NFC Security Deadbolt

Colin Roskos, Daniel Schroeder, Christopher McMahon
Faculty Mentor: Dr. Puteri Megat Hamari
ECET Department, Minnesota State University, Mankato

BACKGROUND

Home security is one of the most important and least thought of area of personal protection for an average consumer. An average consumer puts even less thought into the vulnerabilities that they build into their homes for the sake of convenience. With more and more homes switching their home lock systems to WiFi/IoT and Bluetooth solutions, which all have known and easily defeated vulnerabilities making your home less safe. With zero-day vulnerabilities being found freely over WiFi (Marciniak, 2019) and BlueTooth vulnerabilities where the attacker only has to see you and then visit your home to gain access (Antonioli, Tippenhauer and Rasmussen, 2019).

Mitigation of added vulnerabilities

The idea of using NFC comes from the need to have a communication that can be secured, can't be listened in on, and is difficult to man-in-the-middle. This combined with a reputable physical lock can make for a more secure alternative while still being a convenient solution.

PROPOSED SOLUTION

Our proposed solution (Figure 1) is comprised of two major components and three minor components. (1) The Phone System, an Android application (Figure 2) on an NFC enabled device, (2a) The Software/Embedded Hardware component of the Lock System which is comprised of an Arduino (Figure 3) and an NT3H2111 chip mounted on a Tag2 click board (Figure 4), (2b) The physical door lock system (Figure 5) whose body is a off-the-shelf Lockly Model 7s. This lock has no connection to WiFi/Internet and no Bluetooth connectivity to avoid known and future unknown vulnerabilities.

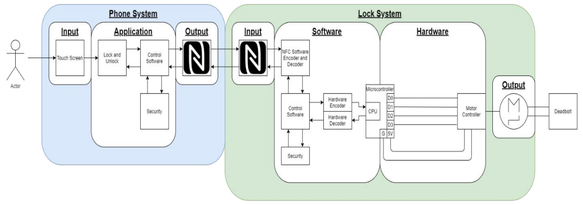
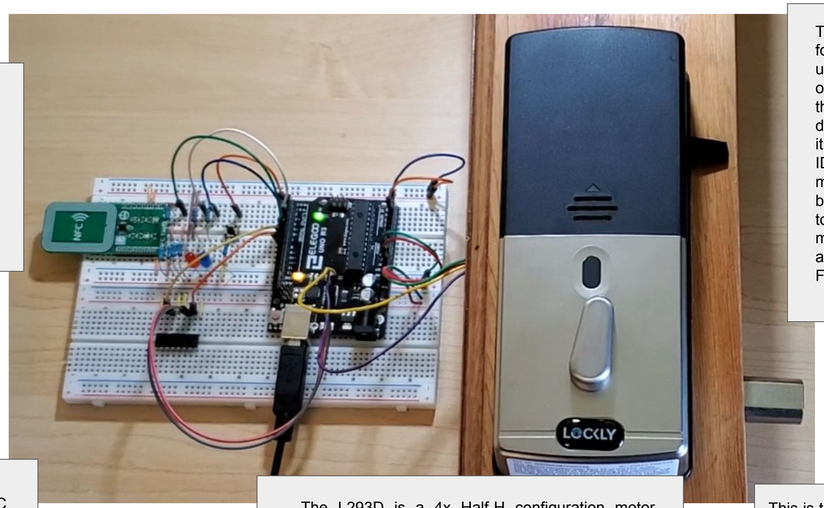


Figure 1

SYSTEM DESIGN

Figure 5
Lockly 7s

The locking mechanism used for our prototype was selected because of its design capability. This lock was designed to be actuated with a key, code, bluetooth application, and wifi application. Since the lock was already able to be actuated by an application, we utilized the internal motor and gears in conjunction with our NFC circuit to operate the locking mechanism.



This is an image of the Android application for NFC communication. This application utilizes the NFC API for android devices in order to communicate with the NFC tag on the breadboard. The application waits until it detects the field of an NFC tag, at which point it will send the UDID of the phone to it. That ID will then be processed by the microcontroller, after which a certain code will be sent back to the phone. This code is used to notify the phone of the action taken by the microcontroller, displaying a message such as "Matching Key Found," "No Matching Key Found," "Device Successfully Paired," etc...

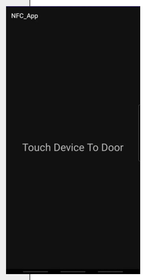


Figure 2
Samsung
Galaxy S10

Figure 4
NFC Module

NFC module, using an NT3H2111 chip as an NFC controller module. The NT3H2111 has built-in I2C for easy communication and interaction with the microcontroller and easy read/write access for interfacing with the Phone System.

Figure 6
Motor driver

The L293D is a 4x Half-H configuration motor driver to drive the internal 5V DC motor. We configured this motor using two Half-H's for use as a powered H-Bridge to power the lock's internal 5V DC motor.

Figure 3
Arduino Uno

This is the SBC Arduino Uno which utilizes the ATMEGA processor. After a phone is touched to the NFC tag, the UDID of the device will be sent to the microcontroller. Depending on the current state of the microcontroller, this ID may be used in several different manners. For example, the main use of this ID is to be compared against a list of values store in the microcontrollers EEPROM. If the ID of the phone is found, it will unlock and lock the door, otherwise, it will keep it locked.

FUTURE DIRECTION

- Design a custom case for the locking mechanism
- Implementation of a stronger factor of security
- Implementation of a smaller NFC module
- Implementation of a PCB
- Implement an embedded, high efficiency processor
- Extend battery life

ACKNOWLEDGEMENTS

We would like to thank our Junior Design professor, Dr. Puteri Megat Hamari.

REFERENCES

Antonioli, Daniele, et al. "BIAS: Bluetooth Impersonation AttackS." 2020 IEEE Symposium on Security and Privacy (SP), 2019, doi:10.1109/sp40000.2020.00093.

K. Marciniak, Digital lockpicking - stealing keys to the kingdom, 11-Dec-2019. [Online]. Available: https://labs.f-secure.com/blog/digital-lockpicking-stealing-keys-to-the-kingdom. [Accessed: 22-Apr-2021].

CONTACT INFORMATION

Feel free to contact us at daniel.schroeder-2@mnsu.edu, colin.roskos@mnsu.edu, and christopher.mcmahon@mnsu.edu with any questions