Authentication Mechanisms Using Raspberry Pi

Matthew Kendrick D. Co
`matthewdeeco@gmail.com`

Jon Kiefer S. Yap
`kiefer.yap@gmail.com`

April 24, 2015

Abstract

Modern keyless door security systems remain largely inaccessible to the public, due to their high cost and low transparency. Our system, SpoonPi, is a cost-effective solution that is designed to be intuitive to use, and easy to customize or extend. It supports five different authentication mechanisms involving three factors: RFID, fingerprint and PIN. The single-door security provided by SpoonPi easily scales to multiple doors via the accompanying web app, ForkPi, which provides secure, centralized management of multiple SpoonPis over a local network.

By choosing Raspberry Pi as the platform, we are able to open source the code, and make the system easy to replicate. In this paper, we discuss the details of our design and implementation, and evaluate our system in terms of security, usability, and cost-effectiveness. We find that the system possesses a viable level of security, users find it easy to use, and it is reasonably priced for a system of its capability.

1 Introduction

Modern keyless door security systems are still largely inaccessible, primarily due to their high cost [2]. As a result, such systems are currently confined in the business setting. Moreover, most door security systems are proprietary black boxes, meaning their code is closed to the public, and their components are non-removable and non-interchangeable. Without knowing what is under the hood, end users cannot tweak the code to suit their private needs, and should a component fail, they are left with no choice but to replace the entire unit.

The goal of this study is to create a door security solution that is more accessible to the public, by lowering the acquisition cost, releasing the code publicly, and making the individual components customizable. Anyone should be able to replicate the entire system simply by assembling the components, and running our code.

There are two main components to our system. SpoonPi is the component that is installed onto doors; it is responsible for allowing or denying users access. ForkPi is the component where you register new users; it is responsible for maintaining the database that all SpoonPis will access. There are as many SpoonPis as there are doors to be secured, but only one ForkPi for the entire network. To save on resources, the single ForkPi unit can also function as a SpoonPi unit, although there are some drawbacks to this set-up which will be discussed later on.

Our system supports five authentication mechanisms: single-factor RFID, single-factor fingerprint, RFID & PIN, fingerprint & PIN, and RFID & fingerprint. There are no system-wide constraints with regards to the mechanism to be used. Users can choose to authenticate using any combination they wish; SpoonPi can handle all five mechanisms by default.

2 Background

2.1 Authentication Factors

To pass through a locked door, a person would need to present one or more authentication factors. In traditional keyed doors, that factor would be a single (metal) key, which is an example of a possession-based factor. Possesion-based is one of three major types of authentication factors:

1. **Knowledge**: Something the user knows (e.g. PINs)
2. **Possession**: Something the user has (e.g. RFID cards)
3. **Inherence** or **Biometrics**: Something the user is (e.g. fingerprints)

Each factor type has its own strengths and weaknesses, as illustrated in the table below. For consistency, each criterion is stated such that a Y is an advantage.

	Knowledge	Possession	Inherence
Does not generate false positives/negatives	Y	Y	
Does not have to be carried around	Y		Y
Cannot be cloned or stolen	Y		Y[2]
Cannot be guessed by brute force		Y[1]	Y
Fast input and processing time		Y	
Cannot be lost or forgotten			Y[3]

[1] RFID security can be brute forced if the RFID reader can be spoofed by cards with reprogrammed UIDs (unique identifiers). The attacker can simply try all possible UIDs by repeatedly changing the UID on the same card.

[2] Fingerprints can be cloned if the scanner cannot distinguish between real and replicated fingerprints.

[3] People can lose their fingerprints, but it is a much rarer event than losing keys or forgetting passwords.

2.2 Authentication Mechanisms

In choosing the appropriate authentication mechanism to use for a door security system, one needs to consider each factor type's strengths and weaknesses as mentioned above. For example, if only RFID security is employed, it would be easy for a thief to steal a card and grant himself access. This vulnerability can be solved by employing fingerprints instead, as those cannot be stolen, but in turn, it will make the system unreliable. Depending on the accuracy of the fingerprint matching algorithm, authorized persons might be denied access, or worse, unauthorized persons might be granted access.

However, modern door security systems are not limited to employing only a single factor. Multi-factor authentication is a common way to combine the strengths and mitigate the weaknesses of individual factors. For example, before withdrawing money from an ATM (Automated Teller Machine), one has to present his/her ATM card (a possession-based factor) followed by the PIN (a knowledge-based factor). Gunson et al. [1] observed that users find single-factor to be more convenient and easier to use, while multi-factor is more secure but takes longer to complete.

2.3 Raspberry Pi

After deciding the authentication mechanism/s to be used, a device would be needed to control all the necessary peripherals. For example, in a two-factor RFID & fingerprint security system, the peripherals would be the RFID reader, the fingerprint scanner, the electric lock, and optionally the display. This device can be either a computer or a microcontroller, and should preferably be cheap and small since one unit would have to be embedded on each door.

The Raspberry Pi is an example of one such device. It is a credit-card sized computer that comes with pins that can be used to communicate with or provide power to peripherals. The Raspberry Pi model we have, Model B [3], is an obsolete model that costs $35, uses an SD card for storage, and comes with 26 pins, 2 USB ports and 512 MB RAM. For the same price, one can buy the newer and better Raspberry Pi 2 Model B [4] instead, which uses a micro SD card for storage, comes with 40 pins, 4 USB ports and 1 GB RAM. Both models have an ethernet port and an HDMI port for video output.

3 Related Work

In this section, we look at similar door security systems that are available, and compare their features with our system's. "Capacity" refers to the maximum number of users that can be registered at any given time. For fingerprint accuracy, "FAR" (false acceptance rate) refers to the rate at which unregistered fingerprints turn out a match, while "FRR" (false rejectionr rate) refers to the rate at which registered fingers turn out no match.

3.1 Commercial Systems

These systems are readily available on the market. Since they are prepackaged and mass produced, the total cost is cheaper than if you had bought the parts individually and assembled it yourself.

3.1.1 CD-R King Time Attendance System

Supported factors: RFID, Fingerprint, PIN
Capacity: 2000 users
Fingerprint accuracy: FAR $< 0.0001\%$, FRR $< 0.1\%$
PIN length: Any length

3.1.2 F6 Fingerprint Access Control

Supported factors: RFID, Fingerprint, PIN
Capacity: 500 users
Fingerprint accuracy: FAR $< 0.0001\%$, FRR $< 0.01\%$
PIN length: 4-6 digits

3.2 Open Source Systems

3.2.1 Pi-Lock

Supported factors: RFID, PIN
Platform: Raspberry Pi
Capacity: Proportional to SD card capacity
PIN length: 4 digits

3.2.2 Open Access Control

Supported factors: RFID, PIN
Platform: Arduino
Capacity: 200 users
PIN length: Any length

4 Design & Architecture

4.1 Hardware Configuration

4.2 Software Overview

5 Implementation

5.1 SpoonPi

5.2 ForkPi

6 Evaluation

6.1 Security

6.2 Usability

6.3 Cost-effectiveness

7 Future Work and Conclusion

References

[1] Nancie Gunson, Diarmid Marshall, Hazel Morton, and Mervyn Jack. User perceptions of security and usability of single-factor and two-factor authentication in automated telephone banking. *computers & security*, 30(4):208–220, 2011.

[2] Pros and cons of a keyless door entry, October 2014. http://www.locksmithorting.com/pros-and-cons-of-a-keyless-door-entry. Last accessed 18 April 2015.

[3] Raspberry Pi 1 Model B+. https://www.raspberrypi.org/products/model-b-plus/. Last accessed 19 April 2015.

[4] Raspberry Pi 2 Model B. https://www.raspberrypi.org/products/raspberry-pi-2-model-b/. Last accessed 19 April 2015.