(U) DEF CON 23 Crypto And Privacy Village Badge Design Document

~~(U//FOUO)~~ This document contains the firmware specifications for the DEF CON 23 Crypto and Privacy Village Badge, including all behavior, flags, and easter eggs.

(U) Testing

~~(U//FOUO)~~ When the badge is first powered up, it enters a self-test mode. All LEDs and segments on the display are lit for one second. After that, the badge cycles through all LEDs and segments individually. Pressing the left or right buttons cause an "L" or "R" to be displayed. Pressing both buttons simultaneously exits the self-test mode. The badge will not re-enter self-test mode without clearing the NVM.

(U) Operation

(U) Display Mode

~~(U//FOUO)~~ The badge is normally in "display mode," which cycles through the words "DEFCON23," "CRYPTO," "AND," "PRIVACY," "VILLAGE." There are 12 challenges to complete. The green LEDs corresponding to each challenge pulsate to indicate which challenges have been completed.

~~(C//REL)~~ If the Matrix easter egg is enabled, then the cycling of strings is slower. Part of the cycle time is used to resolve randomized characters to their actual characters. The random characters and resolution positions are generated by a 16-bit maximal LFSR. Any subset of the seven segments can be lit.

~~(C//REL)~~ If the LED1 easter egg is enabled, then the green LEDs randomly light every 250 milliseconds as chosen by a 16-bit maximal LFSR.

~~(C//REL)~~ If the LED2 easter egg is enabled, then the green LEDs perform a "walk." LEDs start lighting up clockwise from the "walk" position until reaching the "walk" position, at which point the LEDs are extinguished clockwise until reaching the "walk" position again. The "walk" position then advances.

~~(C//REL)~~ If the Count easter egg is enabled, then the green LEDs count in binary, with the 12 o'clock position being the least-significant bit, and the 11 o'clock position being the most-significant bit.

~~(C//REL)~~ If the Pong easter egg is enabled, then the green LEDs perform a "pong" display. One LED advances slowly clockwise. Another LED advances either counter-clockwise or clockwise until it hits the slowly-advancing LED, at which point it reverses direction.

~~(C//REL)~~ If any easter egg messages are enabled, they will scroll after the "DEFCON23 CRYPTO AND PRIVACY VILLAGE" message is displayed.

~~(C//REL)~~ The preceding easter eggs are temporary and do not persist across power-cycles.

~~(C//REL)~~ If the EFF donor easter egg is activated, then users may cycle through a subset of the easter eggs (LED1, LED2, Pong, Matrix, and an "I fight for the users" message) by pressing the up button. The EFF donor flag persists across power-cycles but the easter egg enabled does not.

~~(TS//REL)~~ If all challenges are completed, the green LEDs randomly light every 50 milliseconds.

~~(TS//REL)~~ By pressing Up Up Down Down Up Down Up Down in "display mode," the flag display mode can be entered which can be used to verify flags submitted.

(U) Flag Entry Mode

~~(U//FOUO)~~ To enter the solution to a challenge (hereinafter referred to as a "flag"), press the right button in display mode. The green LEDs extinguish and the main display starts blinking an underscore to indicate that it is ready to accept an entry. Pressing the up and down buttons cycle through the characters of the current position, which blinks. An underscore indicates a space. Holding the down button for one second advances the character position. Advancing from the last position submits the flag for verification. Holding the up button for one second performs a backspace. Backspacing from the first position returns to "display mode." Flags may also be submitted by pressing both buttons simultaneously. Empty spaces at the end of a flag will be converted to NULs before flag validation.

~~(U//FOUO)~~ Upon entry of a correct flag, the display will fade up the word "SUCCESS" and the corresponding green LEDs begins to pulsate. An animation of the other LEDs accents the newly lit LED. After five seconds, the badge reverts to "display mode."

~~(C//REL)~~ Entry of any easter egg will activate that particular easter egg. Easter eggs are discussed below.

~~(C//REL)~~ Entry of a flag that is not a valid flag or easter egg will cause "LOL FAIL" to display for five seconds before reverting to "display mode."

~~(S//REL)~~ Cycling through characters backwards through "A" will reveal 12 more non-unique characters, which light a corresponding green LED. These characters are used in a puzzle.

~~(S//REL)~~ Baudot/SSE Mode

~~(S//REL)~~ Upon entry to the Baudot mode, "LOOK IN TO MY EYES" scrolls across the display. Two sets of five green LEDs light in sequence to spell out characters using Baudot encoding. LEDs on the left side of the badge are the first, third, etc. characters, and LEDs on the right side of the badge are the second, fourth, etc. characters. Bits are ordered most-significant to least-significant from 11 o'clock to 1 o'clock.

~~(S//REL)~~ Tetris/RF mode

~~(S//REL)~~ Upon entry to Tetris mode, all LEDs and segments are extinguished except for the 3 o'clock LED, which stays lit. The 3 o'clock LED is modulated to provide music (commonly known as the "Tetris theme") broadcast at 550 kHz using AM. At the end of this song, a message in Morse code is played at 15 WPM.

~~(C//REL)~~ Party/Rager mode

~~(C//REL)~~ After entering these easter eggs, the display scrolls "Are you sure?" followed by a display of "Y N." If the left button is pressed (corresponding to Y), party mode is entered. If the right button is pressed, the badge goes back to "display mode." If party mode is entered, a bit is set in NVM recording this fact. The duration of party mode (15 minutes for "party", 60 minutes for "rager") is also stored in NVM as a bit vector.

~~(C//REL)~~ In party mode, the green LEDs blink at 128 BPM. The LEDs are on for the duration of a sixteenth note at 128 BPM. The display scrolls "PARTY" back and forth, moving the position at 128 WPM. **Party mode cannot be stopped.** Every 60 seconds, the party duration counter is decremented in NVM. If the party duration reaches 0, the party bit in NVM is reset and the badge goes back to "display mode."

~~(C//REL)~~ The "fuck" lockout

~~(C//REL)~~ If the word "fuck" is submitted as a flag, a bit is set in NVM indicating this fact. Display mode will not show anything but a series of dashes when this flag is set. Additionally, flag entry mode will not accept any flag except "sorry." Other valid flags or easter eggs will cause "LOL FAIL" to be displayed. If "sorry" is submitted, the badge says "please don't do it again," clears the bit in NVM, and returns to display mode.

~~(C//REL)~~ Bullet time

~~(C//REL)~~ If the bullet time easter egg is entered, the display and LEDs are refreshed at a much slower interval (every 20 milliseconds).

~~(C//REL)~~ Resetting NVM

~~(C//REL)~~ The NVM can be completely erased by submitting "factoryr." This will restore the self-test mode on the next power-cycle and clear all flags and other bits set.

~~(U//FOUO)~~ Flags

~~(S//REL)~~ Flags are "hashed" by through repeated encryptions by the XXTEA algorithm using the flag as the key. The initial input to XXTEA is 0x0000000000000001, and subsequent inputs are the outputs of previous iterations. Flags are hashed 3001 times. The output of the 3000th round is used as an XXTEA decryption key for easter egg messages.

~~(U//FOUO)~~ Flag list

~~(TS//REL)~~

12 o'clock	N	
1 o'clock	NNE	
2 o'clock	ENE	
3 o'clock	E	
4 o'clock	ESE	
5 o'clock	SSE	
6 o'clock	S	
7 o'clock	SSW	
8 o'clock	WSW	
9 o'clock	W	
10 o'clock	WNW	
11 o'clock	NNW	

~~(S//REL)~~ Puzzle mode enablers

SSE	SSE	Enters Baudot mode
NNW	TETRIS	Enters Tetris mode

~~(C//REL)~~ Easter Eggs

~~(C//REL)~~ Messages

HACK	"Drink all the booze hack all the things"
1337	"got root"
CYBER	"GOVERNMENT MEDIA NOOB DRINK"
CYBER2	"CYBER CYBER CYBER CYBER CYBER CYBER"
WBM	"FDHNER CRT VA N EBHAQ JBEYQ"
SUPERSAT	"HACKER EXTRAORDINARE"
JORGE	"The creator or dad"
GIBSON	"Hack the planet crash and burn"
ACIDBURN	"crash and burn"
ZEROCOOL	"mess with the best die like the rest"
JEFFMOSS	"ICANN PARTY"
TRAVIS	"FUCK YOU NEIGHBOR"
OSSMANN	"such radio much sniff wow"
GMARK	"don't fuck it up"
NSA	"I C U P"
GOON	"HI PRIEST"
BEER	"take a drink"
HAD	"hackaday"
NINJA	"NINJA PARTY"
NEON	"LIZARD MOHAWKS FOR LIFE"
DIFFIE	"I love discrete logs"
HELLMAN	"Watch out for Mallory"
1o57	"e ahzojr nrjx qbr Amfx, qyeyxs ume xev myfpxpnxffr"
DEFCON	"canceled next year"
DEFCOIN	"cash rules everything around me"
ALICE	"bit ly alicenbob"
BOB	"Alice is sending her message to Bob Protecting that transmission is crypto's job"
EVE	"Eve is jealous of Alice"
ROT13	"So secure"
OPENSSL	"Open Season"
EFF	"Fighting for the users"
DARTHNULL	YGcpeevgCIKgfnMwefXzvGUHe3BgQKdxkMFeappqmVT0cNOkvGY6ehfo"
WARGAMES	"Shall we play a game"
SNEAKERS	"The world isn't by weapons anymore or energy or money its run by little ones and zeros little bits of data Its all just electrons."
SETEC	"Too many secrets marty"
LOTR	"Keep it secret keep it safe"
SCORPION	"250 years of bullshit er human thought every 90 minutes"

~~(C//REL)~~ Other easter eggs

MATRIX	Enables Matrix Mode
FUCK	Enables the “fuck” lockout
LED1	Enables LED1 easter egg
LED2	Enables LED2 easter egg
PONG	Enables PONG easter egg
COUNT	Enables Count easter egg
PARTY	Enables 15 minute party mode
RAGER	Enables 60 minute party mode
SORRY	Removes the “fuck” lockout
3FFD0N0R	Says “thank you for supporting the EFF” and set the EFF supporter bit
OVERCLOK	Sets ledMaxBrightness to 0xff (already 0xff on final firmware)
BULLETYM	Enables bullet time easter egg
FACTORYR	Performs a full erase of the NVM