

DEFCON Badge Hacking Contest

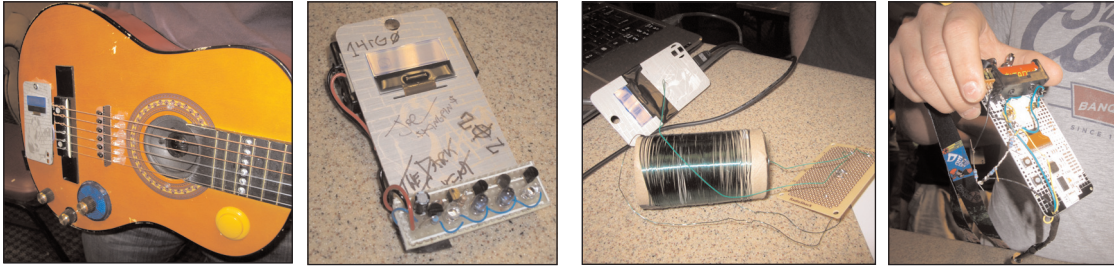


FIGURE A. A montage of Badge Hacking Contest entries.

The DEFCON Badge Hacking Contest exists to award the most ingenious, obscure, or technologically astounding badge modifications created during the weekend-long conference. It's a fun way for attendees to get involved with electronics, learn something new, and/or show off their chops.

There were 21 entries in the 2010 contest. The submissions ranged from pure firmware modifications to extravagant hardware creations. The top three winners are detailed below, along with a sampling of other contest entries. **Figure A** shows pictures of a few of the entries.

1ST PLACE: GoatBar UPC-A/UPC-E Barcode

Writer/Emulator by Brad Threatt

Fool the self-checkout systems common in large retail stores by entering a UPC barcode of a lower-priced item with the badge's two buttons, scanning the barcode displayed on the LCD with the laser at checkout, and placing a higher-priced item into your bag. Obviously, this mischievous entry should not be used in the real world, but it exemplifies a security weakness of barcodes.

2ND PLACE: STDin by Team Redacted

Virus propagation and social network analysis. Passing "friendly" viruses between badges with capability to track propagation path and originator. Code also ported to work with two DEFCON 17 badges.

3RD PLACE: The Badge-a-Lyzer by Dan Z.

Breathalyzer using an alcohol gas sensor to detect alcohol concentration on the user's breath, and LCD to display current level of intoxication.

HONORABLE MENTION: Origami Dragon from the Paper Badge by Doug

Doug's finely crafted origami dragon showed how to make the most of an unfortunate situation (in this case, DEFCON running out of all 7,780 electronic badges). Folding instructions from www.origami-instructions.com/origami-dragon.html.

OTHER SELECTED ENTRIES (in no particular order):

Mossmann

DEFCON Super Rocker 18 Guitar

Guitar containing a stroboscopic tuner for each string (working) and optical pickups (could not get them working before the contest ended).

501d3r Guy and 14rG0

(youngest participant at 13 years old)

Long-range TV-B-Gone

Red Lambda

Slot Machine a.k.a., "DEFCON Slots"

Play a game of slots on your badge. Used a PRNG (pseudo-random number generator) w/ a nice character/graphic set.

Sk3tch

RFID & Barcode Emulator a.k.a., "Retail Ripper"

Two part hack: 125 kHz RFID emulator and UPC barcode emulator. Both identifiers are hard-coded into the source.

Austin

Personal Oscilloscope

Uses the badge's LCD to display the voltage level of a signal and how it changes over time.

Bo

Web-of-Trust

Sharing of unique IDs between badges over USB.

Determines degrees of separation using Bloom filter.