A Five-Year History of

Electronic Badges

by Joe Grand
aka Kingpin

Me.

electrical engineer.

hardware hacker.

daddy.

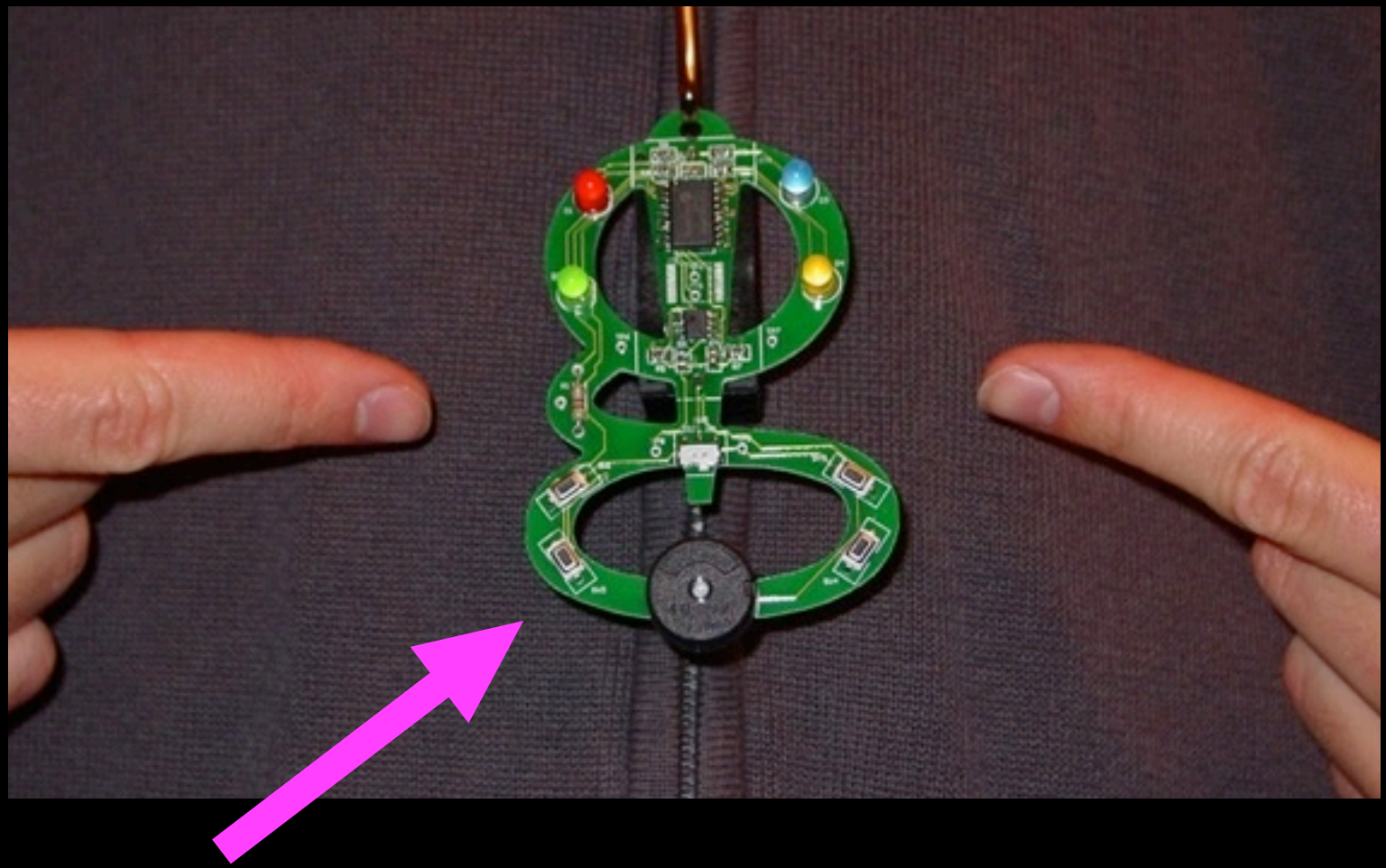
runner.

washed-up tv host.

DEFCON

- ★ The largest and oldest continuously running hacker/ security con in the whole wide world!
- ★ Held annually in Las Vegas
- ★ Celebrates all forms of technology subversion and underground culture
- ★ DEFCON 1 = 1993, ~100 people
- ★ DEFCON 18 = 2010, > 8000 people

What started it all...



Custom PCB developed in 2005 for my
Black Hat Hardware Hacking Training course

The Dark Tangent saw this and said "Make it happen."

Then.

- Hardware/electronics not well represented in the hacker world
- Not aware of any conference that had an active, artistic electronic badge
- No one knew what to expect!


w/ Black Badge status!
Award the most ingenious, obscure, mischievous, or technologically astounding badge modifications created over the weekend.
Badge hacking contest!

2006

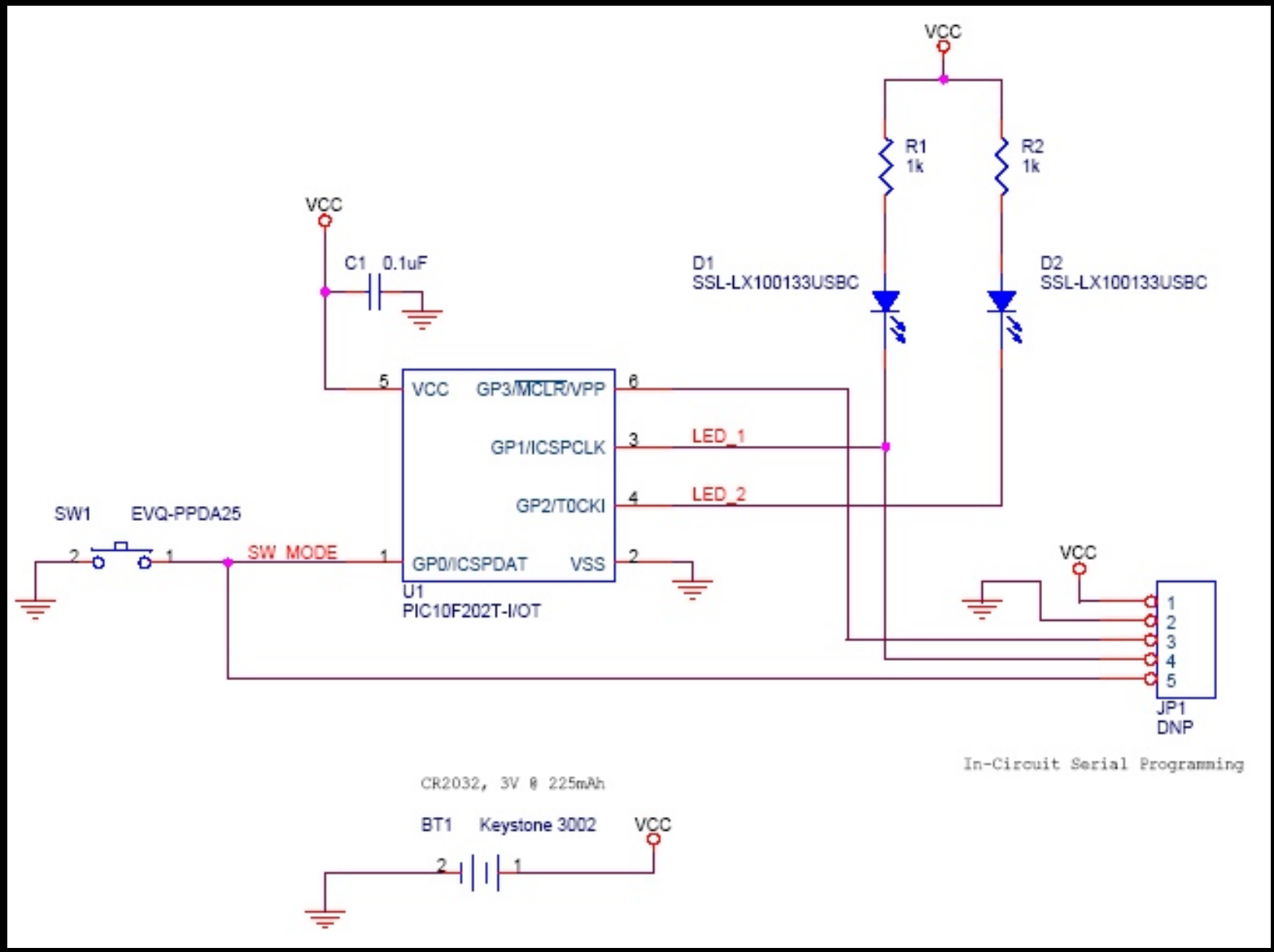
DC14: Beauty Shots

DC14: Beauty Shots

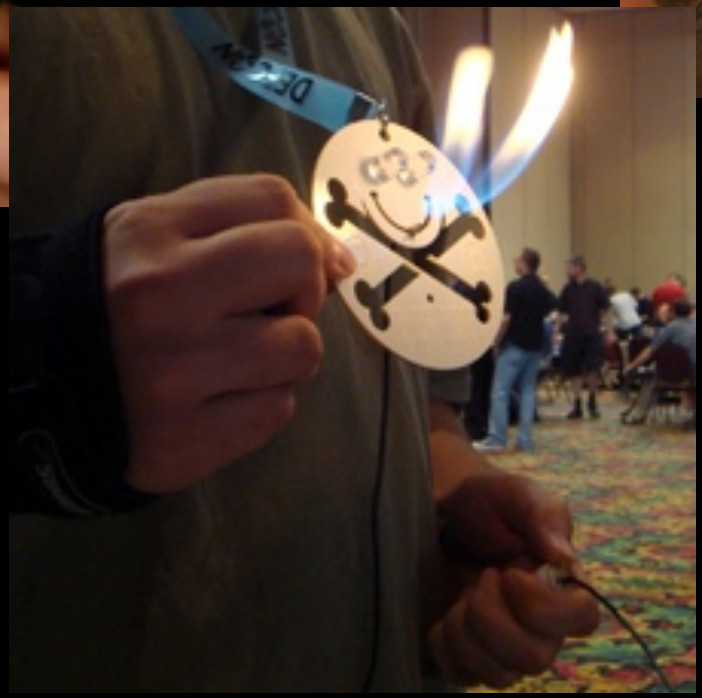
DC14: Functionality

- ★ Single pushbutton cycles through states:
  - ◉ Both LEDs On
  - ◉ Both LEDs Blinking
  - ◉ Alternating LEDs
  - ◉ Pseudo-Random Pattern
  - ◉ Sleep

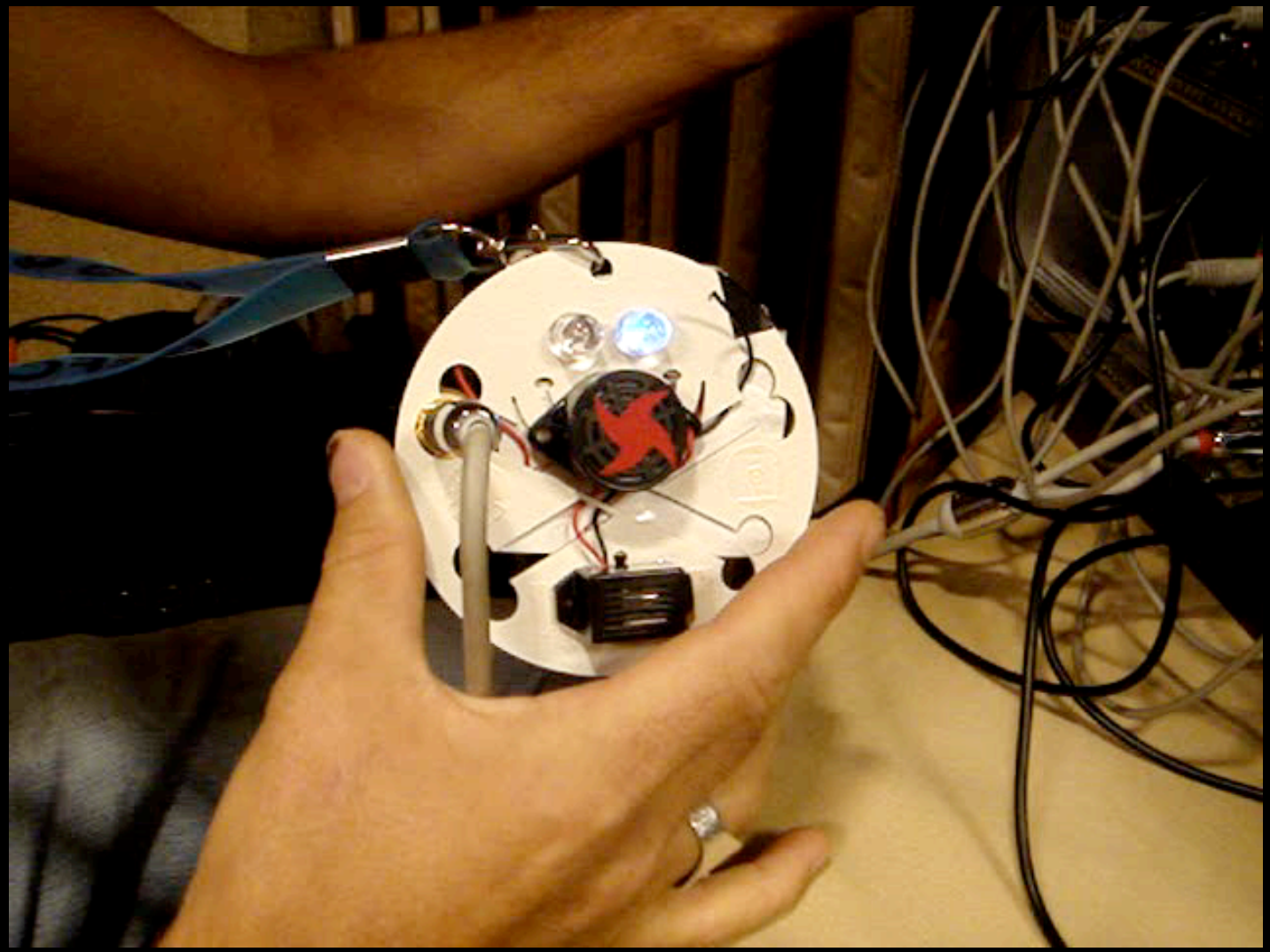
DC14: Schematic



DC14: Badge Hacking



DC14: Event Ghoul Generator



Scott Scheferman aka Shagghie

LEDs as event generators into analog synthesizer

DC14: Awards Ceremony

2007

DC15: Beauty Shots

DC15: Beauty Shots

DC15: Functionality

- ★ Text Message Display
  - ◉ Default = "I <heart> DEFCON 15"
- ★ Text Message Entry
- ★ Scroll Speed Selection
- ★ Persistence-of-Vision (POV)
- ★ Sleep

DC15: An Ode to the Badge

170 hours...

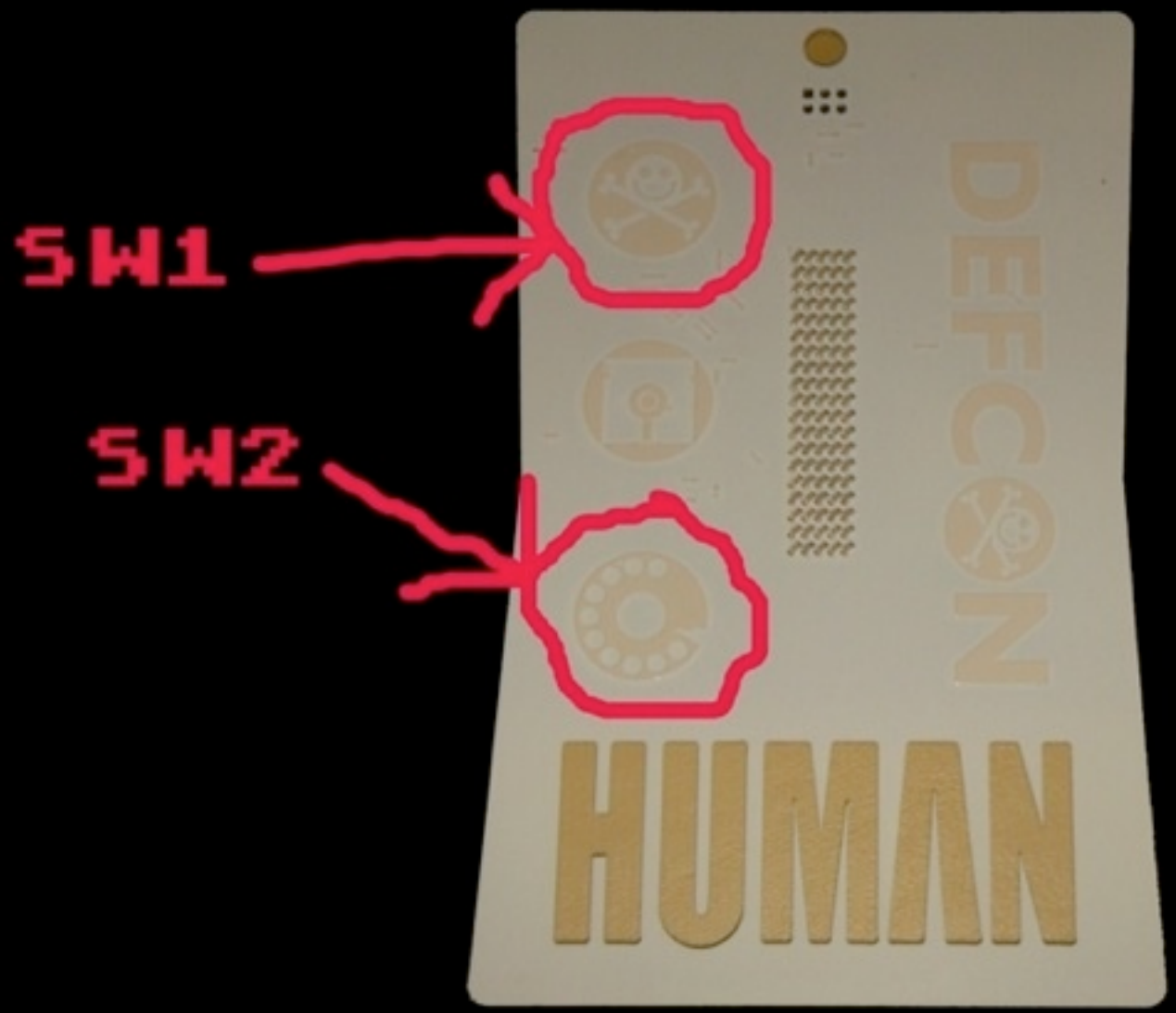
2 nights of my honeymoon...

3 PCB revisions...

863,600 total components...

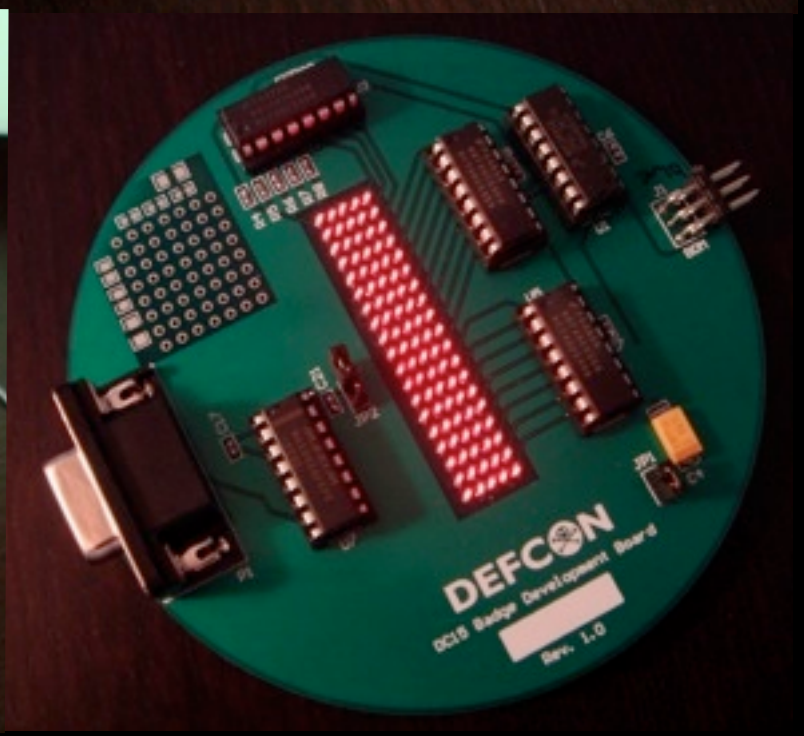
6,800 hackers...

DC15: Subsystems

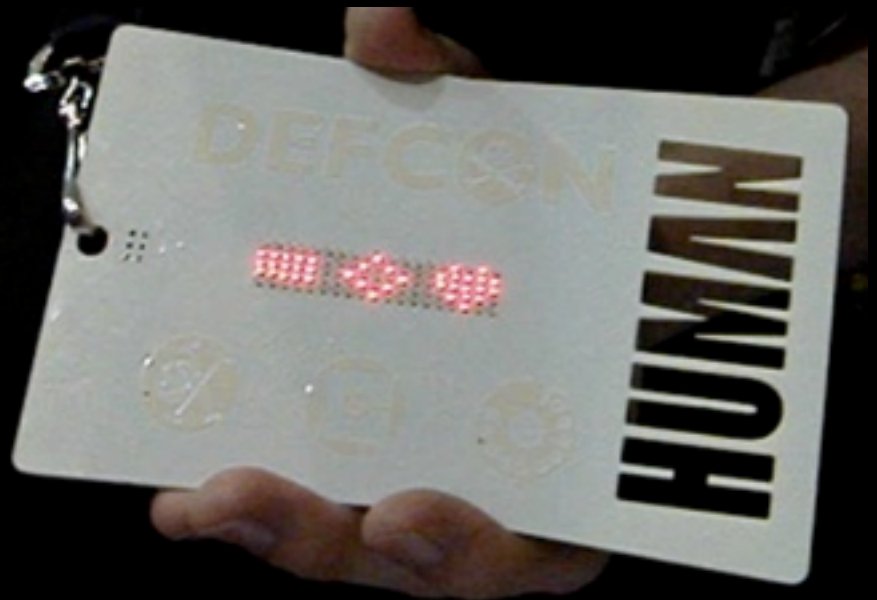


DC15: Subsystems

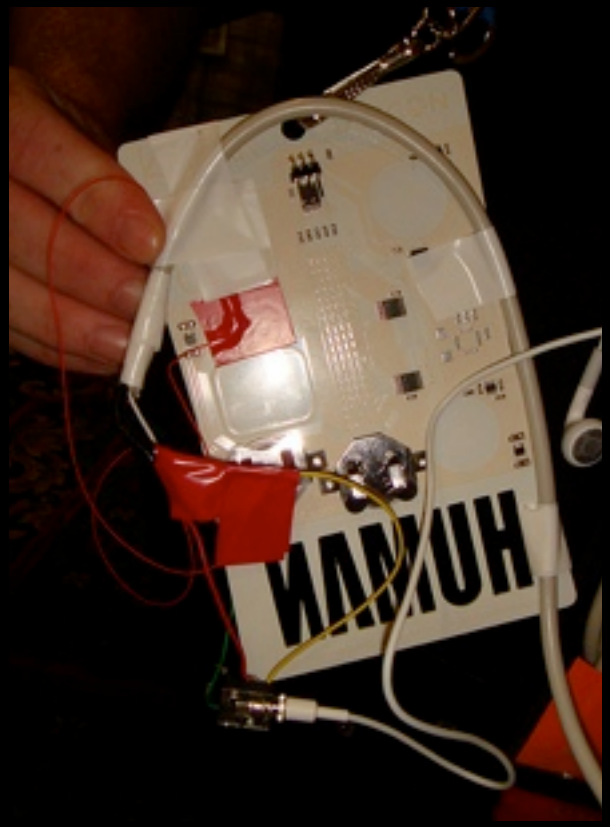
DC15: Development

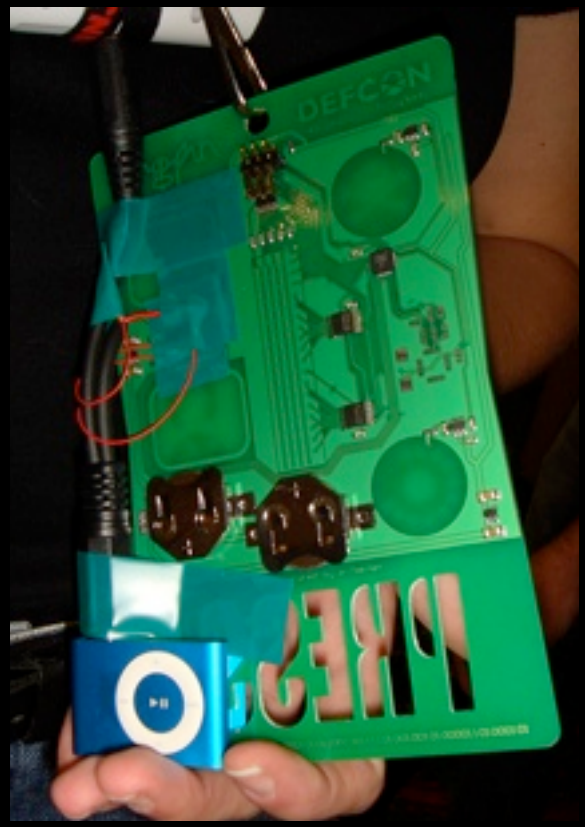


DC15: Badge Hacking



DC15: Badge Hacking





Team Osogato

VU Meter using A/D input & LED matrix

Worked w/ The Brothers Grimm to create a rap song (!) from my poem

DC15: Awards Ceremony

2008

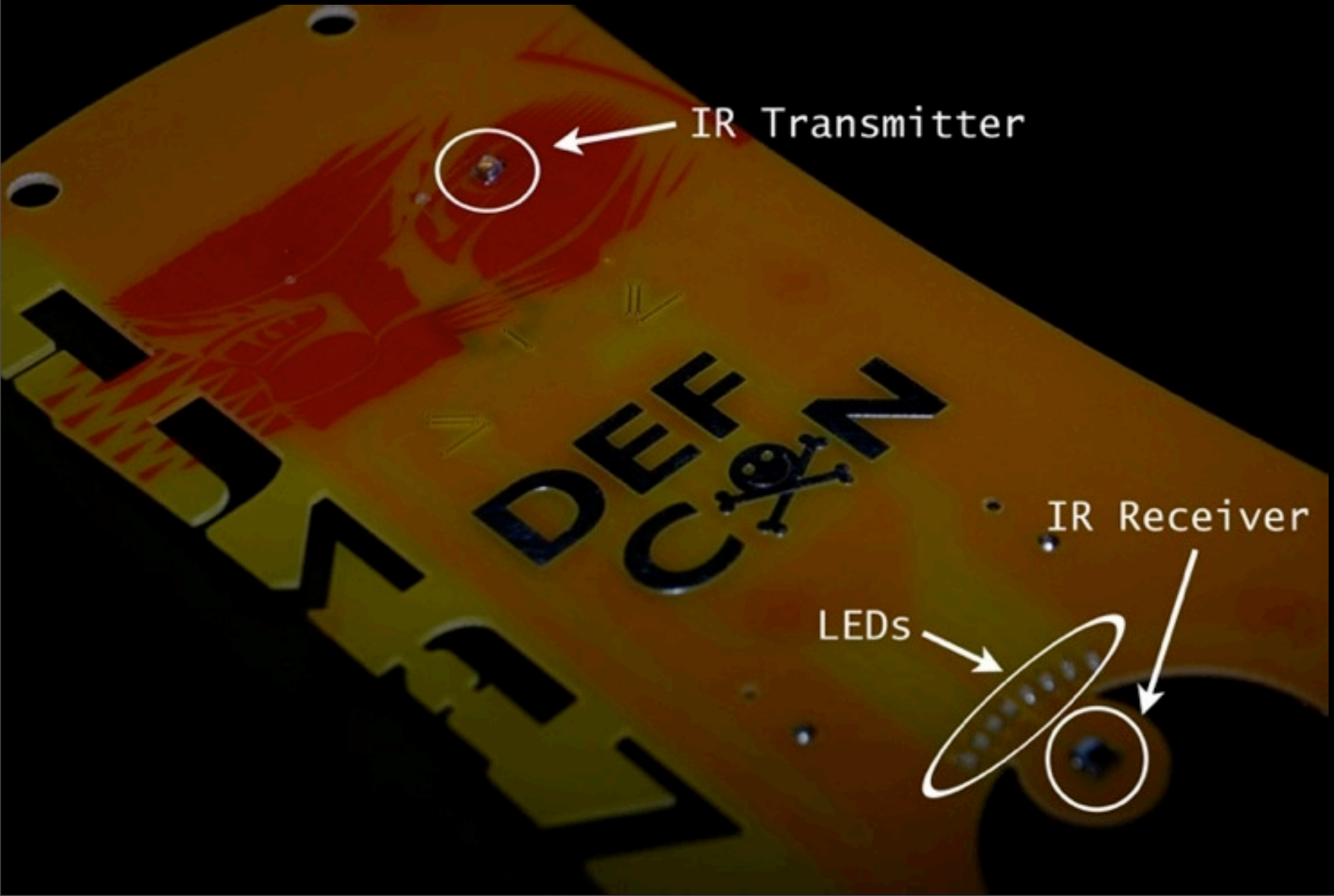
DC16: Beauty Shots

DC16: Beauty Shots

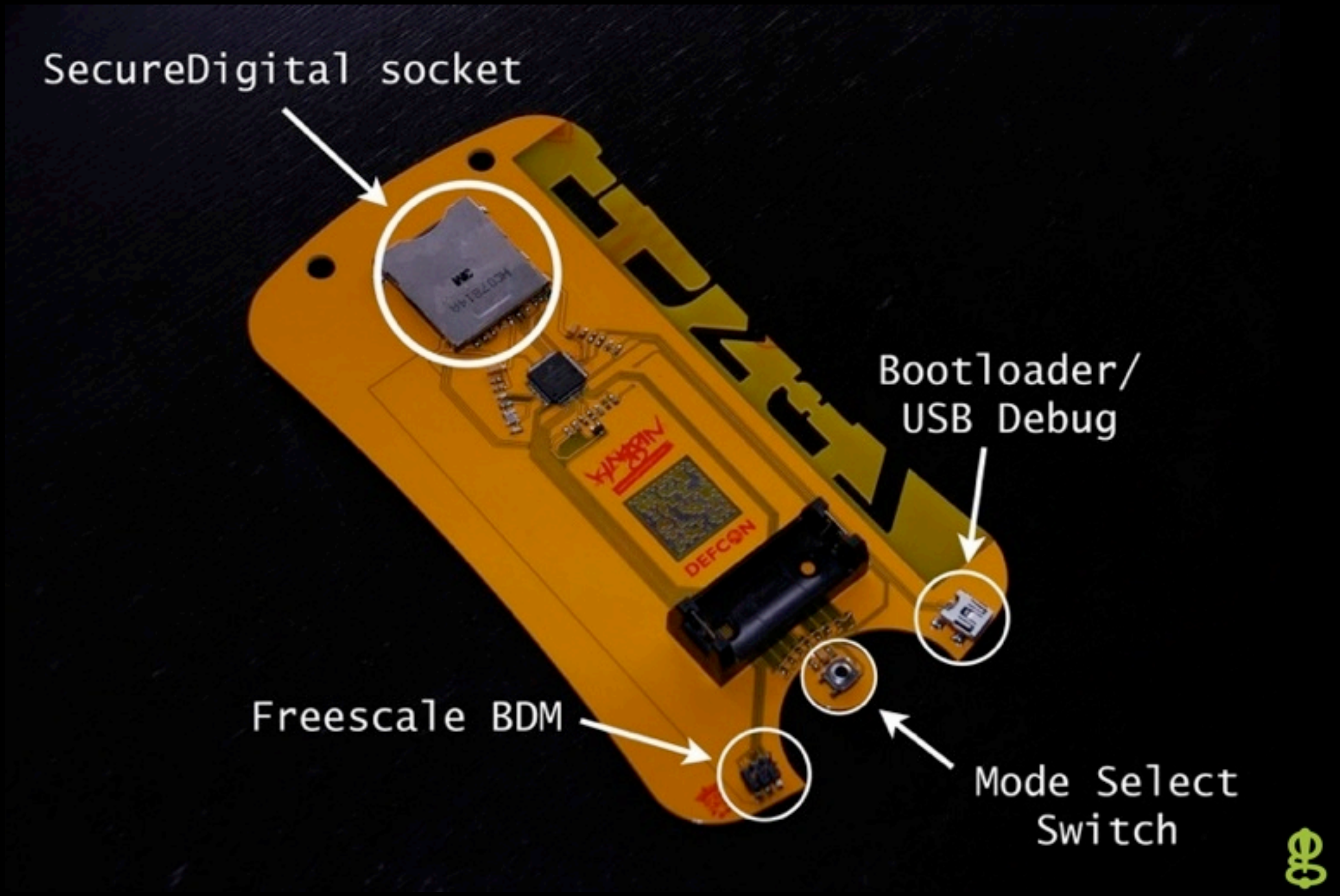
DC16: Functionality

- ★ TV B GONE®
  - ◉ Cycles through all known TV power off codes
  - ◉ `www.tvbgone.com`
- ★ Transmit File via Infrared
  - ◉ SD Card/FAT16 support
- ★ Receive File via Infrared
- ★ USB Bootloader/Debug Port
- ★ Sleep

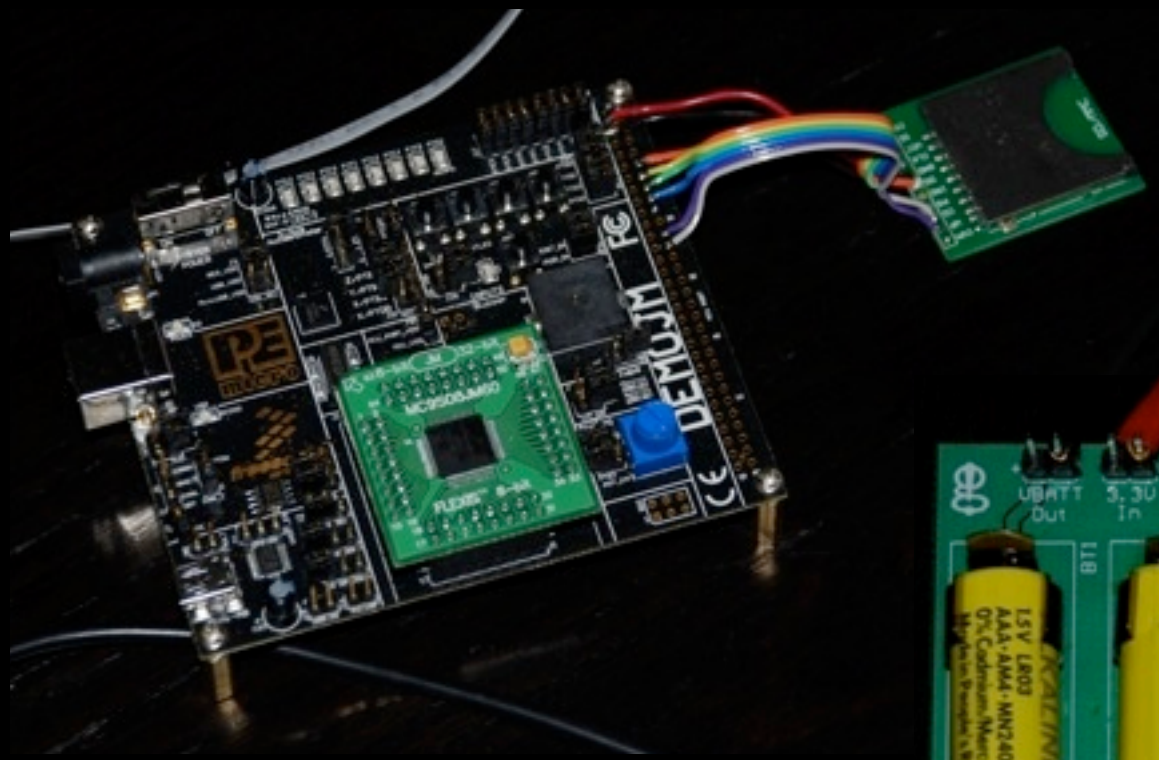
DC16: Subsystems



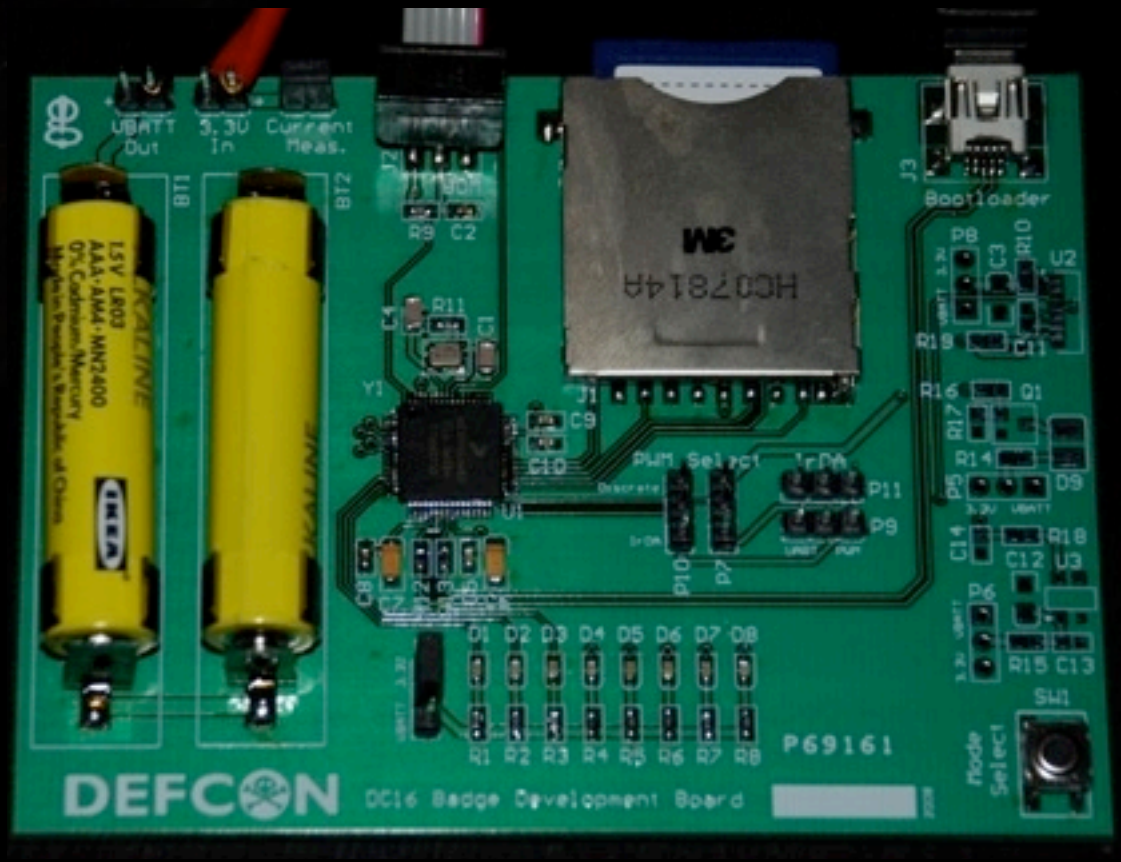
DC16: Subsystems



DC16: Development

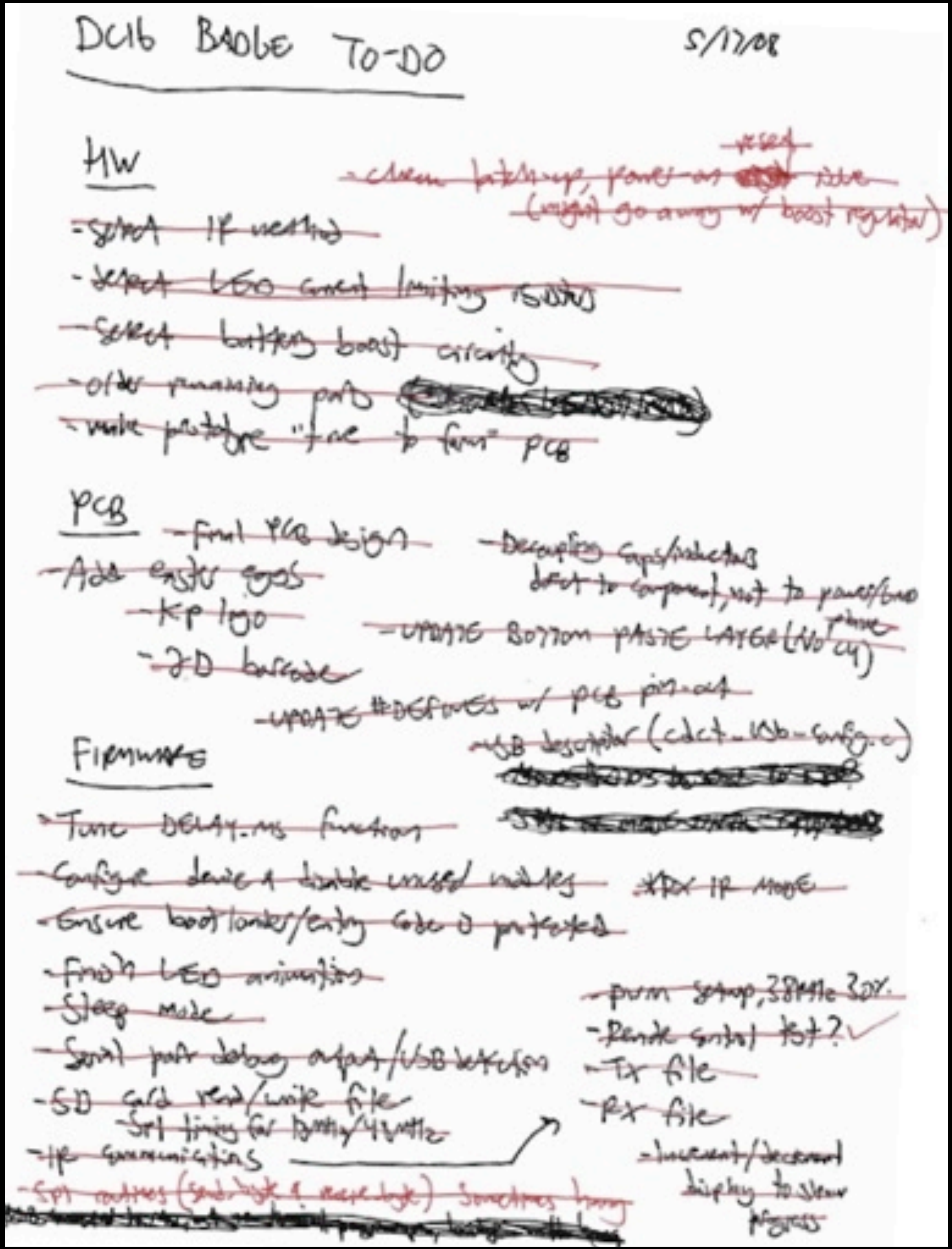


1. Freescale DEMOJM w/ MC9S08JM60 module



2. Custom development board to test & verify H/W

DC16: Development



DC16 BADGE TO-DO 5/17/08

HW

- ~~clean lockups, power-on reset issue (might go away w/ boost regulator)~~
- ~~select IR method~~
- ~~select LED current limiting resistors~~
- ~~select battery boost circuitry~~
- ~~order remaining parts~~ [redacted]
- ~~make prototype "fine to form" PCB~~

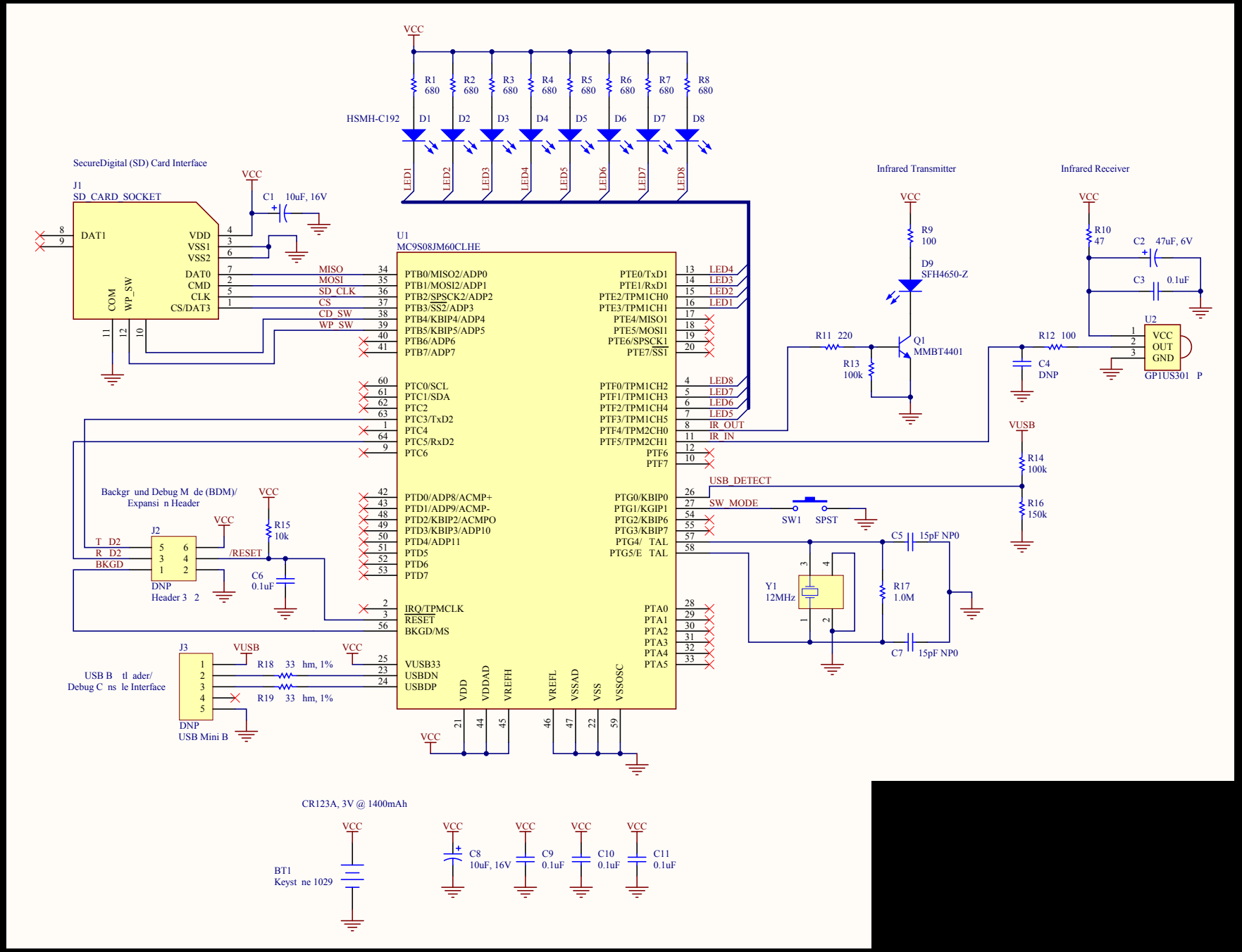
PCB

- ~~final PCB design~~
- ~~Decoupling caps/inductors direct to component, not to power/gnd plane~~
- ~~Add easter eggs~~
  - ~~KP logo~~
  - ~~2D barcode~~
- ~~UPDATE BOTTOM PASTE LAYER (No C4)~~
- ~~UPDATE #DEFINES w/ PCB pin-out~~

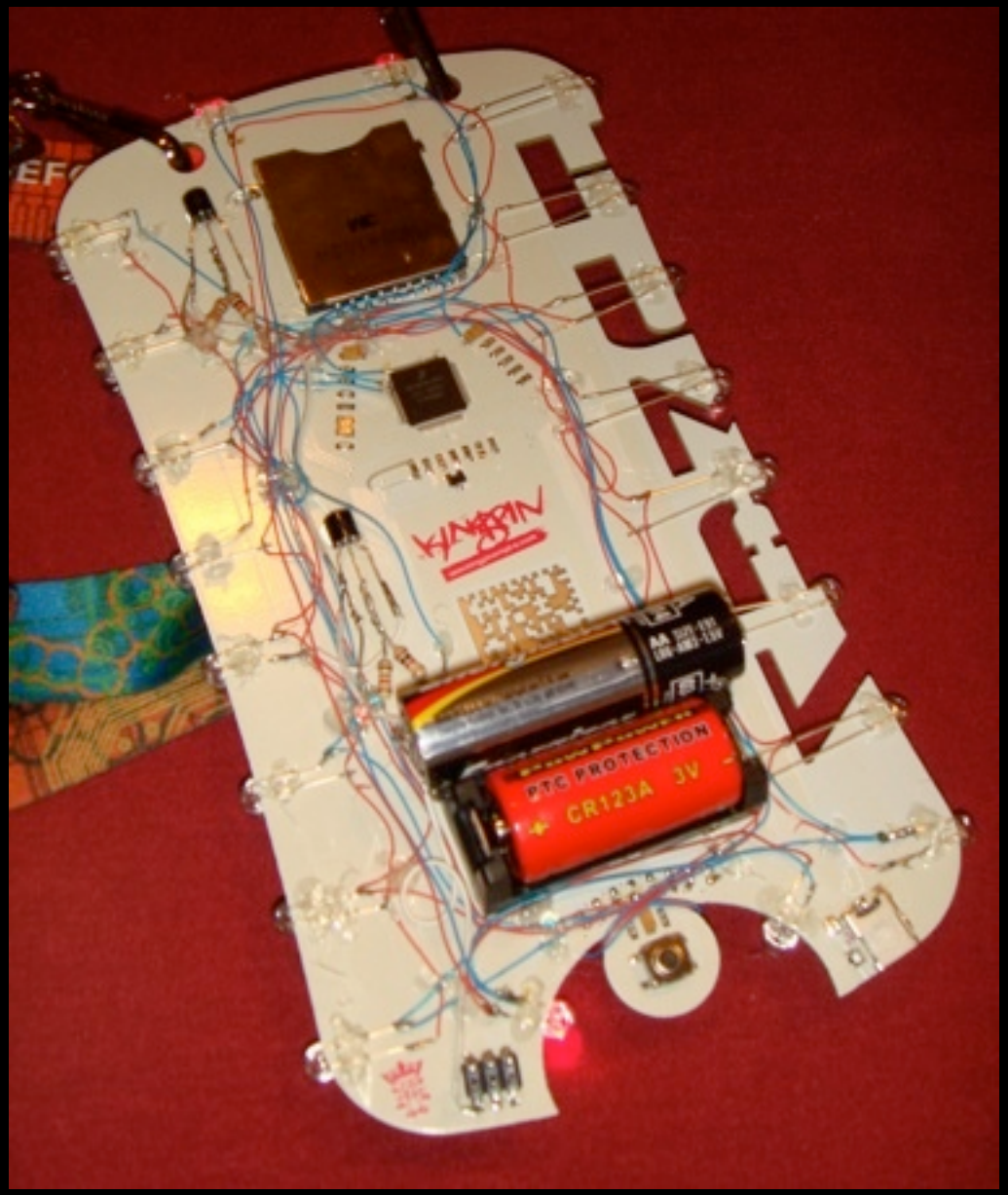
FIRMWARE

- ~~USB descriptor (cdc_usb_config.c)~~
- [redacted]
- ~~Tune DELAY_MS function~~
- ~~Configure device & disable unused modules~~
- ~~*RX IR MODE~~
- ~~Ensure boot loader/entry code is protected~~
- ~~Finish LED animations~~
- ~~Sleep mode~~
- ~~Serial port debug output/USB detection~~
- ~~SD card read/write file~~
  - ~~Set timing for 38kHz/4MHz~~
- ~~IR communications~~ →
  - ~~pwm setup, 38kHz 30%~~
  - ~~Remote control test?~~ ✓
  - ~~Tx file~~
  - ~~Rx file~~
  - ~~increment/decrement display to show progress~~
- ~~SPI routines (send byte & receive byte) sometimes hang~~
- [redacted]

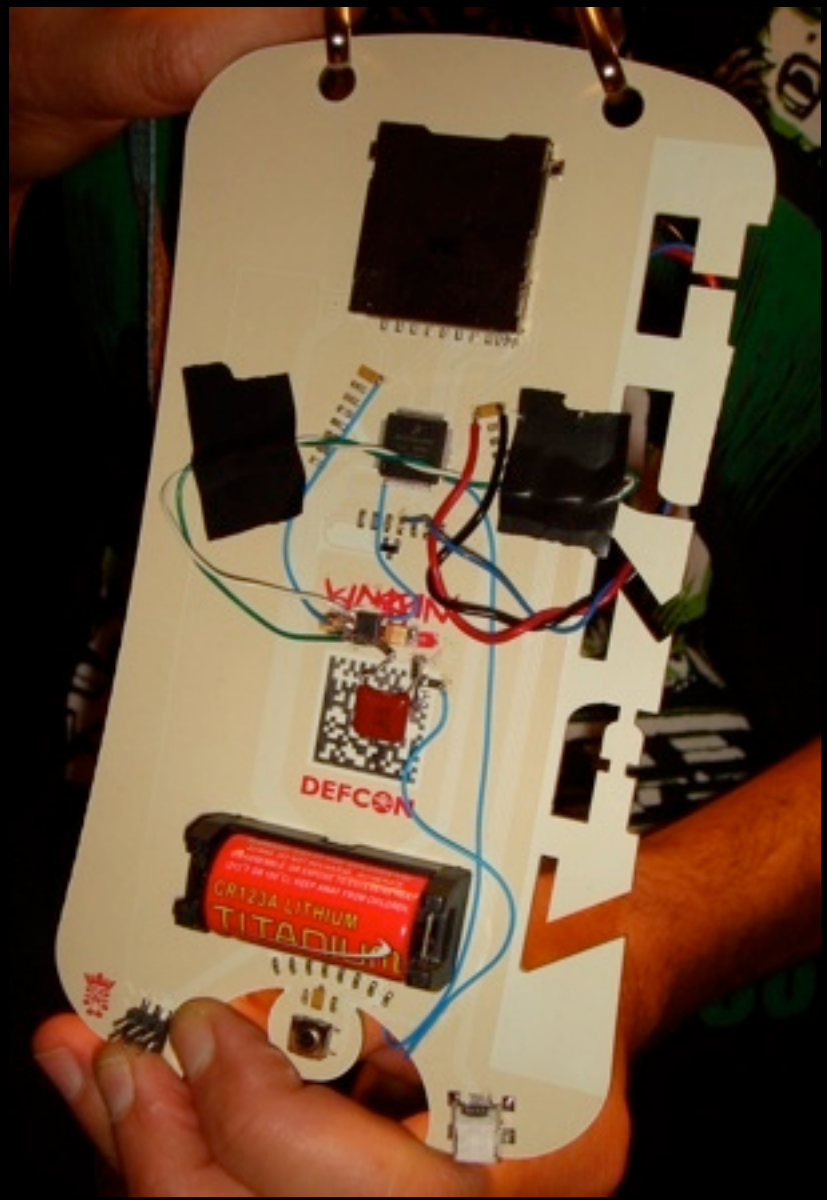
DC16: Schematic



DC16: Badge Hacking



DC16: Badge Hacking



DC16: Front Row Badge

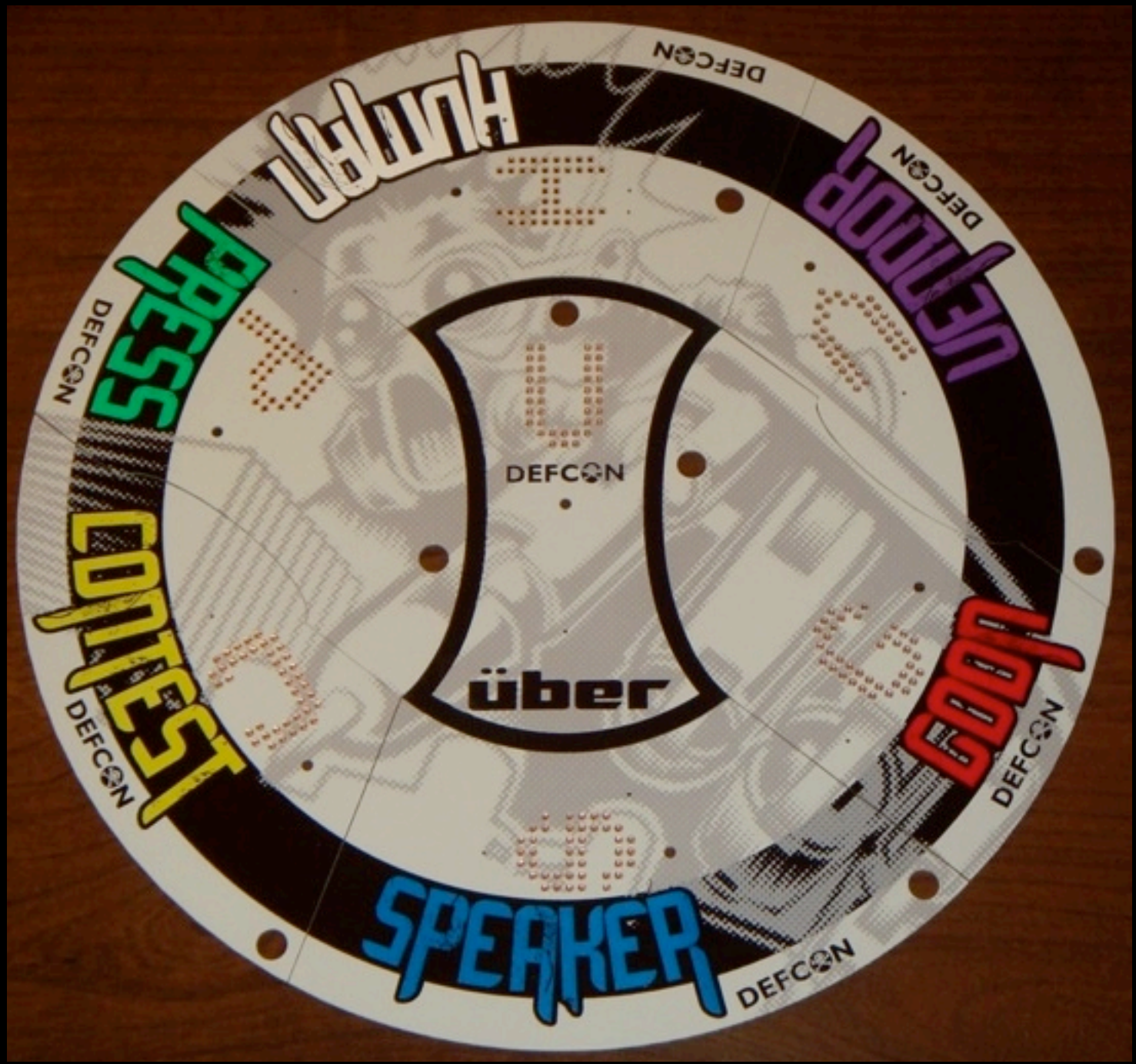
BonzoESC, Sterling, Critta, Jymbolia

Apple Front Row/HP Pavilion DV

IR remote emulation

2009

DC17: Beauty Shots



DC17: Beauty Shots

DC17: Functionality

- ★ Three modes determined by sound level/ frequency
  - ◉ Party: RGB LED controlled via Fast Fourier Transform (FFT)
  - ◉ Quiet/Idle: RGB LED slowly blends through colors
  - ◉ Sleep: When sound level is below a pre-defined threshold
- ★ Multi-badge communication
  - ◉ Physically connected via I2C (3 wires)
  - ◉ Individually addressable
- ★ Static serial bootloader
- ★ Secret modes

DC17: A Poem

DEFCON 17 Haiku
Joe Grand aka Kingpin
Electronic badge

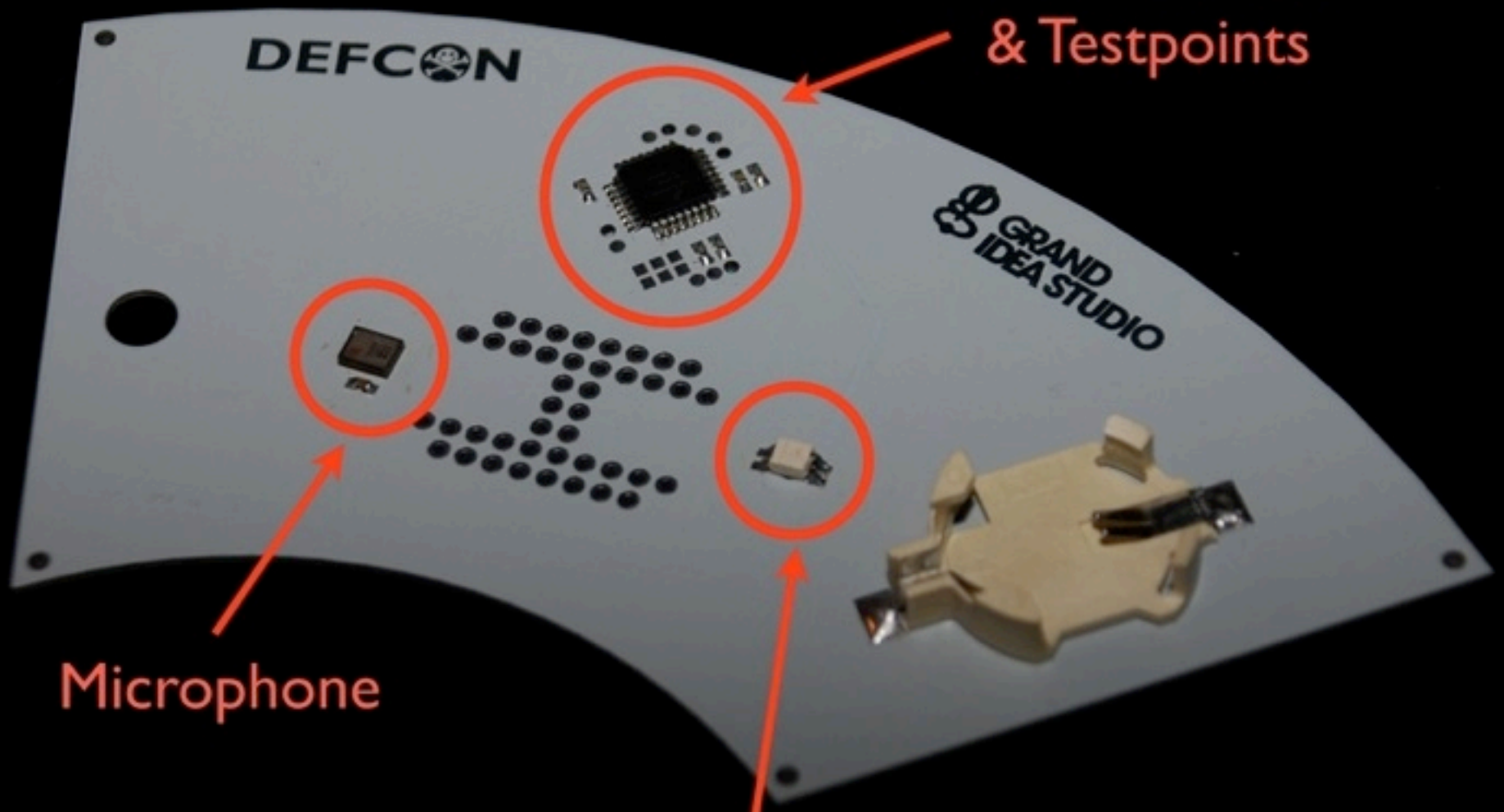
Audio input
Affects LED output
Sound and light combined

Upload new firmware
With serial bootloader
Voltage reassigned

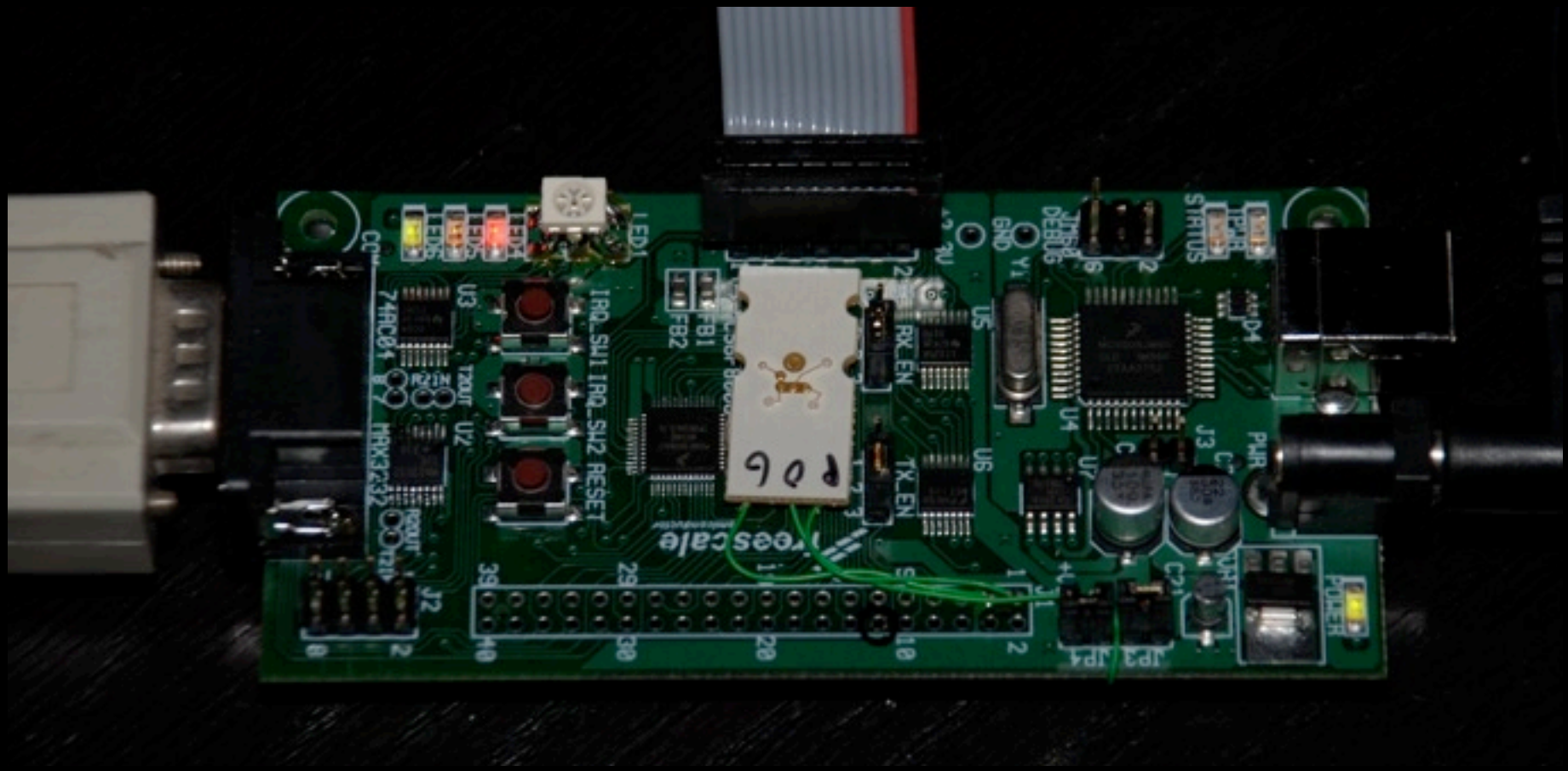
Puzzle of seven
Badge-to-badge interfacing
Using I2C

Hack badge for prizes
Clever modifications
Can you impress me?

DC17: Subsystems

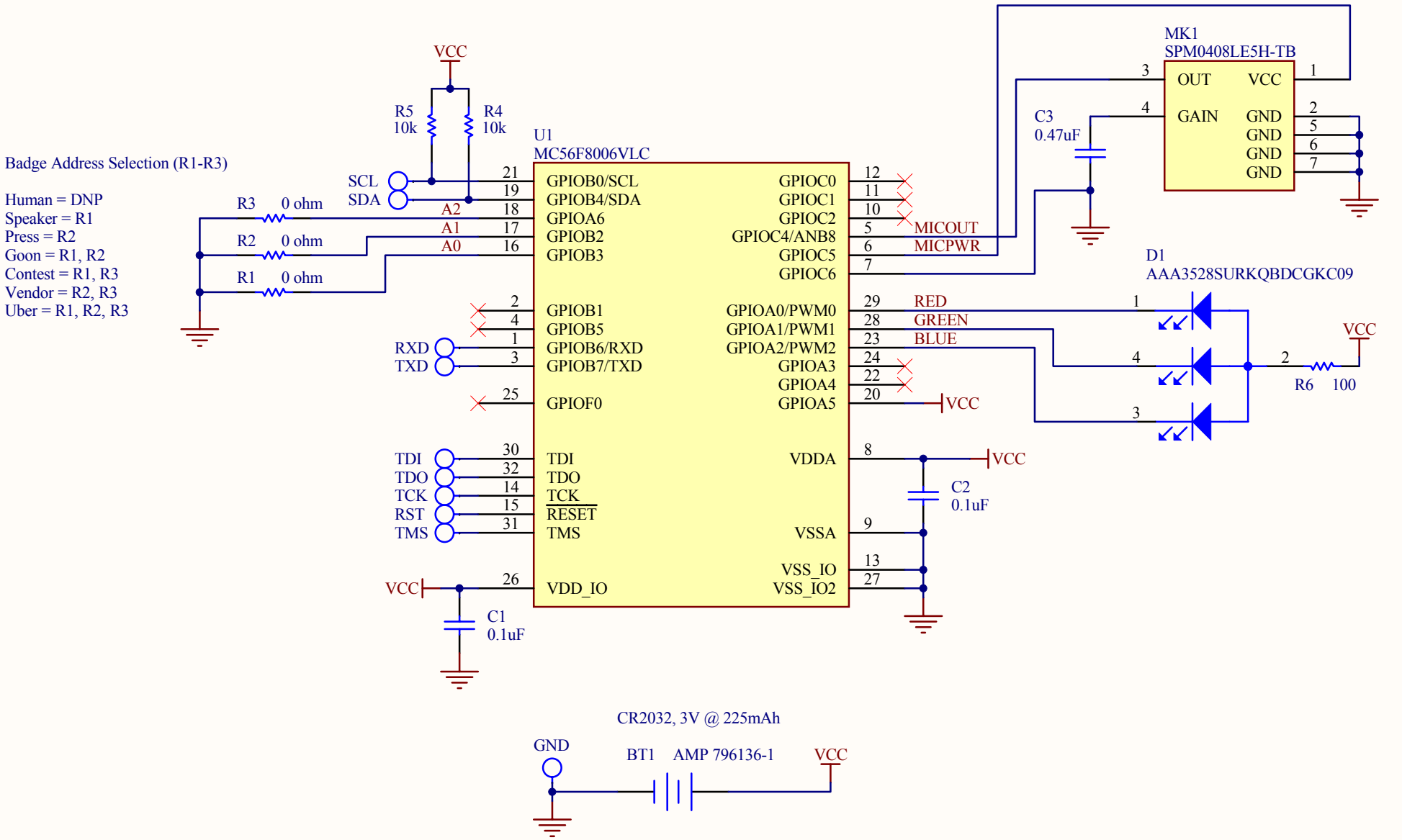


DC17: Development

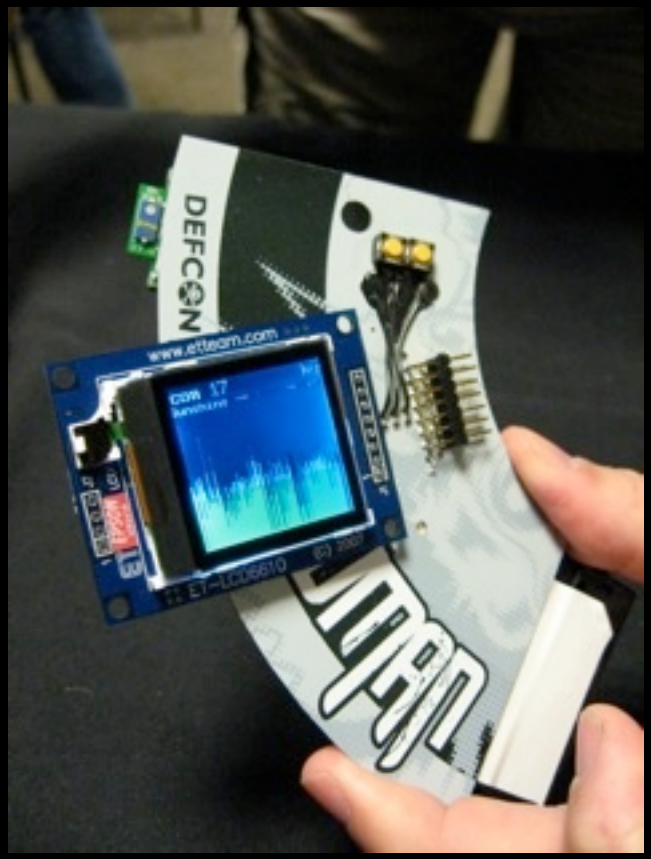


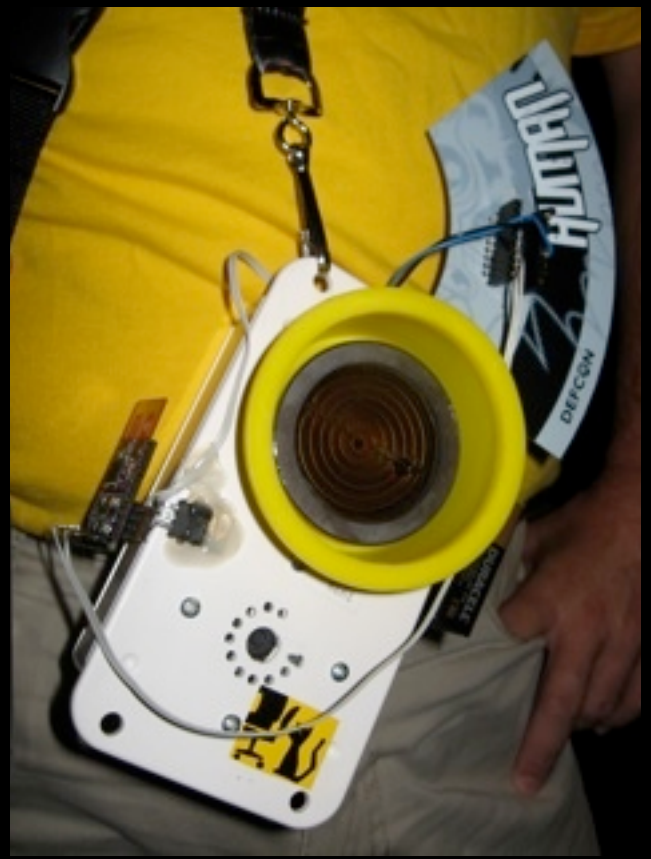
Freescale MC56F8006-DEMO board + custom circuitry

DC17: Schematic

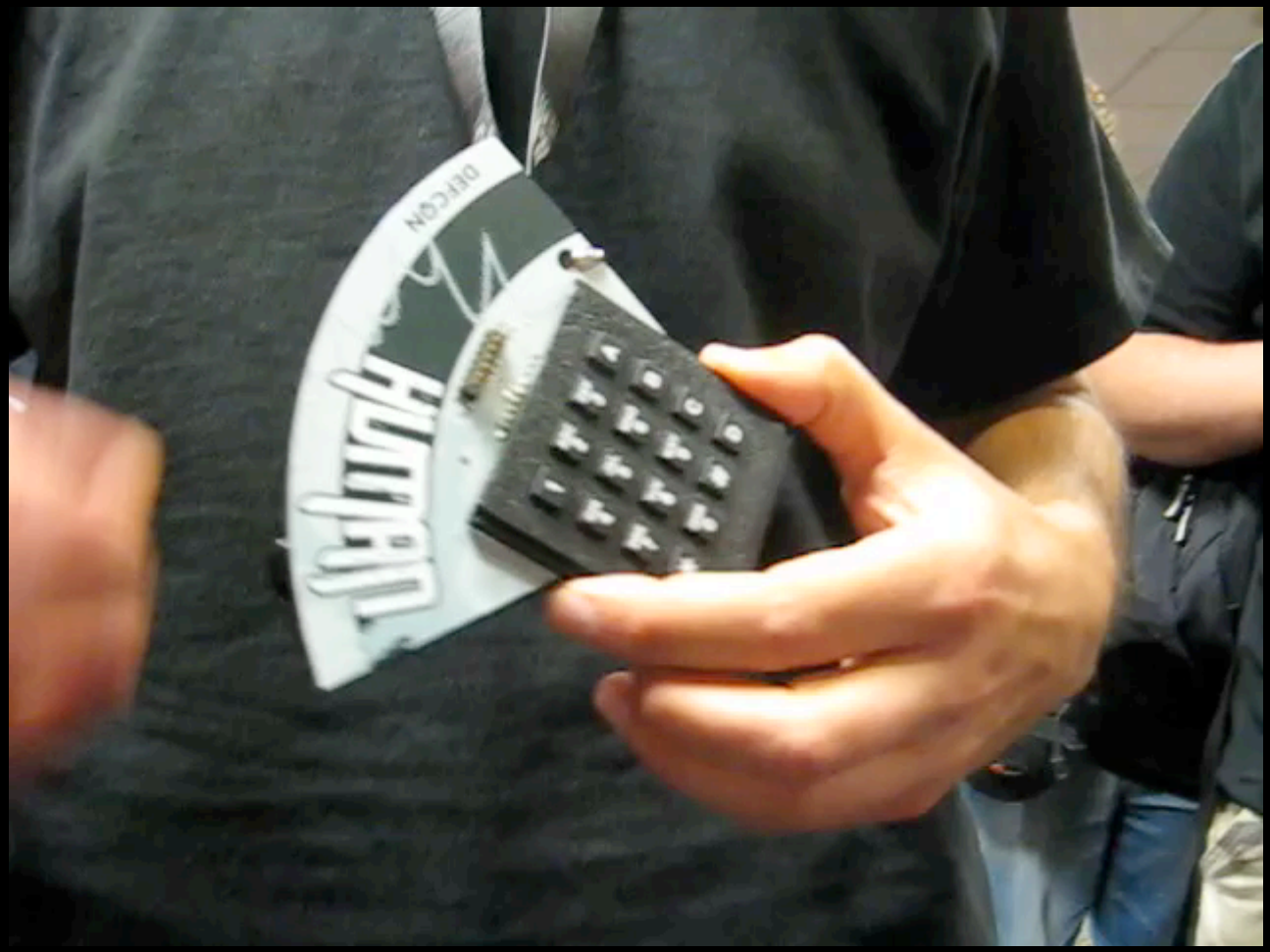


DC17: Badge Hacking





DC17: Tone Generator



501d3r Guy

Multifunction Tone Generator &
Voice Amplifier

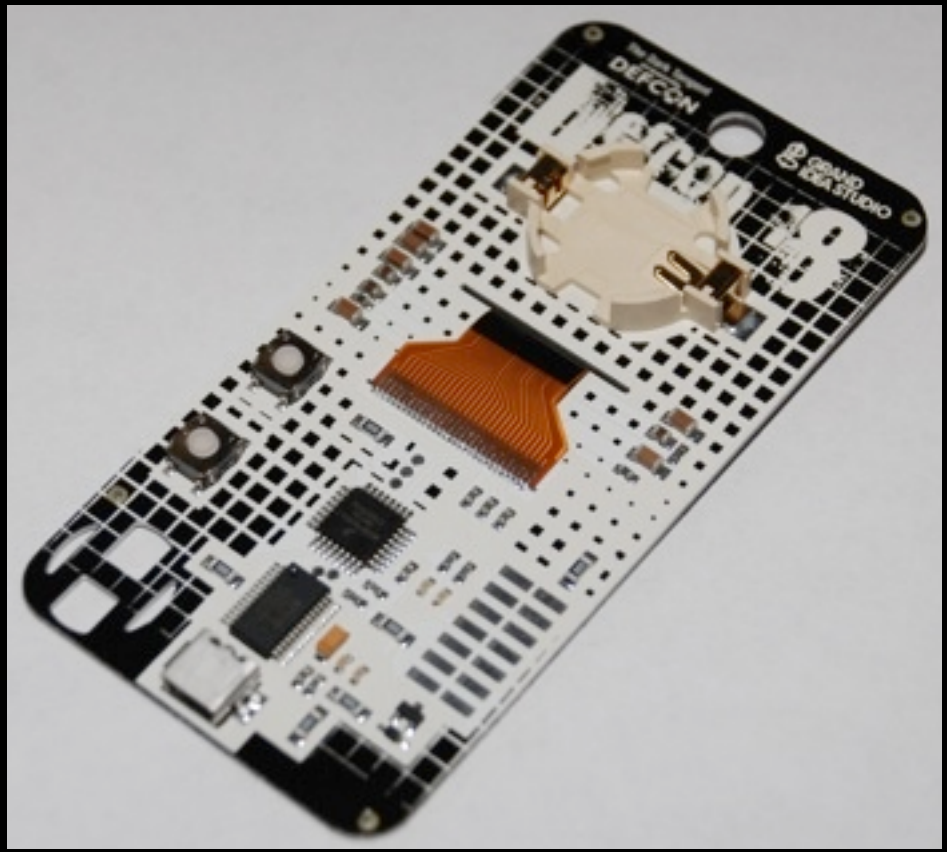
DC17: Super Mekka Uber Badge

Smitty & The Minions

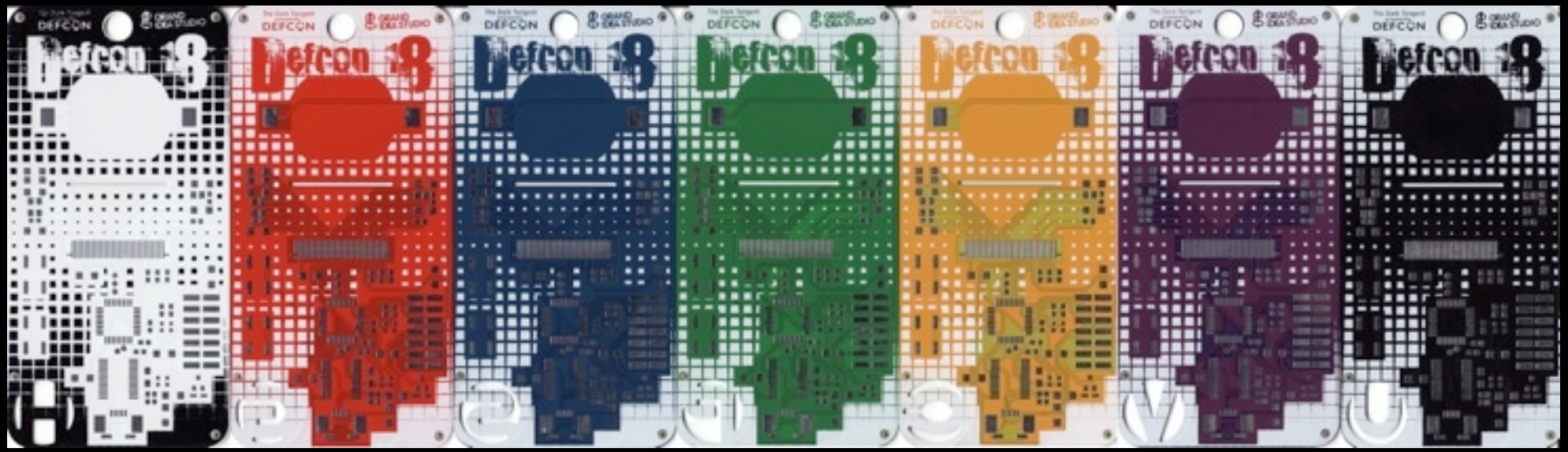
Multi-Badge Communication & LED Animations

2010

DC18: Beauty Shots

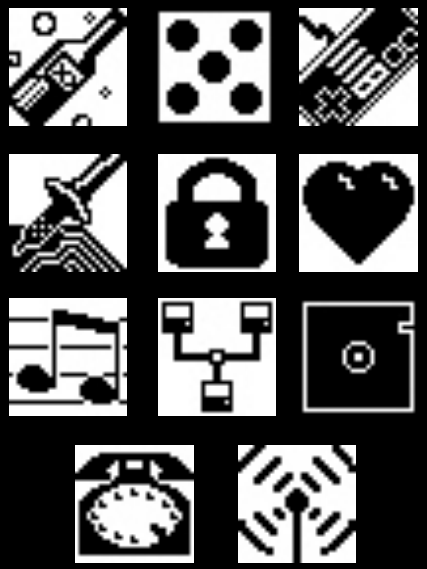


DC18: Beauty Shots



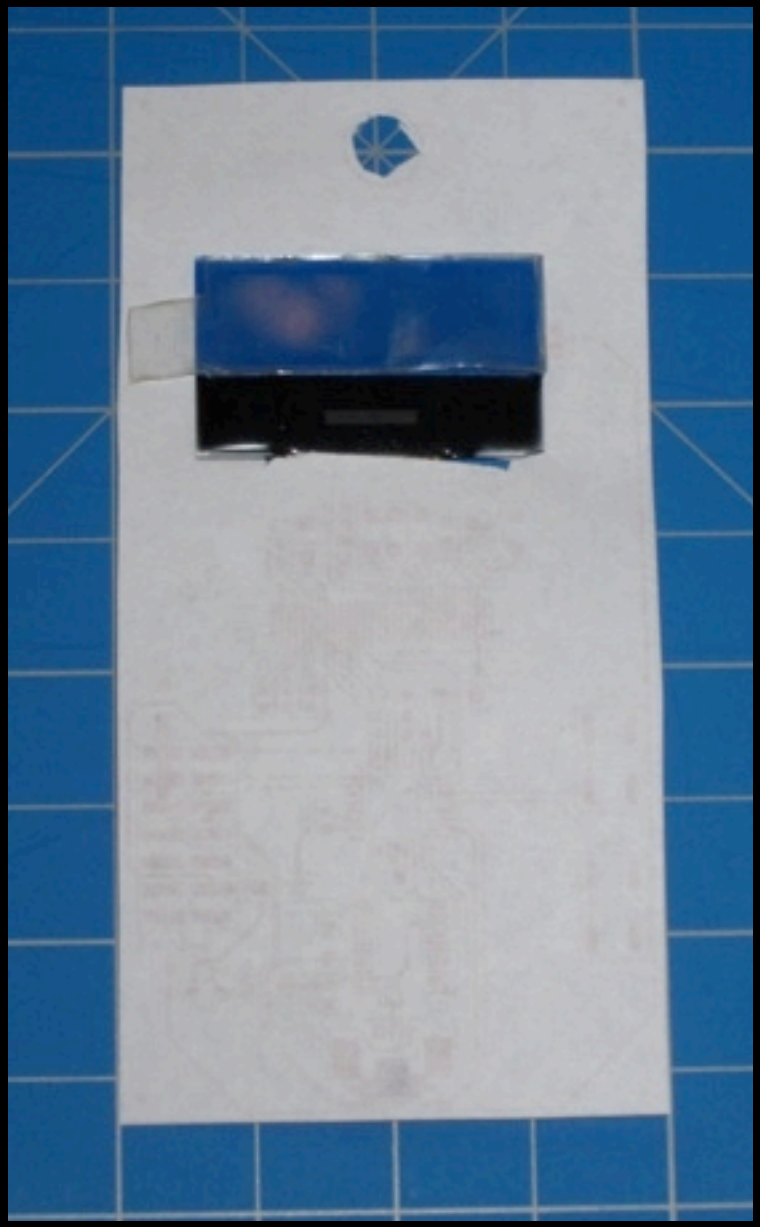
DC18: Functionality

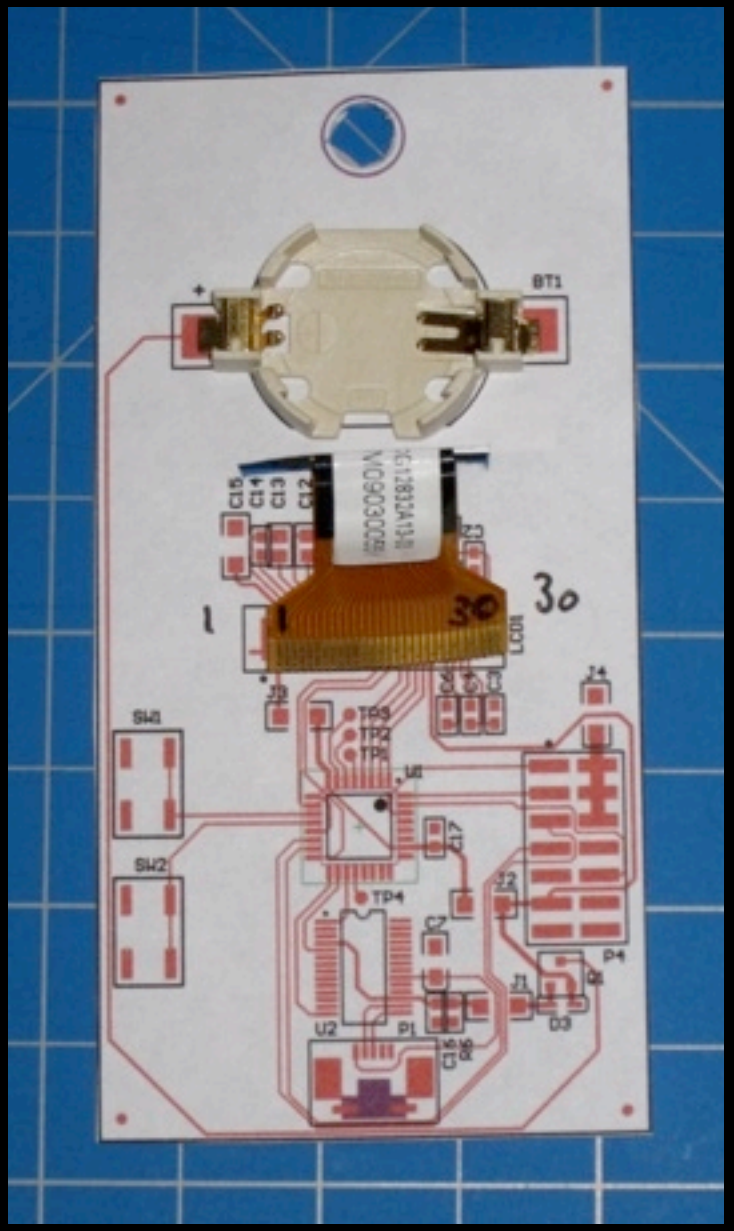
- ★ Glyph selection & display
- ★ LCD control API (via USB virtual serial port)
- ★ Static serial bootloader
- ★ Secret modes (lots)



DC18: Development

Paper mock-up

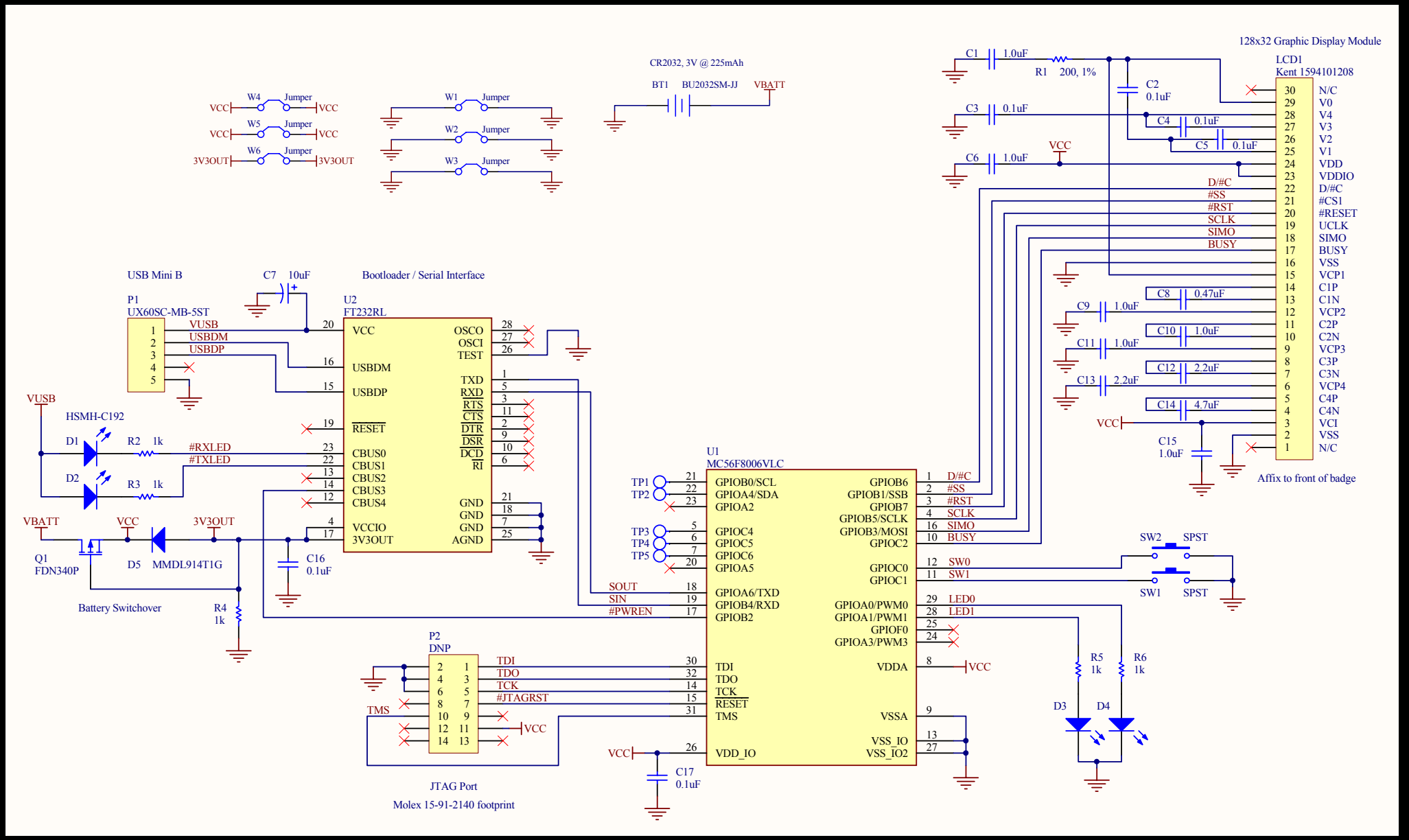




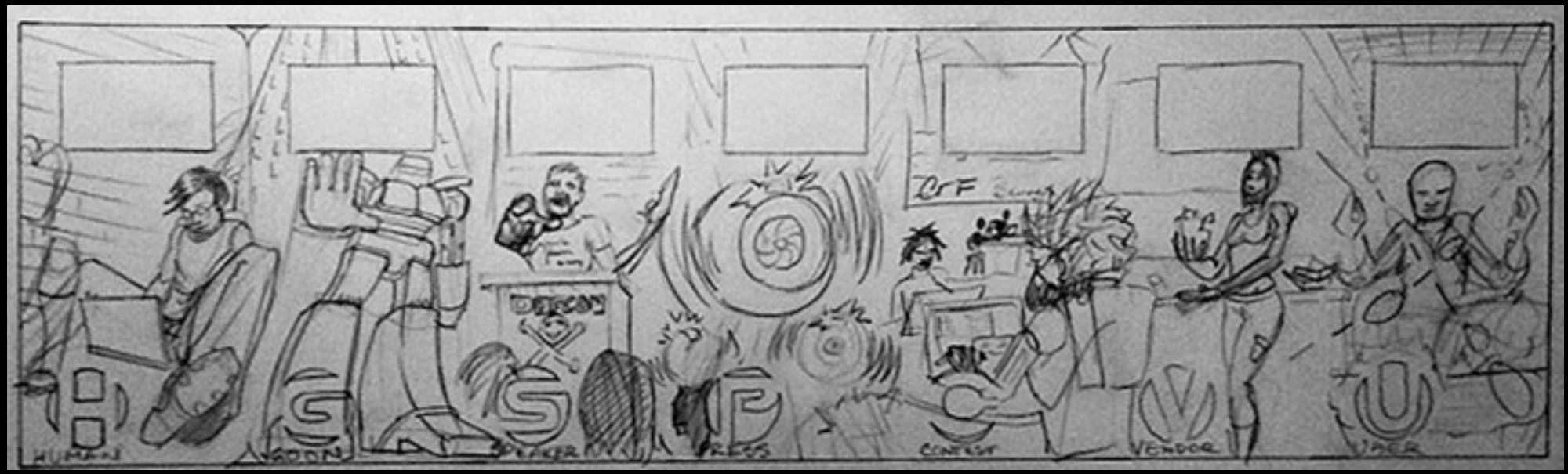
DC18: Development

Prototype hardware

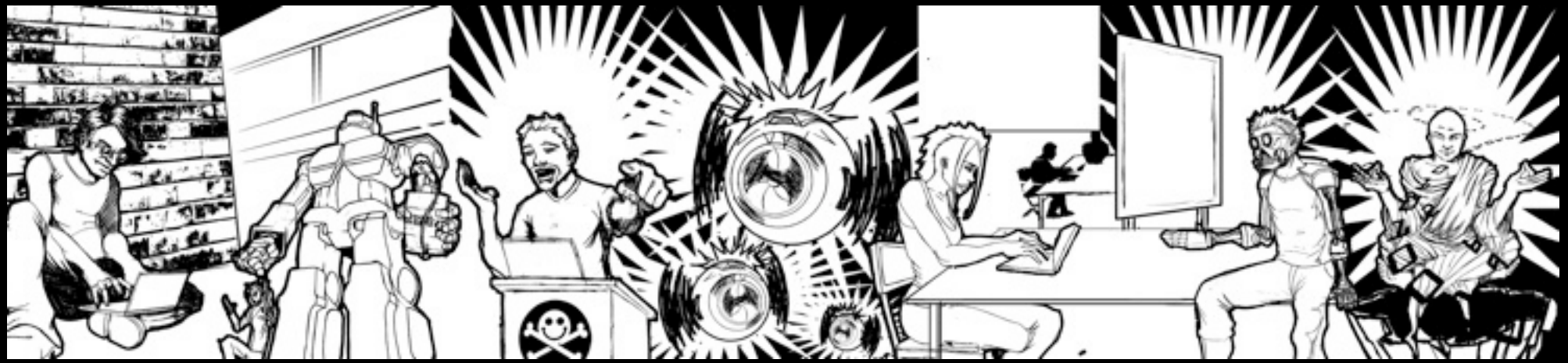
DC18: Schematic



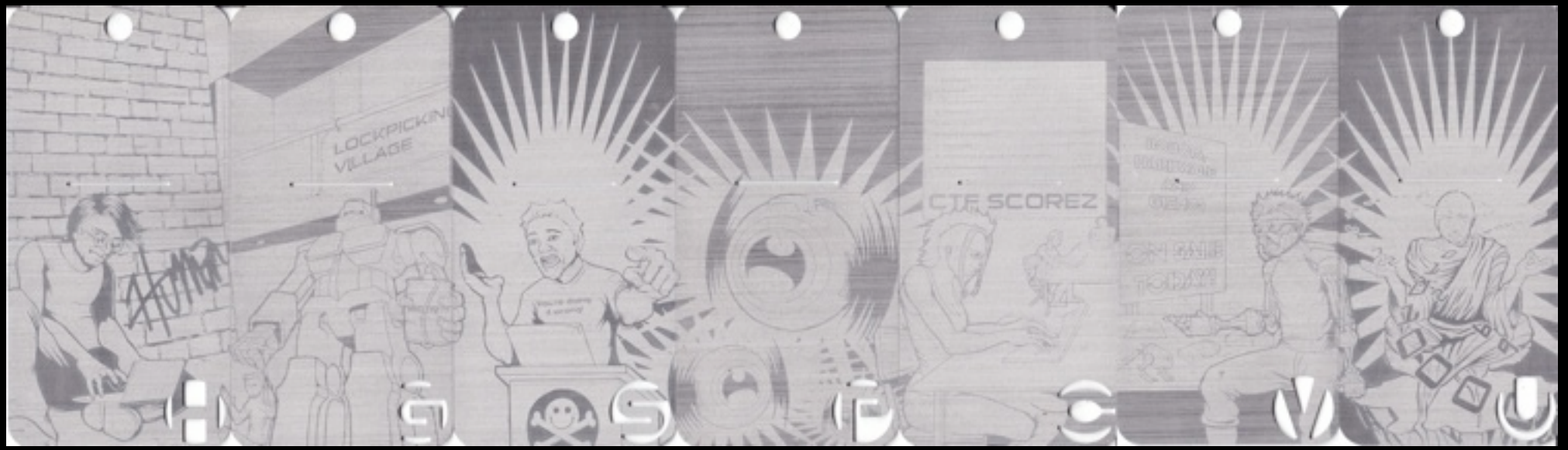
DC18: Laser Engraving



DC18: Laser Engraving



DC18: Laser Engraving



DC18: Badge Hacking

DC18: Badge Hacking

DC18: Barcode Writer/Emulator

Brad Threatt

UPC-A/UPC-E barcode emulator
to fool self-checkout systems

DC18: Badge-a-Lyzer

Dan Z.

Breathalyzer using an alcohol gas

Result displayed on LCD

By the Numbers

	TOTAL QUANTITY	UNIT COST	DEVELOPMENT TIME
	6055	$5.36	35
	6800	$10.93	170
	8500	$10.72	220
	6694	$7.05	186
	7780	$14.12	150

Now.

- Electronic badges have become the norm
- People got used to having an electronic badge
  - Just taken for granted?
  - The thrill/element of surprise was gone
- Hardware hacking is alive and strong
- Time for new blood
  - The hacker community should constantly be evolving

MORE BADGE DETAILS AT:
WWW.GRANDIDEASTUDIO.COM/
PORTFOLIO/DEFCON-19-BADGE
4 = 4, 5, 6, 7, 8

THE END ?

JOE@GRANDIDEASTUDIO.COM