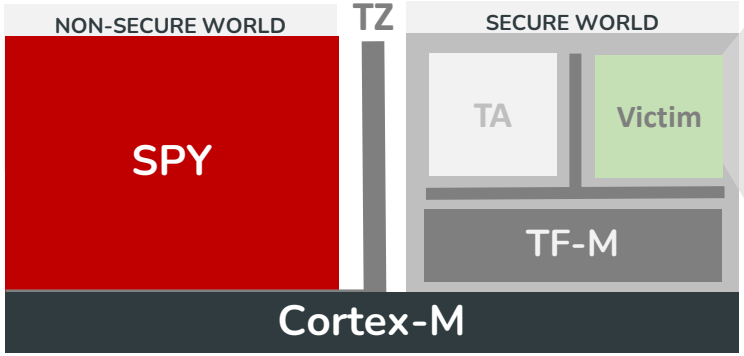
BUSted Attack




```
signed int read_keypad(void){
    int is_pressed, mask = 0x1;
    int new_key_state = get_keypad_state();                    read key
    for (int key = 0; key < KYPD_NB_KEYS; key++){
        is_pressed = (new_key_state & mask) & ~(key_state & mask);
        if (is_pressed)                                        if branch (leak)
          pin[pin_idx++] = key;
        else                                                   else branch
          dummy_pin[dummy_pin_idx++] = key;
        dummy_pin_idx = 0;
        mask <<= 1;                                            for loop
    }
    key_state = new_key_state;
    return (4 - pin_idx);
}
void read_pin(){
  signed int pin_len = PIN_LEN;
  while(pin_len>0)
    pin_len = read_keypad();                                   while loop
}
```

Code based in Sancus and Texas Reference Implementation of a Keypad [1,2]

[1] https://github.com/sancus-tee/vulcan/blob/master/demo/ecu-tcs/sm_tcs_kypd.c
[2] Implementing An Ultra-Low-Power Keypad Interface With MSP430™ MCUs