Behind the Scenes of the
BADGE
by Joe Grand
aka Kingpin
Me.
electrical engineer.
hardware hacker.
product designer.
Retrospective: DEFCON 15
Retrospective: DEFCON 15
Retrospective: DEFCON 16
SecureDigital socket

Freescale BDM

Bootloader/USB Debug

Mode Select Switch
Retrospective: DEFCON 17
Retrospective: DEFCON 17

- Freescale DSC & Testpoints
- Microphone
- RGB LED
Badges by Christmas?
Timeline

★ Fall 2009: Initial brainstorming (DT, Black Beetle, Neil)
★ January 2010: Preliminary design & parts selection
★ January: Prototype hardware design
★ February: Low-level firmware completed
★ February: Production design finalized
★ March: Production component orders
★ April-May: Finish firmware
★ June: Program microcontrollers (Avnet)
★ June-July: Badge fabrication, assembly & test (e-Teknet)
★ July: Badges shipped to DEFCON (on time!)
The Development Process
Picture Show

Original sketch

- LCD ARF 5.60 V
- DOUBLE SIDED TAPE
- FLEX CABLE
- SLIT IN PCB FOR CABLE - CONNECTOR ON BACK
- LASER ENGRAVED GRAPHICS
- ALUMINUM FRONT

BADGE
WHATEVER SHAPE YOU WANT
The Development Process
Picture Show 2

Paper mock-up
The Development Process
Picture Show 3

Prototype hardware
The Development Process

Testing hardware
The Development Process
Picture Show 5

Writing low-level drivers
The Development Process
Picture Show 6

It works!
The Development Process

Picture Show 7

Final firmware development
Laser Engraving!

★ 0.040" single-sided aluminum substrate PCB
★ Killer graphics by Neil, the DEFCON resident artist
★ Difficult to find a vendor that would take on this work
★ ...and do it for an affordable price
Laser Engraving! 2
Laser Engraving! 3
Laser Engraving! 4
Early Block Diagram

- Kent Displays
- 128x32 Reflex LCD
- SPI
- Freescale MCS6F8006
- JTAG
- JTAG Header
  - Footprint 2x7
  - JTAG
  - LED x 6
  - Pushbuttons
- FTDI FT232-R
- Mini-USB
- Hirose UX60-MB-5S
- VCC Bypass Battery
  - When Connected to PC?
- MOUNT ON FRONT OR ON BACK W/ TAPE
  - Direct Solder (Hot Bar)
Freescale MC56F8006

★ Digital Signal Controller

- Part of the 56800/E family
- Main product page: http://tinyurl.com/mc56f8006-info/

- 16KB of Flash
- 2KB of RAM
- 6-channel PWM
- 18-channel, 12-bit A/D
- Timer/RTC
- 2 PGA, 3 analog comparators
- Serial communication/UART/I2C/SPI
- Up to 22 GPIO
- 32-pin LQFP, 7mm x 7mm
- 1.8V-3.6V operation
Freescale MC56F8006

Note: All pins are muxed with other peripheral pins.
Kent Displays

Reflex Graphic Display Module

- 128 x 32 pixels, 118 DPI
- Reflective Cholesteric LCD
- Bistable = no power or refresh needed to retain image on screen
- Control via SPI-like slave serial interface
- Full screen update ~1.7 seconds
- Affixed to badge with 3M 468MP adhesive tape
- Originally designed for use in Verbatim InSight USB Portable Hard Drive
- Not used in the first moon landing
Kent Displays

Reflex Graphic Display Module
## Bill-of-Materials

Approx. per badge cost = $14.12 (!)

Big ticket items = LCD and laser engraving ($3.84)

<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>
<th>Unit Price</th>
<th>Per Badge</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>BT1</td>
<td>MPD</td>
<td>Digi-Key</td>
<td>BU2032SM-JJ-GTR</td>
<td>Digi-Key</td>
<td>BU2032SM-JJ-GTR-ND</td>
<td>Single-cell battery holder for CR2032, SMD</td>
<td>$0.40000</td>
<td>$0.4060</td>
</tr>
<tr>
<td>11</td>
<td>N/A</td>
<td>Panasonic</td>
<td>Digi-Key</td>
<td>CR2032</td>
<td>Digi-Key</td>
<td>P189-ND</td>
<td>CR2032 Lithium 3V Coin Cell Battery (225mAh)</td>
<td>$0.13750</td>
<td>$0.1375</td>
</tr>
<tr>
<td>6</td>
<td>C1, C6, C9, C10, C11, C15</td>
<td>TDK</td>
<td>Digi-Key</td>
<td>C3216X7R1H105K</td>
<td>Digi-Key</td>
<td>445-1423-2-ND</td>
<td>1.0uF ceramic capacitor, 50V, X7R, 1206</td>
<td>$0.03100</td>
<td>$0.1943</td>
</tr>
<tr>
<td>18</td>
<td>C2, C3, C4, C6, C16, C17</td>
<td>Kemet</td>
<td>Digi-Key</td>
<td>C0803C104K4RACTU</td>
<td>Digi-Key</td>
<td>399-1096-2-ND</td>
<td>0.1uF ceramic capacitor, 16V, X7R, 0603</td>
<td>$0.00240</td>
<td>$0.0143</td>
</tr>
<tr>
<td>1</td>
<td>C7</td>
<td>Kemet</td>
<td>Newark</td>
<td>T491A106M016AG</td>
<td>Digi-Key</td>
<td>BU2032SM-JJ-GTR-ND</td>
<td>10uF capacitor, 20%, 16V, tantalum, size A</td>
<td>$0.06900</td>
<td>$0.0693</td>
</tr>
<tr>
<td>1</td>
<td>C8</td>
<td>Taiyo Yuden</td>
<td>Digi-Key</td>
<td>UMK212B7474KG-T</td>
<td>Digi-Key</td>
<td>587-1288-2-ND</td>
<td>0.47uF ceramic capacitor, 50V, X7R, 0805</td>
<td>$0.03900</td>
<td>$0.0524</td>
</tr>
<tr>
<td>2</td>
<td>C12, C13</td>
<td>Taiyo Yuden</td>
<td>Digi-Key</td>
<td>TMK212B225KG-T</td>
<td>Digi-Key</td>
<td>587-1292-2-ND</td>
<td>2.2uF ceramic capacitor, 25V, X5R, 0805</td>
<td>$0.02600</td>
<td>$0.0582</td>
</tr>
<tr>
<td>1</td>
<td>C14</td>
<td>Kemet</td>
<td>Digi-Key</td>
<td>C0803C475K8ACTU</td>
<td>Digi-Key</td>
<td>399-5503-2-ND</td>
<td>4.7uF ceramic capacitor, 10V, X5R, 0603</td>
<td>$0.03900</td>
<td>$0.0466</td>
</tr>
<tr>
<td>4</td>
<td>D1, D2, D3, D4</td>
<td>Avago</td>
<td>N/A</td>
<td>HSMMH-C192</td>
<td>N/A</td>
<td>N/A</td>
<td>LED, Red, 0603, 1.8Vf, 17mcd @ 20mA</td>
<td>$0.02900</td>
<td>N/A</td>
</tr>
<tr>
<td>11</td>
<td>D5</td>
<td>ON Semiconductor</td>
<td>Mouser</td>
<td>MMMDL914TTG</td>
<td>Mouser</td>
<td>863-MMMDL914TTG</td>
<td>Diode, Switching, 100Vr, 1Vf @ 10mA, 5uA Ir @ 75V, SOD-323</td>
<td>$0.02400</td>
<td>$0.0251</td>
</tr>
<tr>
<td>1</td>
<td>LCD1</td>
<td>Kent Displays</td>
<td>Mouser</td>
<td>1594101208</td>
<td>N/A</td>
<td>N/A</td>
<td>LCD, 128x32 Reflex Graphic Display Module</td>
<td>$3.49000</td>
<td>$3.4900</td>
</tr>
<tr>
<td>11</td>
<td>N/A</td>
<td>GM Nameplate</td>
<td>N/A</td>
<td>N/A</td>
<td>N/A</td>
<td>N/A</td>
<td>3M 468MP adhesive tape for LCD attachment, 1&quot; x 1/2&quot; strips</td>
<td>$0.07870</td>
<td>$0.0822</td>
</tr>
<tr>
<td>1</td>
<td>P1</td>
<td>Hirose</td>
<td>Digi-Key</td>
<td>UX60SC-MB-5ST(80)</td>
<td>Digi-Key</td>
<td>H11671TR-ND</td>
<td>Connector, Mini-USB Type B, R/A, 5 position, SMD</td>
<td>$0.37500</td>
<td>$0.4198</td>
</tr>
<tr>
<td>1</td>
<td>Q1</td>
<td>Fairchild</td>
<td>Digi-Key</td>
<td>FDN340P</td>
<td>Digi-Key</td>
<td>FDN340PTR-ND</td>
<td>Transistor, MOSFET, P-Channel, 20V, 2A, SSOT3/SOT23</td>
<td>$0.11100</td>
<td>$0.1180</td>
</tr>
<tr>
<td>1</td>
<td>R1</td>
<td>Yageo</td>
<td>Mouser</td>
<td>RC0603FR-07200RL</td>
<td>Mouser</td>
<td>603-RC0603FR-07200RL</td>
<td>200 ohm, 1%, 1/10W, 0603</td>
<td>$0.00200</td>
<td>$0.0030</td>
</tr>
<tr>
<td>5</td>
<td>R2, R3, R4, R5, R6</td>
<td>Panasonic</td>
<td>Digi-Key</td>
<td>ERJ-3GEY102V</td>
<td>Digi-Key</td>
<td>P1.0KGR-T-ND</td>
<td>1k, 5%, 1/10W, 0603</td>
<td>$0.00120</td>
<td>$0.0063</td>
</tr>
<tr>
<td>2</td>
<td>SW1, SW2</td>
<td>C&amp;K</td>
<td>Digi-Key</td>
<td>KSC201JLFS</td>
<td>Digi-Key</td>
<td>401-1756-2-ND</td>
<td>SPST tactile momentary switch, 120gf, 6.2 x 6.2mm, J-Lead</td>
<td>$0.16600</td>
<td>$0.3469</td>
</tr>
<tr>
<td>1</td>
<td>U1</td>
<td>Freescale</td>
<td>Avnet</td>
<td>MC56F8006VLC</td>
<td>Avnet</td>
<td>N/A</td>
<td>Microcontroller/Digital Signal Controller, LQFP32</td>
<td>$1.50000</td>
<td>N/A</td>
</tr>
<tr>
<td>1</td>
<td>U2</td>
<td>FTDI</td>
<td>Mouser</td>
<td>FT232RL</td>
<td>Mouser</td>
<td>895-FT232RL</td>
<td>USB-to-Serial UART Converter, SSOP28W</td>
<td>$1.89000</td>
<td>$1.8900</td>
</tr>
<tr>
<td>11</td>
<td>N/A</td>
<td>N/A</td>
<td>Avnet</td>
<td>N/A</td>
<td>N/A</td>
<td>N/A</td>
<td>Microcontroller programming service</td>
<td>$0.10000</td>
<td>$0.1000</td>
</tr>
<tr>
<td>16</td>
<td>W1, W2, W3, W4, W5, W6</td>
<td>Panasonic</td>
<td>Digi-Key</td>
<td>ERJ-5GEY0R000V</td>
<td>Digi-Key</td>
<td>P0.0ETR-ND</td>
<td>Jumper, 0 ohm resistor, 1/4W, 1206</td>
<td>$0.00380</td>
<td>$0.0284</td>
</tr>
<tr>
<td>11</td>
<td>PCB</td>
<td>e-Teknet</td>
<td>N/A</td>
<td>DC18</td>
<td>N/A</td>
<td>N/A</td>
<td>PCB (fabrication, laser, assembly, test)</td>
<td>$6.83000</td>
<td>$6.8300</td>
</tr>
</tbody>
</table>
Assembly Drawing
Core Badge Functionality

★ Glyph selection
★ LCD control API
★ Secret modes
Glyph Selection

★ Choose your favorite 4 glyphs/icons to show off on your LCD
★ Now you don't have to talk to someone to find out if they have the same interests as you :) 
★ Enter Glyph Selection mode by pressing SW2 from the DEFCON logo
★ Use SW1 and SW2 to cycle through the glyphs
★ Press SW1 and SW2 together to select the glyph
★ Lather, rinse, repeat
LCD Control API

★ Control the LCD via serial commands sent over USB virtual COM port
  • 9600, 8N1

★ Use terminal program or scripts

★ Display nifty graphics and text on the LCD

★ No hardware hacking experience necessary!
LCD Control API 2

With USB plugged in, send '#' to enable mode
Badge will return welcome string (in ASCII)

'C' = clear frame buffer
'L aa aa vv' = load byte vv into frame buffer location aa
ex.: L 00 01 0A
valid locations 0x000 to 0x1FF
see LCD data sheet pg. 9 for mem. map
0 = pixel on (dark), 1 = pixel off (light)

'U' = update LCD w/ frame buffer contents
'X' (or power cycle) = exit LCD mode

Badge will return ACK ('.' ') after a valid command
# LCD Control API 3

<table>
<thead>
<tr>
<th>PAGE</th>
<th>BIT</th>
<th>COLUMN ADDRESS</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>0-7</td>
<td>DON'T CARE</td>
</tr>
<tr>
<td>1</td>
<td>0-6</td>
<td>DON'T CARE</td>
</tr>
<tr>
<td></td>
<td>7</td>
<td>B B B B</td>
</tr>
<tr>
<td>2</td>
<td>0</td>
<td>B B B B</td>
</tr>
<tr>
<td></td>
<td>1</td>
<td>B B B B</td>
</tr>
<tr>
<td></td>
<td>2</td>
<td>B B B B</td>
</tr>
<tr>
<td></td>
<td>3</td>
<td>B B B B</td>
</tr>
<tr>
<td></td>
<td>4</td>
<td>B B B B</td>
</tr>
<tr>
<td></td>
<td>5</td>
<td>B B B B</td>
</tr>
<tr>
<td></td>
<td>6</td>
<td>B B B B</td>
</tr>
<tr>
<td></td>
<td>7</td>
<td>B B B B</td>
</tr>
<tr>
<td>3</td>
<td>0</td>
<td>DON'T CARE</td>
</tr>
<tr>
<td></td>
<td>1</td>
<td>DON'T CARE</td>
</tr>
<tr>
<td></td>
<td>2</td>
<td>DON'T CARE</td>
</tr>
<tr>
<td></td>
<td>3</td>
<td>DON'T CARE</td>
</tr>
<tr>
<td></td>
<td>4</td>
<td>DON'T CARE</td>
</tr>
<tr>
<td></td>
<td>5</td>
<td>DON'T CARE</td>
</tr>
<tr>
<td></td>
<td>6</td>
<td>DON'T CARE</td>
</tr>
<tr>
<td></td>
<td>7</td>
<td>DON'T CARE</td>
</tr>
<tr>
<td>4</td>
<td>0</td>
<td>DON'T CARE</td>
</tr>
<tr>
<td></td>
<td>1</td>
<td>DON'T CARE</td>
</tr>
<tr>
<td></td>
<td>2</td>
<td>DON'T CARE</td>
</tr>
<tr>
<td></td>
<td>3</td>
<td>DON'T CARE</td>
</tr>
<tr>
<td></td>
<td>4</td>
<td>DON'T CARE</td>
</tr>
<tr>
<td></td>
<td>5</td>
<td>DON'T CARE</td>
</tr>
<tr>
<td></td>
<td>6</td>
<td>DON'T CARE</td>
</tr>
<tr>
<td></td>
<td>7</td>
<td>DON'T CARE</td>
</tr>
<tr>
<td>5</td>
<td>0</td>
<td>DON'T CARE</td>
</tr>
<tr>
<td></td>
<td>1</td>
<td>DON'T CARE</td>
</tr>
<tr>
<td></td>
<td>2</td>
<td>DON'T CARE</td>
</tr>
<tr>
<td></td>
<td>3</td>
<td>DON'T CARE</td>
</tr>
<tr>
<td></td>
<td>4</td>
<td>DON'T CARE</td>
</tr>
<tr>
<td></td>
<td>5</td>
<td>DON'T CARE</td>
</tr>
<tr>
<td></td>
<td>6</td>
<td>DON'T CARE</td>
</tr>
<tr>
<td></td>
<td>7</td>
<td>DON'T CARE</td>
</tr>
<tr>
<td>6</td>
<td>0</td>
<td>DON'T CARE</td>
</tr>
<tr>
<td></td>
<td>1-7</td>
<td>DON'T CARE</td>
</tr>
<tr>
<td>7</td>
<td>0-7</td>
<td>DON'T CARE</td>
</tr>
</tbody>
</table>

B = Don't Care
Secret Modes

Call-for-Integration to invite DEFCON participants to hide code and/or data in the badge (March 2010)

Lots of cool stuff? Find it all!
Other Badge Stuff You Might Want To Know.
Development Environment

Freescale CodeWarrior for 56800/E Digital Signal Controllers

★ Special Edition free for up to 64KB Flash
★ Windows only, but works fine in a VM
★ All tools/materials on DEFCON CD
★ http://tinyurl.com/mc56f8006-dev/
Development Environment 2

Processor Expert

- GUI for peripheral configuration
- Generates required drivers/function code for desired modules
Static Serial Bootloader

- USB port + terminal program = Load your own firmware onto the badge

- Hold down SW1 & SW2 on power-up
  - Ideally by inserting USB cable (remove battery first)
  - Both top LEDs will remain on
  - Virtual USB COM port will appear on your machine

- Use CodeWarrior dev. tools to hack/modify firmware and re-compile
When modifying the User Code:

- Need to ensure reset and COP vectors point to BOOTLOADER_ADDR (0x1B00) and not user code!
- If you change the linker file, you'll need to re-patch it, as well
- Read the comments in /CODE/cpu.c for full details
Send the hex file and the badge will do the rest...

- 9600, 8N1, Xon/Xoff
- `/output/scr01_pROM_xRAM.elf.S`
- Typical load time ~90 seconds
In Case Of Bricking...

★ MC56F8006 JTAG interface
★ Just like last year, but 2x7 connector footprint is provided this time
★ Engineers are standing by in the Hardware Hacking Village
  ‒ I brought ~100 connectors
In Case Of Bricking... 2

★ Use in conjunction with 56800E Flash Programmer tool to reload original firmware (including static bootloader)
  • dc18-with-boot.s

★ Only reprogram/debug with USB cable attached to ensure normal speed (non-reduced) operation
  • Device does not sleep when powered via USB
**Converting BMP to C**

- Load your own graphics onto the badge
  - Requires Kent Display development tools (on CD)
  - Convert BMP to array and replace the one(s) in `graphics.h`

- Maximum image size = 128 x 32 pixels

1. Convert to 132 x 32 canvas size with image at far left
2. BMP-to-C using "132x64 BMP to C" tool
3. Erase unused bytes within resultant C file
4. Copy relevant data into array
Converting BMP to C 2
Converting BMP to C 3

![Image of software interface for converting BMP to C]

- Source File: C:\Documents and Settings\...\defcon.bmp
- Target File: C:\Documents and Settings\...\defcon.c
- Generate C Array button is highlighted

Status: Image Loaded
Converting BMP to C 4

Status: C Array Generated
Converting BMP to C 5
Converting BMP to C 6
Power Consumption

CR2032 Lithium coin cell: 3V @ 225mAh to 2V

- Idle (Wait) = 0.7mA
- Active (LCD update) = 8.3mA @ 930mS
- Serial port TX = 6.7mA

Idle mode only = 13.4 days

Typical daily use: 1H active, 23H idle = 9 days
Power Consumption 2

Graph Name: 
Upload Time: 
Form Saved Time: 6/1/2010 3:12:18 PM

DEFCON 18 Badge

Current consumption measurements

<table>
<thead>
<tr>
<th>Start Time</th>
<th>Duration</th>
<th>Max Time</th>
<th>Max Average</th>
<th>Min Time</th>
<th>Min Average</th>
<th>Description</th>
<th>Stop Time</th>
</tr>
</thead>
<tbody>
<tr>
<td>3:08:19 PM</td>
<td>0:00:01</td>
<td>3:08:19 PM</td>
<td>7.909 mA DC</td>
<td>4.302 mA DC</td>
<td>3:08:20 PM</td>
<td>Interval</td>
<td>3:08:20 PM</td>
</tr>
<tr>
<td>3:08:20 PM</td>
<td>0:00:01</td>
<td>3:08:21 PM</td>
<td>0.675 mA DC</td>
<td>0.676 mA DC</td>
<td>3:08:20 PM</td>
<td></td>
<td>3:08:21 PM</td>
</tr>
<tr>
<td>3:08:21 PM</td>
<td>0:00:01</td>
<td>3:08:22 PM</td>
<td>0.677 mA DC</td>
<td>0.678 mA DC</td>
<td>3:08:21 PM</td>
<td></td>
<td>3:08:22 PM</td>
</tr>
<tr>
<td>3:08:22 PM</td>
<td>0:00:01</td>
<td>3:08:23 PM</td>
<td>0.677 mA DC</td>
<td>0.678 mA DC</td>
<td>3:08:22 PM</td>
<td></td>
<td>3:08:23 PM</td>
</tr>
<tr>
<td>3:08:23 PM</td>
<td>0:00:01</td>
<td>3:08:23 PM</td>
<td>0.679 mA DC</td>
<td>0.679 mA DC</td>
<td>3:08:23 PM</td>
<td></td>
<td>3:08:24 PM</td>
</tr>
<tr>
<td>3:08:24 PM</td>
<td>0:00:01</td>
<td>3:08:24 PM</td>
<td>0.678 mA DC</td>
<td>0.678 mA DC</td>
<td>3:08:24 PM</td>
<td></td>
<td>3:08:25 PM</td>
</tr>
<tr>
<td>3:08:25 PM</td>
<td>0:00:01</td>
<td>3:08:25 PM</td>
<td>0.678 mA DC</td>
<td>0.678 mA DC</td>
<td>3:08:25 PM</td>
<td></td>
<td>3:08:26 PM</td>
</tr>
<tr>
<td>3:08:26 PM</td>
<td>0:00:01</td>
<td>3:08:27 PM</td>
<td>0.678 mA DC</td>
<td>0.679 mA DC</td>
<td>3:08:26 PM</td>
<td></td>
<td>3:08:27 PM</td>
</tr>
<tr>
<td>3:08:27 PM</td>
<td>0:00:01</td>
<td>3:08:27 PM</td>
<td>0.679 mA DC</td>
<td>0.679 mA DC</td>
<td>3:08:27 PM</td>
<td></td>
<td>3:08:28 PM</td>
</tr>
</tbody>
</table>

Test Purpose:
- Single LCD refresh
- Multiple mode changes
- Serial port transmitting
Seamless Power Switching

- P-channel MOSFET on by default via R4
- When USB plugged in, 3V3OUT (FT232) goes HIGH
- MOSFET turns off and battery is isolated from circuit
- Body diode of MOSFET prevents battery from getting reverse fed by 3V3OUT (small nA leakage is OK)
- Voltage drop across D5 causes VCC to be lower for USB-powered (2.7V) than battery powered (3V)
- Higher forward voltage (Vf) -> lower reverse leakage (Vr)
Seamless Power Switching 2

- Battery to USB
Seamless Power Switching 3

- USB to Battery
### Total Badge Types

<table>
<thead>
<tr>
<th>Badge Type</th>
<th>Count</th>
</tr>
</thead>
<tbody>
<tr>
<td>Human</td>
<td>7000</td>
</tr>
<tr>
<td>Speaker</td>
<td>200</td>
</tr>
<tr>
<td>Goon</td>
<td>200</td>
</tr>
<tr>
<td>Press</td>
<td>180</td>
</tr>
<tr>
<td>Vendor</td>
<td>100</td>
</tr>
<tr>
<td>Contest</td>
<td>70</td>
</tr>
<tr>
<td>Uber</td>
<td>30</td>
</tr>
</tbody>
</table>

**Total = 7780**
Time flies, but who's counting?

TOTAL: 150 hours
Badger Hacking Contest

Badger Hacking Contest HQ @ Hardware Hacking Village

Submit your entry to Kingpin starting at 2pm Sunday in the HHV

Previous results at
www.grandideastudio.com/portfolio/defcon-1x-badge/

x = 4, 5, 6, 7

Complete schematic, source code, tools, etc. on DEFCON CD

Now w/ Black Badge status!
THE END!

joe@grandideastudio.com