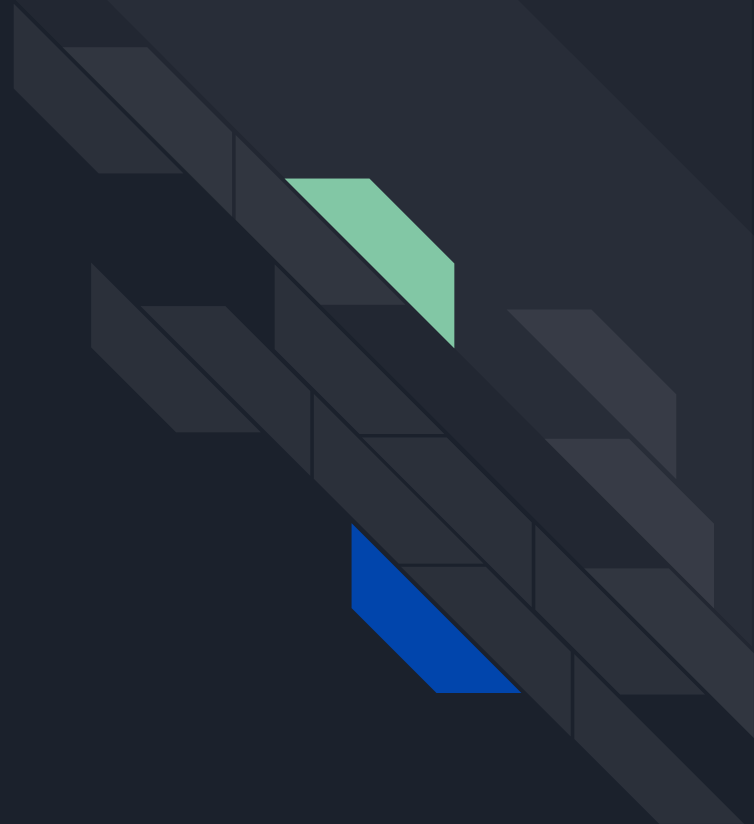




# **zkTap:** A Zero-Knowledge Trustless Authentication Protocol

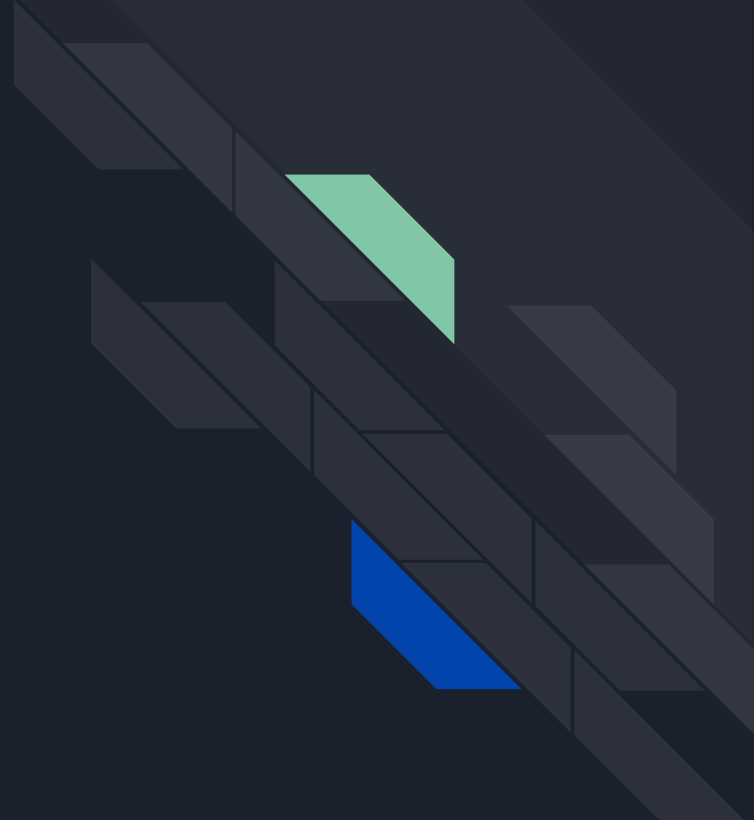
Team 33: Joseph Kuo, Majdi Hassan, Lilan Yang

TA: Evan Widloski; Professor: Arne Fliflet





# What Problems Do We Solve?





T0py

@InfoSecFriends

Follow



3F90EBF0910F7B6F

HID iClass Master key

Thanks @Amm0nRa <3

#kiwicon



1:39 PM - 16 Nov 2016

28 Retweets 83 Likes



A readout of activity that took place on the hotel room's electronic door lock indicated that an attempt was made to reprogram al-Mabhouh's electronic door lock at this time. [citation needed] The investigators believe that the electronic lock on al-Mabhouh's door may have been reprogrammed and that the killers gained entry to his room this way.<sup>[41]</sup> The locks in question, VingCard Locklink brand,<sup>[42]</sup> can be accessed and reprogrammed directly at the hotel room door.

## Assassination of Mahmoud al-Mabhouh



**Location** Dubai, United Arab Emirates

**Date** 19 January 2010

**Target** Mahmoud al-Mabhouh

**Attack type** Assassination

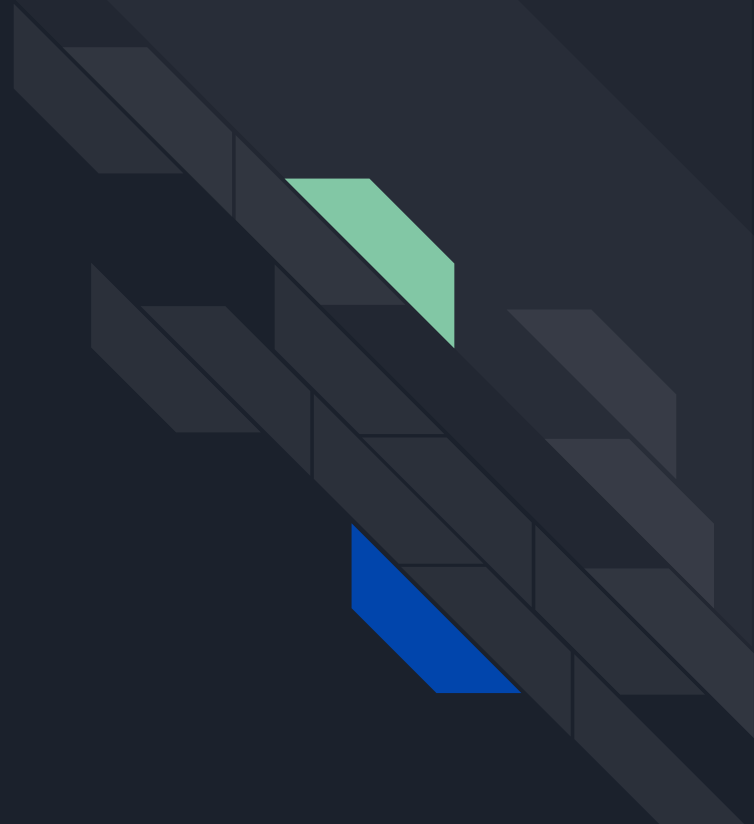
**Weapons** Pillow, muscle relaxant

**Deaths** 1

**Perpetrators** 33 people, using forged and fraudulently obtained passports



# Our Solution

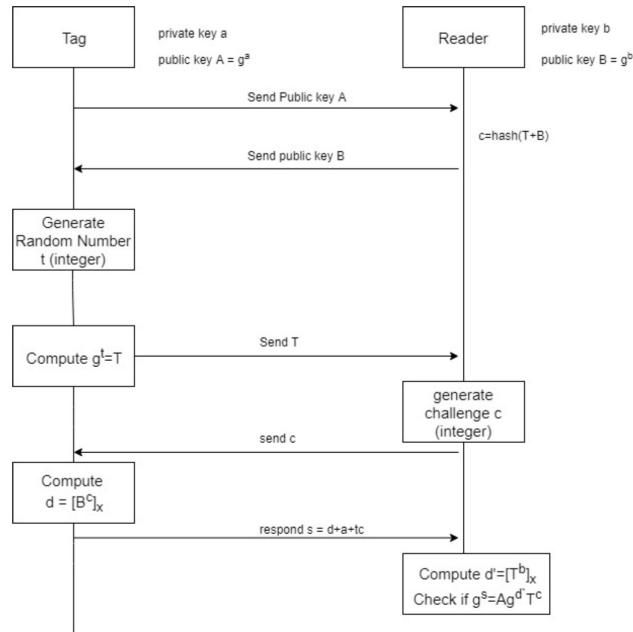




# Security Protocol

- The tag and reader exchange public keys which is their claim of their identification
- The two systems communicate back and forth so the tag proves it is who it claims to be
- After the tag is verified, the reader grants or denies access depending if tag has privileges

# Schnorr-Peeters Protocol



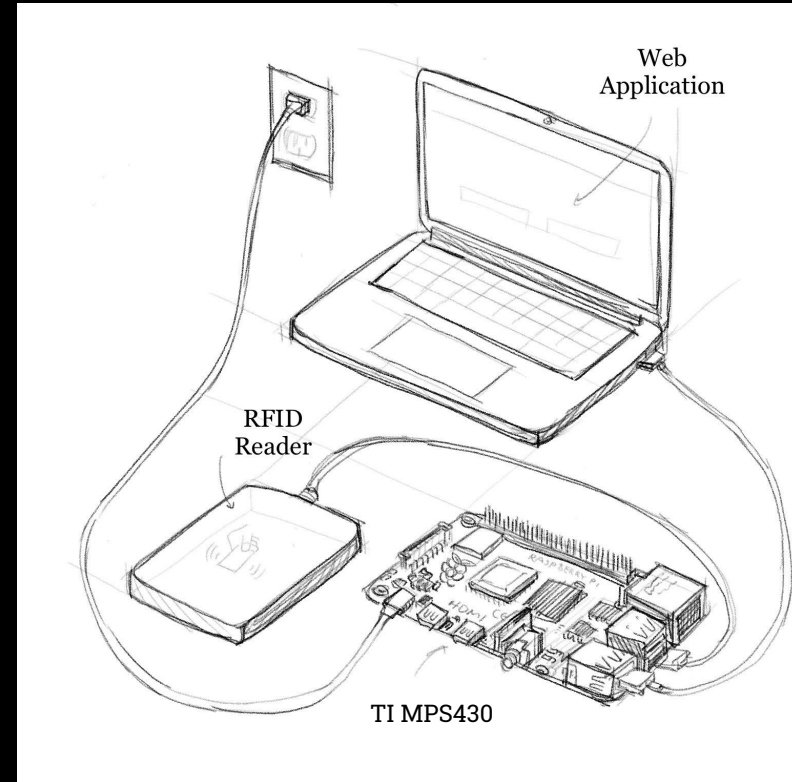
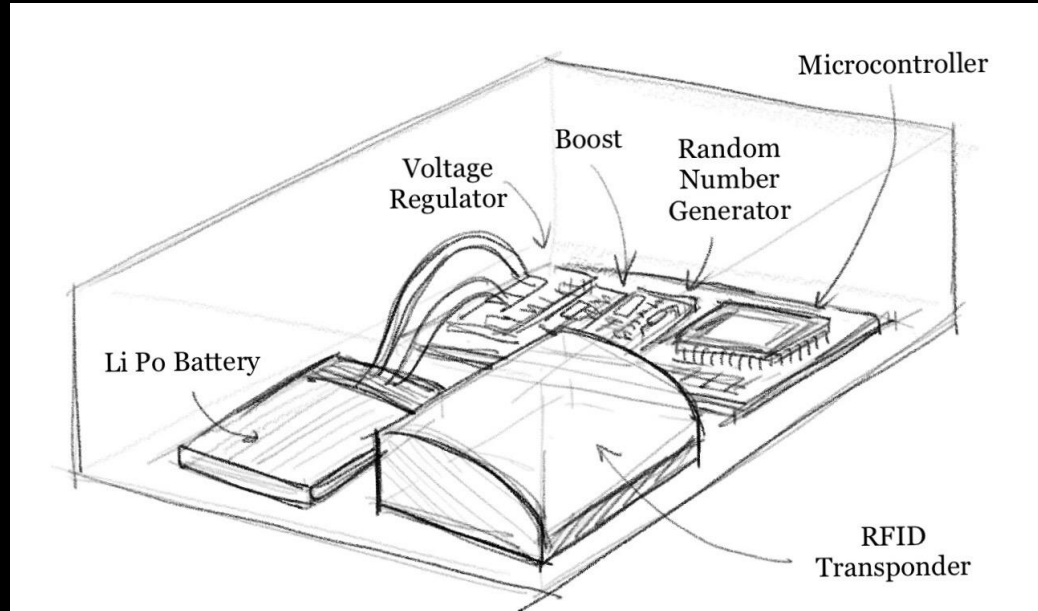
Blinding Factor: 0x5f7e3a0347bd0  
Commitment: 0x11bc0429e6efa  
Tag's private key: 0xece445  
Tag's public key: 0xeacf224b9d457

Reader's private key: 0xececafe  
Reader's public key: 0x7532a02443798  
Challenge: 0xa2e169b1c335f

Shared Secret: 0x8c864f1650952  
Tag's Answer to the challenge: 0xd823281e72c11

Verification: 0xeacf224b9d457

# Physical Diagram

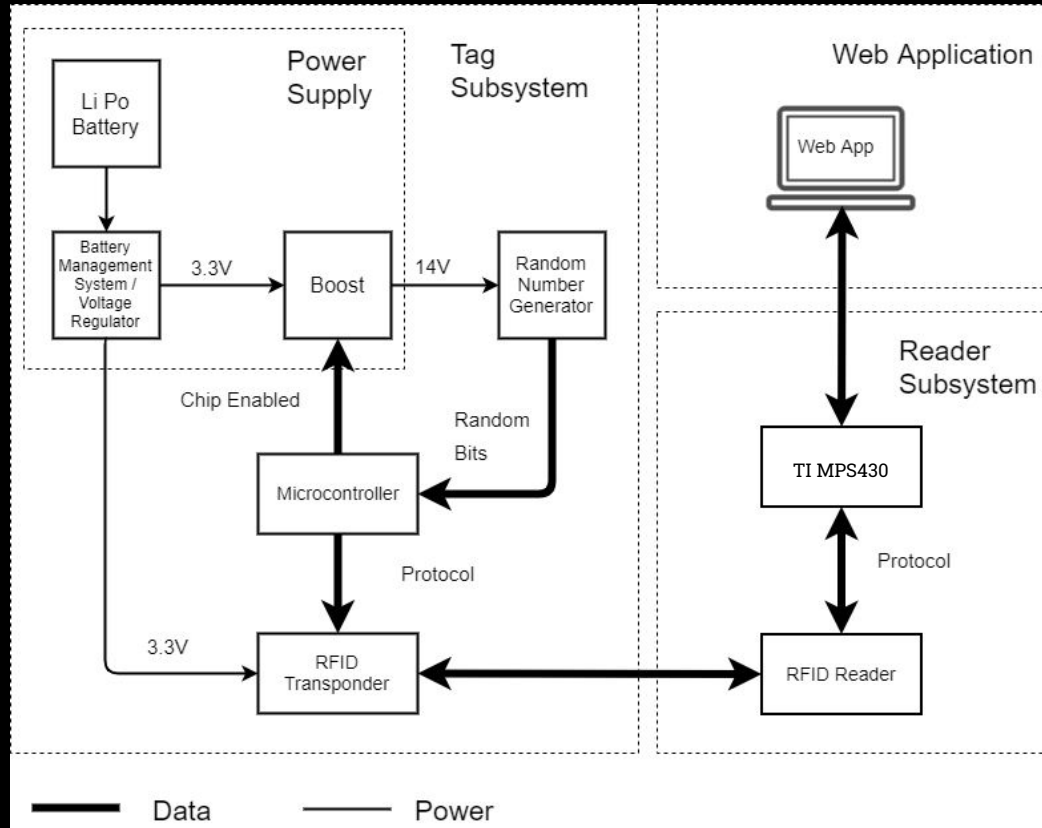




# High-Level Requirements

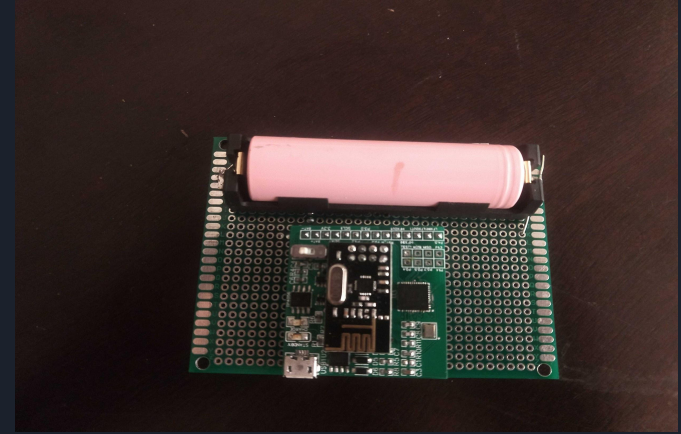
- 01 The response given by the correct tag must be accepted by the reader with all but negligible probability (on the order of being rejected  $\sim 1\%$  of the time).
- 02 A user must be authenticated in under 10 seconds.
- 03 An eavesdropper must not be able to impersonate a user (except by guessing responses).

# Block Diagram



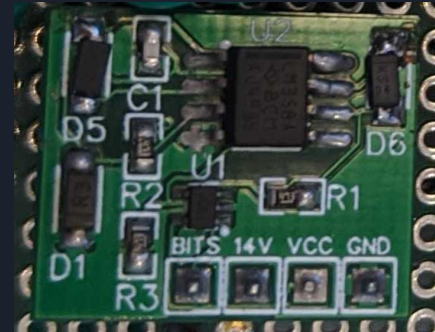
# Tag Subsystem

- The subsystem consists of:
  - power supply and management system
  - random number generator
  - a microcontroller with msp430 chip
  - NRF24I01 chip
- Power supply supplies power to the rest of the system and uses a battery so that it is portable
- Microcontroller manages the security protocol
- NRF24I01 enables communication via the air

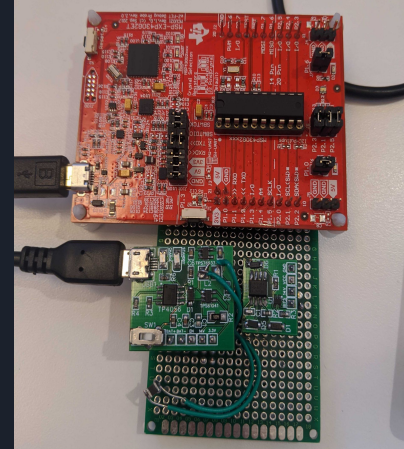
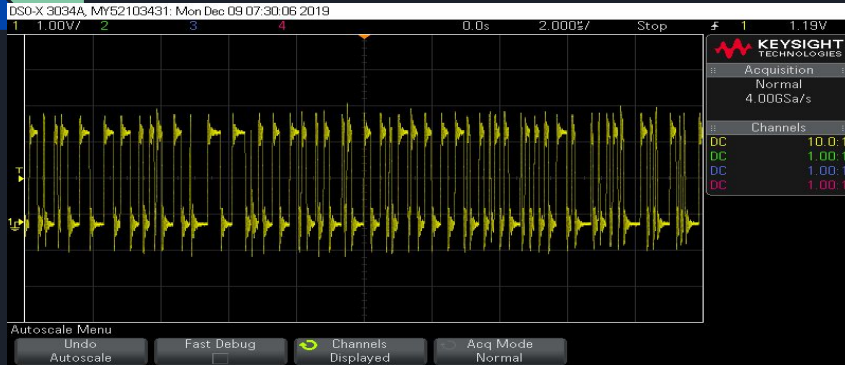


# Random Number Generator

- Zener diode
- Avalanche Noise
- Discretize



# RNG Results & Verification



```
[joseph@null cpp]$ ./ea_iid ../bin/rng2.bin
Calculating baseline statistics...
H_original: 7.868209
H_bitstring: 0.995580
min(H_original, 8 X H_bitstring): 7.868209

** Passed chi square tests

** Passed length of longest repeated substring test

Beginning initial tests...
Beginning permutation tests... these may take some
** Passed IID permutation tests
```

```
[joseph@null cpp]$ ./ea_non_iid ../bin/rng2.bin
Running non-IID tests...

Running Most Common Value Estimate...

Running Entropic Statistic Estimates (bit strings only)...

Running Tuple Estimates...

Running Predictor Estimates...

H_original: 7.353758
H_bitstring: 0.885569
min(H_original, 8 X H_bitstring): 7.084548
```



# Tag Transponder

- The RFID transponder is responsible for transmitting data to the reader and receiving data from the reader
- The NRF24I01 chip allows for the tag to broadcast messages over the air
- The tag follows a security protocol implemented in msp430 and uses the random number generator to prove that the user is who it claims to be

Requirements: The data sent should be resistant toward corruption

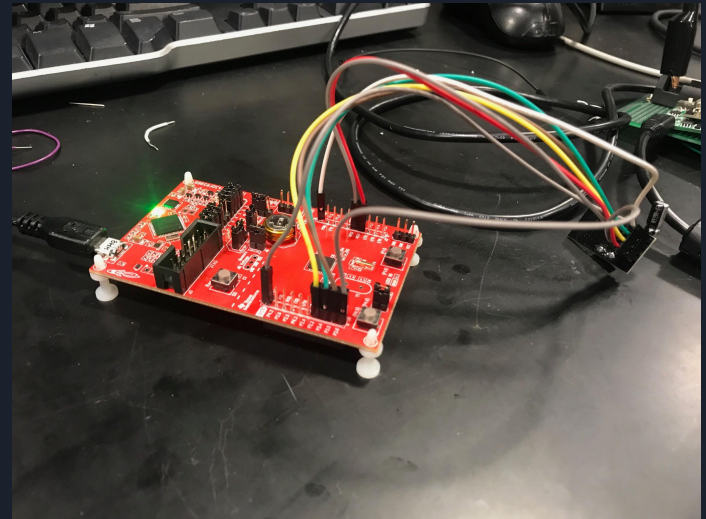
Verification: We collected 1000 messages and it was a success if 99% messages were uncorrupted

# Reader Subsystem

- The reader subsystem consists of NRF24I01 chip and a msp430 board.
- The chip enables the reader to receive messages from the tag
- The msp430 verifies the tag's identification and transmits this information to the web application

Requirements: It reads data from RFID transponder

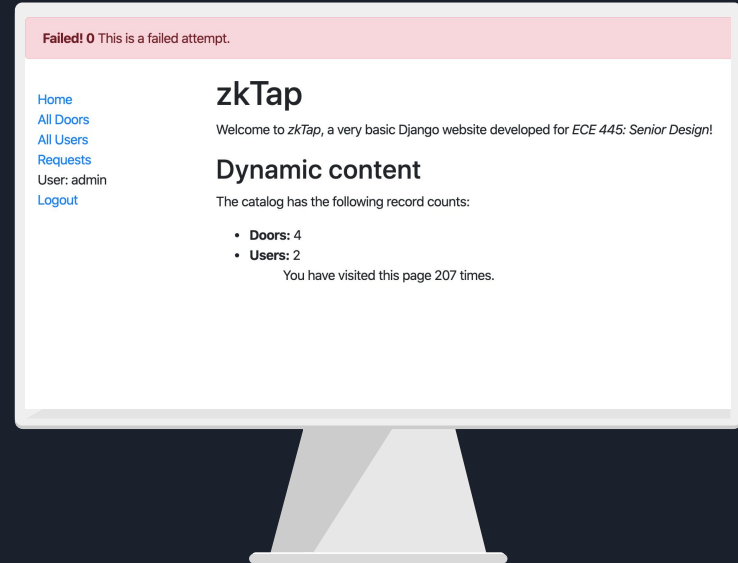
Verification: reader authenticates tag and sends information to web app. If web app displays the information, then authentication is successful



# Web Application

## Function as visual aid

- View all doors and users
- User can request door access
- Admin can either revoke or accept door access requests
- Alert if there's successful or failed attempts



# Database

## SQLite

Django administration

WELCOME, [ADMIN](#) [VIEW SITE](#) / [CHANGE PASSWORD](#) / [LOG OUT](#)

Home > Catalog > Doors

✔ The door "Senior Design Lab" was changed successfully.

Select door to change

ADD DOOR +

Q

Search

Action: 

-----

Go

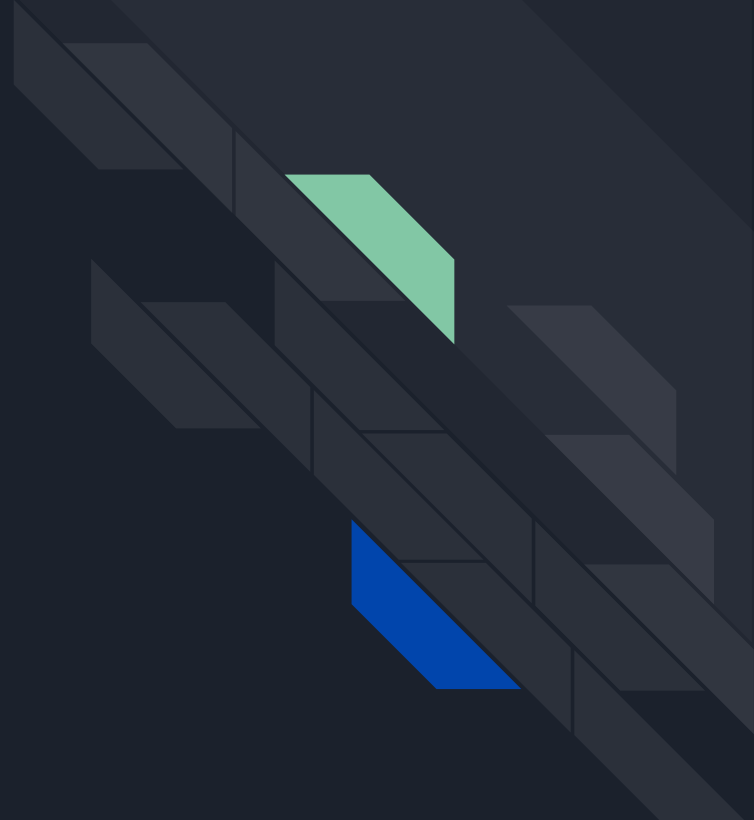
 0 of 4 selected

| <input type="checkbox"/> | DOOR NAME                                | LOCATION  | DOOR PUBLIC KEY                                                |
|--------------------------|------------------------------------------|-----------|----------------------------------------------------------------|
| <input type="checkbox"/> | <a href="#">Grainger Auditorium</a>      | ECEB 1002 | ab22314136356fe1163d9321fe5719ac1dec167ea1cff48a902ab1d39f63   |
| <input type="checkbox"/> | <a href="#">Instructional Clean Room</a> | ECEB 1003 | 47bae8a6d57fb7b961863eefbffe10955f23a0a5586cba486e30e96a131a31 |
| <input type="checkbox"/> | <a href="#">EWS Computer Lab</a>         | ECEB 2022 | dfc25eb85f19cce14b991c54e52e84784637d248b81cea3c9da3d135215915 |
| <input type="checkbox"/> | <a href="#">Senior Design Lab</a>        | ECEB 2070 | b9eed58fcc17f78d1be4da2c74e877bfa3c96de083d216e881d28378a1a264 |

4 doors

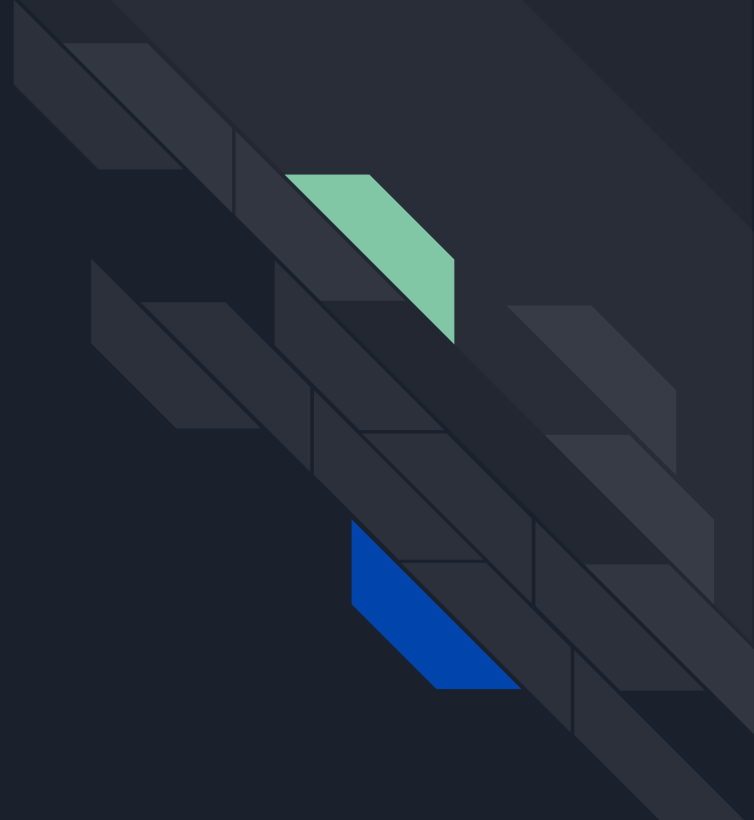


# What's Our Biggest Challenge?





# What's Next?



The background is a dark navy blue. In the top-left corner, there are two overlapping triangles: a blue one on the left and a light green one on the right. In the bottom-left corner, there is a circular inset showing a detailed, grayscale image of a printed circuit board (PCB) with various electronic components. In the top-right corner, there is a grayscale image of a complex, multi-layered circuit board structure.

**Thank you!**