DESIGNING A LOCK AND HOME SECURITY SYSTEM TO PREVENT PORCH PACKAGE THEFT

(Technical Paper)

AN INVESTIGATION OF THE IMPACT OF TIERED HOME ACCESS SECURITY

(STS Paper)

A **Thesis Prospectus** submitted to the

Faculty of the School of Engineering and Applied Science
University of Virginia | Charlottesville, Virginia

In partial fulfillment of the requirements of the degree
Bachelor of Science, School of Engineering

Derek Martin
Technical Portion written in collaboration with
John Chrosniak, AJ Given, and Jamison Stevens
October 2021

On my honor as a University Student, I have neither given nor received unauthorized aid on this assignment as defined by the Honor Guidelines for Thesis-Related Assignments.

Signature Derek Martin Date 5/7/22
Derek Martin

Approved _____ Date 27 November 2021
Richard Jacques, Department of Engineering and Society

Approved _____ Date May 11,2022
Harry C. Powell, Department of Electrical and Computer Engineering

Introduction

Since the start of the Coronavirus pandemic, more individuals are opting for online shopping experiences to stay healthy, while potentially saving more time and money. However, as society is starting to return to more pre-pandemic lifestyles, this increased shopping has led to the unintended consequence of increased opportunities for package pirates to raid people's front porches and package rooms ("Package Thieves Thrive During Pandemic.," 2020). The improved home security system uses a digitally controlled locking system that offers keyless entry through a master code or limited-use password, as well as video recording for added security. The owner will use the master code to unlock the system and set limited-use passwords for guests that should have only temporary access. The limited-use passwords unlock the system for either a single use or a predetermined duration so that package deliverers can store packages in a secure place until the owner returns. Consumers can use the device on a standard door, a pet door-equivalent for packages, or a package box, depending on the user's security preferences. This project involves the use of a microcontroller with wireless capabilities, keypad to enter a passcode, and an interface to control the door-locking hardware. This project was seen as an opportunity to prevent package thefts and provide secure and easy to manage tiered home security access.

Technical Project Description

The security system consists of an external keypad, a web app to program the system, and a camera. The system allows the owner to register a root user password that can be entered internally to program the device. The device allows single use or fixed duration passwords to be generated along with a nickname. The passwords generated are cryptographically secure and

random so that the owner doesn't have to worry about creating secure passwords and the chances of someone guessing a valid passcode even after being assigned one is negligibly small. Every time a passcode is entered, the system stores a timestamp along with the nickname corresponding to the valid code so that the owner can monitor which user entered the house at what time. Each time the door is unlocked, the camera is activated to record a video of the person attempting to enter the house. This camera deactivates when the door is locked again, or after 30 seconds if the door is left unlocked. This video is then sent to an AWS hosted server to store the data for future viewing within the app.

The system is designed using KiCad, a tool used to convert electrical circuit schematics into Printed Circuit Board (PCB) designs. The software for this project will run on a Raspberry Pi computer that connects directly to the external keypad, camera, and interfaces via Wi-Fi to a cloud hosted AWS server which can be accessed through a web application. The Pi will also connect to an electric strike locking mechanism which can be passed a current to lock or unlock the door. The camera will be powered by the circuit board, and the board will be connected to a dual power supply that connects directly into the AC line of the house through an outlet and connects to a backup rechargeable battery supply, so the house is still accessible even if the power goes out. If the home power does go out, the device cannot program new codes, but all existing codes remain valid for the previously set bounds and all video footage will be stored locally on the device until power is restored and the device can send all of the saved footage to the cloud. The rechargeable batteries are designed to last multiple days on their own so if an adversary cuts the power to your home hoping to break in, they would have to wait around for an extended period, which is far greater effort than breaking into a house through a window and

would attract attention from neighbors making this method of forced entry not the path of least resistance for a burglar.

The user interface for programming the device is a web application written in Python using the Flask framework. This interface is laid out with separate pages for viewing and deleting video footage, monitoring which codes were used when, and a page for managing existing passcodes. When the video footage page is loaded, the application checks the cloud storage and displays all videos saved there, as well as when each video was recorded and the nickname associated with the code entered. The user can then choose to delete specific video clips from within the application, which permanently deletes the videos from the cloud. When creating a new code or updating an existing one within the passcode manager page of the website, the changes are pushed up to the cloud where the Raspberry Pi reads and updates the information stored locally once a minute. This process allows the device to save resources by not constantly checking for updates, but checks enough to not interfere with daily use.

STS Project Details

As discussed, the issue of porch package theft has increased in prevalence over the past few years. Many products working to address this issue act to deter potential thieves using motion-activated cameras and do nothing to guarantee safety of packages (Morris, 2021). Most existing electronic locks do not allow for dynamic update conditions and use fingerprint or keypad entry that replaces a physical key, but still require human configuration and management. (Xin et al., 2020) This method creates security risks of its own by leaving your home exposed

every time an access code is shared, until the owner manually changes or removes the shared code.

To improve secure home access, you must optimize the tradeoff between security and upkeep time and effort. On the extreme ends is a security system where each time someone wants to enter, the owner must screen them and authorize them manually, and a house that doesn't lock. As established above, we wish to improve home security by allowing it to dynamically update, so our baseline will be passcode entry where passcodes can only ever be entered once. This procedure is secure as the owner prescreens each entry, and saves time by not requiring the owner to be present or approve of the entry at the time of entry. With each code deleted after a single use, someone being given entry to your house once does not mean they can return for nefarious purposes later. This method falls short, however, in that there are cases where you want to provide access for more than one use and the owner has the added effort of generating and distributing an additional code. This process also creates a problem of someone exiting your house and leaving something inside, or realizing they did not complete the task you wanted them to do by giving them access in the first place, thus requiring an additional code that is not readily available to them.

This system can be further improved by checking additional factors before granting entry. By allowing the owner to specify attributes for each user, such as a time range or number of entries per day, the screening process can be handled in advance as before, while also providing more structured entry (Chin et al., 2010). If someone, such as a housekeeper, is only to be entering your house on Mondays between 8 and 10 am, this improved system ensures that both the housekeeper cannot return at an unexpected time and steal from you and if the housekeeper's code is exposed to someone else who wishes to steal from you the code will not

allow them to enter except during that specific time. These added constraints also solve the problem with the previous system of needing to generate the second code if the user mistakenly locks themselves out, as the owner can set conditions to allow an additional entry before locking out that specific code if it is entered a short duration after the first entry. This in advance screening process does create additional overhead for the owner as they must fill out the details of each user before the first entry, but the settings can carry over saving time in the long run. This feature also requires that the owner knows specific information about the user at the time of programming the device as they risk improperly denying entry or increasing complexity of the system without improving its security (Xin et al., 2020).

The security system can be expanded one step further in the case that one central system is controlling multiple locks such as a property manager. Individual access can be adjusted to also be location specific so that for example the owner can access any property and assign codes to any property, while individual tenants can access and assign access to only their specific property. This protocol will allow security for all parties while also allowing maintenance people to access whatever property they need with only a single code.

A similar system can be created to apply to secure package or mail delivery if a security system was designed in conjunction with delivery companies to allow delivery drivers to have a unique code tied to their employee identification that would be assigned to limited access to houses or package boxes based on the location for individual homes and the time corresponding to the anticipated delivery time within the delivery companies' internal system.

Conclusion

Package theft continues to be a be an issue not fully addressed by modern home security systems. With entry to one's house being something so carefully protected, it is increasingly necessary to design a system that allows for efficient access while preventing the spread of long term or permanent access. This home security can most securely be accomplished using a combination of dynamically updating passcode access and attribute-based access control. The former used to eliminate periods of home exposure before the owner deletes a password given out to the third party that is no longer to have access and the latter to ensure that because an individual possess a valid passcode does not mean they automatically gain entry to your home. We hope to design a physical system capable of implementing such a secure method of access control, and designing a software system that runs on it to take advantage of said control.

Word Count: 1721

References

Chin, S.-K., Older, S. B., & Stinson, D. R. (2010). *Access Control, Security, and Trust: A Logical Approach*. CRC Press LLC.

Morris, J. (2021). SURVEILLANCE BY AMAZON: THE WARRANT REQUIREMENT, TECH EXCEPTIONALISM, & RING SECURITY. *Journal of Science & Technology Law*, *27*(1), 237–269. Computers & Applied Sciences Complete.

Package Thieves Thrive During Pandemic. (2020). *USA Today Magazine*, *149*(2907), 10–10. MasterFILE Premier.

Xin, Z., Liu, L., & Hancke, G. (2020). AACS: Attribute-Based Access Control Mechanism for Smart Locks. *Symmetry (20738994)*, *12*(6), 1050–1050. Academic Search Complete.