Hacked The Badge

- *Home*
- *How it works*
- *The Story*
- **Make your own**
- *The Team*

Digg

Requirements

- DEFCON 16 Badge
- USB Micro-B Receptacle
- USB A-type to B-type Cable
- Female DE-9 Connector
- Alligator Clips
- 18 Gauge Wire
- Low Wattage Solder Iron
- Very Small Solder
- 2Gb SD Memory Card
- 3V Wall Wart
- Multimeter
- Seven beers (Twelve if you want to get it done in an hour)

Solder on the USB ConnectorAll the badges from DEFCON came with the ability to be programmed (thanks Kingpin). To do these, you must sauder a USB Micro-B receptacle onto your badge. I don't think it matters what you do with pin 4, it isn't hooked to anything. Download Freescale CodeWarriorTo compile the badge's code you need to download Evaluation: CodeWarrior for Microcontrollers. The IDE creates the DC16.abs.s19 file needed to be loaded onto the badge. **Freescale CodeWarrior 6.2 Evaluation** Download Freescale JM60 GUITo re-flash the code onto the badge, you need Freescale's JM60 GUI. The only version I've used is V1.1 however the only thing I could find on line is V1.2. You can find version 1.1 on the DC16 CD. **Freescale JM60 GUI V1.2** Get the source codeThe DC16 Web-Badge's source code is stored on github. It contains everything you need to create the DC16 Web-Badge. git clone **git://github.com/OrbitalsFear/dc16-web-badge.git** Compile the source code

1. Start CodeWarrior IDE
2. Click Start Using CodeWarrior
3. Click File – Open – DC16.mcp
4. Ensure that the compile mode is P&E Multilink/Cyclone Pro
5. Press F7 to Compile
6. dc16.abs.s19 now exists and your are done compiling

Flash the badge

1. Connect the USB on the badge to a Windows computer.
2. Presh and hold the button on the badge.

3. Power up the badge and ensure LEDS 1 and 8 are solid on.
4. If a driver is needed, its on your DC16 CD
5. Start Freescale JM60 GUI
6. Select Bootloader
7. Select your newly created dc16.abs.s19 file
8. Click Execute
9. Unplug the USB from your badge and reboot it

The Dc16 Web-Badge's source code is stored on github. It contains everything you need to create the Dc16 Web-Badge. SD card

1. Format the SD card to be Fat16
2. Copy the contents of the webpage folder or make your own
3. Ensure there are no folders on the SD card
4. Set the SD card to read only
5. Insert the SD card
6. LED 8 should go solid on

RS 232 connectionHere you have some choices. There are two SCI interfaces to choose from. SCI2 are the top left 2 pins on the six pin connector. SCI1 are LED's 3 and 4. SCI1 is more hard core because you must break the LED's 3,4 off your badge; then solder to top top connection on each. SCI2 can be solder to without breaking anything. Also the solder pads are bigger and easier to get to. DC16 Web Badge user interfaceWhen the badge boots up, the user must configure how its going to operate. There are two input's you can give to the badge, click the button, and hold the button. Holding the button will change the configuration on that step, and clicking the button will save that step and move to the next. Below is the boot up sequence.

Boot sequence

1. CPU Speed
   - 1:0 – 48Mhz USB Enabled (default)
   - 0:1 – 24Mhz
2. SCI Interface
   - 1:0 – SCI2 (default)
   - 0:1 – SCI1
3. Baud Rate
   - 1:1 – 115200 (48Mhz default)
   - 1:0 – 38400
   - 0:1 – 9600 (24Mhz default)

After boot sequence

- LED 1 – RX
- LED 2 – TX
- LED 8 – SD Present

Testing your badge

1. Connect the TX,RX to pins 2 and 3
2. Connect the DE-9 to your computer
3. minicom – ttyUSB0 – 9600 8N1 – exit W/O reset
4. Power up your badge
5. Select USB enabled mode
6. Select SCI 1 or 2
7. Select 9600 baud
8. echo "GET / Something" > /dev/ttyUSB0&
9. cat /dev/ttyUSB0
10. The file called INDEX.HTM should have been printed out