DEF CON 26 Badge Write-up

https://78.media.tumblr.com734ba6db5941cd39f175f61ccf33b980tumblr_nn64n5qJS41qabnxjo3_500.gif

Badge Team:

- **Whisker (@whixr) – Game Art/Game Mechanics/Design + overall architecture**
- **Addie (@atdiy) – Game Art/Story/Parts Procurement**
- **Wire (@wireengineer) – Hardware**
- **Ninja – Software**

> “Our thought was - hackers are everywhere, should be everywhere, and can make decisions that are anti-Orwellian from anywhere.”

Badge Philosophy and Interactivity:

The theme of the DEF CON conference this year was 1983, the year before the predicted dystopian collapse of society as written about in George Orwell’s 1984. We still have the metaphorical opportunity to make decisions that can change the future and prevent Orwellian demise. In 1984, there are multiple ministries – Ministry of Peace, Ministry of War, Ministry of Love, and Ministry of Truth – which inspired our decision to create buildings. We entertained the idea of making elaborate art deco buildings, but then we came across those viral 8-bit pixel-graphic gifs that have calming scenes and simple animations of little cats moving their tails.

When we weighed this against the concept of intentional decision making, it was further cemented that we should choose buildings that everyday hackers would have access to or would work out of. Our thought was - hackers are everywhere, should be everywhere, and can make decisions that are anti-Orwellian from anywhere. It was also at this point we realized we wanted the LEDs to backlight the art as if there were windows being lit in buildings – so it would look like a living building. The exposed PCB fiberglass helps to take advantage of the LED bleed for this effect.

Story-wise, we felt the theme highlighted a Schroedinger’s cat environment where given a set of situations, each person has the opportunity to either create/do good/be part of the solution, or contribute to a dystopian future. The hope is that normal people, through their small contributions and seemingly inconsequential decisions, can collectively do good. But we didn’t want people to be silos in their own badge. Just like in real life, we wanted the decisions that people made on their own, to affect the options/decisions that were available to others in their game, especially if they were connecting to each other. We wanted people to convince others to make the “right decisions” – if not only to benefit themselves, to also benefit the person being convinced.

One consideration that informed the circuit design and interactivity was determining how people could interact with the badge. Given the high likelihood of a game, would we use screens? Could people play with the badges during #linecon? How would we bring in people who would never plug in a USB device into their computers?

- We historically do not use screens in our badge designs as I’m a proponent of the idea that LEDs are underutilized for conveying information rather than just blinkiness. Timewise, we also just did not have the time to prototype, source, and roll the drivers for a custom screen. So no screen!

- But, what's a game without an actual interface? We decided we would do an ANSI version of the badge. The ANSI would allow the game to be fleshed out and bring in some retro graphics for good ole' nostalgic fun. This would also allow people to see what directions they could go in and what color their lights were via the terminal. (More on that below)!

- For those who would never plug in a USB device during DEF CON, they could still move their little character up and down, even if ill-informed as to what they were doing. While they couldn't solve anything per se, they could still play around with the badge and through pattern recognition get some of their letters to turn Green.

https://i.pinimg.com/736x/55/98/f4/5598f4ac9e85d1fb489fda822298fd02--funny-images-funny-pics.jpg

Art:

- ANSI – We chose ANSI because the text-mode art scene uses that standard – it's a classic – also it had the character set we wanted to use. We only used 4 of the possible ANSI characters so that we could compress the images down to only needing 2 bits per pixel. That allowed us to fit all 8 maps for all 8 badges into the firmware while still looking graphically appropriate.

- The screen is 80 columns wide and the way that the ANSI characters break each pixel down, each pixel is a 4 x 8 grid where you can fill up the right, the left, the top half, the bottom half, or the center. So we based our grid for the artwork along those same constraints. So when I drew the pencil art, I limited myself to the ANSI character set we were going to use as much as possible. Whisker wrote a script that analyzed the line art and generated ANSI from it. This led to a 1:1 copy between the art on the physical badge and the ANSI version.

- Note that the art and terminal also limited the text length we could use. I had to use some creative abbreviations to get all of the text lines to be 80 characters or less!
- A special nod to Whisker also who used his art magic to finesse essentially all of the vector lines and graphics. The well-loved up/down/left/right D-pad and “A” and “B” buttons have been done in many other forms before, so he wanted to give it just a little extra flair by being made in the DEF CON logo and year 26.
- You may notice that the icons for the mini goon and yourself are indeed little people! We wanted to make sure people could recognize who they were moving. And for those who may have tried, you can’t really control where the mini goons go ☺️.

Use of connectors:

I’m giving this decision point its own category because a lot of thought went into this portion too. I personally did not know that hermaphroditic connectors even existed until seeing Queercon’s badge from last year. We’ve done other badges that have physical connects via two headers (again inspired by Queercon’s badges), but doing it in one header seemed like such a clever idea. We thought it’d be really funny too if we were able to get other badges to incorporate the badge bus standard into their badges. So for example, if you had a goon that had an opposite alignment as you and you were trying to distract them, you could connect into a Queercon badge and the little goon would get distracted in an amazing party. Or if it connected to a Whiskey Pirates badge, the little goon in the badge would get a bottle of whiskey and be distracted while you went around taking care of business. Though it didn’t quite work out with the unofficial badges, it seemed people had a lot of fun connecting to strangers ☺️.

So let’s talk timeline and other considerations:

- **Consideration: That the batteries last the con and minimized the need to replace batteries.**
    - The badge design was built to work off of 2 batteries, but the 2 batteries would have only lasted around 32 hours or so, so we added another 2 batteries so that people wouldn’t have to change out their batteries. There was reverse polarity protection which protects the badge, but not batteries from being placed in backwards. That amounted to people essentially recharging non-rechargeable batteries which led to a number of them outgassing/leaking. Those occurrences guarantee we will never use more than 2 batteries on a badge ever again.

- **Consideration: Minimization of the ability to counterfeit the badges**.
  - Some folks have said they heard there were counterfeit human badges – just to come into the conference, but I haven't heard of many people making their badge go from human to goon, or to some other badge type.
  - All LEDs besides the DEF CON LEDS were in a different place for different badges.

We were given the theme in November for the DEF CON 26 badges. The fleshing out of the badge philosophy was initiated beginning of December. The art for all 8 badges was drawn out by the end of December. The direction we were going in was essentially approved in January, so we were able to move forward. The puzzles were decided upon by early February. Purchase orders for parts went out in February/Early March. Prototype circuits were designed in February. We got the prototype boards working in April and finessed resistor/capacitor values. Software also started in February. Board circuitry was done mid-May and final art was completed June 1st. Boards were sent off to the fab June 2nd. Software was completed on June 5th. The following describes some of the issues we encountered with this size of a production run, and I do not wish it on anyone:

Parts from Supplier A:

- The hermaphroditic connectors came through Supplier A – and the purchase orders for these were put through in Feb/March. We were told in May that the parts would not be available until July 24th and that they would not be able to provide any other update – ie WAY too late. So I contacted the manufacturer and said essentially we needed these by mid-June or we'd have to return all of them and figure out another option. Thankfully the manufacturer responded and the fab had them in hand by June 8th or so. I'm not sure whether Supplier A even contacted the manufacturer, but I had an answer from them within 48 hours.

- Knowing that we would likely not get the code done until earliest late-May, I asked them to reserve the main PIC32MM with Microchip so that when we sent them the code, they'd be able to get us the first article, and program all of the chips immediately. That didn't happen since I think it was closer to May that they contacted Microchip. June 5th was when we sent Supplier A the hex file. July 3rd, we received a first article which didn't work. We found out the configuration bits (which are part of the hex file) hadn't been programmed. We let them know, showing them screenshots of what it should be versus what they had the config bits as, and they let us know that due to the holiday, people wouldn't be back until the following week. So July 10th we had a meeting where we told them – hey, config bits, not programmed. They said they wanted to take a closer look and on July 12th, they said, hey guess what we figured out – the config bits weren't programmed. Sometime during this week, they also sent us screenshots of their programming machines to see if we could help them figure out what checkboxes should be checked to ensure the configuration bits were programmed. In addition to all of this, the chips weren't at the programming center, so they had to be shipped there. So the chips arrived on July 17th with the plan being that the "second" article chips needed to be programmed and sent overnight to me so that I could test them and make sure they worked. That afternoon, I asked them if the chips were enroute to me and they said there was a problem and that they'd have to talk to their cohorts in the UK the next day to see if there was something that could be done. That was about as much patience as I could have had and I told them no thanks, please send these to the fab overnight. Overnight apparently meant 5 days, so the chips didn't arrive to the fab until July 23. Thankfully I worked with the fab to ensure that there would be no delay in terms of customs, otherwise we could have waited another 2-3 days.

Parts from Supplier B:

- So when I had talked to our Supplier B handler, we were looking at battery packs that were packaged in pairs. We let them know we wanted to buy 58000 pairs of batteries since each badge needed 4 batteries. They said no problem – storage and shipping wasn't going to be a problem and I checked in with them on a monthly basis to make sure things were still on point.

- Registration contacted us on Tuesday before the con letting us know that they were out of batteries and hadn't packed nearly what we thought should be there. When we looked at the boxes, the labels said QTY 800, and the boxes said 400 packs (800 pcs).

Parts from Microchip:

These went super smoothly. They were happy to reserve parts months in advance of our programming them, which was great. This helped prevent any hangups due to lack of inventory.

Electronic Design + Puzzles:

We debated between having the non-human badges sent to our home for manual programming so that each badge type would have different firmware, but for logistics sake, decided that **all** the code for **all** of the badges would need to be on the chip. Wire used pin strapping – where three pins on each badge was either pulled to power or ground, and depending on how they were set, the firmware would know what kind of badge it was.

- There are 2 ways to change the personality of your badge.

- Pins 2, 3, 4 are the hardware straps that set the personality of the badge. If you change them your badge will have the other personality.

  - strap_ID BID badge
    - 0 0x0001 human
    - 1 0x0003 goon
    - 2 0x0007 speaker
    - 3 0x0002 contest
    - 4 0x0006 press
    - 5 0x0005 vendor
    - 6 0x0004 artist
    - 7 0x0008 CFP
- #2 You can modify this line and recompile the code:
  - //#define SET_STRAP 7 // undef = straps, 0 = human, 1 = goon, 2 = speaker, 3 = contest, 4 = press, 5 = vendor, 6 = artist, 7 = CFP

We knew we wanted to have multiple software and hardware puzzles of varying difficulty, and to merge the two of them together so that it wasn't as easy as solving the badges from one direction. Each badge type has these four puzzles somewhere on themselves. So here are the following puzzles and extra hints:

- **Hall Effect Sensor** – Essentially a magnetometer where if you put a magnet over the sensor, it'd register as solved. We were inspired by Lost's Record badge that led to a buy-out of record players in Las Vegas – we wanted to do the same for magnets ☺️.
- **Dip Flip Whixr Trick** – This was first demonstrated and documented by Joe Grand in POC||GTFO 17. For our iteration – in the default orientation, the PIC12F508 chip generates a 64-bit LFSR bit stream that clocks out one bit per clock cycle. When rotated 180 degrees and reinstalled, the chip generates an 8-bit LFSR stream with a different starting key – this provides a weaker bit stream that is easier to compute.
  - https://www.alchemistowl.org/pocorgtfo/pocorgtfo17.pdf
  - Note that just solving this isn't enough – it may need to be the last puzzle you solve, or it may need to not ever be "solved"/flipped.

- **Hysteresis** – This puzzle is made out of a 74LVC1G57 multichip. This can be configured as a multitude of different gates. For this puzzle, 2 of the inputs are under the micro/user control. The third input is set up as a negative feedback with a timing RC network. The part's output therefore oscillates and the user needs to disable that oscillation via shorting the capacitor out and choosing the correct two inputs via the game.

- **Stealth Chip** – This puzzle takes the bitstream from the Dip Flip Whixr Trick and combines it with a user data stream. It is a PIC10F200 pretending to be a 74LVC1G57 chip on power on. But if a specific bit stream is fed into it (0xFEEDB0B0DEADBEEF), it swaps mode to a 2 input XOR between the user input and the LFSR input. This would have been used for the long hex strings in the puzzles. This puzzle had to be solved before the strings could have been decoded.

- **Other Hints:**

    - In the game – there are a series of decisions that need to be made where order matters, and others that as long as you have the correct toggles chosen, that'll get you your green letter.

    - On certain badges – doors between rooms can only be opened if you connect to certain badges with Green N's.

    - Hints given to you by connections with Red N's are harder than those given to you by Green N's, or really, just entirely useless.

    - You'll notice multiple hex strings. Some of these can be entered into the terminal directly, with the default LFSR key – but some strings require multiple passes with both LFSR keys. Because we're meanies.

    - There is an inventory system of sorts which if the goon in your badge resets where you are, you may lose that inventory and need to reacquire those items again.

- There exists a hardware debug menu.

- **SAO Addition**

    - If you went to DEF CON this year, or saw any of the #badgelife tags on Twitter, you'll know that a TON of unofficial badges and SAOs were created for DEF CON this year. We wanted to give a nod to the other badgemakers and put the 4-pin SAO standard on the Official Badge for maximal bling!

Known issues, Lessons Learned, and Implications for Future Builds:

- No more than 2 batteries. For both polarity's sake and for weight sake. People will just have to change out their batteries if we have a need for that amount of power!

- Physical interconnects, while fun, are subject to the physical forces of nature. Some folks had them come off entirely and others dealt with ones that were slightly bendy. Resoldering them on would have helped. Likely going to use short distance IR for future badges or some other non-contact interface.

- The regulator on about 50 badges, which we know of, got hot to the touch though the badge would still function otherwise. It was likely due to some sort of solderball/short. Some forensics has also potentially highlighted the inductor as a reason for the regulator's malfunction (Courtesy of @cybermarajade). Reflowing/reseating the part helped fix a number of these. Wire is looking at another regulator with a friendlier package type/size, but it's difficult to find buck boost regulators that are any bigger than the current leadless QFN packages we deal with due to industry uses.

- Approximately 6 that we know of had issues with soldermask registration where a short between ground and power occurred. If the solder on the battery pack pins were retouched to avoid creating a short, this usually fixed the issue. We'll know to give wider keep-out regions for the planes to prevent this in future designs.

- Firmware bugs. This is completely my fault because I am apparently a pretty terrible alpha tester, though I did only have 2 prototype badges to test with! Your forgiveness is requested!

    - First article hardware builds from fab did not arrive until after final firmware had been sent.

    - There was an issue with people being able to get "good" text when hooking up with a Green N of another badge type. My fault for using a debug menu to test text flipping as opposed to using the physical connection.

    - There was also an issue with the badge registering that the hysteresis puzzle had been solved.

        - There was apparently a documentation error in one of the low level APIs. The upper level code was correct per documentation (and tested good via emulation) but was one bit value off from what the final hardware actually did.

    - The stealth chip puzzle hadn't been incorporated into the firmware – I think this was because we were using interchangeable words for different puzzles which sounded similar. Sneaky/Stealthy/Tricky/etc . Note to self, use the same words for the same puzzles across multiple instances.

    - During testing of the fix, we found there was also a documentation issue that would have kept this from being smoothly implemented.

General thoughts:

- This was a very VERY tight schedule for our team given that we had a badge due in November, the Cyphercon badge due in mid-April, the DEF CON China badge due in mid-May, and all elements for the DEF CON badge due in early June if not sooner. Oh and the Wisconsin badge that should have been due in Mid-April but time constraints made it so we couldn't deliver until DEF CON. If we are invited again, thank goodness we'll have more than 6 months to do such a build.

- You may be amused, but most of the builds we've done have been 500-700 badges. For the majority of those badges, I was the pick and place machine for the parts, and responsible for assembly. I did seriously consider whether I could put together 29000 badges by hand to ensure quality, but then realized how much time that would actually translate to, and then realized there was no way I would be able to do that.

- We also considered using Lipo batteries because they're just so much more powerful and lighter than AAs or coincells and again we're usually the ones who hand charge these. I thought about our electricity bill and also the amount of time it'd take to charge all of these and decided against it.

Our favorite stories:

- We were invited by a group of 25 people who had managed to get all 8 badges to come to their get-together to help figure out what was going on with the badge puzzles (http://www.deaddialect.com/articles/2018/8/17/badge-story). That led to some forensic analysis of the code and a realization that there were some bugs. We were able to fix one and offered the team the firmware fix by putting it on our badge and letting them borrow the badge. They had to dump the hex, flash their own badges, and rework the puzzles. By this time, it was like….1 or 2 AM. I had no idea other people were actively working on the badge, but then one of the members of this team said:

    - Awesome Guy: "Hey, you guys know what we have to do?"

    - Me: "Go to sleep since it's 1AM?"

    - Awesome Guy: "We have to bring this badge firmware update and information to the other badge teams working on this. It's important that they know this."

    - Other awesome guys: "Yeah! We're coming with!"

  - Meanwhile I’m thinking “OMG. You guys. ALL THE FEELS”

- The other team was at Flamingo, so we trucked it over this group to the other 50 (!) some odd people who were banging their heads against the hardware, the software, the everything. Apparently, 4-5 other groups had coalesced to form one larger group just to solve the puzzles. Seriously - there were emulators made, a non-hacker who had come just to support their spouse had made the badges colorblind-friendly, there was discovery of dark current magic which made the Robot head light-up. They were kind enough to think we were sneaky enough to put that into the badge ☺️. There were people new to DEF CON, people who had solved black badge challenges, people who were veterans, all working together. It was inspiring!

- The group was kicked out of the Flamingo chill room not long after people started updating their badges, and we all trucked back to a Caesar’s Palace chill room. 70-some people put tables together and started working on the puzzles while shushing each other so that hotel security outside wouldn’t hear them working. They worked until 6-7AM on Sunday and managed to get all of the lights green by single stepping through the code, working through the puzzles, and essentially fixing our code. We love you all, and are so grateful to have witnessed the teamwork and comradery you exhibited. I was told by many DEF CON vets that this is the DEF CON they remember and that what you guys did was exactly why they come back year after year.

- We were hanging out at the Hardware Hacking Village answering some questions about the badges and I explained the importance of connecting with other individuals with Green N’s to a particular individual. She had been connecting with lots of different people but didn’t realize the alignment mattered. Standing next to her were two other individuals who had just joined to listen in, and I noticed they had green N’s.
  - Me: “You may want to connect with them since they have green N’s! But it is kind of risky because you’ll be giving your red human setting to him, while he’s giving you his green human setting.”
  - Her: “Oh! Well I don’t want to give him something bad!” *the three start thinking*
  - Him 2: “Wait, can’t I save you?”
  - Him 1: “Yeah! Here, I’ll give you my green human, and then he and I can reconnect, and he’ll get me back to having a green Human setting”
  - Cue not only strangers helping each other, but people helping save each other. <3.

Our Deepest Thanks

- To the registration team and the group of individuals who drove out into the Las Vegas heat to get the remaining batteries (A big thank you to BigEzy [sp?] and his wife and their team).

- To inhuman registration goons and Active X specifically – for troubleshooting/replacing badges that came back. I'll probably never forget those black gloves.

- To CyberMaraJade and her team for their work at the Hardware Hacking Village and the time they put towards fixing badges and troubleshooting any hardware issues. We're so grateful!

- To the in-human badge groups who were targeted by humans – especially to those who had CFP badges of which there were NOT MANY, and yet who still were willing to connect with hundreds of others when they were just trying to walk to the next event.

- And to all of you who came up to say hi and ask about the badges – this was so much fun for us!