Side Channel Timing Attacks on MSP430 Microcontroller Firmware

by Travis Goodspeed
EMC^2
Oak Ridge National Lab
<travis at utk.edu>

Thesis

A timing vulnerability exists
in version 2.12
of the MSP430's BSL
which allows the BSL password
to be guessed by an attacker.

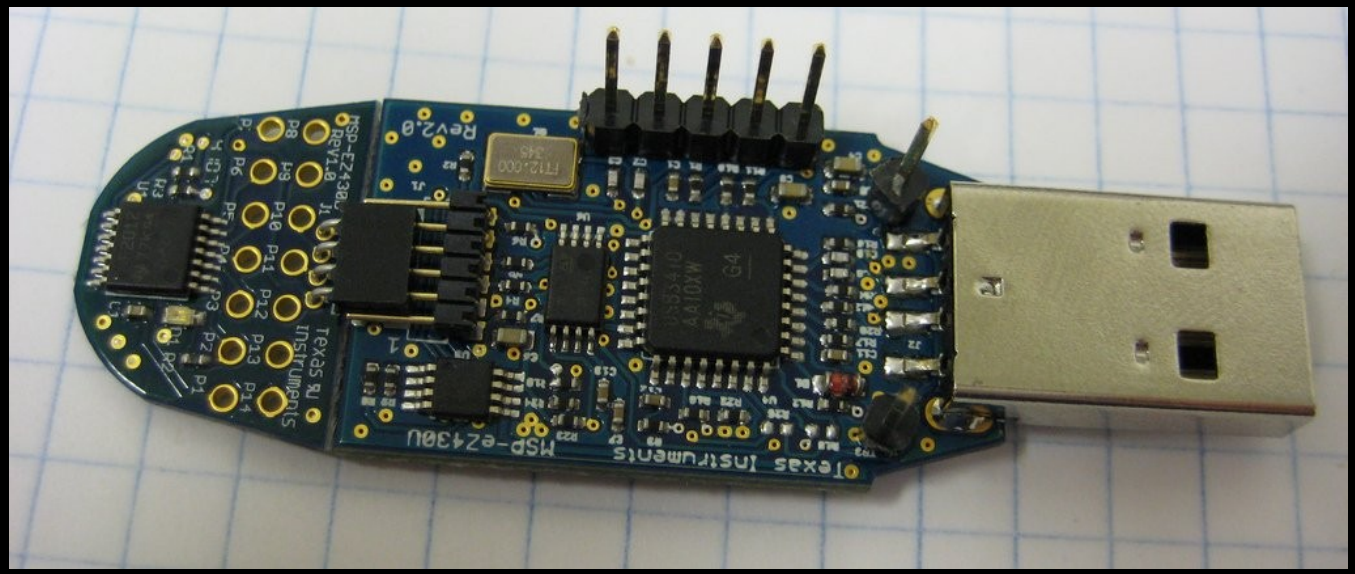
Prospectus

- JTAG and Spy-Bi-Wire
- BSL -- Serial Bootstrap Loader
- Manufacturing Considerations
- BSL Details
- Password
- Brute Force Attack
- Timing Attack
  - Theory
  - Simulation
  - Hardware

What is the MSP430?

- 16 bit RISC MCU
- Ultra-Low Power
  - 1μs clock startup
  - 0.8 μA standby
  - 250 μA/MIPS
- Usage
  - Low Power Wireless
  - Medical

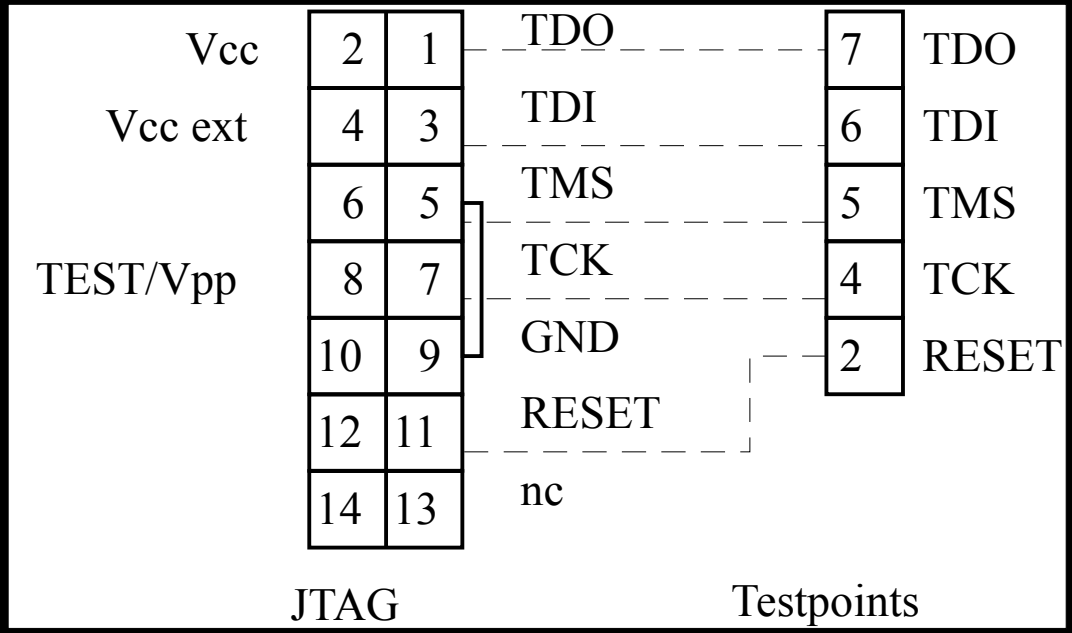
EZ430 Kit



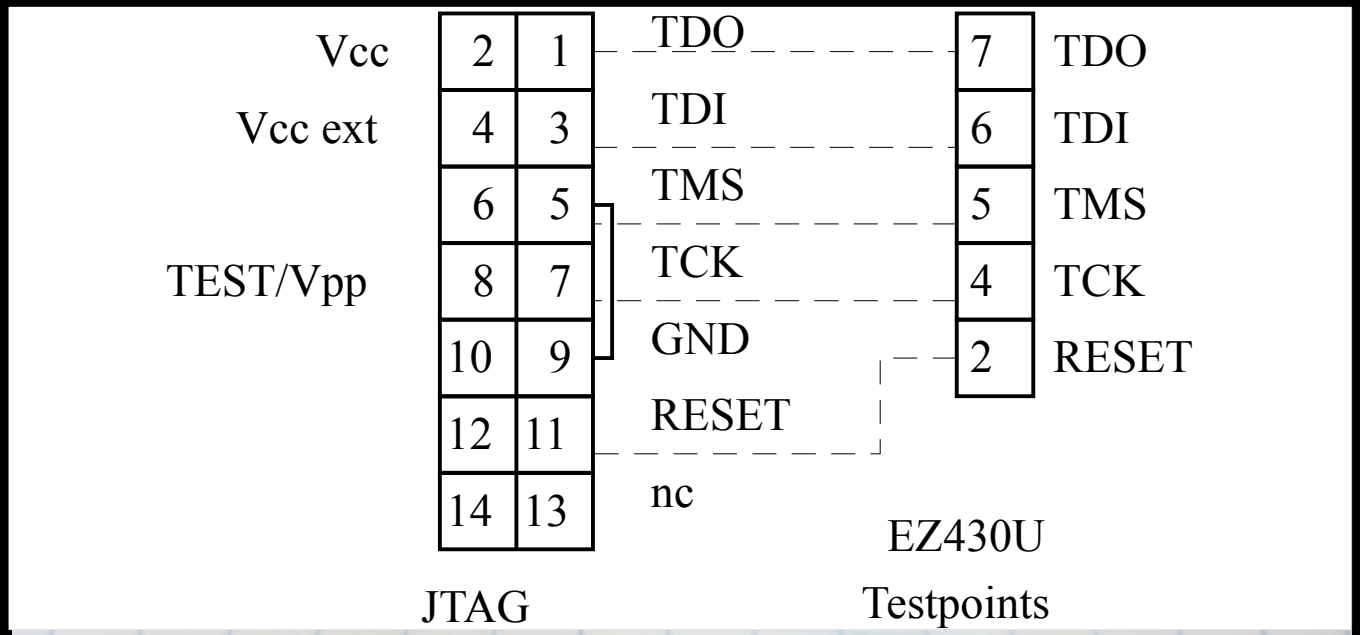
- $20 to $50
- Debugger/Carrier
- Target Boards
  - 2012 with an LED
  - 2274 with a Radio

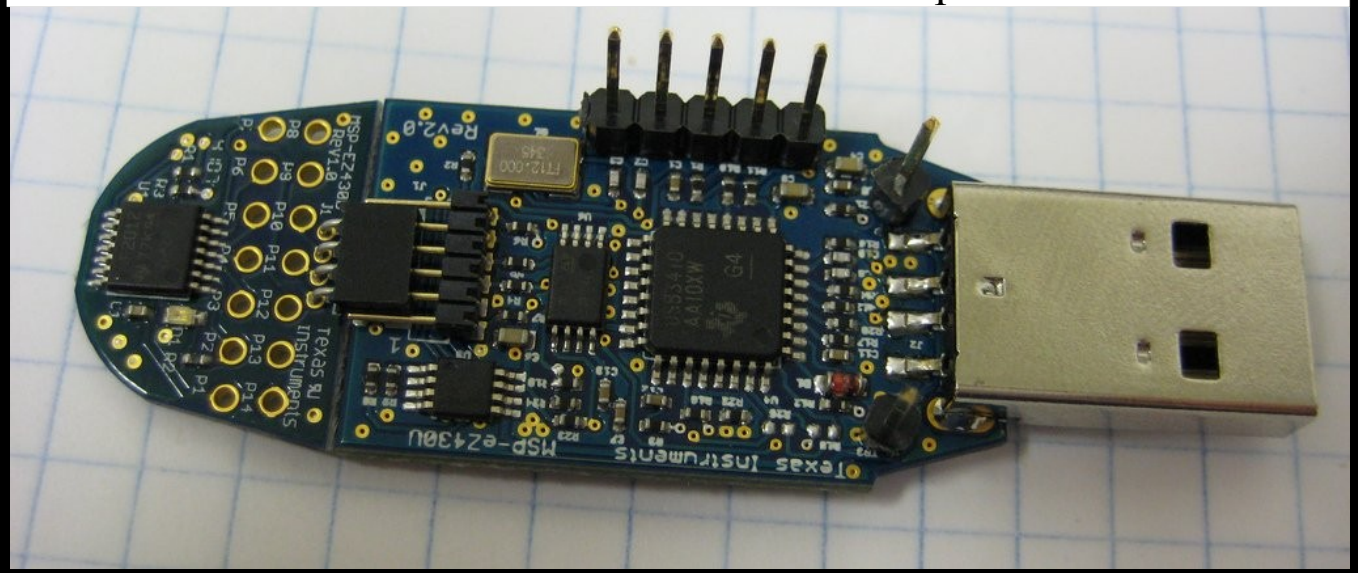
JTAG and Spy-Bi-Wire

- Programming
- Debugging
  - Registers
  - Single-Stepping
  - Breakpoints
- Fuse Protection



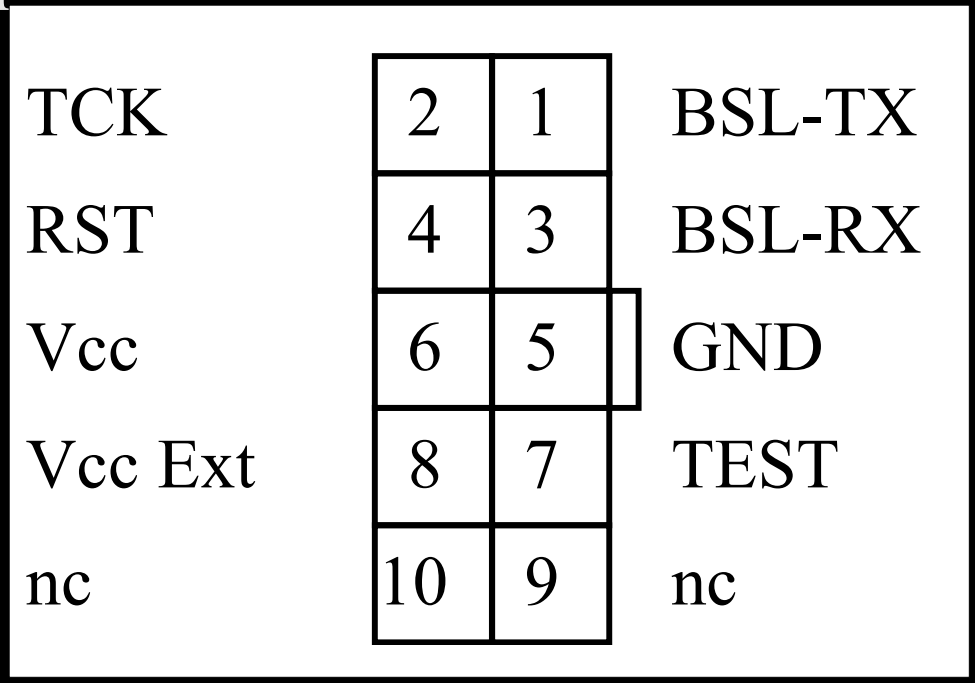
JTAG and Spy-Bi-Wire



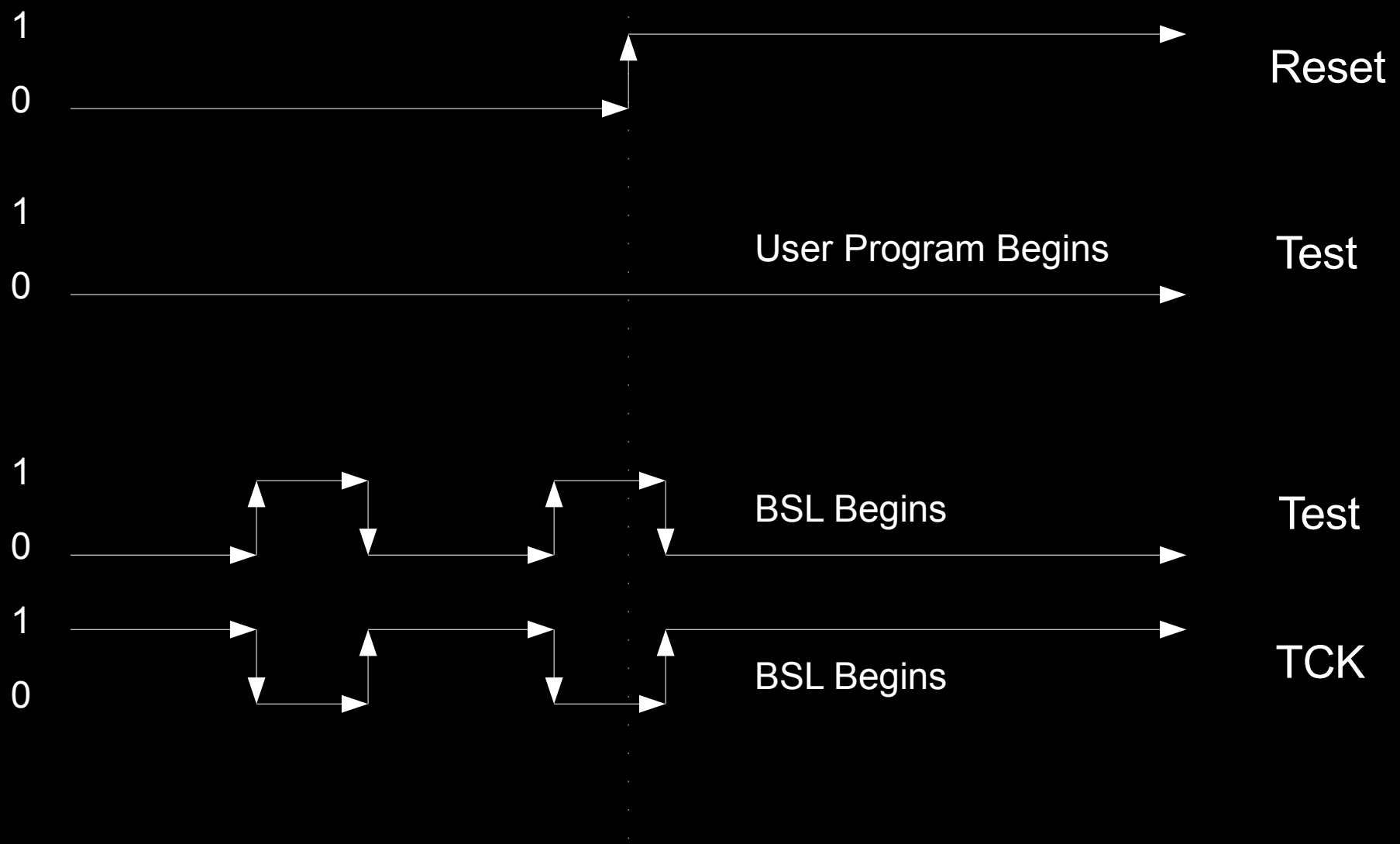


BSL: Serial Bootstrap Loader

- Just for Programming
- Serial Protocol
- Password Protected
- Disabled by Flash Token
  - Ignores JTAG Fuse



Initializing the BSL



BSL Commands

- RX Data
- RX Pass
- Erase Segment
- Mass Erase
- Erase Check
- Change Baud
- Load PC
- TX Data
- TX BSL Version

-
- RX Pass
-
- Mass Erase
- Erase Check
- Change Baud
-
-
- TX BSL Version

TX BSL Version

- Chip Info
- BSL Version

- F4 6F
- 32 40
- 00 00
- .. ..
- 00 00
- 02 12

Mass Erase

- Erases all of memory.
  - Resets password.
  - Nothing left to steal.

1	1	1	1	1	1	1	1
1	1	1	1	1	1	1	1
1	1	1	1	1	1	1	1
1	1	1	1	1	1	1	1
1	1	1	1	1	1	1	1
1	1	1	1	1	1	1	1
1	1	1	1	1	1	1	1
1	1	1	1	1	1	1	1

Change Baud

- Unprotected
  - BSL 1.60 and 1.61
- F1xx/F2xx
  - DCOCTL
  - BCSCTL1
- F4xx
  - SCFI0
  - SCFI1

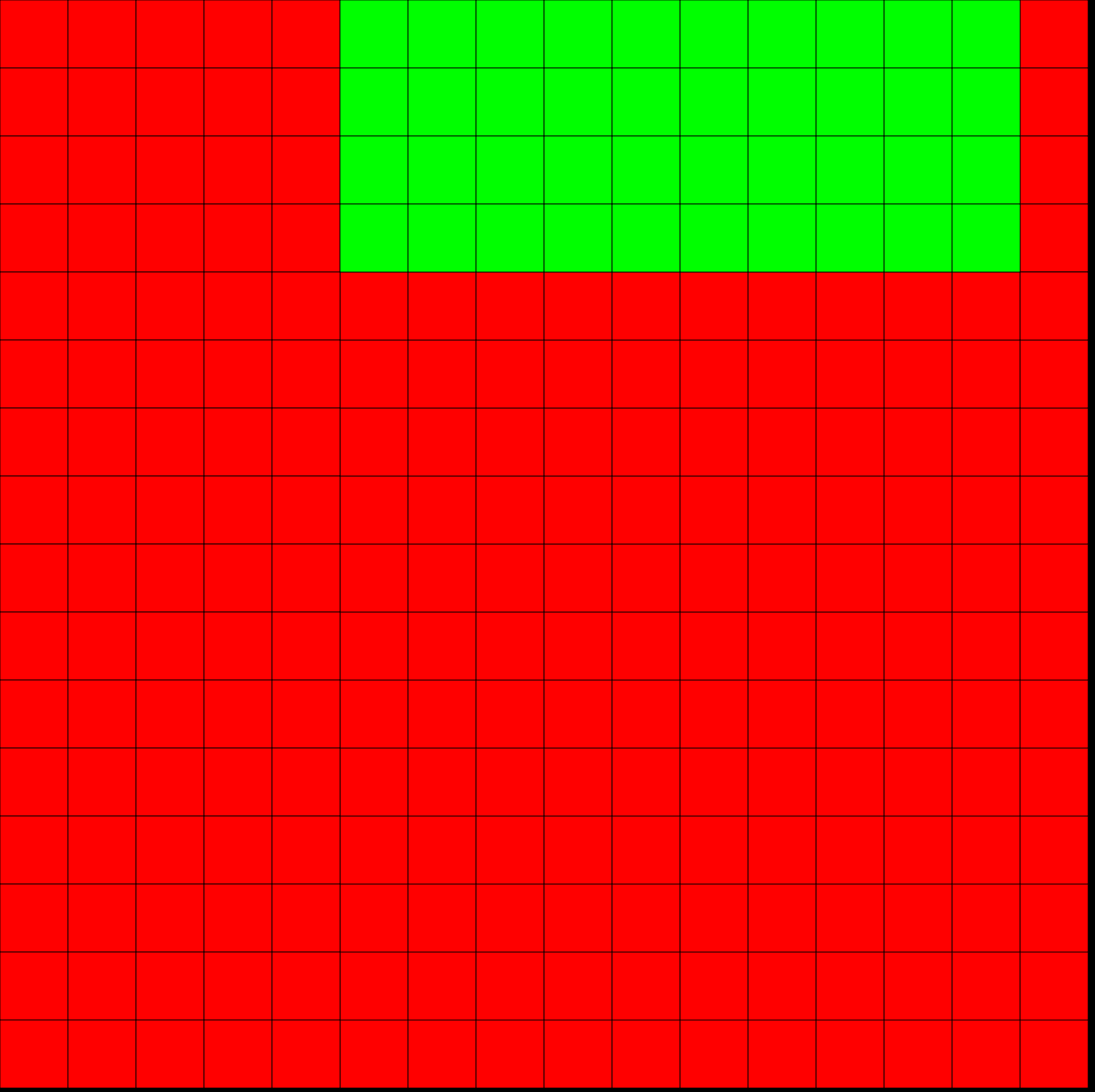
- Untrusted Data
- Control Registers

RXPass

- Receives BSL Pass
- Unlocks if correct.

BSL Password

- 256-bit Interrupt Vector Table
- 16 Vectors
  - 16 bits
  - pointers to interrupt handlers
- How many bits are actually random?
  - At least 40.
  - Tampering with Motes:
    Real-World Physical Attacks
    on Wireless Sensor Networks
    - Becher, et al



16*16=256 Bits

16*15=240 Bits

15*15=225 Bits

4*15=60 Bits

4*10=40 Bits

Brute Forcing 40 Bits, Becher

- 12 Pass/Sec at 9600
  - 31 Pass/Sec at 38400
  - 81 Pass/Sec with modified behavior
  - Round up to 2^7
- 2^(40-7-1) seconds
  - 2^32 seconds
  - 128 years

How Change Baud Rate Works

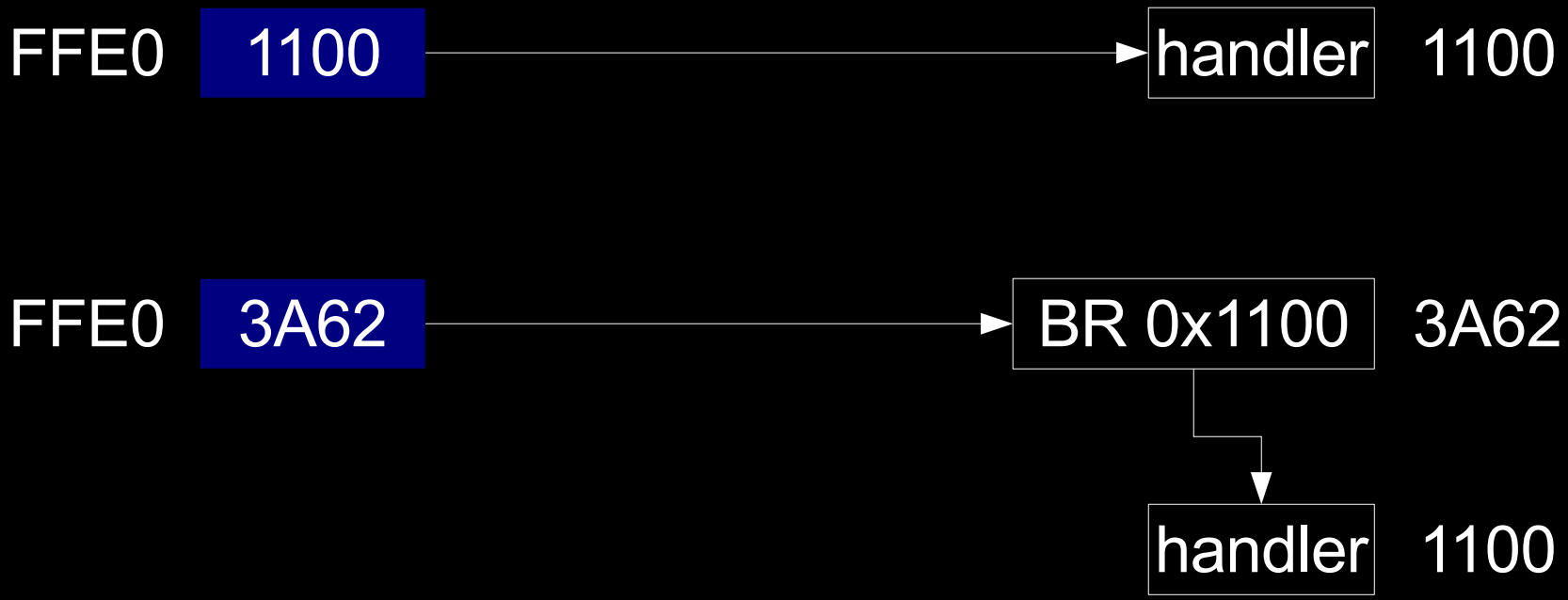
baud	mhz	years
9600	1.05	
19200	2.1	
38400	4.2	128
	8	
	16	32

Brute Forcing 40 Bits, Goodspeed

- 12 Pass/Sec at 9600
  - 31 Pass/Sec at 38400
  - 81 Pass/Sec with modified behavior
  - Round up to 2^7
- 2^(40-7-1) seconds
  - 2^32 seconds
  - 128 years
- Reclock from 4mhz to 16mhz
  - 2^30 seconds
  - 32 years

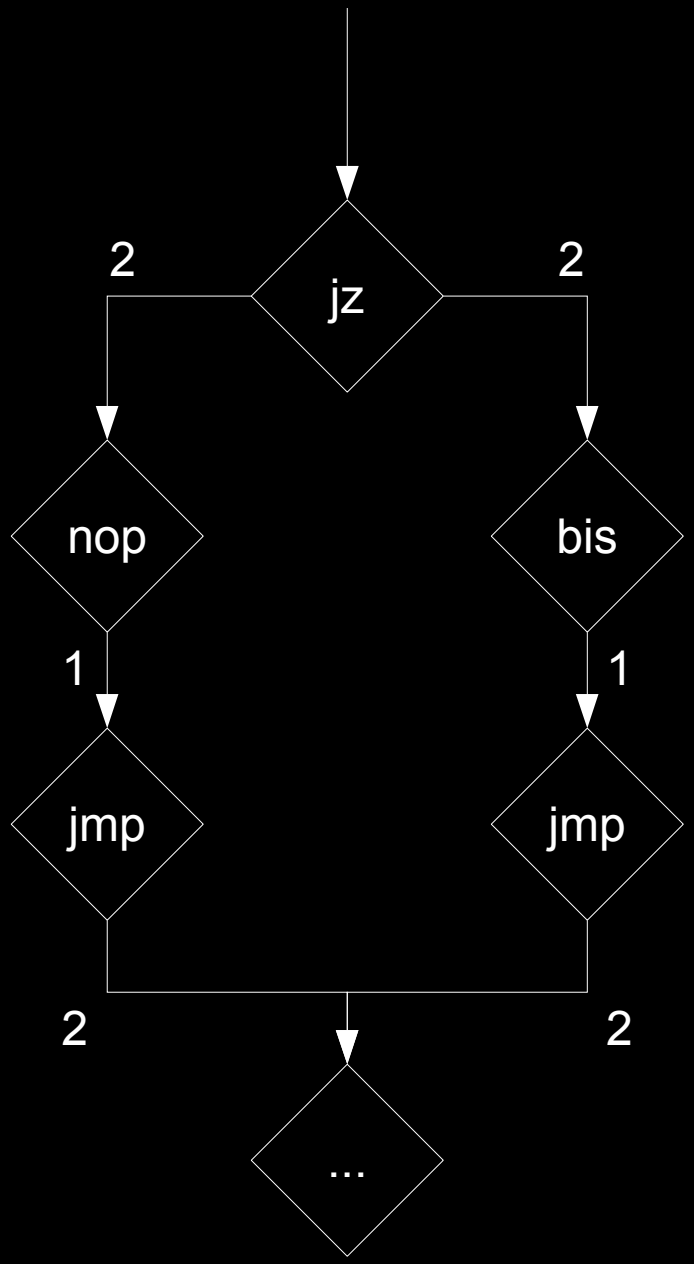
Becher's Password Fix

- Perl Script
- Randomizes Interrupt Vectors



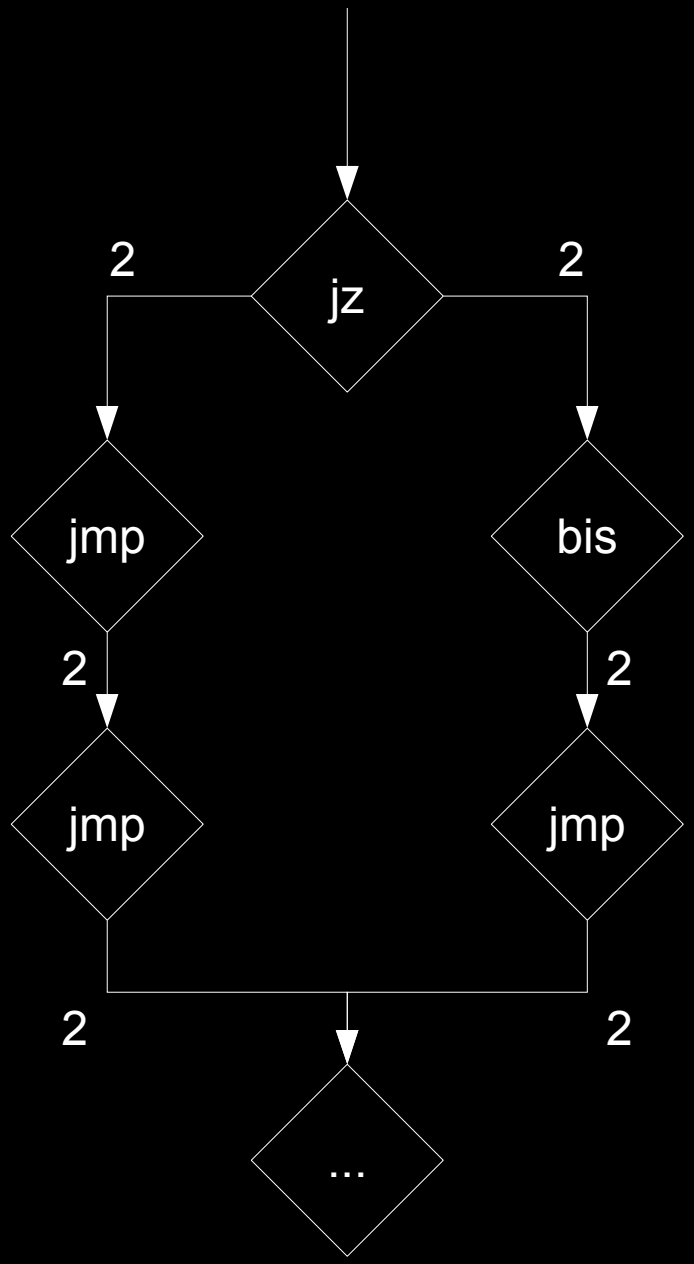
Password Comparison MSP430F1612

- for(i=0; i<32; i++)
  - b=getbyte();
  - if(b!=IVT[i])
    - access=denied;
  - else
    - wait;



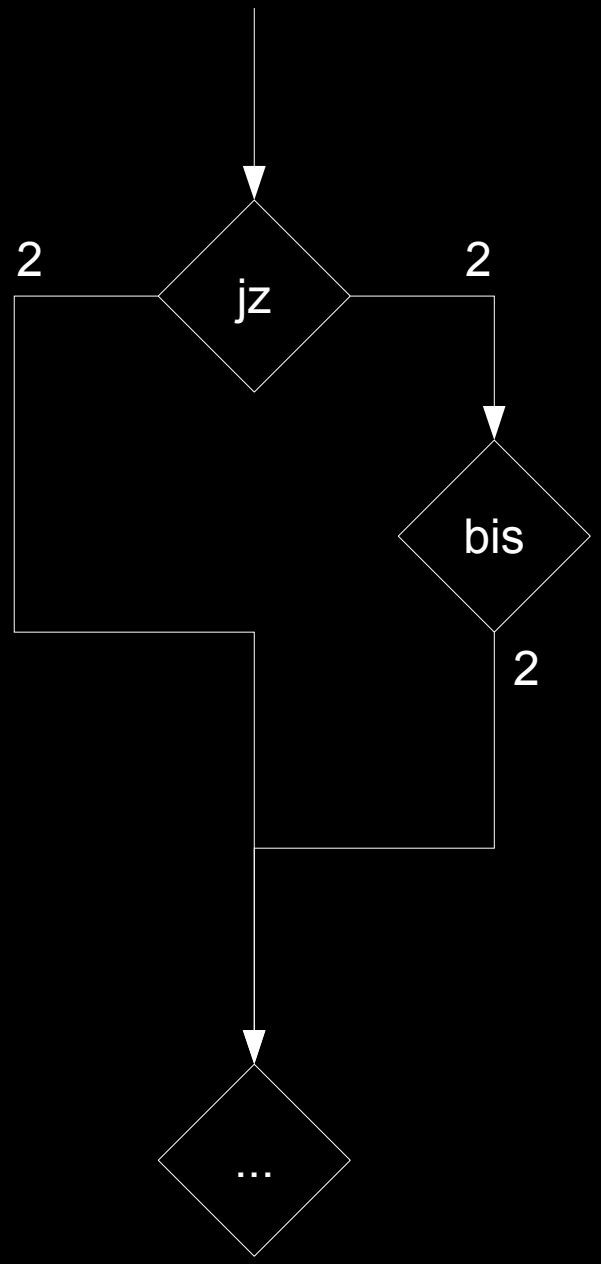
Password Comparison MSP430F2274

- for(i=0; i<32; i++)
  - b=getbyte();
  - if(b!=IVT[i])
    - access=denied;
  - else
    - wait;



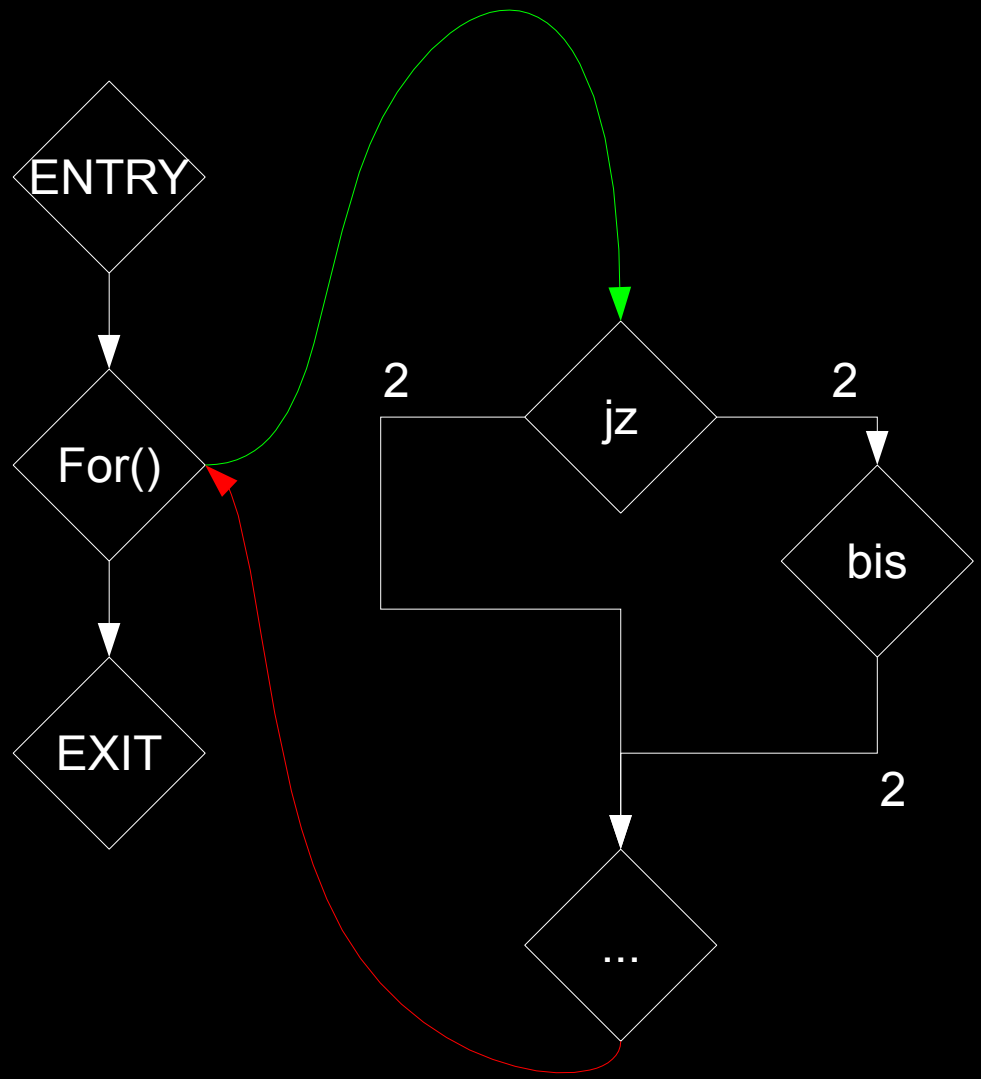
Password Comparison MSP430FG4618

- for(i=0; i<32; i++)
  - b=getbyte();
  - if(b!=IVT[i])
    - access=denied;



Simulation

- MSP430simu
- C Wrapper
  - Patches BSL
- Tested 256 Passwords



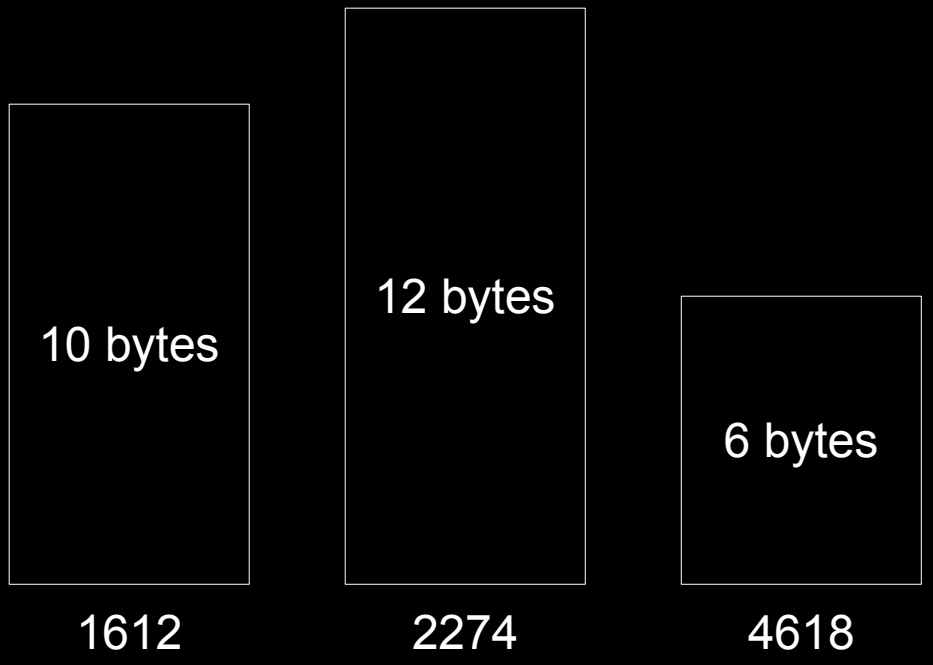
Simulation Results

	Cycles	Δ	Δ/2
others	6543	0	0
00*	6541	2	1
11*	6511	32	16
3A*	6513	30	15

IVT	
113A	1100
113A	113A
113A	113A
113A	113A
113A	113A
113A	113A
113A	113A
113A	113A
113A	113A

Why was this done?

- Space Constraints?
  - C00 to FFF
  - 1024 Bytes
- Feature Creep
- Instruction Set



Feature Creep

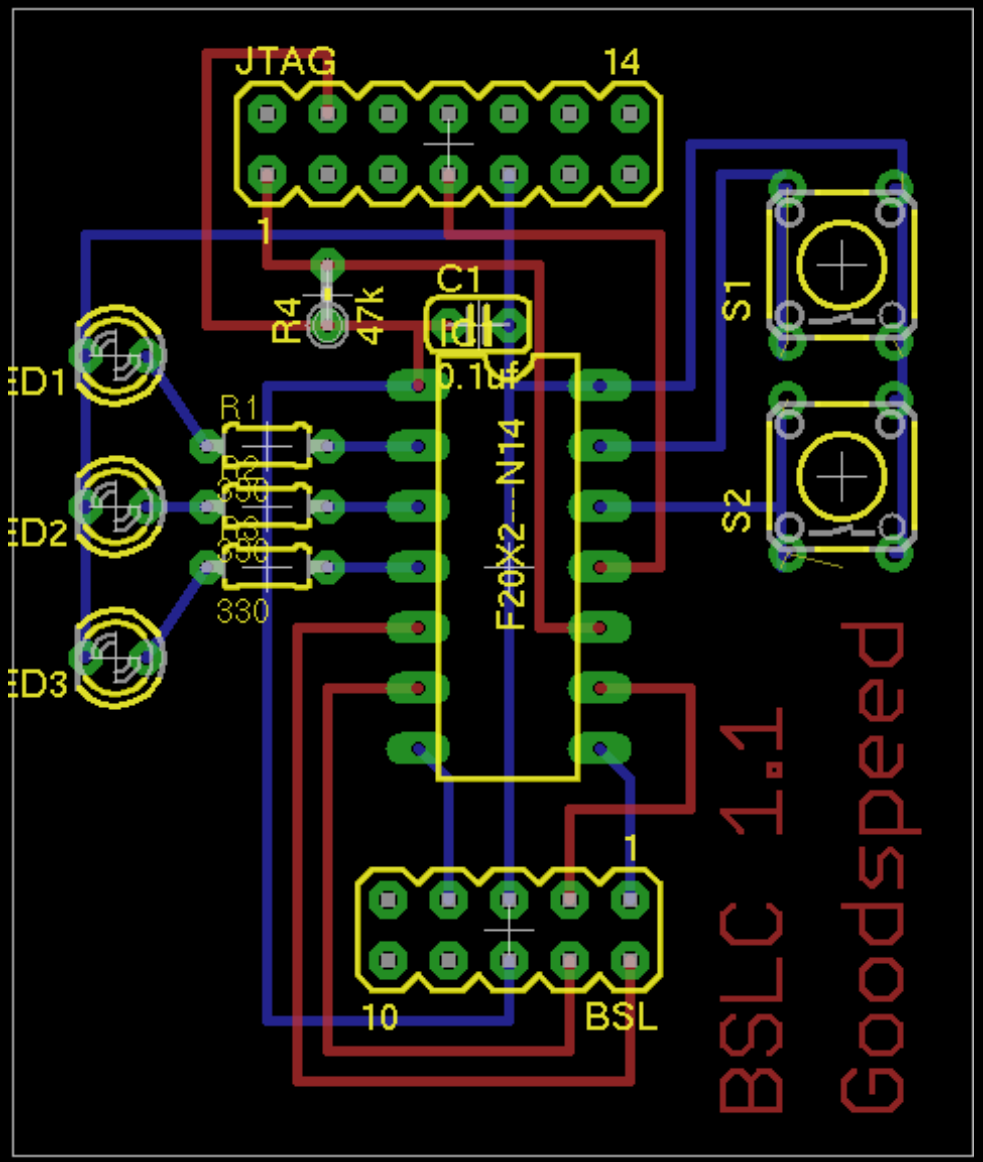
- 1.60
  - TX BSL Version
  - Change Baud
- 2.01
  - Change Baud Fixed
- 2.12
  - Set Memory Offset
  - 20-bit Extensions

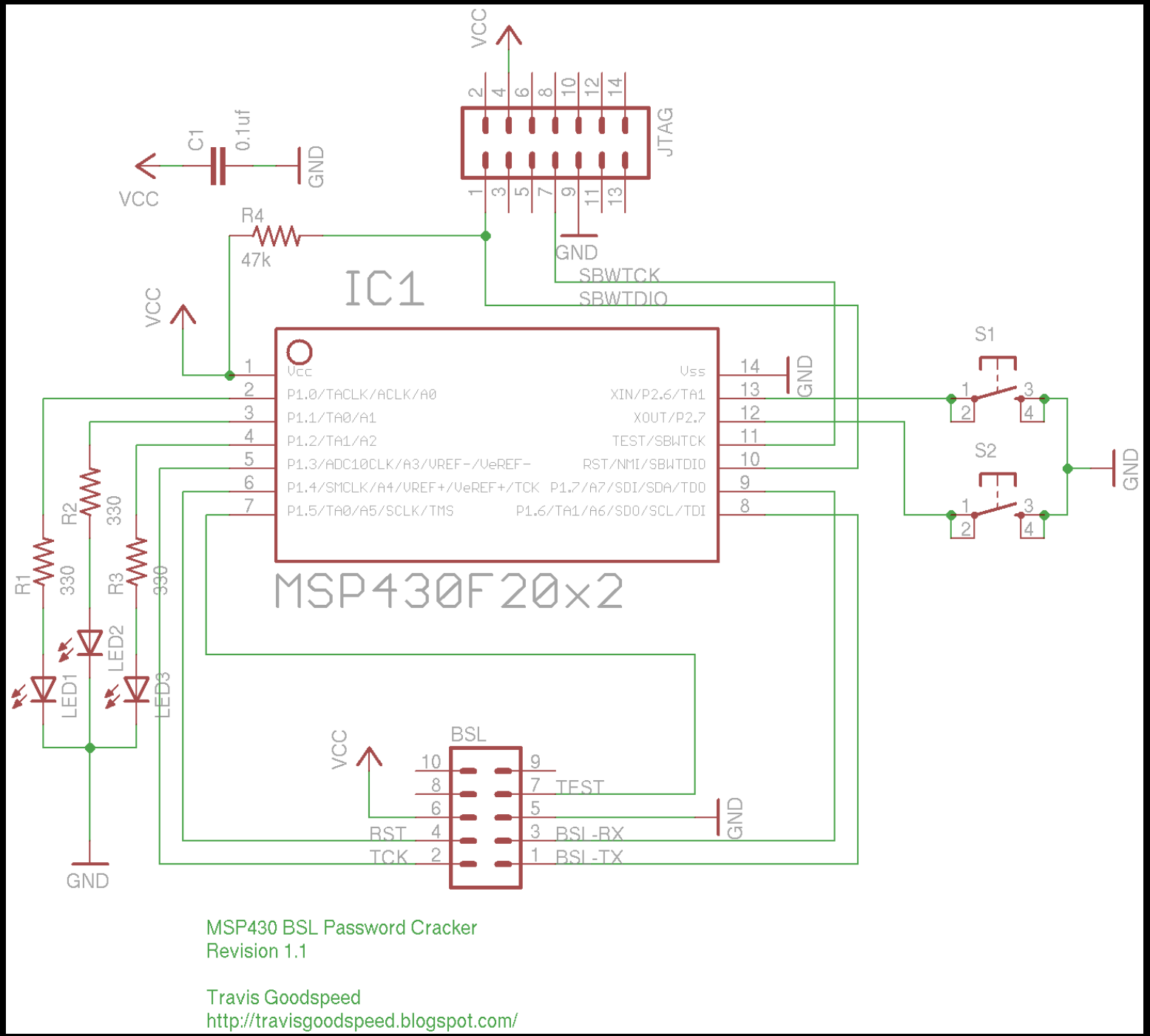
Instruction Set Change

- MSP430
  - 16-bit architecture
- MSP430X
  - 20-bit address extension
  - Prefix Extension Word

BSLCrack

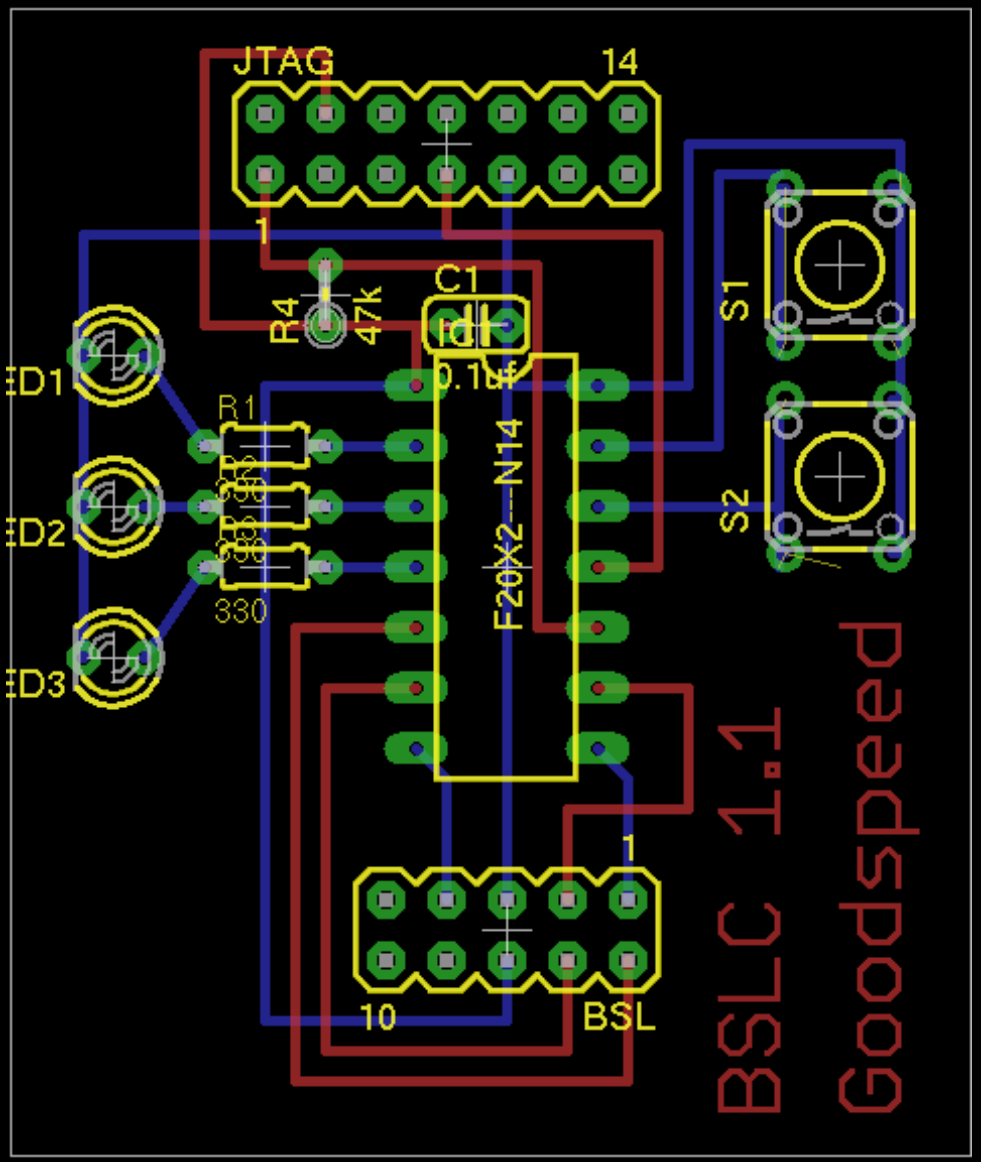
- Low Latency
  - 1 mhz target clock
  - 2 cycles of drift
- MSP430F2012
- 3 LEDs
- 2 Buttons




VCC
JTAG
C1
0.1uf
GND
R4
47k
IC1
SBWTCK
SBWTDIO
S1
S2
Vcc
Vss
P1.0/TACLK/ACLK/A0
P1.1/TA0/A1
P1.2/TA1/A2
P1.3/ADC10CLK/A3/VREF-/VeREF-
P1.4/SMCLK/A4/VREF+/VeREF+/TCK
P1.5/TA0/A5/SCLK/TMS
XIN/P2.6/TA1
XOUT/P2.7
TEST/SBWTCK
RST/NMI/SBWTDIO
P1.7/A7/SDI/SDA/TDO
P1.6/TA1/A6/SDO/SCL/TDI
MSP430F20x2
R1
330
R2
330
R3
330
LED1
LED2
LED3
BSL
TEST
RST
TCK
BSL-RX
BSL-TX
MSP430 BSL Password Cracker
Revision 1.1
Travis Goodspeed
http://travisgoodspeed.blogspot.com/

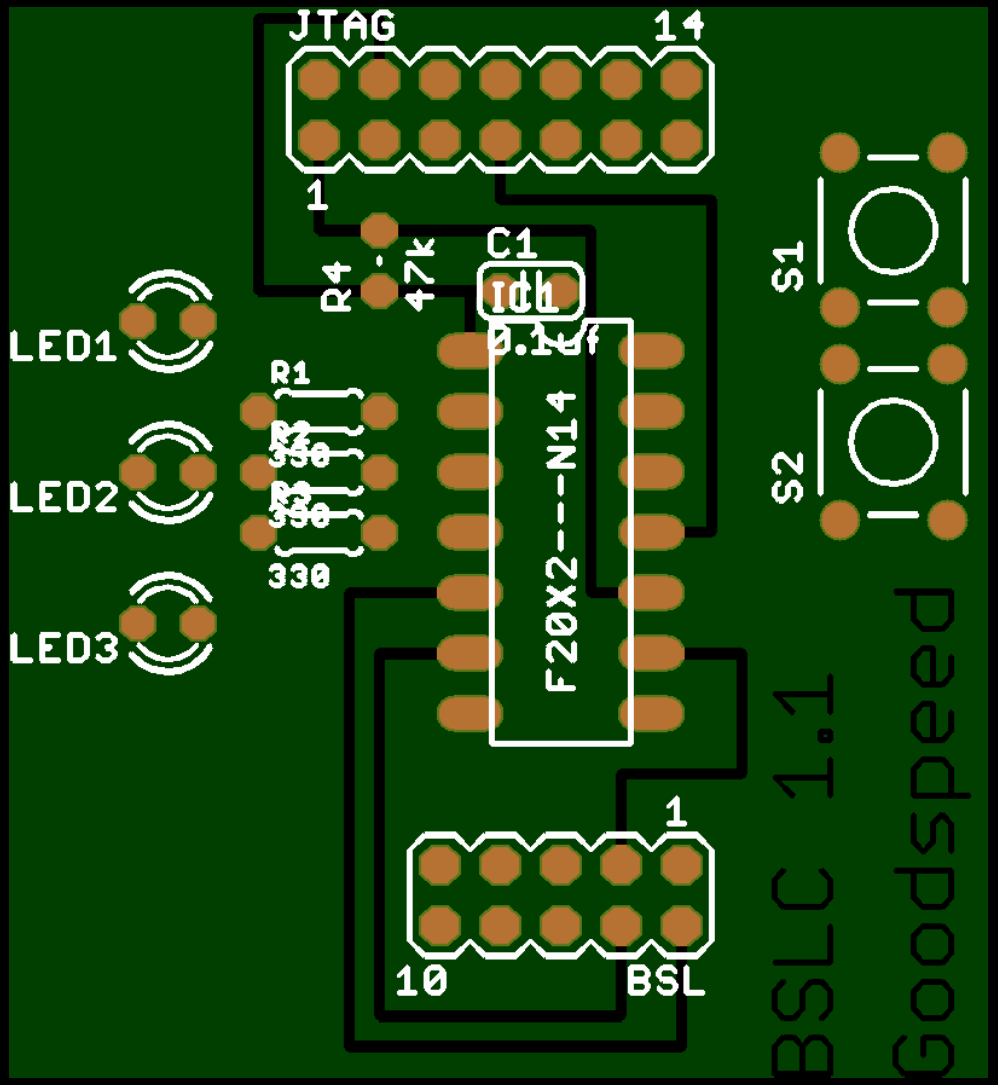
BSLCrack Software

- Verify Version
- False Password
  - 0x0001 repeated
- Byte Guesses
  - 0x00 repeated,
  - 0x01 repeated,
  - ...
- Enumerate Remainder



BSLCrack

- Results
  - Stored in ROM
  - Indicated by LED
  - Retrieved by JTAG
- Construction
  - No SMD Components
  - Breadboardable



Concluding Remarks

<travis at utk.edu>
http://travisgoodspeed.blogspot.com/

Questions?

<travis at utk.edu>
http://travisgoodspeed.blogspot.com/