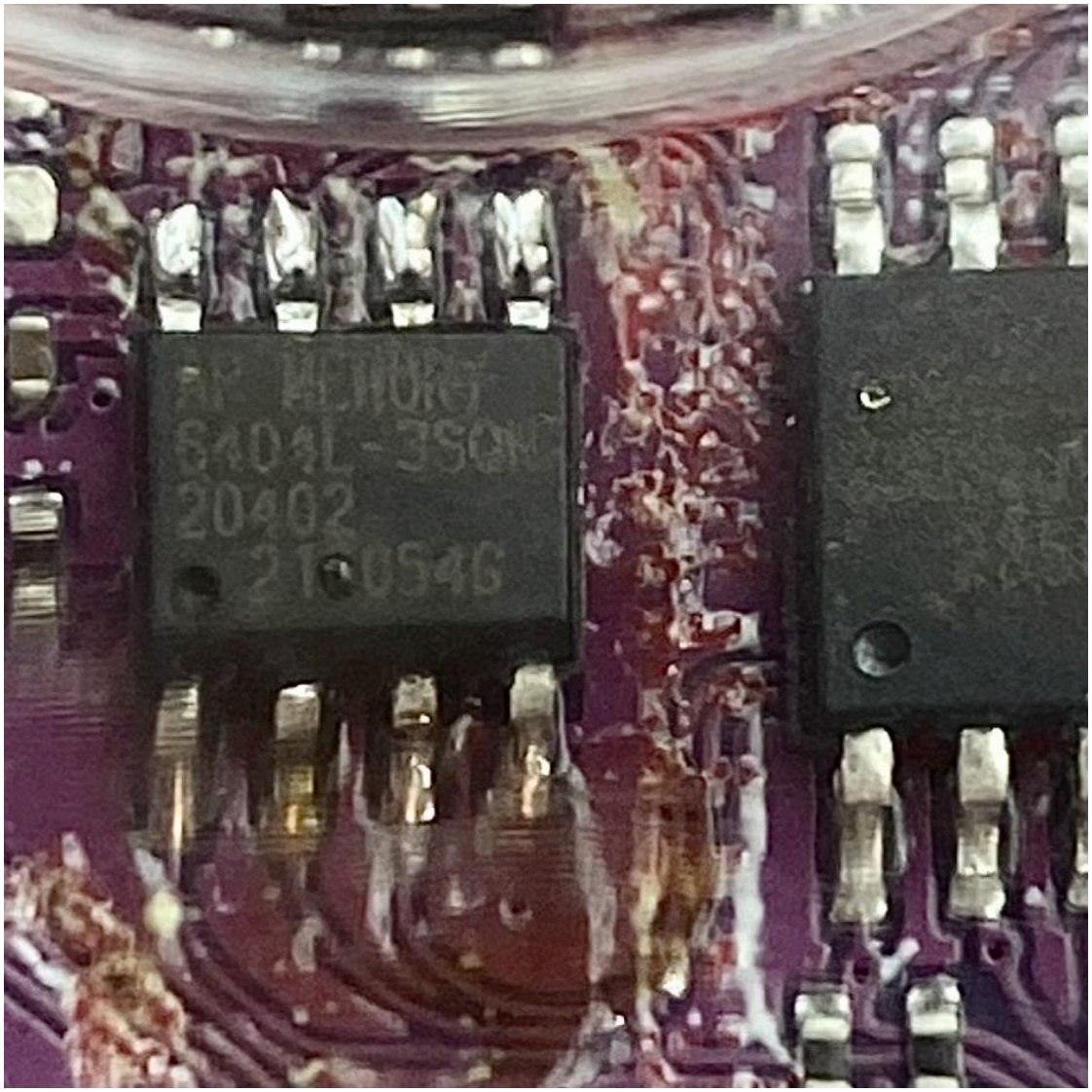
Hardware features:

- 2.4” LCD (CH240QV23A-T)
- 3-axis accelerometer (LIS3DHTR)
- Real-time clock (PCF8563T/5,518)
- Resistive touchscreen controller (NS2009)
- RGB LEDs (WS2812E-V5)
- MicroSD card slot (TF-115YY-BCP9)
- 1500 mAh LiPO cell (LP603759)
- IrDA module (ZHX1010MV115TH)
- 32 Mb QSPI flash (W25Q32JVSSIQ)
- Speaker (SMD-8503-3627-16)


TETRIS™
1PLAYER
2PLAYER
©1989 Nintendo
DEFCON

De

Upgradeable ram



- Solderable ram extension for palmOS, linux, etc.
- Data sheet: https://www.apmemory.com/wp-content/uploads/APM_PSRAM_E3_QSPI_APS6404L-3SQN-v2.6-KGD_PKG.pdf
- Product page: IOT RAM/PKG x4 QSPI APS6404L-3SQN https://www.apmemory.com/products/psram-iot-ram/
- Purchase: https://www.mouser.com/ProductDetail/AP-Memory/APS6404L-3SQN-SN?qs=IS%252B4QmGtzzqCot9%252BeIJwKw%3D%3D&srsltid=AfmBOoojNA_jXv4osLCkhM2HXC5HK6fHblznIVPFHKUyuBi5UthMWl0K
- (I was not the one who purchased nor attached the ram so I cannot be 100% sure)

Firmware

- 1.5 Firmware (fix for save and load)
- FN Screen First Firmware
    - New firmware created by Ethan/firelizzard that load you into the FN screen when the badge powers on. This bypasses the need to switch to a new ROM for the save to commit to the sd card (somehow)
    - Uf2 and BIN
- Original Firmware (Maybe??
    - Uf2
- Nuke Firmware
    - General-itdc32

Firmware Flash:

- Plug into PC, Hold BOOT, click RESET, and then drag uf2 file into newly mounted drive. Badge will auto disconnect and reboot to install the firmware (happens within seconds). You can then press the function button (bottom right of the back) and go to “About…” to confirm the firmware version you are on.

Firmware Flash Nuke:

- Download the custom nuke rom from this message: (search term "flash_nuke.uf2" by Emmy Heart 8/8/2024 4:44 PM Las Vegas time) general-dc32
- (The reason for this is documented at "Resetting Flash memory" in https://www.raspberrypi.com/documentation/microcontrollers/pico-series.html#resetting-flash-memory, but the badge works with the custom uf2 file.)
- Also download the up to date firmware from a trusted source like a pinned message.
- With your badge connected to the machine you have downloaded the uf2 files, boot the badge into bootloader mode by holding the Boot button (next the to "Reset"/shutoff button), touch the reset button once, let go of the Boot button. This should mount a RP2350 folder that you can see from your file browser.
- First copy flash_nuke.uf2 by Emmy Heart into that folder. This will reset the memory of the device.

- Boot again into bootloader mode again.
- Now load the up to date firmware uf2 file. Hopefully you now should be back to the menu to choose a rom to load.

Self Test

Running the test: (Test only works with a valid uGB firmware)

- On Battery
    - Turn badge off
    - Hold START and SELECT then press POWER
- On Charge
    - Hold START and SELECT
    - Press RESET

SD Card

1. Get a new SD card. The con ones are cheap garbage, despite all the love and effort that went into them.
    a. As of 4pm 8/8 Gamestop in the Fashion Show Mall had 64 Gb ones for $12, other sizes available too
    b. If you have a car, you can check stock and preorder Best Buy or Walmart pickup nearby
    c. You can also buy one on Amazon and have it shipped to an Amazon locker (at a 7/11 or other nearby spot). Multiple 32GB for $6.99 or 128GB for $14.99
2. Windows
    a. Format using the SD Formatter from the sdcard.org website (for mac, use disk utility instead)
    b. Delete any existing partition using diskmgmt
    c. Do not use "fast formatting" when creating a new partition (MBR Required)
    d. It might've helped to start with a 2GB FAT16 partition first, but now I've expanded to a 4GB FAT32 partition
    e. Make sure to put your roms in the ROM on to folder

    Using Diskpart (Alternative to above)

    list disk

    select disk <### SD CARD>

    clean

    convert mbr

create partition primary align=2048 size=4096
format fs=fat32

3. Linux:

```
Unset
lsblk # to get <sd_card> path
fdisk /dev/<sd_card>
> d # Deletes the partition
> o # Sets MBR
> n # creates new partition
>> p # primary
>> 1 # partition number
>> 2048 # Start Sector
>> +4G  OR >> <default for smaller than 4GB> # Last Sector
> t # Type
>> 0b OR >> 06 # 0b for FAT32, 06 for FAT16 (<4GB)
> w # Writes to drive
mkfs.fat -F 32 (OR 16 <4GB) -s 64 /dev/<sd_card_partition>
```

If using Gparted make sure to create a msdos partition table prior to formatting with fat32.

4. MacOS

```
Unset
diskutil list # to get <sd_card> drive name

# replace /dev/diskX with drive name e.g. /dev/disk4
sudo diskutil partitionDisk /dev/diskX MBR FAT32 Partition1 4G

diskutil eject /dev/diskX
```

5. Mount the sd card and reload the ROM folder (with ‘DEFCON BADGE GAME v1.0.gbc’ and another ROM
    a. NOTE: May no longer be required with FN Screen First Firmware
    b. Highly recommend Wario Land 3…
6. Create a new folder on the root of the SD card named "SAVE"

    a. NOTE: This may not be necessary and has caused problems among some people (including myself). Solution for me (@errorz) was to ONLY have the “ROM” folder within the formatted drive
7. Unmount and load SD card back into the badge

Load a ROM Without a Working SD Card

You can load a custom ROM without an SD card by directly flashing the internal flash of the Pi Pico via the USB-C. All you need is `picotool` and the ROM you want to play. This can get you by playing better games w/o an SD card for now until you can get one. Saves still won't work since they require a working SD card.

1. Download & install `picotool` https://github.com/raspberrypi/picotool
2. Put your badge into BOOTSEL mode (Hold BOOT, click RESET, and then plug the badge into your PC)
3. Then the command to do this is:
    a. `./picotool load <ROM-file> -t bin -o 0x10100000`
    b. **NOTE:** Replace <ROM-file> above with your ROM of choice.
    root@Nomad-1:~/source/picotool/build# ./picotool load DOOMGB_a04.gb.bin -t bin -o 0x10100000
    Loading into Flash: [==============================] 100%

CAUTION #1: If you entirely erase the flash (e.g. via Firmware Flash Nuke), this trick will not work because the emulator (and I suppose bootloader) will be gone!
CAUTION #2: Without changing the save file name, your saves will keep overwriting each other. Because that string is the name for the file in /SAVE. However, this is already a problem for you if you don’t have a working SD card.

Notes (from dmitrygr): In order to know the file name to make for the save, there is another place in Flash before one megabyte where the name of the game is stored You would need to put a valid file name there. Any valid string. See memmap.h in sources:
#define QSPI_FILENAME_START 0x100DF000 //filename to save savegames correctly
#define QSPI_FILENAME_MAXLEN 0x00001000.
The firmware checks for a valid name there before deciding that the ROM is valid This is only an issue if you attempt to erase the flash. But if you do replace games using picotool, without changing that name, your saves will keep overwriting each other. Because that string is the name for the file in /SAVE.

Reference I found helpful for this section:
https://petewarden.com/2024/01/16/understanding-the-raspberry-pi-picos-memory-layout/

Save Game Fix

1. Load the FN Screen First Firmware
    a. Hold BOOT, click RESET, and then plug the badge into your PC
    b. Put the uGB.uf2 file and uGB.bin on the root of your sd card
2. Save Game
3. ???
4. Profit

OR

1. With existing FW (v1.3x), once in game, make sure to save ofc.
    a. This saves the game to the EEPROM
2. Load and start a different ROM **THEN** power down.
    a. This does two things:
        i. It moves the save from the EEPROM to the SD card.
        ii. It also avoids a bug on bootup. Loading a save doesn't work when starting up.
    b. NOTE: The first time I did this I got an error saying it couldn't save to disk, but it began working after that. I suspect this error is from creating the SAVE folder on disk
3. You **need** to start the badge on a different ROM, then go to change ROM, and it will load the save

Game Play

The badge is a fully-working Gameboy/Gameboy Colour emulator. It will load ROMs from the `ROM` directory on the SD card. It has been tested so far with:

- 4-in-1 Funpack
- 4-in-1 Funpack vol II
- Animaniacs
- Balloon Kid
- Bionic Commando - Elite Force

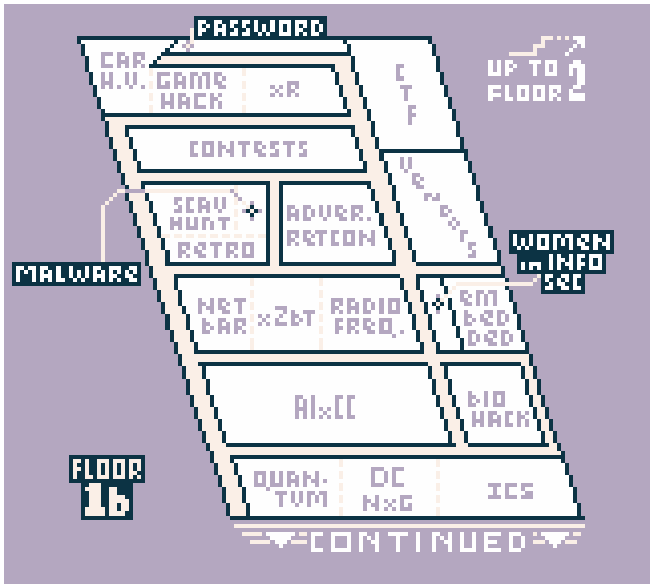
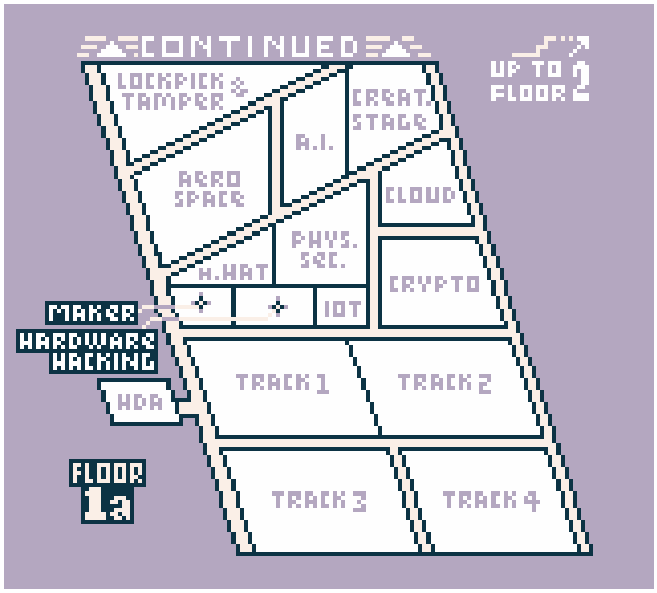
- Bomberman GB
- Bonk's Adventure
- Burger Time Deluxe
- Bust-a-Move 2: Arcade Edition
- Caesar's Palace
- Casino FunPak
- Castlevania - The Adventure
- Castlevania Legends
- Contra: The Alien Wars
- Duck Tales
- Kirby's Dream Land
- Mario Tennis
- Metal Gear Solid
- Pokemon Crystal
- Pokemon Red++
- Pokemon Silver
- Pokemon Yellow
- Pokemon Puzzle Challenge
- Simpsons Treehouse of Horrors
- SpongeBob SquarePants: Legend of the Lost Spatula
- Super Mario Bros Deluxe
- Super Mario Land
- Tetris
- Tetris DX
- Unearthed
- Wario Land 3

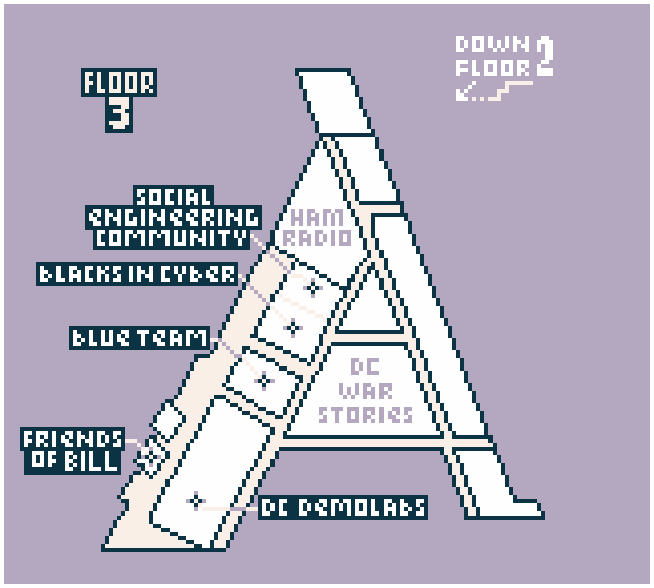
Bad ROMs:

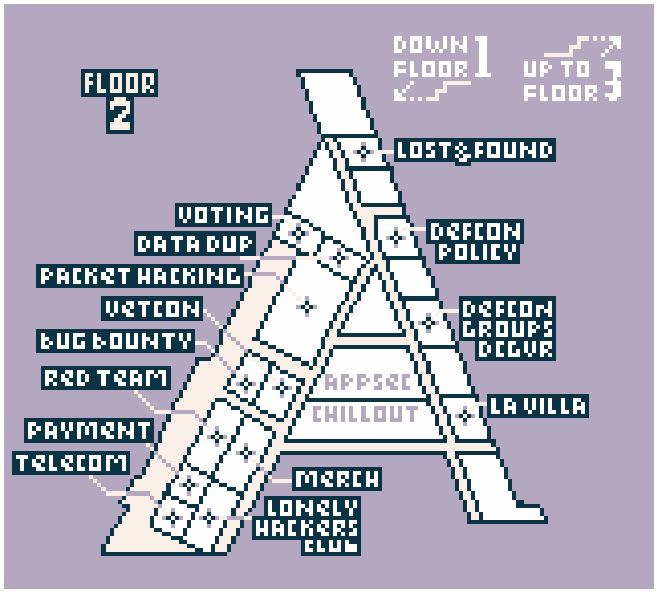
- LEGO Racers (US image)

DEF CON 32 Game

The game on the badge is an RPG set around a recreation of the Convention Centre. There are three floors with many rooms and NPCs. In each room there is generally one NPC to describe the room and some have another one with a quest, normally wanting an item.

- 
PASSWORD
CAR H.V.
GAME HACK
xR
C T F
UP TO FLOOR 2
CONTESTS
U M P O R S
SCAV HUNT
RETRO
ADVER. RETCON
WOMEN in INFO SEC
MALWARE
NET BAR
xZBT
RADIO FREQ.
RM BED DEP
AI×CC
BIO HACK
FLOOR 1b
QUAN. TUM
DC N×G
ICS
CONTINUED
- 
CONTINUED
UP TO FLOOR 2
LOCKPICK & TAMPER
A.I.
CREAT STAGE
AERO SPACE
CLOUD
PHYS. SEC.
H.HAT
CRYPTO
IOT
MAKER HARDWARE HACKING
TRACK 1
TRACK 2
HDA
FLOOR 1a
TRACK 3
TRACK 4





The track rooms will tell you the current talk happening based on the time you set in the badge at startup.

3 Cats

There is an objective to find 3 cats and open a portal in the Cat Statue. They are in:

1. Car Hacking VIllage (Floor 1) - In the van at the top, the code is **1337** (a participant in the “Super Cool Guys Club" locked room on the east of Floor 3 mentions this code). The **White Cat** is inside.
2. Lockpick & Tamper Village (Floor 1) - In the locked cabinet. Lockpicking game involves picking the pins in order. The order is **4, 2, 1, 3.** The **Cute Kitty** is inside.
3. Full order for finding the Black Cat:

    1. Get the **Screen** from the cat in Hardware Hacking Village on Floor 1
    2. Get the **Crypto Book** (a laptop) from Lost and Found on Floor 2
    3. Take the Crypto Book to the Crypto Village on Floor 1 to get the **Soldering Iron**.
    4. Take the Soldering Iron to DC War Stories on Floor 3, to the character on the Far Right Side to get the **Top Secret Briefcase**.
    5. Take the Top Secret Briefcase to Networking Bar on Level 1 to get **Water** (or get Water from any vending machine).
    6. Give Water to Nikita who is near the entrance to HDA on Floor 1. She will give you a **Bedazzled Shoe**
    7. Give the Bedazzled Shoe to the person in Social Engineering on Floor 3. They will give a **Phone**.
    8. Give the Phone to the person in Telecom on Floor 2. They will give you the **Microwave**.
    9. Give the Microwave to the person in front of AI Village on Floor 1 and they will give you the **Screwdriver**.
    10. Give the Screwdriver to the person in HAM Village on Floor 3 and they will give you a **Key**.
    11. Take the Key to the east of Floor 3. There is a locked room north of the road cones where you will find the **Black Cat**.
4. After getting the key from the turn in quests, go to the third floor right side and open the locked rooms (the locked room on top has the cat)
5. After getting all three cats, proceed to the Vendors room on Floor 1 and stand on the middle DEF CON Symbol in front of the Cat Statue
6. Win the Game. (All LEDs Turn Green)

Video Walkthrough of “Easiest” known Win
https://youtu.be/PELlj3GNehY?si=1b6nMSAMi1KdoAQM

QR Code Locations

1. DEF CON lobby entrance under the right stairwell
2. Hotel Room
3. Outside Lockpick and Tamper Village
4. Track 3 (corner of the room)
5. Defcon Groups
6. Game Hacking Village
7. Restrooms
8. CTF
9. Outside xZbT door
10. Hallway east of Track 2
11. Track 1
12. Vendors

QR Code Links

1 - https://youtu.be/oHg5SJYRHA0?si=PD23O0ukCkhFNlX_
2 - https://hackertracker.app/conferences/DEFCON32/schedule/
3 - https://archive.org/details/MITLockGuide
4 - https://www.gbstudio.dev/
5 - https://spux.art/
6 - https://media.defcon.org/DEF%20CON%2015/DEF%20CON%2015%20badge/DEF%20CON%2015%20-%20grand es-ode_to_defcon_badge.pdf
7 - https://youtu.be/xvAS6Req0q8?si=2KLyF8kQgGmZnBDs
8 - http://www.phrack.org/archives/
9- https://archive.org/details/colossus-the-forbin-project-1970
10 - https://defcon.org/html/defcon-32/dc-32-badge-adventure.html
11 - https://www.youtube.com/watch?v=3ctQOmjQyYg
12 - https://defcon.social/about

Rooms and Items

- Floor 1, HHV, Reward: **Screen**
- Floor 1, Crypto Village Needs **Crypto Book** Reward: **Soldering Iron**
- Floor 1, Hallway outside Registration - Nikita, requires a bottle of water. Can be obtained from a vending machine OR from the Networking Bar quest. Reward: **Bedazzled Shoe**
- **Floor 1,** Get microwave give to guy in Hallway by Ai
- Floor 1, Networking Bar - required **Top Secret Briefcase**, Reward: **Water**
- Floor 1, Music Room - A **Photo**
- Floor 2, Telecom Room - Requires **Phone** Reward: **Microwave**
- Floor 2, Red Team Village - Find a Fed?
- Floor 2, Lost and Found - A **Crypto Book**
- Floor 3, Ham Radio Village - requires **Screwdriver**
- Floor 3, Social Engineering - Requires a **Bedazzled Shoe**, obtained from Nikita. Reward: **Phone**
- Floor 3, DC War Stories Far Right Side - Requires both a **Screen** (Mar, Hardware Hacking) and **Soldering Iron** (Trivia Answer, ICS or from Crypto Village after giving a Crypto Book from Lost and Found). Reward: **Top Secret Briefcase**

Dark Tangent?

They run after speaking to them once and the user is locked.
Then they disappear if chased.

- Can be found in each floor, if talked to three consecutive times, the player may receive Dark Chocolate.

    - You can get the chocolate 100% of the time by going to the third floor and confronting DT there. It looks similar to when DT runs away in the first floor hallways, but does not vanish.
    - Why does the chocolate mke you teleport to a different room?
- Locations:
    - Floor 1b: next to contests and scavenger hunt on the left side
    - Floor 1a: north west corner of Track 2
    - Floor 3: far east hallway

Trivia

The Trivia questions normally reward photos (though can reward Soldering Iron). These look to have been taken on the Gameboy Camera.

- What is the best selling British computer? **Raspberry Pi.** (Outside HDA)
- When did Hackers come out? **1995**.
- First wall of sheep? **Paper Plates**
- Who was not in Hackers? **Kevin Mitnick**
- First Location of DefCon: **Sands**
- What is the Blood Alcohol limit for drivers in Las Vegas? Answer: **0.08%** (Network Bar, 1b)
- What three planes were flown by members of the Aerospace village? **Tornado, F22, E6**
- What was the very first AI village talk on? **Adversary Patches** (AI Villiage, 1a)
- What is the login for the 1985 Video Game Hacker by activision? **Australia**
- At Defcon 24 Toool debuted a new piece of equipment what was it? **WICKED WAVES**
- What doesA ICS stand for? **Indust. ControlSys** Reward is not a photo, it's a **Soldering Iron**.
- Who was the first CTF lead for BIC Village CTF? **Socks**
- What is the standard FTP port? **21** (Track 1)

Unknown INFO?

AIxCC = Room is on fire? Badge lights up red
Biohacking Village - does not let you in, cutscene asks if you are broccoli? (Reference to Reginald Barclay in STTNG episode The Nuth Degree)
XR Village - can enter one of the treadmills for a cutscene - if you decline you get an energy drink
Music Room (between Vendors and WISP) - Badge lights up rainbow
Game Hacking Village - Space War game seems to have no reward whether you win or lose, maybe commentary on war having no winners though
Adversary Retcon Village - south door jumps you to middle of a hallway
Malware Village - has an error where it says Retro Club on the entrance, it is the northern Retro Club entrance from the outside

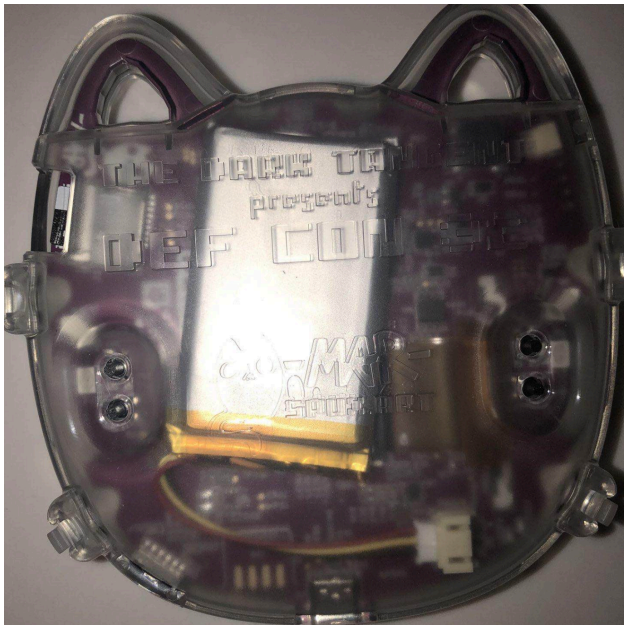
Restroom top toilets are “out of order”
Hardware Hacking Village - the top character changes colour to match yours
CAT can burn out, what does this affect? - running around and not talking to anyone
Where is photo 11?
First Floor Toilets in the Top of the Map (near Car Hacking Village) turn all lights pink/purple

Badge Dump

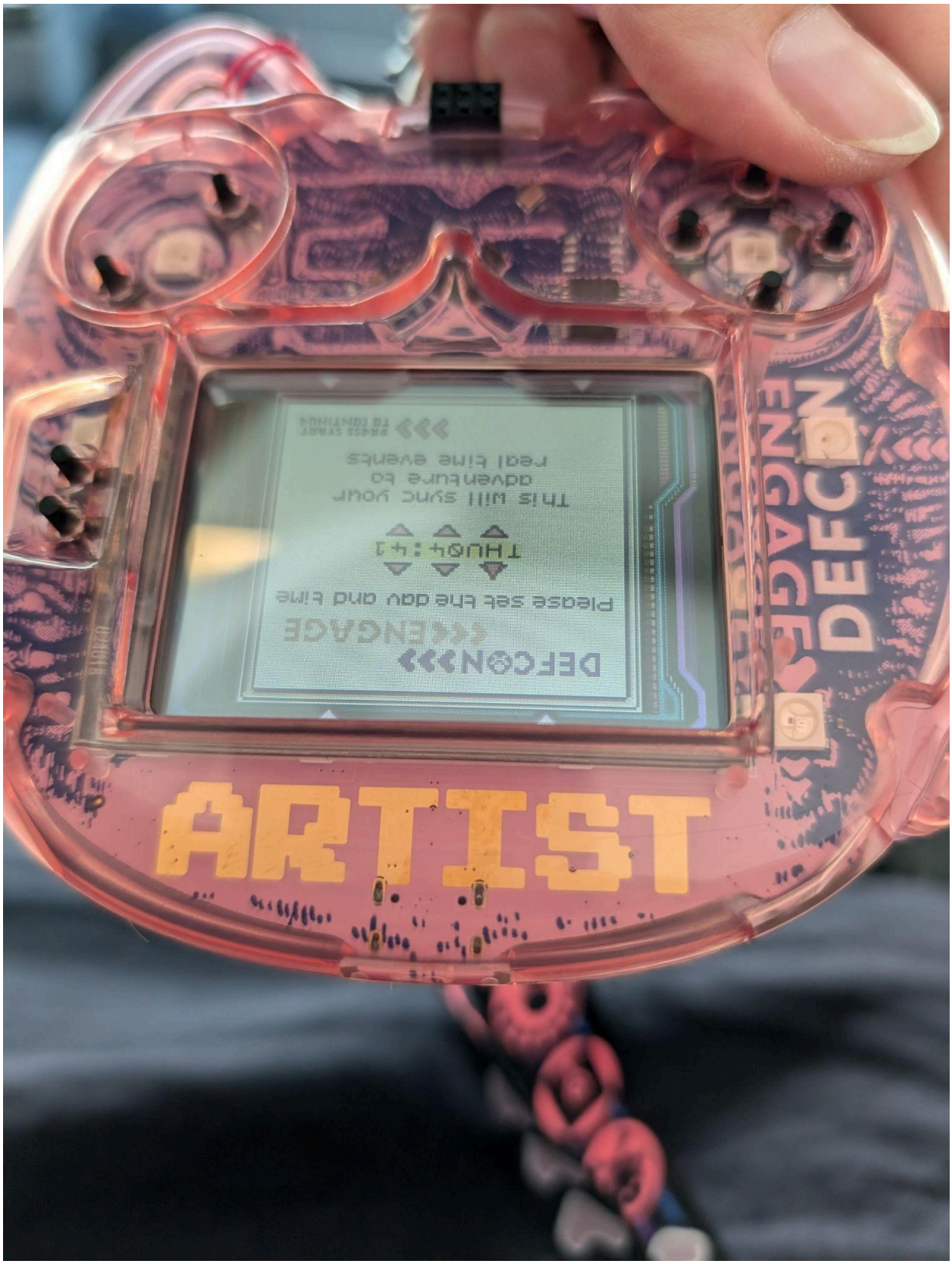
- https://github.com/billyjbryant/DC32-Badge-Hack

Badge Photos

Human



Artist


ARTIST
DEFCON
ENGAGE
DEFCON
ENGAGE
Please set the day and time
THU 04:41
This will sync your
adventure to
real time events

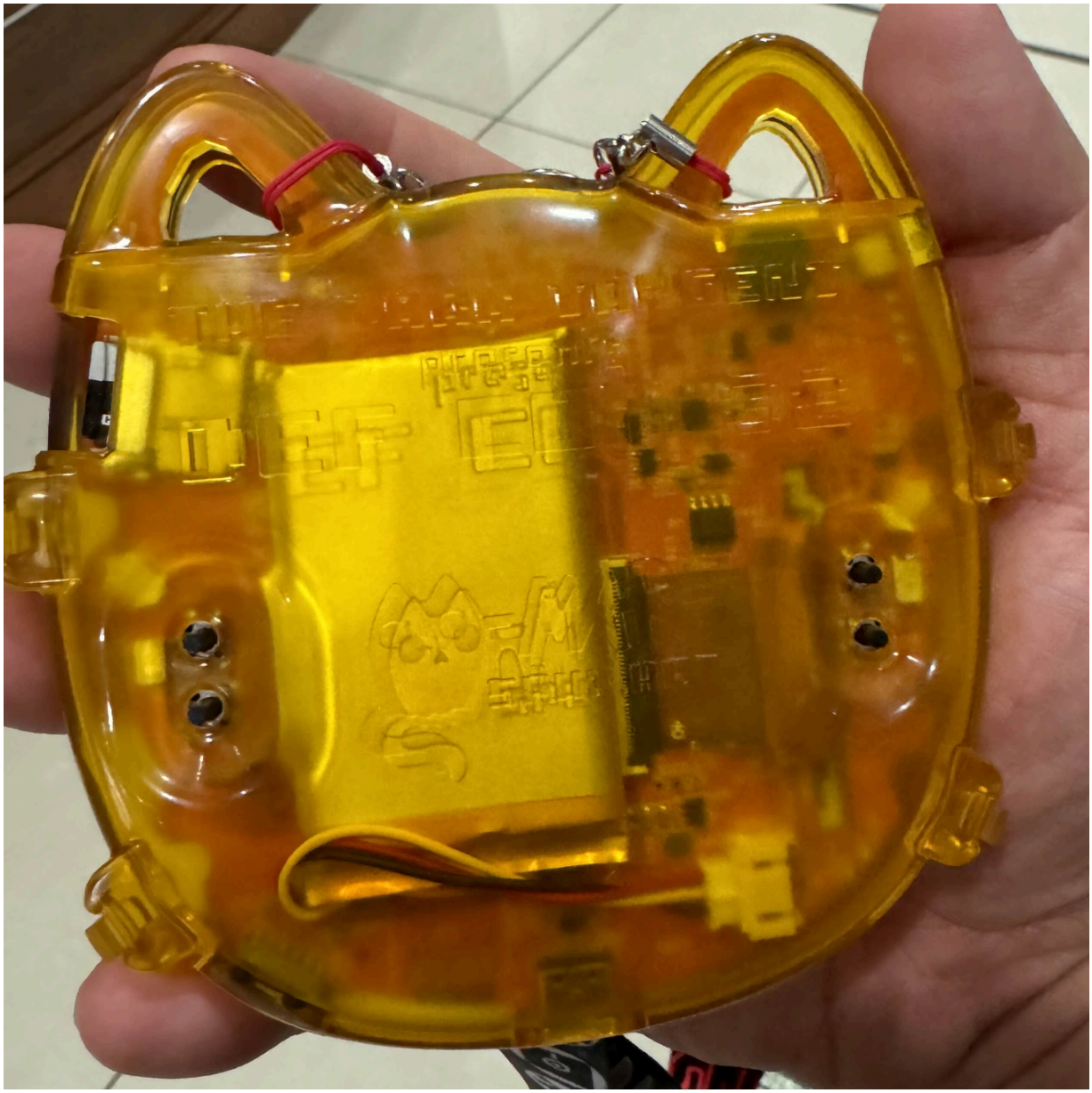
Speaker


DEFCON
ENGAGE
CONTEST

Contest

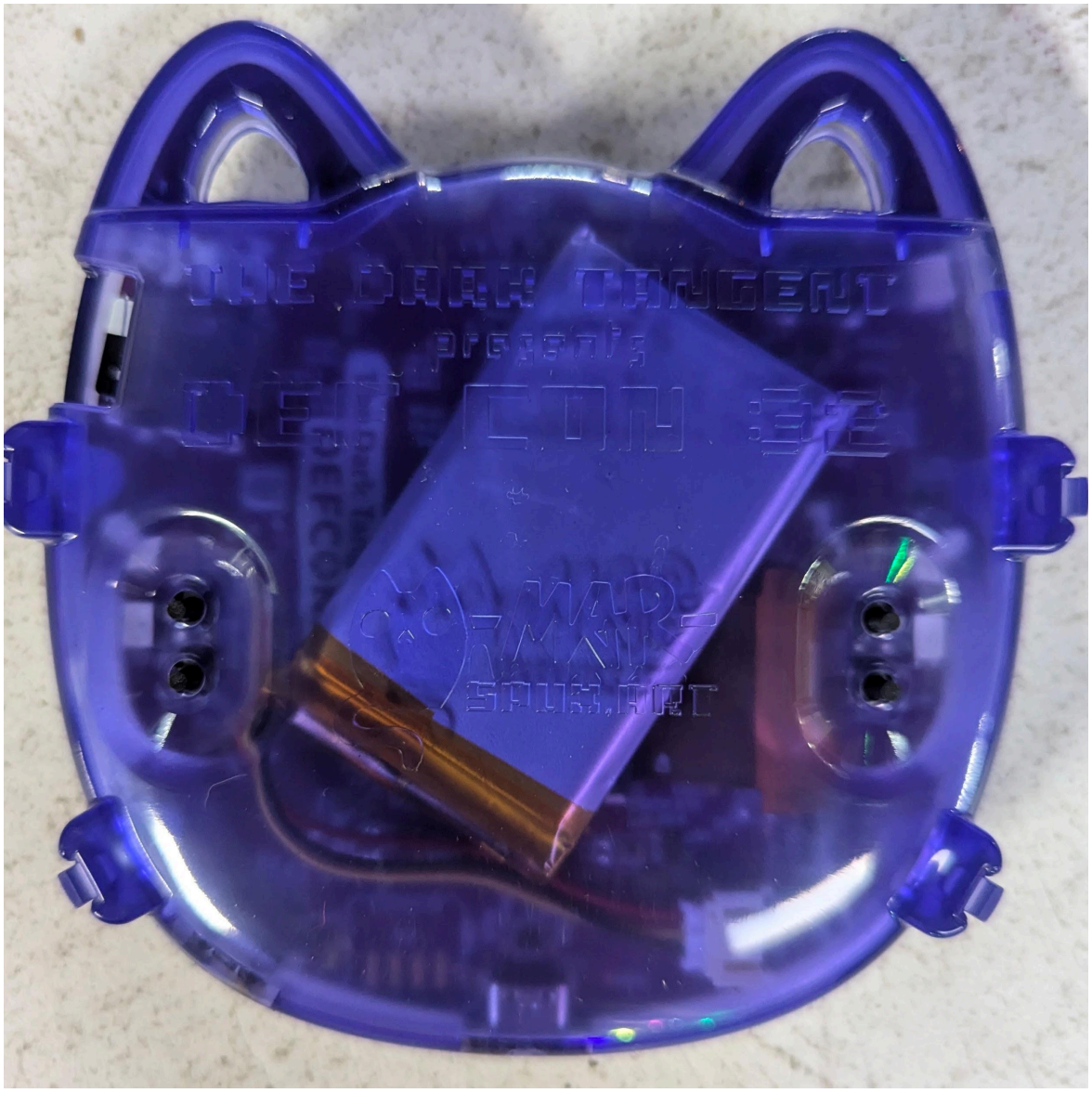
Village


VILLAGE
ENGAGE
DEFCON



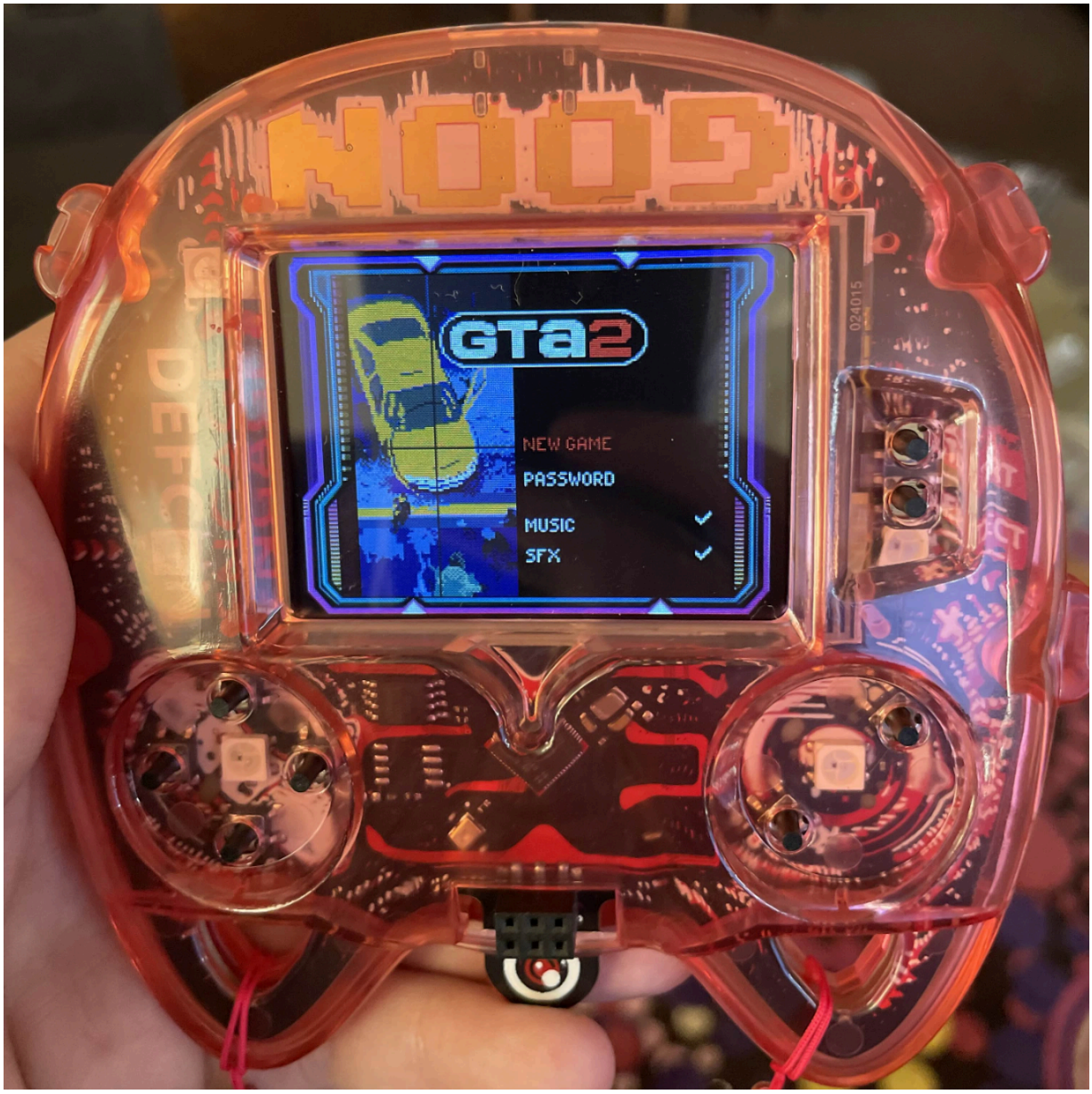
Vendor

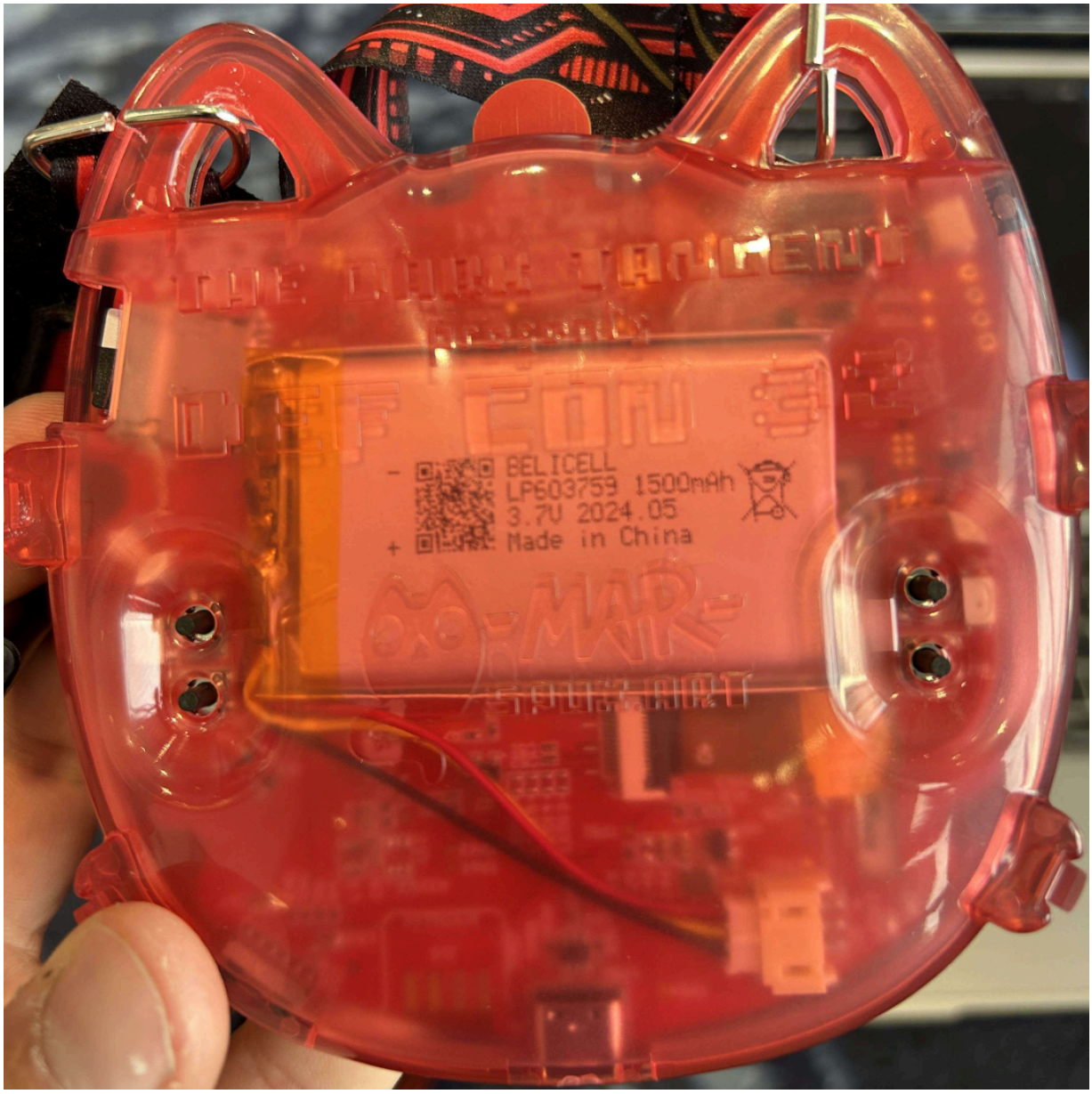

VENDOR
DEFCON



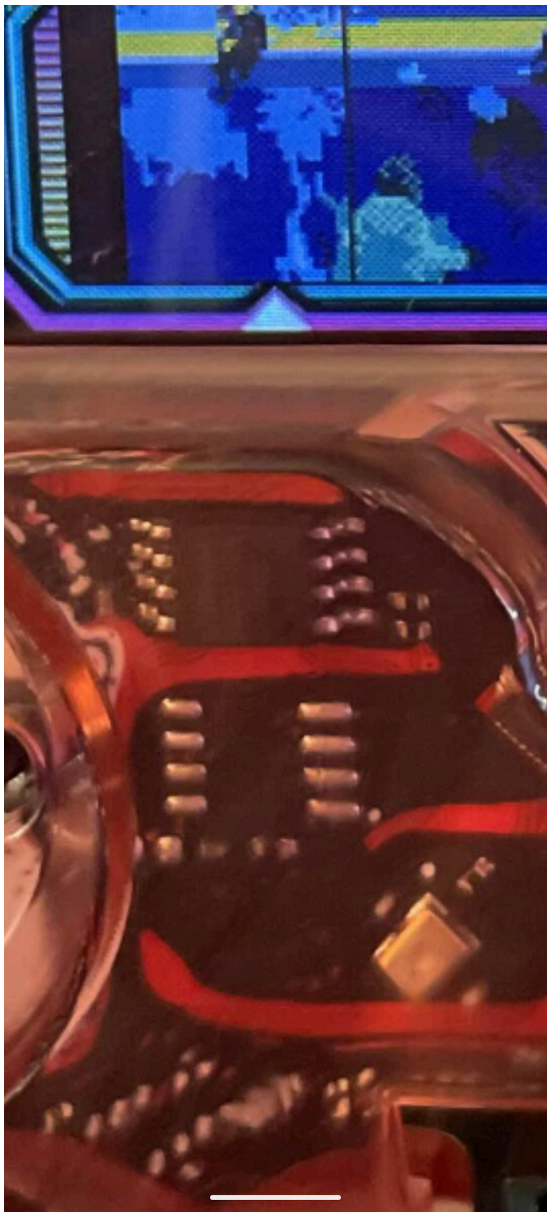
Goon

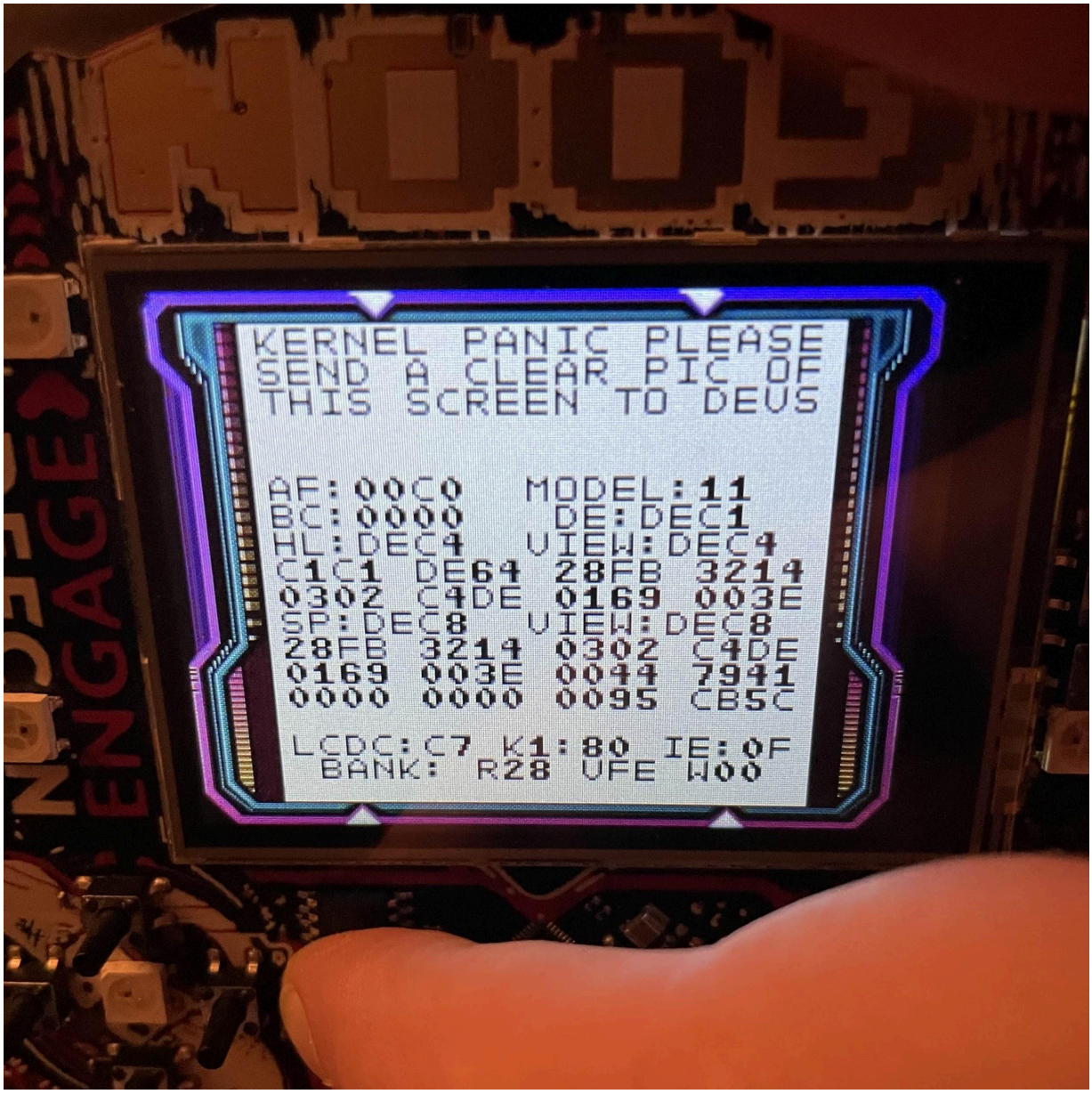

GOON


NOOG
GTa2
NEW GAME
PASSWORD
MUSIC
SFX


BELICELL
LP603759 1500mAh
3.7V 2024.05
Made in China

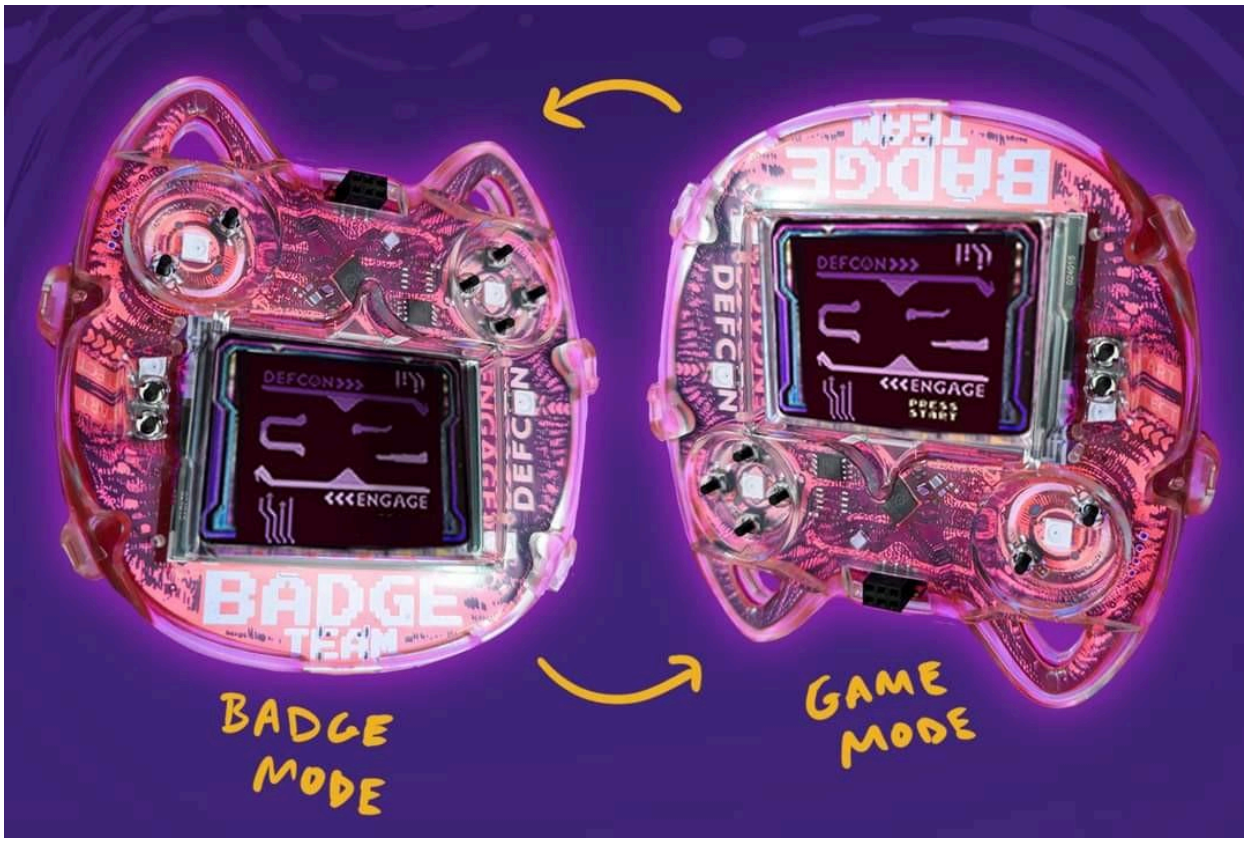
Misc Badge Images





Courtesy of Mar on Mastodon https://defcon.social/@mar/112928115964016459


DEFCON
ENGAGE
VILLAGE
CONTEST
CTF
PRESS
COMMUNITY
VENDOR


DEFCON
ENGAGE
BADGE TEAM
BADGE MODE
GAME MODE
PRESS START