1 Introduction

1.1 Objective
The dorms on campus currently do everything that they can to prevent theft in each room. The measures that currently exist to prevent this are icard scanners in order to enter each building, and deadbolt locks on each individual student’s room. Yet, there are still thefts that occur on campus from the dorms every year as evidenced by the University’s police department’s crime log\(^1\). The reason for this is quite simple. It is very easy to enter the building by simply following someone who lives there into the building, thus bypassing the first layer of security. Secondly, people tend to leave their doors unlocked either as a personal preference, or because they think that they’ll be back quickly. In either case, this is when most thefts occur in the dorms.

In order to counteract this problem, we are creating a dorm door lock attachment which will automatically lock any dorm door that it is attached to. One problem that arises out of a door that does this is when a student leaves their room without their key on hand. In order to prevent this from being an issue, we will be creating this attachment with alternate entry methods in mind. We will be using a pin pad and an RFID scanner to allow the student to unlock the door without the use of a key. This entire system will be battery powered with the option to plug the attachment into the wall while still on the door to simultaneously recharge the batteries while the system is in use.

1.2 Background
Lock systems are ubiquitous in today’s world and are used for a variety of purposes. Lock systems have been around for more than 6,000 years and were first seen in Egypt when a wooden post was affixed to the door, and a horizontal bolt slid into the post\(^2\). Today, locks are important to provide personal security and to prevent intruders from gaining access to unauthorized places; however, locks become inconvenient if the key is lost or forgotten inside the room.

There are many types of locks out there today which replace the typical deadbolt-key locking system. These include locks that take a PIN, fingerprint, and/or key fob (RFID). However, all of these types of locks must completely replace the deadbolt that currently exists on the door. Meaning, that if you are currently renting a space, or simply are not allowed to alter the door in question, you are unable to use any of the lock replacements that currently exist on the market. This is the niche that our product will fill in the market. Our product will be an attachment that does not alter the door permanently in any way. Thus, we will be able to reach a currently untapped market for these types of lock improvements.
1.3 High Level Requirements List

- We will implement at least two additional methods of unlocking the door: Numerical PIN keypad and RFID icard sensor.
- We will allow the student to program which methods (or combination of methods) can open the door.
- The entire device will run on one or more rechargeable batteries, which would be charged by an AC power source.
- Use power in the most efficient way possible by implementing a passive low power mode and an active high power mode.
- The door will automatically lock itself when it closes.

2 Design

2.1 Block Diagram

2.2 Physical Design

The premise for this design is that it is meant to be an attachment that fits over an existing deadbolt lock without altering it in any way. As such the side of the deadbolt on the inside of the door will have a cover over it that will turn the lock when the microcontroller determines that the door must lock or unlock. The external side of the cover will have a knob on it that the user can use to lock and unlock the door independent of the locking mechanism. This cover will also have all components on the inside of the door (i.e. everything except the PIN pad and the card scanner) attached to it just above the cover so that no one can tamper with the system from outside of the door.

There will then be an adjustable length bar going between the door frame and the door that will hold the outside components in place. This bar is adjustable to allow the user to attach and remove the cover with ease. The only things holding the lock attachment to the door is
the tension in the bar which allows the cover to hold onto the lock. We also plan to use velcro if we determine that the friction and tension is not enough to hold it on.

The outside of the door will consist of only the sensors and wiring that send the signals from the sensor back to the microcontroller on the inside of the door. Doing this ensures minimal risk of someone using information gleaned from signals from the microcontroller to break into the door using our mechanism. Ideally, the wiring will be contained within the frame of our mechanism to prevent damage to and tampering with the wiring.

2.3 Functional Overview

2.3.1 RFID
The RFID scanner acts as one of the two input options. The scanner part of the block will read a nearby card and send the card data to an arduino. The arduino will interpret the input and test it against the acceptable stored values and send a success or failure signal out of the RFID block and to the controller for interpretation.

2.3.2 Keypad
The second input is a keypad that takes in a 6 - 8 digit input from a user. This entire number is sent via data bus to the microcontroller for verification. The verification is done on the inside of the door so “open” signals can’t be spoofed from the outside.

2.3.3 Controller
The microcontroller is what makes the decision to unlock or lock the door. Input information from the RFID block, the keypad, and the proximity sensor is used to generate two bits named “lock” and “unlock” that will be output to the lock mechanism. Because of the physical implication of these bits, only one can be high at a time. During the AND mode operation (when the keypad and the RFID must both be entered) when the microcontroller determines that either of these inputs is correct it will remember that decision for a set period of time (6 seconds for example). During this time, if the second input get an affirmative signal the door will open, otherwise it will return to the wait state, waiting for both signals again.

2.3.4 UI
The user interface on the inside of the door is a set of switches that the user can use to manage which sensors are acceptable methods of unlocking the door. Each of the two sensors will have a corresponding switch that marks that sensor as “in-use” or “not in-use”. A third switch will turn on the AND functionality that would require a correct PIN and card scan. When the AND functionality is disabled, any active unlock method can be used to unlock the door. These three bits of info are sent to the microcontroller to help it decide when to send the “open” signal to the lock mechanism. There will also be reset buttons that the user will press to change the acceptable PIN and RFID codes. We will require that the correct corresponding authentication is received before the reset buttons will work.

2.3.5 Power Supply
The power supply will consist of five components. These are the AC Voltage Source, a Lithium Ion Charger, a Lithium Ion Battery, a voltage regulator, and a power led. The AC
Voltage source is simply a wall plug to provide a recharging source to the battery. It is not used at all to power the circuit. The lithium ion charger is used to recharge the battery supply within the the system. This is to ensure that the battery can last indefinitely. The lithium battery supply is used to power the circuit. This ensures that there are no security concerns from the wall power being cycled and creating errors in our system. The voltage regulator works as the name suggests and ensures that the circuit receives the correct voltage input. The power led will only turn on when the power is low to signal to the user to either plug it into the wall, or change the batteries.

2.3.6 Proximity Door Sensor
The proximity sensor will be placed at the top of the door on the inside of the room. It consists of a magnetic tag(which will be fixed on the frame of the door) and a sensor(which will be fixed on the moving part of the door at the top). Whenever the magnetic tag comes within a certain range of the sensor ( at least 0.25 to at most 0.70 inches, according to our chosen proximity sensor\(^3\)) and remains there for a certain period of time (say 5 seconds), the door will lock. When the magnetic tag goes out of range of the sensor (beyond 0.7 inches\(^3\)), the door is considered open and the door will not lock. The proximity sensor is important to add the automatic locking feature (i.e. when the door is closed for a certain period of time, it will automatically lock).

2.3.7 Lock mechanism
The lock mechanism is the physical part that unlocks and locks the deadbolt. The system takes in two bits, one to lock and one to unlock the door. These signals will turn on the motor that pushes the deadbolt handle in the corresponding direction to either lock or unlock the door.

2.4 Block Requirements

<table>
<thead>
<tr>
<th>Name of Block</th>
<th>Requirement(s)</th>
<th>Corresponding Verification Method(s)</th>
</tr>
</thead>
</table>
| Power Supply        | 1] Must provide sufficient power for operation during locking/unlocking and ensure that the circuit draws the minimum amount of power when not in use (by implementing low power modes)  
                      | 2] Malfunctions of the system in the event of loss of temporary loss of AC power are avoided                                  | 1] The locking mechanism works when a user wants to either set a new combination, change the preferred settings, wishes to unlock from outside, etc.  
                      |                                                                                                                             | 2] System works even if the power supply is lost for few minutes.                                                         |
| RFID Card Scanner   | 1] Card scanner must be able to scan any U of I id-card and transmit the information to the Arduino interface via the data bus.     | 1] Scan multiple U of I id-cards and analyze the bits received on the Arduino Interface via the data bus  
                      | 2] Card scanner must be able to go into a low-power mode when not in use to conserve power                                   | 2] Measure the power output of the card scanner when in active use and when in passive use to ensure that the power output of passive operation is significantly lower than that of active operation |
| Arduino Interface   | 1] Must successfully interpret the information received from the RFID card scanner and distinguish between different id-cards.   | 1] Use multiple cards on the RFID card scanner and distinguish between the information received on the Arduino Interface from each of the cards |
| Numerical Pin Pad   | 1] Must be able to output unique information for every                                                                         | 1] Based solely on the information received on the                                                      |
button that is pressed. Each of these unique outputs must be distinguishable on the Arduino interface. Arduino, it is possible to accurately predict which key on the numerical pin pad was pressed.

<table>
<thead>
<tr>
<th>User Interface</th>
<th>1] Must be intuitive for the user and properly labeled. 2] The user should not need a manual to tell what everything on the interface does</th>
<th>1] Show the UI to people not involved in the project and ask what each part does. If the majority answers incorrectly, we need to redesign that part.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Microcontroller</td>
<td>1] Must output the correct signals to each component depending on the state of the controller 2] Must have a method for determining the passage of time for all time based components.</td>
<td>1] Run simulations of our circuit design before creating it in a PCB 2] Ensure that the PCB output the correct signal given the correct inputs after it is created.</td>
</tr>
<tr>
<td>Lock Mechanism</td>
<td>1] Ensure that the motors for the lock mechanism can unlock as well as lock the door when necessary 2] Must be able to allow the user to operate the knob on the inside of the door without any interference from the motors</td>
<td>1] Lock the door manually and have the motors unlock it. Unlock the door and have the motors lock it. 2] Test the door knob to make sure that the design is non-invasive enough to let the user lock/unlock the door from the inside/outside without damaging the motors</td>
</tr>
<tr>
<td>Proximity Door Sensor</td>
<td>1] Make sure the 2 states of door closed, and door not closed are easily distinguishable by the sensor</td>
<td>1] Distinguish between the signals given by the proximity sensor</td>
</tr>
</tbody>
</table>

2.5 Risk Analysis
The one block in our project that may be the most difficult to make work successfully may be the lock mechanism. So far, we have come up with a design that will accomplish the goal of locking and unlocking the door when necessary. The design will involve a motor system of one or more motors (as necessary) The motor system would not be fixed directly onto the deadbolt, but would be close enough to be able to nudge the deadbolt either into the locked state or the unlocked state. A deadbolt cover for the motor system would prevent the motors from being tampered with physically. The risk here is making sure that the motors are small enough to fit onto the door and within the deadbolt cover for the motor system, but large/powerful enough to move the deadbolt.

The other difficult part of this project will be the power efficiency that is required in this circuit. We will eventually want to have the locking mechanism run solely on battery power for weeks at a time. Doing so necessitates that we implement a low power mode for our circuitry and select components that consume as little power as possible.

3 Ethics and Safety
We will be powering our circuit primarily by an AC outlet, with a lithium-ion battery acting as backup. We plan to wire it in parallel with the circuit and AC source so that the battery only draws power when it is not fully charged and only discharges when the AC source is for some reason off or unavailable. Lithium-ion batteries are very useful but they come with a number of considerations. We must never allow the battery to be short-circuited because it can easily overheat. Li-ion batteries also run the risk of thermal runaway if their temperature gets too high; we expect our low-power design to minimize the battery requirement and keep the temperature at a reasonable level. Finally we must make sure that the batteries are not exposed to a voltage outside of the acceptable voltage range by carefully designing the circuit and battery enclosure.
As this project is at its core a lock, we must carefully consider [4] IEEE Code of Ethics 9: “to avoid injuring others, their property, reputation, or employment by false or malicious action.” Users will be trusting our design to work to protect themselves and their property from harm and theft. Poor design on our part can expose users to both. We are working to add security to our design in a number of ways. First, only input signals will exist on the outside of the door so the “open” signal cannot be injected anywhere. Next, we will limit inputs such that the controller only takes inputs about once a second. This will prevent anyone on the outside from spamming, for instance, every possible keypad combination until the door opens. We can also lockout devices after a number of failed attempts to further reduce the chance of brute-forcing combinations.

Another concern is malicious resets. For instance, if one could enter the room they could hit the “reset” button and quickly program their card or a PIN so they could access the room later. Unfortunately, access to the reset button is hard to prevent because that access requires one to be inside the room, indicating the user has some level of trust in that person. The most we can do is make the reset require verification first so the only ones that can update the codes is the ones who know the current codes. This system of course still has flaws, but we have to trust that the user will not lose their card, key or write down their PIN anywhere.

References