Making (and Hacking) the DEFCON 17 Badge
by Joe Grand aka Kingpin
Me.
electrical engineer.
hardware hacker.
daddy.
Hackers: The Next Generation

Last Year

This Year
Introduction

Hardware

Firmware

Manufacturing
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?
Microphone
RGB LED
Freescale DSC & Testpoints
Badge Operation

★ Bootloader
★ Party Mode
★ Quiet Mode
★ Sleep
★ ???
Timeline

- Fall 2008: Recover from DEFCON 16
- December 2008: Initial design & parts selection
- January 2009: Prototype hardware design
- February: PCB design completed, production order
- March: Production component orders
- April: Firmware frozen
- May: All components shipped to e-Teknet China
- June: Wait for Customs to release the only box containing parts we couldn't easily get duplicates of
- July: Badge assembly/test
<table>
<thead>
<tr>
<th>Location</th>
<th>Date</th>
<th>Local Time</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ZHUHAI CN</td>
<td>22/07/2009</td>
<td>10:35</td>
<td>DELIVERED</td>
</tr>
<tr>
<td>GUANGZHOU CN</td>
<td>22/07/2009</td>
<td>3:41</td>
<td>DEPARTURE SCAN</td>
</tr>
<tr>
<td>GUANGZHOU CN</td>
<td>21/07/2009</td>
<td>21:47</td>
<td>ADDITIONAL IMPORT DOCUMENTATION IS REQUIRED FOR CLEARANCE / RELEASED BY CLEARING AGENCY. NOW IN-TRANSIT FOR DELIVERY</td>
</tr>
<tr>
<td></td>
<td>21/07/2009</td>
<td>21:47</td>
<td>ADDITIONAL IMPORT DOCUMENTATION IS REQUIRED FOR CLEARANCE / RELEASED BY CLEARING AGENCY. NOW IN-TRANSIT FOR DELIVERY</td>
</tr>
<tr>
<td>GUANGZHOU CN</td>
<td>17/07/2009</td>
<td>14:23</td>
<td>ADDITIONAL IMPORT DOCUMENTATION IS REQUIRED FOR CLEARANCE / UPS CONTACTED THE RECEIVER</td>
</tr>
<tr>
<td>GUANGZHOU CN</td>
<td>16/07/2009</td>
<td>16:47</td>
<td>ADDITIONAL IMPORT DOCUMENTATION IS REQUIRED FOR CLEARANCE / UPS CONTACTED THE RECEIVER</td>
</tr>
<tr>
<td>GUANGZHOU CN</td>
<td>09/07/2009</td>
<td>15:38</td>
<td>ADDITIONAL IMPORT DOCUMENTATION IS REQUIRED FOR CLEARANCE</td>
</tr>
<tr>
<td>GUANGZHOU CN</td>
<td>08/07/2009</td>
<td>11:38</td>
<td>ADDITIONAL IMPORT DOCUMENTATION IS REQUIRED FOR CLEARANCE</td>
</tr>
<tr>
<td>GUANGZHOU CN</td>
<td>30/06/2009</td>
<td>11:18</td>
<td>ADDITIONAL IMPORT DOCUMENTATION IS REQUIRED FOR CLEARANCE</td>
</tr>
<tr>
<td>GUANGZHOU CN</td>
<td>29/06/2009</td>
<td>13:28</td>
<td>ADDITIONAL IMPORT DOCUMENTATION IS REQUIRED FOR CLEARANCE</td>
</tr>
<tr>
<td>GUANGZHOU CN</td>
<td>23/06/2009</td>
<td>18:12</td>
<td>ADDITIONAL IMPORT DOCUMENTATION IS REQUIRED FOR CLEARANCE</td>
</tr>
<tr>
<td>GUANGZHOU CN</td>
<td>19/06/2009</td>
<td>9:52</td>
<td>ADDITIONAL IMPORT DOCUMENTATION IS REQUIRED FOR CLEARANCE</td>
</tr>
<tr>
<td>GUANGZHOU CN</td>
<td>18/06/2009</td>
<td>9:57</td>
<td>ADDITIONAL IMPORT DOCUMENTATION IS REQUIRED FOR CLEARANCE</td>
</tr>
<tr>
<td></td>
<td>18/06/2009</td>
<td>9:53</td>
<td>ADDITIONAL IMPORT DOCUMENTATION IS REQUIRED FOR CLEARANCE / PACKAGE ABANDONED BY THE SENDER AND THE RECEIVER</td>
</tr>
<tr>
<td></td>
<td>18/06/2009</td>
<td>9:53</td>
<td>ADDITIONAL CUSTOMS CLEARANCE PROCESSING IS REQUIRED FOR FORMAL ENTRY SUBMISSION / PACKAGE ABANDONED BY THE SENDER AND THE RECEIVER</td>
</tr>
<tr>
<td></td>
<td>18/06/2009</td>
<td>9:53</td>
<td>ADDITIONAL CLEARING AGENCY INFORMATION OR DOCUMENTATION IS REQUIRED FOR CLEARANCE / PACKAGE ABANDONED BY THE SENDER AND THE RECEIVER</td>
</tr>
<tr>
<td></td>
<td>18/06/2009</td>
<td>9:52</td>
<td>ADDITIONAL CLEARING AGENCY INFORMATION OR DOCUMENTATION IS REQUIRED FOR CLEARANCE / UPS CONTACTED THE RECEIVER</td>
</tr>
<tr>
<td>GUANGZHOU CN</td>
<td>16/06/2009</td>
<td>17:57</td>
<td>ADDITIONAL IMPORT DOCUMENTATION IS REQUIRED FOR CLEARANCE</td>
</tr>
<tr>
<td>GUANGZHOU CN</td>
<td>11/06/2009</td>
<td>13:52</td>
<td>ADDITIONAL IMPORT DOCUMENTATION IS REQUIRED FOR CLEARANCE</td>
</tr>
<tr>
<td>GUANGZHOU CN</td>
<td>10/06/2009</td>
<td>9:51</td>
<td>ADDITIONAL IMPORT DOCUMENTATION IS REQUIRED FOR CLEARANCE</td>
</tr>
<tr>
<td>GUANGZHOU CN</td>
<td>09/06/2009</td>
<td>11:00</td>
<td>ADDITIONAL IMPORT DOCUMENTATION IS REQUIRED FOR CLEARANCE</td>
</tr>
<tr>
<td>GUANGZHOU CN</td>
<td>08/06/2009</td>
<td>11:44</td>
<td>ADDITIONAL IMPORT DOCUMENTATION IS REQUIRED FOR CLEARANCE</td>
</tr>
<tr>
<td>GUANGZHOU CN</td>
<td>01/06/2009</td>
<td>11:53</td>
<td>ADDITIONAL IMPORT DOCUMENTATION IS REQUIRED FOR CLEARANCE / DOCUMENTS OR INFO REQUESTED FROM THE CUSTOMER WERE RECEIVED AND ARE BEING PROCESSED FOR CLEARANCE</td>
</tr>
</tbody>
</table>
China wins!

<table>
<thead>
<tr>
<th>Status</th>
<th>Delivered On</th>
</tr>
</thead>
<tbody>
<tr>
<td>Delivered On:</td>
<td><strong>22/07/2009 10:35</strong></td>
</tr>
<tr>
<td>Signed By:</td>
<td>GUO HEXIANG</td>
</tr>
<tr>
<td>Delivered To:</td>
<td>CN</td>
</tr>
<tr>
<td>Shipped/Billed On:</td>
<td><strong>21/05/2009</strong></td>
</tr>
<tr>
<td>Type:</td>
<td>Package</td>
</tr>
<tr>
<td>Service:</td>
<td>EXPEDITED</td>
</tr>
<tr>
<td>Weight:</td>
<td>27.00 Lb</td>
</tr>
</tbody>
</table>
FedEx gets a small :(, too
DC17 BA6E FINAL BLOCK DIAGRAM 1/14/09

MEMS MICROPHONE

KNOWN Acoustics
SM5408LE5H-T8

FREESCALE
MCS6F8006
LQFP-32
VNC

USB-TAP
JTAG

SERIAL/
BOOTLOADER

INTER-BA6E
COMMUNICATION

RGB
LED

KWBGR167 3.5x2.5mm REAR MOUNT

AAA3578 SUIKQ8KCGKCG09 570mm
Freescale MC56F8006

★ Digital Signal Controller

๏ Part of the MC56F8xxx family
๏ Newly released
๏ Freescale gave us alpha samples to begin badge development back in November 2008
๏ Main product page: http://tinyurl.com/lyorks
๏ John Winters, co-designer of this part, is here at DEFCON!
Freescale MC56F8006

Note: All pins are muxed with other peripheral pins.
It's Not Easy Picking an LED
Kingbright RGB LED

★ AAA3528SURKQBDCGKC09

- Rear-mounting
- Three individual diodes in single package
- 200/80/90mcd @ 20mA (R/G/B)
Knowles Acoustics Microphone

★ Dr. Hugh Knowles developed first balanced armature receiver for hearing aids

★ Developed the first silicon/MEMS microphone in 1988

★ First moon landing: Neil Armstrong was wearing a Plantronics headset with Knowles microphone

★ Nearly 1 billion sold
  ○ Used in laptops, cellphones, headsets

★ www.knowles.com
Knowles Acoustics Microphone 2

- SPM0408LE5H-TB
- Rear-mounting
- Amplified (20dB gain)
- RF protected
Development Hardware

Freescale MC56F8006-DEMO board + custom circuitry
NOTE: RESISTORS ARE IN OHMS +/- 5% AND CAPACITORS ARE IN MICROFARADS, X7R UNLESS OTHERWISE NOTED. SEE BOM FOR ACTUAL VOLTAGE AND SPECIFICATION.

Badge Address Selection (R1-R3)

Human = DNP
Speaker = R1
Press = R2
Goon = R1, R2
Contest = R1, R3
Vendor = R2, R3
Uber = R1, R2, R3

**Schematic**

---

**Badge Address Selection (R1-R3)**

- **R3** 0 ohm SCL
- **R2** 0 ohm SDA
- **R1** 0 ohm RXD
- **R2** 0 ohm TXD

**Badge Address Assignment**

- **Uber**: R1, R2, R3
- **Goon**: R1, R2
- **Contest**: R1, R3
- **Speaker**: R1
- **Vendor**: R2, R3
- **Press**: R2
- **Human**: DNP

**Component Details**

- **U1**: MC56F8006VLC
- **R1**: 0 ohm
- **R2**: 0 ohm
- **R3**: 0 ohm
- **C1**: 0.1uF
- **C2**: 0.1uF
- **R4**: 10k
- **R5**: 10k
- **D1**: AAA3528SURKQBDCGKC09
- **R6**: 100

**Battery Details**

- **CR2032**: 3V @ 225mAh

---

**Defcon 17 Badge**

- **VCC**: 3V @ 225mAh
- **IC**: MC56F8006VLC
- **Components**: U1, R1-R3, C1, D1, R6, CR2032
## Bill-of-Materials

### DEFCON 17 Circuit Board Badge

**Note:** Refer to schematic for R1, R2, R3 population requirements

<table>
<thead>
<tr>
<th>Item</th>
<th>Quantity</th>
<th>Reference</th>
<th>Manufacturer</th>
<th>Manuf. Part #</th>
<th>Distributor</th>
<th>Distrib. Part #</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>1</td>
<td>BT1</td>
<td>AMP</td>
<td>796136-1</td>
<td>Digi-Key</td>
<td>A99327-ND</td>
<td>Single-cell battery holder for CR2032, SMD</td>
</tr>
<tr>
<td>1a</td>
<td>1</td>
<td>N/A</td>
<td>Panasonic</td>
<td>CR2032</td>
<td>Digi-Key</td>
<td>P189-ND</td>
<td>CR2032 Lithium 3V Coin Cell Battery (225mAh)</td>
</tr>
<tr>
<td>2</td>
<td>2</td>
<td>C1,C2</td>
<td>Kemet</td>
<td>C0603C104K4RACTU</td>
<td>Digi-Key</td>
<td>399-1096-2-ND</td>
<td>0.1uF ceramic capacitor, 16V, X7R, 0603</td>
</tr>
<tr>
<td>3</td>
<td>1</td>
<td>C3</td>
<td>Kemet</td>
<td>C0603C474K4RACTU</td>
<td>Digi-Key</td>
<td>399-4922-2-ND</td>
<td>0.47uF ceramic capacitor, 16V, X7R, 0603</td>
</tr>
<tr>
<td>4</td>
<td>1</td>
<td>D1</td>
<td>Kingbright</td>
<td>AAA3528SURKQBDGCJKC9</td>
<td>N/A</td>
<td>N/A</td>
<td>CR2032 Lithium 3V Coin Cell Battery (225mAh)</td>
</tr>
<tr>
<td>5</td>
<td>1</td>
<td>MK4</td>
<td>Knowles Acoustics</td>
<td>SPM0408LESHT-B</td>
<td>N/A</td>
<td>N/A</td>
<td>Microphone, 20dB internal pre-amp, SMD</td>
</tr>
<tr>
<td>6</td>
<td>3</td>
<td>R1,R2,R3</td>
<td>Panasonic</td>
<td>ERJ-3GEY0R00V</td>
<td>Digi-Key</td>
<td>P0.0GTR-ND</td>
<td>0 ohm, 5%, 1/10W, 0603</td>
</tr>
<tr>
<td>7</td>
<td>2</td>
<td>R4,R5</td>
<td>Panasonic</td>
<td>ERJ-3GEYJ103V</td>
<td>Digi-Key</td>
<td>P10KGTR-ND</td>
<td>10k, 5%, 1/10W, 0603</td>
</tr>
<tr>
<td>8</td>
<td>1</td>
<td>R6</td>
<td>Panasonic</td>
<td>ERJ-3GEYJ101V</td>
<td>Digi-Key</td>
<td>P100GTR-ND</td>
<td>100, 5%, 1/10W, 0603</td>
</tr>
<tr>
<td>9</td>
<td>1</td>
<td>U1</td>
<td>Freescale</td>
<td>MC56F8006VL8</td>
<td>Avnet</td>
<td>N/A</td>
<td>Microcontroller/Digital Signal Controller, LQFP32</td>
</tr>
<tr>
<td>9a</td>
<td>1</td>
<td>N/A</td>
<td>N/A</td>
<td>N/A</td>
<td>Avnet</td>
<td>N/A</td>
<td>Microcontroller programming service</td>
</tr>
<tr>
<td>10</td>
<td>1</td>
<td>PCB</td>
<td>e-Teknet</td>
<td>DC17 1.0</td>
<td>N/A</td>
<td>N/A</td>
<td>PCB (includes assembly and testing)</td>
</tr>
</tbody>
</table>
The badges are all puzzle pieces! Want to see a picture of them all together?
Assembly Drawing: Human
Assembly Drawing: Speaker
Assembly Drawing: Goon
Assembly Drawing: Contest
Assembly Drawing: Press
**DC17 Badge Final Power Measurements**

$V_{CC} = 3V$

<table>
<thead>
<tr>
<th>Mode</th>
<th>Current</th>
</tr>
</thead>
<tbody>
<tr>
<td>Idle/RGB Blend</td>
<td>4.8mA - 8mA</td>
</tr>
<tr>
<td>Dance/Color Organ</td>
<td>4.3mA - 7.2mA</td>
</tr>
<tr>
<td>Sleep</td>
<td>1.2mA</td>
</tr>
</tbody>
</table>

We use $\Delta P = 275 \, \text{mW} \rightarrow 2V$.
Battery Life Estimates

Assume: 6 hours e 8mA
       6 hours e 7.8mA
12 hours e sleep 1.2mA

⇒ 48 + 43.2 + 14.4
   = 105.6 mA/day
   = 2.13 days

Note: 8 hours e 6.4mA AVG.
NORMAL
8 hours e 5.75mA AVG.
8 hours e 1.2mA

⇒ 51.2 + 46 + 9.6
   = 106.8 mA/day
   = 2.1 days

If we're lucky
6 hours e 6.4mA AVG.
6 hours e 5.75mA AVG.
12 hours e 1.2mA

⇒ 38.4 + 34.5 + 14.4
   = 87.3 mA/day
   = 2.58 days
Free for up to 16KB Flash

All tools on DEFCON CD (for real, this time)

http://tinyurl.com/kuwloq
Processor Expert

- GUI for peripheral configuration
- Generates required drivers/function code for desired modules
Fast Fourier Transform (FFT)

- Audio/signal processing function
- Separates input signal from mic into N discrete bins (frequency elements)
- Calculates power of each bin
- RGB LED color and brightness vary based on sound/frequency
Badge-to-Badge Communication

★ I2C
- SCL (Serial Clock)
- SDA (Serial Data)
- GND

★ Human = Master

★ Non-Human = Slaves

★ As long as they are all on the bus, it doesn't matter what order they are connected

★ Master only checks for slaves on power-up

- Make sure slave badges are on, then power master
**Badge-to-Badge Communication 2**

- Individually addressable
  - Three resistors for setting device address

- Data format (7 bytes)
  - Address (1) : Red (2) : Green (2) : Blue (2)

![Diagram of Badge Address Selection (R1-R3)]
Static Serial Bootloader

★ Serial port + HyperTerminal = Load your own firmware onto the badge
  ○ TX, RX, GND
  ○ Level-shifter required (HHV kit!)

★ Enabled for 10 seconds on power-up

★ When modifying the User Code, read the comments in cpu.c
  ○ Need to ensure reset vector points to bootloader and not user code
    • Otherwise, you'll never be able to get to the bootloader
Static Serial Bootloader 3

★ Simply upload hex file and the badge will do the rest...
MC56F8006 typically programmed through JTAG interface


But, there is no direct JTAG connector on the badge
I built a small header board that connects to the JTAG test points on the badge using pogo pins.

Unit will be available in the Hardware Hacking Village for emergencies.

You could solder a 2x7 male header onto prototyping area of the badge and connect wires to test points.
Break Glass In Case Of Bricking

★ Use in conjunction with CodeWarrior or 56800E Flash Programmer tool to reload original firmware (including new bootloader)
Production Assembly @ e-Teknet
Production Assembly @ e-Teknet
Total Badge Types

Speaker = 200
Goon = 200
Press = 200
Vendor = 100
Contest = 100
Uber = 50
Human = 5844

Total = 6694

Collect them all!!@#
A Labor of Love...

- Firmware: 44.5% 82:45
- Hardware: 32.7% 60:45
- Research: 4.6% 8:30
- Meetings: 6.5% 12:05
- Documentation: 3.9% 7:20
- Admin: 7.8% 14:35

TOTAL: 186 hours
Badge Hacking Contest

Badge Hacking Contest HQ @ Hardware Hacking Village

Submissions due to Kingpin @ HHV by 2pm Sunday

Complete source code, schematics, etc. on DEFCON CD
This project did not happen in a vacuum.

Freescale (esp. John Winters, Dennis Hicks, Erin Greene, Chris Coleman, William Jiang)

e-Teknet - PCB manufacturing & assembly (esp. Mike, Sam, Thomas, Kitty)

The Dark Tangent, Black Beetle, Neil

Keely & Ben