Authentication Mechanisms Using Raspberry Pi

Jon Kiefer S. Yap   Matthew Kendrick D. Co

University of the Philippines Diliman

May 30, 2015

Outline

Introduction

- The following are properties of modern keyless door access control systems:

[1] *Pros and Cons of a Keyless Door Entry*. http://www.locksmithorting.com/pros-and-cons-of-a-keyless-door-entry. Accessed: 2015-04-18. Oct. 2014.

Introduction

- The following are properties of modern keyless door access control systems:
  - They are still largely inaccessible, primarily due to their high cost[1].

[1] *Pros and Cons of a Keyless Door Entry*. http://www.locksmithorting.com/pros-and-cons-of-a-keyless-door-entry. Accessed: 2015-04-18. Oct. 2014.

Introduction

- The following are properties of modern keyless door access control systems:
  - They are still largely inaccessible, primarily due to their high cost[1].
  - Their code is closed to the public.

[1] *Pros and Cons of a Keyless Door Entry*. http://www.locksmithorting.com/pros-and-cons-of-a-keyless-door-entry. Accessed: 2015-04-18. Oct. 2014.

Introduction

- The following are properties of modern keyless door access control systems:
  - They are still largely inaccessible, primarily due to their high cost[1].
  - Their code is closed to the public.
  - Their components are non-removable, and non-interchangeable.

[1] *Pros and Cons of a Keyless Door Entry.* http://www.locksmithorting.com/pros-and-cons-of-a-keyless-door-entry. Accessed: 2015-04-18. Oct. 2014.

Introduction

- The following are properties of modern keyless door access control systems:
  - They are still largely inaccessible, primarily due to their high cost[1].
  - Their code is closed to the public.
  - Their components are non-removable, and non-interchangeable.
- As a result:

[1] *Pros and Cons of a Keyless Door Entry*. http://www.locksmithorting.com/pros-and-cons-of-a-keyless-door-entry. Accessed: 2015-04-18. Oct. 2014.

Introduction

- The following are properties of modern keyless door access control systems:
  - They are still largely inaccessible, primarily due to their high cost[1].
  - Their code is closed to the public.
  - Their components are non-removable, and non-interchangeable.
- As a result:
  - End users cannot tweak the code to suit their private needs.

[1] *Pros and Cons of a Keyless Door Entry*. http://www.locksmithorting.com/pros-and-cons-of-a-keyless-door-entry. Accessed: 2015-04-18. Oct. 2014.

Introduction

- The following are properties of modern keyless door access control systems:
  - They are still largely inaccessible, primarily due to their high cost[1].
  - Their code is closed to the public.
  - Their components are non-removable, and non-interchangeable.
- As a result:
  - End users cannot tweak the code to suit their private needs.
  - Component failure results to contacting the manufacturing company, potentially resulting to replacing the entire unit.

[1] *Pros and Cons of a Keyless Door Entry.* http://www.locksmithorting.com/pros-and-cons-of-a-keyless-door-entry. Accessed: 2015-04-18. Oct. 2014.

Overview (1 of 5)

- The goal of this study is to make a hardware-based authentication system that is more accessible to the public, implementing the following characteristics:

[2] Jaap-Henk Hoepman and Bart Jacobs. "Increased security through open source". In: *Communications of the ACM* 50.1 (2007), pp. 79–83.

Overview (1 of 5)

- The goal of this study is to make a hardware-based authentication system that is more accessible to the public, implementing the following characteristics:
  - **Do-it-yourself**: The system can be replicated by assembling the components, and running our code. This is to improve overall transparency – users are more likely to trust a system if they know how exactly it was made.

[2] Jaap-Henk Hoepman and Bart Jacobs. "Increased security through open source". In: *Communications of the ACM* 50.1 (2007), pp. 79–83.

Overview (1 of 5)

- The goal of this study is to make a hardware-based authentication system that is more accessible to the public, implementing the following characteristics:
  - **Do-it-yourself**: The system can be replicated by assembling the components, and running our code. This is to improve overall transparency – users are more likely to trust a system if they know how exactly it was made.
  - **Open Source Code**: We have documented our code extensively so that users can easily modify or extend the system functionality. Hoepman and Jacobs[2] found that keeping the source open improves security, because all interested parties can test for vulnerabilities, and promptly fix them.

[2] Jaap-Henk Hoepman and Bart Jacobs. "Increased security through open source". In: *Communications of the ACM* 50.1 (2007), pp. 79–83.

Overview (2 of 5)

- **Increased Flexibility**: Although our system supports multiple authentication methods, users do not have to buy a component they will not use. However, should the need arise, they can easily connect the said component later on. This is an advantage over propriety systems, which typically come as a package and can no longer be modified or extended.

Overview (2 of 5)

- **Increased Flexibility**: Although our system supports multiple authentication methods, users do not have to buy a component they will not use. However, should the need arise, they can easily connect the said component later on. This is an advantage over propriety systems, which typically come as a package and can no longer be modified or extended.
- **Can run on top of existing networks**: Our system uses plain local ethernet for communication between the server and the door controllers. This lessens the cost of hardware set-up and maintainance, and also makes the system more scalable because there is no hard limit on the number of controllable doors.

Overview (3 of 5)

- **Encrypted database and data transmission**: We have designed the system such that no sensitive information is transmitted in plaintext over the network. In the door controller, the data is hashed first before being sent to the server; while in the database, credentials are not stored in plaintext; Instead, they are hashed or symmetrically encrypted.

[3] *BarcodesInc Search: Category: Access Control.* http://www.barcodesinc.com/p/subcategory=Access_Control/. Accessed: 2015-04-26.

Overview (3 of 5)

- **Encrypted database and data transmission**: We have designed the system such that no sensitive information is transmitted in plaintext over the network. In the door controller, the data is hashed first before being sent to the server; while in the database, credentials are not stored in plaintext; Instead, they are hashed or symmetrically encrypted.
- **Low Acquisition Cost**: The cost of a single access control device typically ranges from \$100 to \$350 (based on the prices listed at the online store BarcodesInc[3]). The combined cost of our system's components falls within the lower end of that range.

[3] *BarcodesInc Search: Category: Access Control.* http://www.barcodesinc.com/p/subcategory=Access_Control/. Accessed: 2015-04-26.

Overview (4 of 5)

- There are two main components to our system:

Overview (4 of 5)

- There are two main components to our system:
  - **SpoonPi**: the application that controls the door locks; it is responsible for allowing or denying users access.

Overview (4 of 5)

- There are two main components to our system:
  - **SpoonPi**: the application that controls the door locks; it is responsible for allowing or denying users access.
  - **ForkPi**: the web application that is responsible for registering new users, and for maintaining the database that all the SpoonPis will access.

Overview (4 of 5)

- There are two main components to our system:
  - **SpoonPi**: the application that controls the door locks; it is responsible for allowing or denying users access.
  - **ForkPi**: the web application that is responsible for registering new users, and for maintaining the database that all the SpoonPis will access.
- There are as many SpoonPis as there are doors to be secured, but only one ForkPi for the entire network.

Overview (5 of 5)

- Our system supports five authentication mechanisms:

Overview (5 of 5)

- Our system supports five authentication mechanisms:
  - Single-Factor RFID

Overview (5 of 5)

- Our system supports five authentication mechanisms:
    - Single-Factor RFID
    - Single-Factor Fingerprint

Overview (5 of 5)

- Our system supports five authentication mechanisms:
  - Single-Factor RFID
  - Single-Factor Fingerprint
  - Two-Factor RFID and PIN

Overview (5 of 5)

- Our system supports five authentication mechanisms:
  - Single-Factor RFID
  - Single-Factor Fingerprint
  - Two-Factor RFID and PIN
  - Two-Factor Fingerprint and PIN

Overview (5 of 5)

- Our system supports five authentication mechanisms:
  - Single-Factor RFID
  - Single-Factor Fingerprint
  - Two-Factor RFID and PIN
  - Two-Factor Fingerprint and PIN
  - Two-Factor Fingerprint and RFID

Overview (5 of 5)

- Our system supports five authentication mechanisms:
  - Single-Factor RFID
  - Single-Factor Fingerprint
  - Two-Factor RFID and PIN
  - Two-Factor Fingerprint and PIN
  - Two-Factor Fingerprint and RFID
- There are no system-wide constraints with regards to the mechanism to be used. Each user can choose to authenticate using any combination they wish; SpoonPi can handle all five mechanisms by default.

Three Major Factors

Authentication is performed using various **factors**, which can be classified into three major types:

1. **Knowledge**: Something the entity knows (e.g. passwords)
2. **Biometrics**: Something the entity is (e.g. fingerprints)
3. **Possession**: Something the entity has (e.g. RFID tags)

Factor Strengths and Weaknesses

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

	Knowledge	Possession	Inherence

Factor Strengths and Weaknesses

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

	Knowledge	Possession	Inherence
Does not generate false positives/negatives	Y	Y	

Factor Strengths and Weaknesses

Each factor type has its own strengths and weaknesses, as illustrated in the following table. 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

Factor Strengths and Weaknesses

Each factor type has its own strengths and weaknesses, as illustrated in the following table. 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[3]

Factor Strengths and Weaknesses

Each factor type has its own strengths and weaknesses, as illustrated in the following table. 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[3]
Cannot be guessed by brute force		Y[1]	Y

Factor Strengths and Weaknesses

Each factor type has its own strengths and weaknesses, as illustrated in the following table. 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[3]
Cannot be guessed by brute force		Y[1]	Y
Fast input and processing time		Y[2]	

Factor Strengths and Weaknesses

Each factor type has its own strengths and weaknesses, as illustrated in the following table. 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[3]
Cannot be guessed by brute force		Y[1]	Y
Fast input and processing time		Y[2]	
Cannot be lost or forgotten			Y[4]

Factor Strengths and Weaknesses

Each factor type has its own strengths and weaknesses, as illustrated in the following table. 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[3]
Cannot be guessed by brute force		Y[1]	Y
Fast input and processing time		Y[2]	
Cannot be lost or forgotten			Y[4]

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

Factor Strengths and Weaknesses

Each factor type has its own strengths and weaknesses, as illustrated in the following table. 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[3]
Cannot be guessed by brute force		Y[1]	Y
Fast input and processing time		Y[2]	
Cannot be lost or forgotten			Y[4]

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

[2] In the case of RFID

Factor Strengths and Weaknesses

Each factor type has its own strengths and weaknesses, as illustrated in the following table. 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[3]
Cannot be guessed by brute force		Y[1]	Y
Fast input and processing time		Y[2]	
Cannot be lost or forgotten			Y[4]

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

[2] In the case of RFID

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

Factor Strengths and Weaknesses

Each factor type has its own strengths and weaknesses, as illustrated in the following table. 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[3]
Cannot be guessed by brute force		Y[1]	Y
Fast input and processing time		Y[2]	
Cannot be lost or forgotten			Y[4]

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

[2] In the case of RFID

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

[4] People can lose their fingerprints, but it is a much rarer event than losing keys or

Authentication Mechanisms

- **Knowledge-Based**: PINs were chosen over passwords due to its more specialized key set, which means the SpoonPi units do not require a full keyboard for input.

Authentication Mechanisms

- **Knowledge-Based**: PINs were chosen over passwords due to its more specialized key set, which means the SpoonPi units do not require a full keyboard for input.
- **Possession-Based**: RFID cards were chosen because they are cheaper than smart cards, and more difficult to replicate than barcodes.

Authentication Mechanisms

- **Knowledge-Based**: PINs were chosen over passwords due to its more specialized key set, which means the SpoonPi units do not require a full keyboard for input.
- **Possession-Based**: RFID cards were chosen because they are cheaper than smart cards, and more difficult to replicate than barcodes.
- **Inherence-based**: Fingerprint was chosen because it is the most prevalent and well-supported biometric.

Why Raspberry Pi (1 of 2)

- After deciding the authentication mechanism/s to be used, a device would be needed to control all the necessary peripherals.

Why Raspberry Pi (1 of 2)

- After deciding the authentication mechanism/s to be used, a device would be needed to control all the necessary peripherals.
- 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.

Why Raspberry Pi (1 of 2)

- After deciding the authentication mechanism/s to be used, a device would be needed to control all the necessary peripherals.
- 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.

Why Raspberry Pi (2 of 2)

- The Raspberry Pi model we used for development, Model B[4], is an outdated model that costs $35, uses an SD card for storage, and comes with 26 pins, 2 USB ports and 512 MB RAM.

[4] *Raspberry Pi 1 Model B+*. https://www.raspberrypi.org/products/model-b-plus/. Accessed: 2015-04-19.

[5] *Raspberry Pi 2 Model B*. . https://www.raspberrypi.org/products/raspberry-pi-2-model-b/. Accessed: 2015-04-19.

Why Raspberry Pi (2 of 2)

- The Raspberry Pi model we used for development, Model B[4], is an outdated 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[5] 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.

---

[4] *Raspberry Pi 1 Model B+*. https://www.raspberrypi.org/products/model-b-plus/. Accessed: 2015-04-19.

[5] *Raspberry Pi 2 Model B*. . https://www.raspberrypi.org/products/raspberry-pi-2-model-b/. Accessed: 2015-04-19.

Outline

Related Work (1 of 2)

- In this section, we look at existing and similar door access control systems, and compare their features with ours.

Related Work (1 of 2)

- In this section, we look at existing and similar door access control systems, and compare their features with ours.
- The main specifications we will be looking at are the following:

Related Work (1 of 2)

- In this section, we look at existing and similar door access control systems, and compare their features with ours.
- The main specifications we will be looking at are the following:
  - Supported factors

Related Work (1 of 2)

- In this section, we look at existing and similar door access control systems, and compare their features with ours.
- The main specifications we will be looking at are the following:
  - Supported factors
  - User capacity

Related Work (1 of 2)

- In this section, we look at existing and similar door access control systems, and compare their features with ours.
- The main specifications we will be looking at are the following:
  - Supported factors
  - User capacity
  - Fingerprint accuracy

Related Work (1 of 2)

- In this section, we look at existing and similar door access control systems, and compare their features with ours.
- The main specifications we will be looking at are the following:
  - Supported factors
  - User capacity
  - Fingerprint accuracy
  - PIN lengths supported

Related Work (1 of 2)

- In this section, we look at existing and similar door access control systems, and compare their features with ours.
- The main specifications we will be looking at are the following:
  - Supported factors
  - User capacity
  - Fingerprint accuracy
  - PIN lengths supported
  - Target platform

Related Work (2 of 2)

- Definitions:

Related Work (2 of 2)

- Definitions:
  - **Capacity** maximum number of users that can be registered

Related Work (2 of 2)

- Definitions:
  - **Capacity** maximum number of users that can be registered
  - **FAR** (False Acceptance Rate): the rate at which fingerprints are accepted despite not having registered

Related Work (2 of 2)

- Definitions:
  - **Capacity** maximum number of users that can be registered
  - **FAR** (False Acceptance Rate): the rate at which fingerprints are accepted despite not having registered
  - **FRR** (False Rejection Rate): the rate at which fingerprints are rejected despite having registered

Commercial Systems

- The access control systems we will be looking at are the following:

Commercial Systems

- The access control systems we will be looking at are the following:
  - F6 Fingerprint Access Control

Commercial Systems

- The access control systems we will be looking at are the following:
  - F6 Fingerprint Access Control
  - CD-R King 2.8" Full Colored Biometric

Commercial Systems

- The access control systems we will be looking at are the following:
  - F6 Fingerprint Access Control
  - CD-R King 2.8" Full Colored Biometric
  - HID iCLASS RPK40 Access Control Device

F6 Fingerprint Access Control

- **Supported Factors**: RFID, Fingerprint, PIN

[6] *F6 Fingerprint, RFID & PIN Reader*. http://www.secukey.com.cn/eshowProDetail.asp?ProID=1908. Accessed: 2015-04-26.

[7] *F6 Fingerprint/Keypad/Proximity Access Contol*.

F6 Fingerprint Access Control

- **Supported Factors**: RFID, Fingerprint, PIN
- **Capacity**: 500 users

[6] *F6 Fingerprint, RFID & PIN Reader*. http://www.secukey.com.cn/eshowProDetail.asp?ProID=1908. Accessed: 2015-04-26.

[7] *F6 Fingerprint/Keypad/Proximity Access Contol*.

F6 Fingerprint Access Control

- **Supported Factors**: RFID, Fingerprint, PIN
- **Capacity**: 500 users
- **Fingerprint Accuracy**: FAR $< 0.0001\%$, FRR $< 0.01\%$

[6] *F6 Fingerprint, RFID & PIN Reader*. http://www.secukey.com.cn/eshowProDetail.asp?ProID=1908. Accessed: 2015-04-26.

[7] *F6 Fingerprint/Keypad/Proximity Access Contol*.

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

[6] *F6 Fingerprint, RFID & PIN Reader*. http://www.secukey.com.cn/eshowProDetail.asp?ProID=1908. Accessed: 2015-04-26.

[7] *F6 Fingerprint/Keypad/Proximity Access Contol*.

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
- **Description**:

[6] *F6 Fingerprint, RFID & PIN Reader*. http://www.secukey.com.cn/eshowProDetail.asp?ProID=1908. Accessed: 2015-04-26.

[7] *F6 Fingerprint/Keypad/Proximity Access Contol*.

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
- **Description**:
    - F6 Fingerprint Access Control is a product of Secukey[6], and supports authentication using all three factors that we implemented for our system.

[6] *F6 Fingerprint, RFID & PIN Reader*. http://www.secukey.com.cn/eshowProDetail.asp?ProID=1908. Accessed: 2015-04-26.

[7] *F6 Fingerprint/Keypad/Proximity Access Contol*.

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
- **Description**:
  - F6 Fingerprint Access Control is a product of Secukey[6], and supports authentication using all three factors that we implemented for our system.
  - Its price, $30 in ECPlaza[7], is much lower than our system's. It also supports uploading and downloading user keys through a USB flash drive.

[6] *F6 Fingerprint, RFID & PIN Reader*. http://www.secukey.com.cn/eshowProDetail.asp?ProID=1908. Accessed: 2015-04-26.

[7] *F6 Fingerprint/Keypad/Proximity Access Contol*.

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
- **Description**:
  - F6 Fingerprint Access Control is a product of Secukey[6], and supports authentication using all three factors that we implemented for our system.
  - Its price, $30 in ECPlaza[7], is much lower than our system's. It also supports uploading and downloading user keys through a USB flash drive.
  - However, since it is a standalone device, there is no way to manage users over a network, which limits its scalability.

[6] *F6 Fingerprint, RFID & PIN Reader*. http://www.secukey.com.cn/eshowProDetail.asp?ProID=1908. Accessed: 2015-04-26.

[7] *F6 Fingerprint/Keypad/Proximity Access Contol*.

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
- **Description**:
  - F6 Fingerprint Access Control is a product of Secukey[6], and supports authentication using all three factors that we implemented for our system.
  - Its price, $30 in ECPlaza[7], is much lower than our system's. It also supports uploading and downloading user keys through a USB flash drive.
  - However, since it is a standalone device, there is no way to manage users over a network, which limits its scalability.
  - If there is a new user, one would have to manually add that user to each door, and the reverse if a user leaves permanently.

[6] *F6 Fingerprint, RFID & PIN Reader*. http://www.secukey.com.cn/eshowProDetail.asp?ProID=1908. Accessed: 2015-04-26.

[7] *F6 Fingerprint/Keypad/Proximity Access Contol*.

CD-R King 2.8" Full Colored Biometric

- **Supported Factors**: RFID, Fingerprint, PIN

[8] *CD-R King 2.8" Full Colored Biometric*. http://www.cdrking.com/?mod=products&type=view&sid=15859&main=156. Accessed: 2015-05-03.

CD-R King 2.8" Full Colored Biometric

- **Supported Factors**: RFID, Fingerprint, PIN
- **Capacity**: 2000 users

[8] *CD-R King 2.8" Full Colored Biometric.* http://www.cdrking.com/?mod=products&type=view&sid=15859&main=156. Accessed: 2015-05-03.

CD-R King 2.8" Full Colored Biometric

- **Supported Factors**: RFID, Fingerprint, PIN
- **Capacity**: 2000 users
- **Fingerprint Accuracy**: FAR $< 0.0001\%$, FRR $< 0.1\%$

[8] *CD-R King 2.8" Full Colored Biometric*. http://www.cdrking.com/?mod=products&type=view&sid=15859&main=156. Accessed: 2015-05-03.

CD-R King 2.8" Full Colored Biometric

- **Supported Factors**: RFID, Fingerprint, PIN
- **Capacity**: 2000 users
- **Fingerprint Accuracy**: FAR $< 0.0001\%$, FRR $< 0.1\%$
- **PIN Length**: Unspecified

[8] *CD-R King 2.8" Full Colored Biometric*. http://www.cdrking.com/?mod=products&type=view&sid=15859&main=156. Accessed: 2015-05-03.

CD-R King 2.8" Full Colored Biometric

- **Supported Factors**: RFID, Fingerprint, PIN
- **Capacity**: 2000 users
- **Fingerprint Accuracy**: FAR $< 0.0001\%$, FRR $< 0.1\%$
- **PIN Length**: Unspecified
- **Description**:

[8] *CD-R King 2.8" Full Colored Biometric*. http://www.cdrking.com/?mod=products&type=view&sid=15859&main=156. Accessed: 2015-05-03.

CD-R King 2.8" Full Colored Biometric

- **Supported Factors**: RFID, Fingerprint, PIN
- **Capacity**: 2000 users
- **Fingerprint Accuracy**: FAR $< 0.0001\%$, FRR $< 0.1\%$
- **PIN Length**: Unspecified
- **Description**:
  - The CDR-King 2.8" Full Colored Biometric[8], costs $67.

[8] *CD-R King 2.8" Full Colored Biometric.* http://www.cdrking.com/?mod=products&type=view&sid=15859&main=156. Accessed: 2015-05-03.

CD-R King 2.8" Full Colored Biometric

- **Supported Factors**: RFID, Fingerprint, PIN
- **Capacity**: 2000 users
- **Fingerprint Accuracy**: FAR $< 0.0001\%$, FRR $< 0.1\%$
- **PIN Length**: Unspecified
- **Description**:
  - The CDR-King 2.8" Full Colored Biometric[8], costs $67.
  - This offers support for backing up user data through USB.

[8] *CD-R King 2.8" Full Colored Biometric.* http://www.cdrking.com/?mod=products&type=view&sid=15859&main=156. Accessed: 2015-05-03.

CD-R King 2.8" Full Colored Biometric

- **Supported Factors**: RFID, Fingerprint, PIN
- **Capacity**: 2000 users
- **Fingerprint Accuracy**: FAR $< 0.0001\%$, FRR $< 0.1\%$
- **PIN Length**: Unspecified
- **Description**:
  - The CDR-King 2.8" Full Colored Biometric[8], costs $67.
  - This offers support for backing up user data through USB.
  - It can log up to 100,000 events

[8] *CD-R King 2.8" Full Colored Biometric.* http://www.cdrking.com/?mod=products&type=view&sid=15859&main=156. Accessed: 2015-05-03.

CD-R King 2.8" Full Colored Biometric

- **Supported Factors**: RFID, Fingerprint, PIN
- **Capacity**: 2000 users
- **Fingerprint Accuracy**: FAR $< 0.0001\%$, FRR $< 0.1\%$
- **PIN Length**: Unspecified
- **Description**:
  - The CDR-King 2.8" Full Colored Biometric[8], costs $67.
  - This offers support for backing up user data through USB.
  - It can log up to 100,000 events
  - We tried multiple times to buy this product in order to compare it with ours, but unfortunately it was always out of stock. We found the documentation in the product page to be lacking important details, such as how to set-up the system for networked access (if it is even possible), and if the system also supports one, or two-factor authentication.

[8] *CD-R King 2.8" Full Colored Biometric.* http://www.cdrking.com/?mod=products&type=view&sid=15859&main=156. Accessed: 2015-05-03.

HID iCLASS RPK40 Access Control Device

- **Supported Factors**: RFID, PIN

[9] *HID iCLASS RPK40*. http://www.hidglobal.com/products/readers/iclass/rpk40. Accessed: 2015-05-03.

[10] *About HID - A Trusted Leader in Secure Identity Solutions*. http://www.hidglobal.com/about-hid. Accessed: 2015-05-03.

[11] *HID iCLASS RPK40 Access Control Device*. www.barcodesinc.com/hid/iclass-rpk40.htm. Accessed: 2015-05-03.

HID iCLASS RPK40 Access Control Device

- **Supported Factors**: RFID, PIN
- **Capacity**: 100 users

[9] *HID iCLASS RPK40*. http://www.hidglobal.com/products/readers/iclass/rpk40. Accessed: 2015-05-03.

[10] *About HID - A Trusted Leader in Secure Identity Solutions*. http://www.hidglobal.com/about-hid. Accessed: 2015-05-03.

[11] *HID iCLASS RPK40 Access Control Device*. www.barcodesinc.com/hid/iclass-rpk40.htm. Accessed: 2015-05-03.

HID iCLASS RPK40 Access Control Device

- **Supported Factors**: RFID, PIN
- **Capacity**: 100 users
- **PIN Length**: Unspecified

---

[9] *HID iCLASS RPK40*. http://www.hidglobal.com/products/readers/iclass/rpk40. Accessed: 2015-05-03.

[10] *About HID - A Trusted Leader in Secure Identity Solutions*. http://www.hidglobal.com/about-hid. Accessed: 2015-05-03.

[11] *HID iCLASS RPK40 Access Control Device*. www.barcodesinc.com/hid/iclass-rpk40.htm. Accessed: 2015-05-03.

HID iCLASS RPK40 Access Control Device

- **Supported Factors**: RFID, PIN
- **Capacity**: 100 users
- **PIN Length**: Unspecified
- **Description**:

---

[9] *HID iCLASS RPK40*. http://www.hidglobal.com/products/readers/iclass/rpk40. Accessed: 2015-05-03.

[10] *About HID - A Trusted Leader in Secure Identity Solutions*. http://www.hidglobal.com/about-hid. Accessed: 2015-05-03.

[11] *HID iCLASS RPK40 Access Control Device*. www.barcodesinc.com/hid/iclass-rpk40.htm. Accessed: 2015-05-03.

HID iCLASS RPK40 Access Control Device

- **Supported Factors**: RFID, PIN
- **Capacity**: 100 users
- **PIN Length**: Unspecified
- **Description**:

---

[9] *HID iCLASS RPK40*. http://www.hidglobal.com/products/readers/iclass/rpk40. Accessed: 2015-05-03.

[10] *About HID - A Trusted Leader in Secure Identity Solutions*. http://www.hidglobal.com/about-hid. Accessed: 2015-05-03.

[11] *HID iCLASS RPK40 Access Control Device*. www.barcodesinc.com/hid/iclass-rpk40.htm. Accessed: 2015-05-03.

HID iCLASS RPK40 Access Control Device

- **Supported Factors**: RFID, PIN
- **Capacity**: 100 users
- **PIN Length**: Unspecified
- **Description**:
  - The iCLASS RPK40[9], is a product of HID Global, one of the leaders in secure identity solutions[10].

[9] *HID iCLASS RPK40*. http://www.hidglobal.com/products/readers/iclass/rpk40. Accessed: 2015-05-03.

[10] *About HID - A Trusted Leader in Secure Identity Solutions*. http://www.hidglobal.com/about-hid. Accessed: 2015-05-03.

[11] *HID iCLASS RPK40 Access Control Device*. www.barcodesinc.com/hid/iclass-rpk40.htm. Accessed: 2015-05-03.

HID iCLASS RPK40 Access Control Device

- **Supported Factors**: RFID, PIN
- **Capacity**: 100 users
- **PIN Length**: Unspecified
- **Description**:
  - The iCLASS RPK40[9], is a product of HID Global, one of the leaders in secure identity solutions[10].
  - It has a very steep cost, starting at $380 in BarcodesInc[11]

[9] *HID iCLASS RPK40*. http://www.hidglobal.com/products/readers/iclass/rpk40. Accessed: 2015-05-03.

[10] *About HID - A Trusted Leader in Secure Identity Solutions*. http://www.hidglobal.com/about-hid. Accessed: 2015-05-03.

[11] *HID iCLASS RPK40 Access Control Device*. www.barcodesinc.com/hid/iclass-rpk40.htm. Accessed: 2015-05-03.

HID iCLASS RPK40 Access Control Device

- **Supported Factors**: RFID, PIN
- **Capacity**: 100 users
- **PIN Length**: Unspecified
- **Description**:
  - The iCLASS RPK40[9], is a product of HID Global, one of the leaders in secure identity solutions[10].
  - It has a very steep cost, starting at $380 in BarcodesInc[11]
  - However, the system has been reported to be unable to enroll new RFID cards, lose communication with the controller. Furthermore, the data stored in the system is volatile.

[9] *HID iCLASS RPK40*. http://www.hidglobal.com/products/readers/iclass/rpk40. Accessed: 2015-05-03.

[10] *About HID - A Trusted Leader in Secure Identity Solutions*. http://www.hidglobal.com/about-hid. Accessed: 2015-05-03.

[11] *HID iCLASS RPK40 Access Control Device*. www.barcodesinc.com/hid/iclass-rpk40.htm. Accessed: 2015-05-03.

Open Source Systems

- Open Source systems, as opposed to commercial systems, allow users to first inspect the code, find out exactly what the system can and cannot do, before determining whether to assemble the system or not.

Open Source Systems

- Open Source systems, as opposed to commercial systems, allow users to first inspect the code, find out exactly what the system can and cannot do, before determining whether to assemble the system or not.
- The access control systems we will be looking at are the following:

Open Source Systems

- Open Source systems, as opposed to commercial systems, allow users to first inspect the code, find out exactly what the system can and cannot do, before determining whether to assemble the system or not.
- The access control systems we will be looking at are the following:
  - Open Access Control

Open Source Systems

- Open Source systems, as opposed to commercial systems, allow users to first inspect the code, find out exactly what the system can and cannot do, before determining whether to assemble the system or not.
- The access control systems we will be looking at are the following:
  - Open Access Control
  - Pi-Lock

Open Access Control

- **Supported Factors**: RFID, PIN

[12] *Open Access Control for Hacker Spaces*.
https://code.google.com/p/open-access-control/. Accessed: 2015-05-09

Open Access Control

- **Supported Factors**: RFID, PIN
- **Capacity**: Arduino

[12] *Open Access Control for Hacker Spaces*.
https://code.google.com/p/open-access-control/. Accessed: 2015-05-09

Open Access Control

- **Supported Factors**: RFID, PIN
- **Capacity**: Arduino
- **Fingerprint Accuracy**: 200 users

[12] *Open Access Control for Hacker Spaces*.
https://code.google.com/p/open-access-control/. Accessed: 2015-05-09

Open Access Control

- **Supported Factors**: RFID, PIN
- **Capacity**: Arduino
- **Fingerprint Accuracy**: 200 users
- **PIN Length**: Any length

[12] *Open Access Control for Hacker Spaces*. https://code.google.com/p/open-access-control/. Accessed: 2015-05-09

Open Access Control

- **Supported Factors**: RFID, PIN
- **Capacity**: Arduino
- **Fingerprint Accuracy**: 200 users
- **PIN Length**: Any length
- **Description**:

[12] *Open Access Control for Hacker Spaces*. https://code.google.com/p/open-access-control/. Accessed: 2015-05-09.

Open Access Control

- **Supported Factors**: RFID, PIN
- **Capacity**: Arduino
- **Fingerprint Accuracy**: 200 users
- **PIN Length**: Any length
- **Description**:
  - Open Access Control is an Arduino-based RFID access control system for hacker spaces[12].

[12] *Open Access Control for Hacker Spaces*. https://code.google.com/p/open-access-control/. Accessed: 2015-05-09.

Open Access Control

- **Supported Factors**: RFID, PIN
- **Capacity**: Arduino
- **Fingerprint Accuracy**: 200 users
- **PIN Length**: Any length
- **Description**:
  - Open Access Control is an Arduino-based RFID access control system for hacker spaces[12].
  - According to Orsini[13], the Arduino is the better platform for pure hardware projects, i.e. controlling physical sensors. However, the Arduino is just a microcontroller, while the Pi is a fully functional computer.

[12] *Open Access Control for Hacker Spaces*.
https://code.google.com/p/open-access-control/. Accessed: 2015-05-09

Open Access Control

- **Supported Factors**: RFID, PIN
- **Capacity**: Arduino
- **Fingerprint Accuracy**: 200 users
- **PIN Length**: Any length
- **Description**:
  - Open Access Control is an Arduino-based RFID access control system for hacker spaces[12].
  - According to Orsini[13], the Arduino is the better platform for pure hardware projects, i.e. controlling physical sensors. However, the Arduino is just a microcontroller, while the Pi is a fully functional computer.
  - The question is whether an access control system warrants more power on the hardware (Arduino) or the software (Pi) side. In our case, door controllers need to be able to communicate with the server over a network, in addition to their main function of controlling the door lock, so we find Raspberry Pi to be the more suitable platform.

[12] *Open Access Control for Hacker Spaces.* https://code.google.com/p/open-access-control/. Accessed: 2015-05-09.

Pi-Lock

- **Supported Factors**: RFID, PIN

[14] Paolo Bernasconi. *Raspberry Pi RFID Door Lock*. http://www.pi-lock.com. Accessed: 2015-04-19.

Pi-Lock

- **Supported Factors**: RFID, PIN
- **Capacity**: Raspberry Pi

[14] Paolo Bernasconi. *Raspberry Pi RFID Door Lock*. http://www.pi-lock.com. Accessed: 2015-04-19.

Pi-Lock

- **Supported Factors**: RFID, PIN
- **Capacity**: Raspberry Pi
- **Fingerprint Accuracy**: Depends on SD card capacity

[14] Paolo Bernasconi. *Raspberry Pi RFID Door Lock*. http://www.pi-lock.com. Accessed: 2015-04-19.

Pi-Lock

- **Supported Factors**: RFID, PIN
- **Capacity**: Raspberry Pi
- **Fingerprint Accuracy**: Depends on SD card capacity
- **PIN Length**: 4 digits

[14] Paolo Bernasconi. *Raspberry Pi RFID Door Lock*. http://www.pi-lock.com. Accessed: 2015-04-19.

Pi-Lock

- **Supported Factors**: RFID, PIN
- **Capacity**: Raspberry Pi
- **Fingerprint Accuracy**: Depends on SD card capacity
- **PIN Length**: 4 digits
- **Description**:

[14] Paolo Bernasconi. *Raspberry Pi RFID Door Lock*. http://www.pi-lock.com. Accessed: 2015-04-19.

Pi-Lock

- **Supported Factors**: RFID, PIN
- **Capacity**: Raspberry Pi
- **Fingerprint Accuracy**: Depends on SD card capacity
- **PIN Length**: 4 digits
- **Description**:
  - Pi-Lock is an automated door security system built around the Raspberry Pi[14].

[14] Paolo Bernasconi. *Raspberry Pi RFID Door Lock*. http://www.pi-lock.com. Accessed: 2015-04-19.

Pi-Lock

- **Supported Factors**: RFID, PIN
- **Capacity**: Raspberry Pi
- **Fingerprint Accuracy**: Depends on SD card capacity
- **PIN Length**: 4 digits
- **Description**:
  - Pi-Lock is an automated door security system built around the Raspberry Pi[14].
  - It is similar to our system in that it runs on Raspberry Pi, is written in Python, and comes with a front-end user management web app.

[14] Paolo Bernasconi. *Raspberry Pi RFID Door Lock*. http://www.pi-lock.com. Accessed: 2015-04-19.

Pi-Lock

- **Supported Factors**: RFID, PIN
- **Capacity**: Raspberry Pi
- **Fingerprint Accuracy**: Depends on SD card capacity
- **PIN Length**: 4 digits
- **Description**:
  - Pi-Lock is an automated door security system built around the Raspberry Pi[14].
  - It is similar to our system in that it runs on Raspberry Pi, is written in Python, and comes with a front-end user management web app.
  - However, the fixed length of four for the PIN is too short for it to be used in settings that call for a higher level of security.

[14] Paolo Bernasconi. *Raspberry Pi RFID Door Lock*. http://www.pi-lock.com. Accessed: 2015-04-19.

Our System: ForkPi and SpoonPi

- **Supported Factors**: RFID, Fingerprint, PIN

---

[15] SparkFun Electronics (US). *Fingerprint Scanner - TTL (GT-511C3)*. https://www.sparkfun.com/products/11792. Accessed: 2015-05-19.

[16] *Fingerprint Identification SDK "Smack Finger SDK 3.0" Specification 1.3*

Our System: ForkPi and SpoonPi

- **Supported Factors**: RFID, Fingerprint, PIN
- **Platform**: Raspberry Pi

[15] SparkFun Electronics (US). *Fingerprint Scanner - TTL (GT-511C3)*. https://www.sparkfun.com/products/11792. Accessed: 2015-05-19.
[16] *Fingerprint Identification SDK "Smack Finger SDK 3.0" Specification 1.3*

Our System: ForkPi and SpoonPi

- **Supported Factors**: RFID, Fingerprint, PIN
- **Platform**: Raspberry Pi
- **Capacity**: Depends on SD card capacity

[15] SparkFun Electronics (US). *Fingerprint Scanner - TTL (GT-511C3)*. https://www.sparkfun.com/products/11792. Accessed: 2015-05-19.

[16] *Fingerprint Identification SDK "Smack Finger SDK 3.0" Specification 1.3*

Our System: ForkPi and SpoonPi

- **Supported Factors**: RFID, Fingerprint, PIN
- **Platform**: Raspberry Pi
- **Capacity**: Depends on SD card capacity
- **Fingerprint Accuracy**: FAR $< 0.00001\%$, FRR $< 0.01\%$

[15] SparkFun Electronics (US). *Fingerprint Scanner - TTL (GT-511C3)*. https://www.sparkfun.com/products/11792. Accessed: 2015-05-19.

[16] *Fingerprint Identification SDK "Smack Finger SDK 3.0" Specification 1.3*

Our System: ForkPi and SpoonPi

- **Supported Factors**: RFID, Fingerprint, PIN
- **Platform**: Raspberry Pi
- **Capacity**: Depends on SD card capacity
- **Fingerprint Accuracy**: FAR $< 0.00001\%$, FRR $< 0.01\%$
- **PIN Length**: Any length (at least 4 digits)

[15] SparkFun Electronics (US). *Fingerprint Scanner - TTL (GT-511C3)*. https://www.sparkfun.com/products/11792. Accessed: 2015-05-19.

[16] *Fingerprint Identification SDK "Smack Finger SDK 3.0" Specification 1.3*

Our System: ForkPi and SpoonPi

- **Supported Factors**: RFID, Fingerprint, PIN
- **Platform**: Raspberry Pi
- **Capacity**: Depends on SD card capacity
- **Fingerprint Accuracy**: FAR $< 0.00001\%$, FRR $< 0.01\%$
- **PIN Length**: Any length (at least 4 digits)
- **Description**:

[15] SparkFun Electronics (US). *Fingerprint Scanner - TTL (GT-511C3)*. https://www.sparkfun.com/products/11792. Accessed: 2015-05-19.

[16] *Fingerprint Identification SDK "Smack Finger SDK 3.0" Specification 1.3*

Our System: ForkPi and SpoonPi

- **Supported Factors**: RFID, Fingerprint, PIN
- **Platform**: Raspberry Pi
- **Capacity**: Depends on SD card capacity
- **Fingerprint Accuracy**: FAR $< 0.00001\%$, FRR $< 0.01\%$
- **PIN Length**: Any length (at least 4 digits)
- **Description**:
  - Our system tries to combine the strengths of the other systems mentioned above. The fingerprint scanner we used, the SparkFun fingerprint scanner TTL model GT-511C3[15], uses a fingerprint matching algorithm called the "SmackFinger 3.0 Algorithm", which claims to have the accuracy described above[16].

---

[15] SparkFun Electronics (US). *Fingerprint Scanner - TTL (GT-511C3)*. https://www.sparkfun.com/products/11792. Accessed: 2015-05-19.

[16] *Fingerprint Identification SDK "Smack Finger SDK 3.0" Specification 1.3*

Our System: ForkPi and SpoonPi

- **Supported Factors**: RFID, Fingerprint, PIN
- **Platform**: Raspberry Pi
- **Capacity**: Depends on SD card capacity
- **Fingerprint Accuracy**: FAR $< 0.00001\%$, FRR $< 0.01\%$
- **PIN Length**: Any length (at least 4 digits)
- **Description**:
    - Our system tries to combine the strengths of the other systems mentioned above. The fingerprint scanner we used, the SparkFun fingerprint scanner TTL model GT-511C3[15], uses a fingerprint matching algorithm called the "SmackFinger 3.0 Algorithm", which claims to have the accuracy described above[16].
    - This is more accurate than all the other fingerprint-based systems we looked at. It can accommodate a large number of users, provided that the SD card used also has a large capacity.

[15] SparkFun Electronics (US). *Fingerprint Scanner - TTL (GT-511C3)*. https://www.sparkfun.com/products/11792. Accessed: 2015-05-19.

[16] *Fingerprint Identification SDK "Smack Finger SDK 3.0" Specification 1.3*

Outline

Problem Statement

- Secure hardware-based authentication systems are still expensive when compared to software, making them inaccessible to the world outside of the business setting.

Problem Statement

- Secure hardware-based authentication systems are still expensive when compared to software, making them inaccessible to the world outside of the business setting.
- The goal of this study is to make a hardware-based authentication system that is more accessible to the public.

Problem Statement

- Secure hardware-based authentication systems are still expensive when compared to software, making them inaccessible to the world outside of the business setting.
- The goal of this study is to make a hardware-based authentication system that is more accessible to the public.
- This can be done by lowering its cost while maintaining an acceptable level of security.

Outline

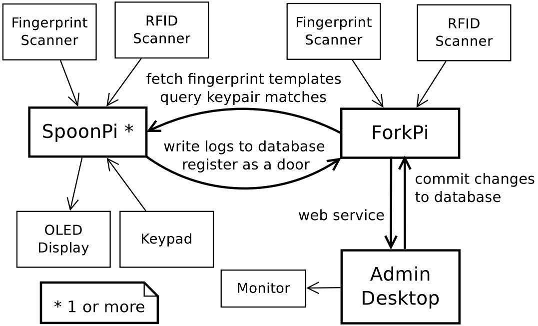
1. Introduction
2. Related Work
3. Problem Statement
4. Design and Architecture
   - Design and Architecture
   - ForkPi
   - SpoonPi
   - Security Options
   - Security Options
5. Evaluation
6. Recommendations

Design and Architecture

- The following shows an overview of how ForkPi and SpoonPi are setup.

Design and Architecture

- The following shows an overview of how ForkPi and SpoonPi are setup.



-

ForkPi Overview

- The ForkPi unit functions as both a web and database server.

ForkPi Overview

- The ForkPi unit functions as both a web and database server.
- The web server runs a locally accessible website where one can register new users into the system, view logs, and perform other administrative actions.

ForkPi Overview

- The ForkPi unit functions as both a web and database server.
- The web server runs a locally accessible website where one can register new users into the system, view logs, and perform other administrative actions.
- The web server has an underlying database run by PostgreSQL.

ForkPi Overview

- The ForkPi unit functions as both a web and database server.
- The web server runs a locally accessible website where one can register new users into the system, view logs, and perform other administrative actions.
- The web server has an underlying database run by PostgreSQL.
- Human administrators view ForkPi as a web server, while SpoonPis view ForkPi as a database server.

Technical Overview

- ForkPi is addressed within the local network using the name forkpi.local, at HTTP port 80.

Technical Overview

- ForkPi is addressed within the local network using the name forkpi.local, at HTTP port 80.
- The database server runs in the port 5432, so SpoonPis will access the database using the host name forkpi.local and the port number 5432.

Technical Overview

- ForkPi is addressed within the local network using the name forkpi.local, at HTTP port 80.
- The database server runs in the port 5432, so SpoonPis will access the database using the host name forkpi.local and the port number 5432.
- A dedicated ForkPi unit does not require the presence of a keypad nor an OLED display, but it requires having the following peripherals attached:

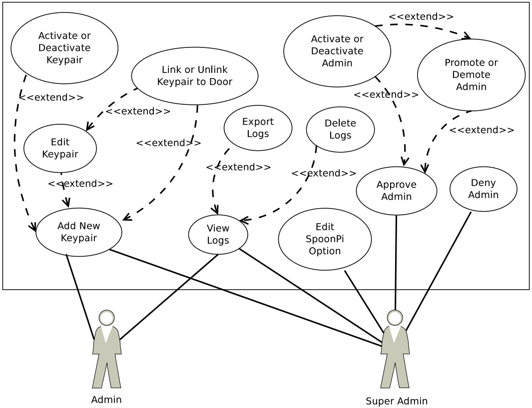
Technical Overview

- ForkPi is addressed within the local network using the name forkpi.local, at HTTP port 80.
- The database server runs in the port 5432, so SpoonPis will access the database using the host name forkpi.local and the port number 5432.
- A dedicated ForkPi unit does not require the presence of a keypad nor an OLED display, but it requires having the following peripherals attached:
  - **RFID Scanner**: for scanning the UIDs of RFID tags to be registered

Technical Overview

- ForkPi is addressed within the local network using the name forkpi.local, at HTTP port 80.
- The database server runs in the port 5432, so SpoonPis will access the database using the host name forkpi.local and the port number 5432.
- A dedicated ForkPi unit does not require the presence of a keypad nor an OLED display, but it requires having the following peripherals attached:
  - **RFID Scanner**: for scanning the UIDs of RFID tags to be registered
  - **Fingerprint Scanner**: for the enrollment of new Fingerprints

Use Case Diagram



Types of Admins

- There are two types of admins: regular admins and super admins.

Types of Admins

- There are two types of admins: regular admins and super admins.
- Super admins can perform everything a regular admin can do, with some additional functions we deemed to be potentially destructive in the hands of the wrong person.

Types of Admins

- There are two types of admins: regular admins and super admins.
- Super admins can perform everything a regular admin can do, with some additional functions we deemed to be potentially destructive in the hands of the wrong person.
- Regular admins have a limited set of permissions, and they can only become super admins with the consent of another super admin, in a process called promotion.

Types of Admins

- There are two types of admins: regular admins and super admins.
- Super admins can perform everything a regular admin can do, with some additional functions we deemed to be potentially destructive in the hands of the wrong person.
- Regular admins have a limited set of permissions, and they can only become super admins with the consent of another super admin, in a process called promotion.
- New admin sign up requires the approval of another admin, and is a regular admin by default.

Types of Admins

- There are two types of admins: regular admins and super admins.
- Super admins can perform everything a regular admin can do, with some additional functions we deemed to be potentially destructive in the hands of the wrong person.
- Regular admins have a limited set of permissions, and they can only become super admins with the consent of another super admin, in a process called promotion.
- New admin sign up requires the approval of another admin, and is a regular admin by default.
- However, if the system is new, admin sign up is automatically approved and is a super admin by default.

SpoonPi Overview

- The SpoonPi units serve as the media for door authentication, and are responsible for granting or denying access through doors. There are as many SpoonPis as doors to be secured.

SpoonPi Overview

- The SpoonPi units serve as the media for door authentication, and are responsible for granting or denying access through doors. There are as many SpoonPis as doors to be secured.
- Each SpoonPi unit needs to register itself first with the ForkPi unit before any authentication can be done.

SpoonPi Overview

- The SpoonPi units serve as the media for door authentication, and are responsible for granting or denying access through doors. There are as many SpoonPis as doors to be secured.
- Each SpoonPi unit needs to register itself first with the ForkPi unit before any authentication can be done.
- SpoonPi performs authentication by communicating with the hardware components (e.g. RFID scanner) to get the input credentials (e.g. RFID UID), then querying the ForkPi database to check if it is valid.

SpoonPi Overview

- The SpoonPi units serve as the media for door authentication, and are responsible for granting or denying access through doors. There are as many SpoonPis as doors to be secured.
- Each SpoonPi unit needs to register itself first with the ForkPi unit before any authentication can be done.
- SpoonPi performs authentication by communicating with the hardware components (e.g. RFID scanner) to get the input credentials (e.g. RFID UID), then querying the ForkPi database to check if it is valid.
- For fingerprint authentication, the verification is done at the SpoonPi side instead of the ForkPi side, because the matching is not a simple string comparison; fingerprint templates have to be uploaded to the scanner, where the actual matching takes place.

Technical Overview

- A SpoonPi unit requires having the following peripherals attached:

Technical Overview

- A SpoonPi unit requires having the following peripherals attached:
    - **Fingerprint Scanner**: for identifying the fingerprint presented

Technical Overview

- A SpoonPi unit requires having the following peripherals attached:
  - **Fingerprint Scanner**: for identifying the fingerprint presented
  - **OLED**: for displaying the current status of the transaction

Technical Overview

- A SpoonPi unit requires having the following peripherals attached:
    - **Fingerprint Scanner**: for identifying the fingerprint presented
    - **OLED**: for displaying the current status of the transaction
    - **RFID** Scanner: for scanning the UID of the RFID tag presented

Technical Overview

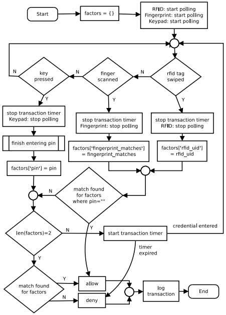
- A SpoonPi unit requires having the following peripherals attached:
    - **Fingerprint Scanner**: for identifying the fingerprint presented
    - **OLED**: for displaying the current status of the transaction
    - **RFID** Scanner: for scanning the UID of the RFID tag presented
    - **Keypad**: for entering the PIN

SpoonPi Flowchart

- The following flowchart describing the main transaction loop:

SpoonPi Flowchart

- The following flowchart describing the main transaction loop:



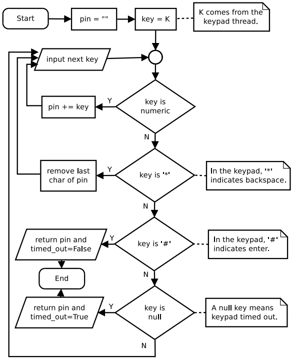
-

SpoonPi PIN Flowchart

- The following flowchart describing the PIN input loop:

SpoonPi PIN Flowchart

- The following flowchart describing the PIN input loop:



-

Security Options (1 of 2)

- **Attempt Limit**: The maximum streak of failed attempts where an RFID tag is presented and the wrong PIN is entered. This is to prevent guessing the PIN via brute force if an RFID tag is cloned or falls into an attacker's hands. The default value is 5 attempts.

Security Options (1 of 2)

- **Attempt Limit**: The maximum streak of failed attempts where an RFID tag is presented and the wrong PIN is entered. This is to prevent guessing the PIN via brute force if an RFID tag is cloned or falls into an attacker's hands. The default value is 5 attempts.
- **Lockout Time (minutes)**: This is the amount of time to block the RFID tag from further use once the incorrect streak reaches the attempt limit. The default value is 30 minutes.

Security Options (1 of 2)

- **Attempt Limit**: The maximum streak of failed attempts where an RFID tag is presented and the wrong PIN is entered. This is to prevent guessing the PIN via brute force if an RFID tag is cloned or falls into an attacker's hands. The default value is 5 attempts.
- **Lockout Time (minutes)**: This is the amount of time to block the RFID tag from further use once the incorrect streak reaches the attempt limit. The default value is 30 minutes.
- **Keypad Timeout (seconds)** This is the maximum amount of time between key presses. The default value is 5 seconds.

Security Options (2 of 2)

- **Max Transaction Time (seconds)**: This is the maximum amount of time between presenting two authentication tokens. The default value is 10 seconds.

Security Options (2 of 2)

- **Max Transaction Time (seconds)**: This is the maximum amount of time between presenting two authentication tokens. The default value is 10 seconds.
- **Lock Release Time (seconds)**: This is the amount of time to release the lock upon a successful attempt. The default value is 5 seconds.

Outline

Security of the PIN Component (1 of 3)

- Let's consider an attacker Oscar, who is trying to gain unauthorized access to a door by exploiting weaknesses inherent to a certain authentication factor used in the system.

Security of the PIN Component (1 of 3)

- Let's consider an attacker Oscar, who is trying to gain unauthorized access to a door by exploiting weaknesses inherent to a certain authentication factor used in the system.
- The main security concern with PIN is its vulnerability to brute force attacks.

Security of the PIN Component (1 of 3)

- Let's consider an attacker Oscar, who is trying to gain unauthorized access to a door by exploiting weaknesses inherent to a certain authentication factor used in the system.
- The main security concern with PIN is its vulnerability to brute force attacks.
- If an attacker Oscar gets hold of an authorized RFID tag, he can gain access to a door if he guesses the corresponding PIN.

Security of the PIN Component (1 of 3)

- Let's consider an attacker Oscar, who is trying to gain unauthorized access to a door by exploiting weaknesses inherent to a certain authentication factor used in the system.
- The main security concern with PIN is its vulnerability to brute force attacks.
- If an attacker Oscar gets hold of an authorized RFID tag, he can gain access to a door if he guesses the corresponding PIN.
- However, a lockout functionality has been implemented for RFID authentication, so Oscar has to wait a long time between guesses.

Security of the PIN Component (2 of 3)

- The following formula is the average time it takes to guess a PIN using brute force in the system:

$$T = (g \cdot t) + (L \cdot \frac{g}{n})$$

Security of the PIN Component (2 of 3)

- The following formula is the average time it takes to guess a PIN using brute force in the system:

$$T = (g \cdot t) + (L \cdot \frac{g}{n})$$

- Where:

Security of the PIN Component (2 of 3)

- The following formula is the average time it takes to guess a PIN using brute force in the system:

$$T = (g \cdot t) + (L \cdot \frac{g}{n})$$

- Where:
  - g is the average number of guesses needed

Security of the PIN Component (2 of 3)

- The following formula is the average time it takes to guess a PIN using brute force in the system:

$$T = (g \cdot t) + (L \cdot \frac{g}{n})$$

- Where:
    - g is the average number of guesses needed
    - t is the average time it takes to try out a single PIN

Security of the PIN Component (2 of 3)

- The following formula is the average time it takes to guess a PIN using brute force in the system:

$$T = (g \cdot t) + (L \cdot \frac{g}{n})$$

- Where:
  - g is the average number of guesses needed
  - t is the average time it takes to try out a single PIN
  - L is the waiting time after a single lock-out

Security of the PIN Component (2 of 3)

- The following formula is the average time it takes to guess a PIN using brute force in the system:

$$T = (g \cdot t) + (L \cdot \frac{g}{n})$$

- Where:
  - g is the average number of guesses needed
  - t is the average time it takes to try out a single PIN
  - L is the waiting time after a single lock-out
  - and n is the number of wrong attempts it takes before being locked-out.

Security of the PIN Component (3 of 3)

- On average, Oscar only needs to enter half of all possible PINs before guessing the correct one.

Security of the PIN Component (3 of 3)

- On average, Oscar only needs to enter half of all possible PINs before guessing the correct one.
- There is no maximum PIN length imposed, which means the number of possible PINs is theoretically infinite, but assuming the following:

Security of the PIN Component (3 of 3)

- On average, Oscar only needs to enter half of all possible PINs before guessing the correct one.
- There is no maximum PIN length imposed, which means the number of possible PINs is theoretically infinite, but assuming the following:
    - All users use 6-digit PINs

Security of the PIN Component (3 of 3)

- On average, Oscar only needs to enter half of all possible PINs before guessing the correct one.
- There is no maximum PIN length imposed, which means the number of possible PINs is theoretically infinite, but assuming the following:
  - All users use 6-digit PINs
  - It takes 5 seconds to try out a single PIN.

Security of the PIN Component (3 of 3)

- On average, Oscar only needs to enter half of all possible PINs before guessing the correct one.
- There is no maximum PIN length imposed, which means the number of possible PINs is theoretically infinite, but assuming the following:
  - All users use 6-digit PINs
  - It takes 5 seconds to try out a single PIN.
  - Lockout time is 30 minutes (default)

Security of the PIN Component (3 of 3)

- On average, Oscar only needs to enter half of all possible PINs before guessing the correct one.
- There is no maximum PIN length imposed, which means the number of possible PINs is theoretically infinite, but assuming the following:
  - All users use 6-digit PINs
  - It takes 5 seconds to try out a single PIN.
  - Lockout time is 30 minutes (default)
  - Attempt limit is 5 (default)

Security of the PIN Component (3 of 3)

- On average, Oscar only needs to enter half of all possible PINs before guessing the correct one.
- There is no maximum PIN length imposed, which means the number of possible PINs is theoretically infinite, but assuming the following:
  - All users use 6-digit PINs
  - It takes 5 seconds to try out a single PIN.
  - Lockout time is 30 minutes (default)
  - Attempt limit is 5 (default)
- Hence,
  $g = \frac{1}{2} \cdot 10^6 = 500,000 \text{ guesses}, t = 5 \text{ s}, L = 1800 \text{ s}, n = 5$

Security of the PIN Component (3 of 3)

- On average, Oscar only needs to enter half of all possible PINs before guessing the correct one.
- There is no maximum PIN length imposed, which means the number of possible PINs is theoretically infinite, but assuming the following:
  - All users use 6-digit PINs
  - It takes 5 seconds to try out a single PIN.
  - Lockout time is 30 minutes (default)
  - Attempt limit is 5 (default)
- Hence,
  $g = \frac{1}{2} \cdot 10^6 = 500,000 \text{ guesses}, t = 5 \text{ s}, L = 1800 \text{ s}, n = 5$
- Plugging in those values, it would take, on average, 50694 hours, or about 5.78 years to crack. This makes brute force an impractical attack to use.

Security of the RFID Component (1 of 2)

- The primary concern with RFID security is the issue of stolen or replicated tags.

Security of the RFID Component (1 of 2)

- The primary concern with RFID security is the issue of stolen or replicated tags.
- While we cannot prevent tags from being stolen, this is not a problem because our system allows admins to edit or deactivate keypairs.

Security of the RFID Component (1 of 2)

- The primary concern with RFID security is the issue of stolen or replicated tags.
- While we cannot prevent tags from being stolen, this is not a problem because our system allows admins to edit or deactivate keypairs.
- Hence, the user simply needs to go to the admin to get his keypair changed or deactivated.

Security of the RFID Component (2 of 2)

- Replication of an RFID tag can be performed by scanning its UID, and reprogramming another tag to have the same UID.

[17] *MiFare Classic (13.56MHz RFID/NFC) Card.* http://www.adafruit.com/product/359. Accessed: 2015-01-02.

Security of the RFID Component (2 of 2)

- Replication of an RFID tag can be performed by scanning its UID, and reprogramming another tag to have the same UID.
- Attackers do not need to have access to the actual tag, as they can find out the UID simply by placing keyloggers near the RFID reader and waiting for it to be scanned.

[17] *MiFare Classic (13.56MHz RFID/NFC) Card.* http://www.adafruit.com/product/359. Accessed: 2015-01-02.

Security of the RFID Component (2 of 2)

- Replication of an RFID tag can be performed by scanning its UID, and reprogramming another tag to have the same UID.
- Attackers do not need to have access to the actual tag, as they can find out the UID simply by placing keyloggers near the RFID reader and waiting for it to be scanned.
- The MiFare cards we used cannot have their UIDs reprogrammed[17], but some MiFare cards are made specially for cloning purposes (called "magic" MiFare cards).

[17] *MiFare Classic (13.56MHz RFID/NFC) Card.* http://www.adafruit.com/product/359. Accessed: 2015-01-02.

Security of the RFID Component (2 of 2)

- Replication of an RFID tag can be performed by scanning its UID, and reprogramming another tag to have the same UID.
- Attackers do not need to have access to the actual tag, as they can find out the UID simply by placing keyloggers near the RFID reader and waiting for it to be scanned.
- The MiFare cards we used cannot have their UIDs reprogrammed[17], but some MiFare cards are made specially for cloning purposes (called "magic" MiFare cards).
- MiFare in general is not known to be secure, as some attacks have been developed for it. De Koning Gans et al recommend that a more advanced RFID card technology with an open design architecture be used over MiFare[18].

[17] *MiFare Classic (13.56MHz RFID/NFC) Card*. http://www.adafruit.com/product/359. Accessed: 2015-01-02.

[18] Gerhard de Koning Gans, Jaap-Henk Hoepman, and Flavio D Garcia. "A practical

Security of the Fingerprint Component (1 of 2)

- The problem with fingerprint security is the possibility of generating false positives and false negatives.

Security of the Fingerprint Component (1 of 2)

- The problem with fingerprint security is the possibility of generating false positives and false negatives.
- While a false negative (denying a user that is supposed to be authorized) might cause some minor inconvenience on the part of the user, a false positive (allowing a user that is not supposed to be authorized) is potentially devastating.

Security of the Fingerprint Component (1 of 2)

- The problem with fingerprint security is the possibility of generating false positives and false negatives.
- While a false negative (denying a user that is supposed to be authorized) might cause some minor inconvenience on the part of the user, a false positive (allowing a user that is not supposed to be authorized) is potentially devastating.
- However, an attacker cannot rely solely on chance in order to generate a false positive, since that probability is infinitesimally small (less than 0.00001% in our case).

Security of the Fingerprint Component (2 of 2)

- What the attacker can do is to make a clone of the registered fingerprint. This can be done by pressing the finger against various materials such as silicone or gelatin, in order to make a mold.

[19] Tsutomu Matsumoto et al. "Impact of artificial gummy fingers on fingerprint

Security of the Fingerprint Component (2 of 2)

- What the attacker can do is to make a clone of the registered fingerprint. This can be done by pressing the finger against various materials such as silicone or gelatin, in order to make a mold.
- We have not personally tested our fingerprint scanner against such clones, but in the study done by Matsumoto et al on 11 fingerprint scanners, they found that 67% of them accepted the gummy fingers[19].

[19] Tsutomu Matsumoto et al. "Impact of artificial gummy fingers on fingerprint

Security of the Fingerprint Component (2 of 2)

- What the attacker can do is to make a clone of the registered fingerprint. This can be done by pressing the finger against various materials such as silicone or gelatin, in order to make a mold.
- We have not personally tested our fingerprint scanner against such clones, but in the study done by Matsumoto et al on 11 fingerprint scanners, they found that 67% of them accepted the gummy fingers[19].
- Hence, it is not unreasonable to assume that our scanner will also be deceived by artificial fingers.

[19] Tsutomu Matsumoto et al. "Impact of artificial gummy fingers on fingerprint

Security of the Fingerprint Component (2 of 2)

- What the attacker can do is to make a clone of the registered fingerprint. This can be done by pressing the finger against various materials such as silicone or gelatin, in order to make a mold.
- We have not personally tested our fingerprint scanner against such clones, but in the study done by Matsumoto et al on 11 fingerprint scanners, they found that 67% of them accepted the gummy fingers[19].
- Hence, it is not unreasonable to assume that our scanner will also be deceived by artificial fingers.
- However, this attack relies on the attacker obtaining an accurate mold of the finger, which usually requires the cooperation and consent of the authorized user.

[19] Tsutomu Matsumoto et al. "Impact of artificial gummy fingers on fingerprint

Security Against Passive Attacks (1 of 2)

- Let us assume that an eavesdropper Eve can read all messages being passed between SpoonPi and ForkPi, and ForkPi and the admin's computer.

Security Against Passive Attacks (1 of 2)

- Let us assume that an eavesdropper Eve can read all messages being passed between SpoonPi and ForkPi, and ForkPi and the admin's computer.
- While Eve can listen in on the exchanges, she cannot modify them.

Security Against Passive Attacks (1 of 2)

- Let us assume that an eavesdropper Eve can read all messages being passed between SpoonPi and ForkPi, and ForkPi and the admin's computer.
- While Eve can listen in on the exchanges, she cannot modify them.
- Hence, our system is secure against such attacks for both communication lines.

Security Against Passive Attacks (1 of 2)

- Let us assume that an eavesdropper Eve can read all messages being passed between SpoonPi and ForkPi, and ForkPi and the admin's computer.
- While Eve can listen in on the exchanges, she cannot modify them.
- Hence, our system is secure against such attacks for both communication lines.
- **Communication between SpoonPi and ForkPi**: When a PIN is entered or an RFID UID is scanned, SpoonPi never queries for matches in plaintext. These two fields are hashed first using SHA-1, so Eve cannot retrieve their original values.

Security Against Passive Attacks (2 of 2)

- **Communication between ForkPi and the admin's computer**:

Security Against Passive Attacks (2 of 2)

- **Communication between ForkPi and the admin's computer**:
  - In the web application, it becomes more difficult to safely transmit the PIN and RFID UID without exposing them to Eve, since admins need to be able to view them in plaintext.

Security Against Passive Attacks (2 of 2)

- **Communication between ForkPi and the admin's computer**:
  - In the web application, it becomes more difficult to safely transmit the PIN and RFID UID without exposing them to Eve, since admins need to be able to view them in plaintext.
  - When an admin logs in, the authentication credentials are not included in the web page. However, when the admin edits a user's keypair, his/her credentials will be sent to ForkPi in plaintext.

Security Against Passive Attacks (2 of 2)

- **Communication between ForkPi and the admin's computer**:
  - In the web application, it becomes more difficult to safely transmit the PIN and RFID UID without exposing them to Eve, since admins need to be able to view them in plaintext.
  - When an admin logs in, the authentication credentials are not included in the web page. However, when the admin edits a user's keypair, his/her credentials will be sent to ForkPi in plaintext.
  - The same goes for when the admin adds a new keypair; the new keypair's credentials might be exposed to Eve. The impact is lessened in a system with multiple doors, since it would become more difficult for Eve to determine which door(s) a keypair is linked to.

Security Against Active Attacks (1 of 3)

- Let us assume that a malicious attacker, Mallory, is actively trying to break into the security of the system, either by targeting a single computer, or by pretending to be a certain computer to another computer.

Security Against Active Attacks (2 of 3)

- **Attack on the Database**:

Security Against Active Attacks (2 of 3)

- **Attack on the Database**:
  - If Mallory was able to guess the username and password of the PostgreSQL database, she would gain access to it.

Security Against Active Attacks (2 of 3)

- **Attack on the Database**:
  - If Mallory was able to guess the username and password of the PostgreSQL database, she would gain access to it.
  - However, she will not be able to retrieve the PIN and RFID UID in plaintext, since they are encrypted in 128-bit AES.

Security Against Active Attacks (2 of 3)

- **Attack on the Database**:
  - If Mallory was able to guess the username and password of the PostgreSQL database, she would gain access to it.
  - However, she will not be able to retrieve the PIN and RFID UID in plaintext, since they are encrypted in 128-bit AES.
  - Gaining access to the database can still potentially damage the system because Mallory can delete all the tables and rows. This is a severe attack on the system, so it is highly recommended to have a strong username and password for PostgreSQL.

Security Against Active Attacks (3 of 3)

- **Man In The Middle Attack**:

[20] M. Krochmal S. Cheshire. *Multicast DNS - RFC 6762.* Feb. 2013.

Security Against Active Attacks (3 of 3)

- **Man In The Middle Attack**:
  - All computers in the local network refer to ForkPi using `forkpi.local`

[20] M. Krochmal S. Cheshire. *Multicast DNS - RFC 6762*. Feb. 2013.

Security Against Active Attacks (3 of 3)

- **Man In The Middle Attack**:
    - All computers in the local network refer to ForkPi using `forkpi.local`
    - Theoretically, Mallory can create a naming collision with ForkPi by setting her own computer's hostname to forkpi, and then running a service under the name `forkpi.local`.

[20] M. Krochmal S. Cheshire. *Multicast DNS - RFC 6762.* Feb. 2013.

Security Against Active Attacks (3 of 3)

- **Man In The Middle Attack**:
  - All computers in the local network refer to ForkPi using `forkpi.local`
  - Theoretically, Mallory can create a naming collision with ForkPi by setting her own computer's hostname to forkpi, and then running a service under the name `forkpi.local`.
  - However, the service discovery software that we use, Avahi, resolves name collisions by appending a number to the hostname (e.g. `forkpi-2.local`), in accordance with the Zeroconf protocol[20].

[20] M. Krochmal S. Cheshire. *Multicast DNS - RFC 6762.* Feb. 2013.

Security Against Active Attacks (3 of 3)

- **Man In The Middle Attack**:
  - All computers in the local network refer to ForkPi using `forkpi.local`
  - Theoretically, Mallory can create a naming collision with ForkPi by setting her own computer's hostname to forkpi, and then running a service under the name `forkpi.local`.
  - However, the service discovery software that we use, Avahi, resolves name collisions by appending a number to the hostname (e.g. `forkpi-2.local`), in accordance with the Zeroconf protocol[20].
  - These numbers are assigned according to the order of start-up. Hence, provided that the ForkPi unit is started before Mallory's computer, `forkpi.local` will refer to the real ForkPi unit. Therefore, it will be hard for Mallory to pass off her own computer as the ForkPi unit.

[20] M. Krochmal S. Cheshire. *Multicast DNS - RFC 6762.* Feb. 2013.

Usability (1 of 4)

- The following figure shows the list of questions and the amount of respondents for each possible response.

Usability (1 of 4)

- The following figure shows the list of questions and the amount of respondents for each possible response.

	1	2	3	4	5
I thought the prototype was too complicated.	7	2	0	0	0
When I was using the prototype, I always knew what I was expected to do.	0	0	0	4	5
I thought the prototype was efficient.	0	0	0	4	5
I would be happy to use the prototype again.	0	0	0	2	7
I found the prototype confusing to use.	6	3	0	0	0
The prototype was friendly.	0	0	0	4	5
I felt under stress when using the prototype.	7	2	0	0	0
I felt this prototype was secure.	0	0	0	4	5
The prototype has a nice user interface	0	0	0	3	6
This prototype has potential.	0	0	0	1	8
I found the prototype frustrating to use.	7	1	1	0	0
I enjoyed using the prototype.	0	0	0	4	5
I felt flustered when using the prototype.	7	0	2	0	0
I think the prototype needs a lot of improvement.	1	6	1	1	0
I had to enter too many details during the prototype.	3	5	1	0	0
I felt the prototype was easy to use.	0	0	0	3	6
I felt that the prototype was reliable.	0	0	1	3	5
I had to concentrate hard to use the prototype.	3	5	1	0	0
I did not feel in control when using the prototype.	4	4	1	0	0
I would use this prototype in my house.	0	1	2	1	5

-

Usability (2 of 4)

- Some of the questions were phrased negatively in order to ensure that the respondents are reading the questions carefully.

Usability (2 of 4)

- Some of the questions were phrased negatively in order to ensure that the respondents are reading the questions carefully.
- There was a total of nine respondents from different walks of life:

Usability (2 of 4)

- Some of the questions were phrased negatively in order to ensure that the respondents are reading the questions carefully.
- There was a total of nine respondents from different walks of life:
  - Four of the respondents were female, while five were male.

Usability (2 of 4)

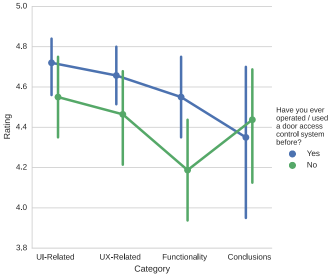
- Some of the questions were phrased negatively in order to ensure that the respondents are reading the questions carefully.
- There was a total of nine respondents from different walks of life:
  - Four of the respondents were female, while five were male.
  - Four of the respondents were within the 18 to 25 age range, the other four were within the 26 to 40 age range, and the remaining respondent was aged 68.

Usability 3 of 4)

- The following figure shows the list of respondents and their answers, grouped by their answer to the question, “Have you ever operated/used a door access control system before?”

Usability 3 of 4)

- The following figure shows the list of respondents and their answers, grouped by their answer to the question, “Have you ever operated/used a door access control system before?”



-

Usability 4 of 4)

- Five of the respondents had no experience at all with keyless door access control systems.

Usability 4 of 4)

- Five of the respondents had no experience at all with keyless door access control systems.
- The respondents who had no experience reviewed the system less favorably, as opposed to the respondents who had experience.

Usability 4 of 4)

- Five of the respondents had no experience at all with keyless door access control systems.
- The respondents who had no experience reviewed the system less favorably, as opposed to the respondents who had experience.
- An exception, however, occurs with questions pertaining to drawing conclusions from the system (e.g. "The prototype has potential."), where the respondents with no experience ranked the system more favorably.

Usability 4 of 4)

- Five of the respondents had no experience at all with keyless door access control systems.
- The respondents who had no experience reviewed the system less favorably, as opposed to the respondents who had experience.
- An exception, however, occurs with questions pertaining to drawing conclusions from the system (e.g. "The prototype has potential."), where the respondents with no experience ranked the system more favorably.
- Overall, the respondents rated the system positively, commenting that the system shows promise and has a lot of potential, especially compared to products that are currently in the market.

Cost-Effectiveness (1 of 3)

- In this section, we list all the hardware components we used for the system, along with their respective prices.

[21] *Amazon.com: Online Shopping for Electronics, Apparel, Computers, Books, DVDs & more*. http://www.amazon.com/. Accessed: 2015-05-28.

Cost-Effectiveness (1 of 3)

- In this section, we list all the hardware components we used for the system, along with their respective prices.
- We then compare the prices of each component against the prices of similar components that can be purchased from the online store Amazon[21].

[21] *Amazon.com: Online Shopping for Electronics, Apparel, Computers, Books, DVDs & more*. http://www.amazon.com/. Accessed: 2015-05-28.

Cost-Effectiveness (1 of 3)

- In this section, we list all the hardware components we used for the system, along with their respective prices.
- We then compare the prices of each component against the prices of similar components that can be purchased from the online store Amazon[21].
- We also compare the total price of our system against similar commercial products that are for sale on Amazon.

[21] *Amazon.com: Online Shopping for Electronics, Apparel, Computers, Books, DVDs & more*. http://www.amazon.com/. Accessed: 2015-05-28.

Cost-Effectiveness (2 of 3)

- In determining the price ranges, we took a look at the price filters on Amazon, and for each price range, we multiplied the number of items by the maximum amount in that range. (e.g.: For the $200 and above price, we set the price to $250.)

Cost-Effectiveness (2 of 3)

- In determining the price ranges, we took a look at the price filters on Amazon, and for each price range, we multiplied the number of items by the maximum amount in that range. (e.g.: For the $200 and above price, we set the price to $250.)
- In determining the lower end of the range, we set the count of the most expensive group to 0, and took the mean price. For the higher end, we set the count of the least expensive group to 0, and took the mean price.

Cost-Effectiveness

	Component	Cost: Project	Cost: Commercial
Base	Raspberry Pi Model B	$35	$35
	OLED Display	$17.50	$10 - $20
	Raspberry Pi Cobbler Breakout	$6.50	$6 - $11
PIN	Keypad	$3.95	$2.5 - $7
RFID	Reader	$39.95	$30 - $80
	MiFare Classic 13.56MHz Card x1	$2.50	$0.5 - $1.5
	Total (Base+RFID+PIN)	$102.9	$80 - $140
Fingerprint	Scanner	$49.95	$40 - $90
	Total (Base+Fingerprint+PIN)	$110.4	$100 - $170
	Total (All Components)	$152.85	$140 - $200

Outline

Recommendations

- In this section, we discuss some of the limitations of our system, and propose various improvements to it.

Recommendations

- In this section, we discuss some of the limitations of our system, and propose various improvements to it.
- These improvements can be implemented by future researchers who plan to either continue this project, or create similar door access control systems.

Recommendations

- In this section, we discuss some of the limitations of our system, and propose various improvements to it.
- These improvements can be implemented by future researchers who plan to either continue this project, or create similar door access control systems.
- Improvements are classified into two categories:

Recommendations

- In this section, we discuss some of the limitations of our system, and propose various improvements to it.
- These improvements can be implemented by future researchers who plan to either continue this project, or create similar door access control systems.
- Improvements are classified into two categories:
    - Vital to use the system in a real world setting

Recommendations

- In this section, we discuss some of the limitations of our system, and propose various improvements to it.
- These improvements can be implemented by future researchers who plan to either continue this project, or create similar door access control systems.
- Improvements are classified into two categories:
    - Vital to use the system in a real world setting
    - Potentially useful as extra features.

Communication with Door Lock

- When implementing the system, a door lock module needs to be installed in the Raspberry Pi.

Communication with Door Lock

- When implementing the system, a door lock module needs to be installed in the Raspberry Pi.
- In the code, however, we have created a dummy door lock class which we give instructions to, like `lock` or `unlock`, so that future researchers will have less trouble implementing the real door lock class.

Exit Button

- Since the SpoonPi controller is only installed outside the room, users who are inside the room need a way to mechanically disable the lock in order to leave the room.

Exit Button

- Since the SpoonPi controller is only installed outside the room, users who are inside the room need a way to mechanically disable the lock in order to leave the room.
- An exit button needs to be connected to the door lock, in order to temporarily unlock it when it is pressed.

Exit Button

- Since the SpoonPi controller is only installed outside the room, users who are inside the room need a way to mechanically disable the lock in order to leave the room.
- An exit button needs to be connected to the door lock, in order to temporarily unlock it when it is pressed.
- This can be implemented using pure hardware wiring; it does not necessarily have to pass through the SpoonPi unit.

Power Supply

- In real world systems, we cannot assume that the power will be consistently on.

Power Supply

- In real world systems, we cannot assume that the power will be consistently on.
- Before a SpoonPi unit loses power, it must be able to unlock all doors, or else someone might get locked inside a room.

Power Supply

- In real world systems, we cannot assume that the power will be consistently on.
- Before a SpoonPi unit loses power, it must be able to unlock all doors, or else someone might get locked inside a room.
- To solve this problem, the SpoonPi must be connected to an emergency power supply, and know how much battery life is left.

Power Supply

- In real world systems, we cannot assume that the power will be consistently on.
- Before a SpoonPi unit loses power, it must be able to unlock all doors, or else someone might get locked inside a room.
- To solve this problem, the SpoonPi must be connected to an emergency power supply, and know how much battery life is left.
- Such a power supply would enable SpoonPi to function even after a power outage, and determine when to release all door locks and shut down.

Power Supply

- In real world systems, we cannot assume that the power will be consistently on.
- Before a SpoonPi unit loses power, it must be able to unlock all doors, or else someone might get locked inside a room.
- To solve this problem, the SpoonPi must be connected to an emergency power supply, and know how much battery life is left.
- Such a power supply would enable SpoonPi to function even after a power outage, and determine when to release all door locks and shut down.
- Another potential improvement for the system is the use of Power Over Ethernet (PoE), so that only one cord needs to be attached to each Raspberry Pi unit. With this, we can provide power and transmit data over the same wire.

Connectivity Indicator

- Like the power supply, we cannot assume that all SpoonPi units will always be able to connect to the ForkPi database.

Connectivity Indicator

- Like the power supply, we cannot assume that all SpoonPi units will always be able to connect to the ForkPi database.
- If network connectivity fails, then SpoonPi will not be able to query ForkPi for keypair matches, hence the whole system falls apart.

Connectivity Indicator

- Like the power supply, we cannot assume that all SpoonPi units will always be able to connect to the ForkPi database.
- If network connectivity fails, then SpoonPi will not be able to query ForkPi for keypair matches, hence the whole system falls apart.
- If we cannot recover from a network failure, we should at least be able to release control of the lock, and communicate the disconnectivity to users.

Connectivity Indicator

- Like the power supply, we cannot assume that all SpoonPi units will always be able to connect to the ForkPi database.
- If network connectivity fails, then SpoonPi will not be able to query ForkPi for keypair matches, hence the whole system falls apart.
- If we cannot recover from a network failure, we should at least be able to release control of the lock, and communicate the disconnectivity to users.
- This can be done in the form of a LED light that is only on when it is connected to ForkPi.

Cached Keypairs

- Should SpoonPi lose its connectivity with ForkPi, SpoonPi has no way of determining which keypairs are authorized, so it has to release the door lock.

Cached Keypairs

- Should SpoonPi lose its connectivity with ForkPi, SpoonPi has no way of determining which keypairs are authorized, so it has to release the door lock.
- Instead of querying the ForkPi database for every transaction, it would be better for the SpoonPi to maintain its own copy of authorized keypairs, so that it can function after a network failure.

Cached Keypairs

- Should SpoonPi lose its connectivity with ForkPi, SpoonPi has no way of determining which keypairs are authorized, so it has to release the door lock.
- Instead of querying the ForkPi database for every transaction, it would be better for the SpoonPi to maintain its own copy of authorized keypairs, so that it can function after a network failure.
- This can be implemented as a cached database copy, which is periodically updated whenever SpoonPi is connected to ForkPi.

ForkPi Hierarchy

- In our system, there is only one ForkPi unit in the entire network. This makes ForkPi a single point of failure.

ForkPi Hierarchy

- In our system, there is only one ForkPi unit in the entire network. This makes ForkPi a single point of failure.
- It is possible to introduce a hierarchy of ForkPis, such that there is a Raspberry Pi unit (called KnifePi) that is dedicated to talking to ForkPis, while the ForkPis are the ones that talk to the SpoonPis.

ForkPi Hierarchy

- In our system, there is only one ForkPi unit in the entire network. This makes ForkPi a single point of failure.
- It is possible to introduce a hierarchy of ForkPis, such that there is a Raspberry Pi unit (called KnifePi) that is dedicated to talking to ForkPis, while the ForkPis are the ones that talk to the SpoonPis.
- Each ForkPi must be able to stand on its own without the help of KnifePi, so that KnifePi does not become a single point of failure.

ForkPi Hierarchy

- In our system, there is only one ForkPi unit in the entire network. This makes ForkPi a single point of failure.
- It is possible to introduce a hierarchy of ForkPis, such that there is a Raspberry Pi unit (called KnifePi) that is dedicated to talking to ForkPis, while the ForkPis are the ones that talk to the SpoonPis.
- Each ForkPi must be able to stand on its own without the help of KnifePi, so that KnifePi does not become a single point of failure.
- ForkPi units can be connected to different networks, as long as KnifePi can reach all of them. For example, one ForkPi can be dedicated to each floor, and one KnifePi for the entire building.

Data Backup and Restore

- Since the memory on the ForkPi's SD card is limited, we want to be able to permanently delete obsolete data in order to free up space.

Data Backup and Restore

- Since the memory on the ForkPi's SD card is limited, we want to be able to permanently delete obsolete data in order to free up space.
- In the ForkPi web app, we already provided a way to export logs to CSV, and delete them from the database.

Data Backup and Restore

- Since the memory on the ForkPi's SD card is limited, we want to be able to permanently delete obsolete data in order to free up space.
- In the ForkPi web app, we already provided a way to export logs to CSV, and delete them from the database.
- However, there is no easy way to back-up keypairs to a file such that they can be restored later if the need arises.

Data Backup and Restore

- Since the memory on the ForkPi's SD card is limited, we want to be able to permanently delete obsolete data in order to free up space.
- In the ForkPi web app, we already provided a way to export logs to CSV, and delete them from the database.
- However, there is no easy way to back-up keypairs to a file such that they can be restored later if the need arises.
- Theoretically, this can be done by dumping the PostgreSQL database and restoring it, but we want to be able to do this inside the web app for convenience.

Date and Time-based Permissions

- In some environments, users can be granted access through a door only at a certain time of the day, or on certain days of the week.

Date and Time-based Permissions

- In some environments, users can be granted access through a door only at a certain time of the day, or on certain days of the week.
- When a keypair is linked to a door, it might be beneficial to be able to specify at which specific times the keypair is valid for that door.

Date and Time-based Permissions

- In some environments, users can be granted access through a door only at a certain time of the day, or on certain days of the week.
- When a keypair is linked to a door, it might be beneficial to be able to specify at which specific times the keypair is valid for that door.
- For example, students should only be allowed into classrooms when they have a class at that time.

Realtime Log Analysis

- Our logging system allows admins to review the logs and check for intruders in the system. In a system with thousands of users, manually checking the logs will become infeasible.

Realtime Log Analysis

- Our logging system allows admins to review the logs and check for intruders in the system. In a system with thousands of users, manually checking the logs will become infeasible.
- Ideally, intrusion detection should be automatically done. For example, if the same keypair was presented to two SpoonPis at around the same time, then one of them might have been an intruder, especially of the two SpoonPis are geographically far apart.

Realtime Log Analysis

- Our logging system allows admins to review the logs and check for intruders in the system. In a system with thousands of users, manually checking the logs will become infeasible.
- Ideally, intrusion detection should be automatically done. For example, if the same keypair was presented to two SpoonPis at around the same time, then one of them might have been an intruder, especially of the two SpoonPis are geographically far apart.
- The hardware components, like the Pi controller or the door knob, can also be checked for damage, since an intruder may try physically breaking the system in order to get in by force.

Conclusion(1 of 2)

- Our system aims to provide cost-effective security to the public.

Conclusion(1 of 2)

- Our system aims to provide cost-effective security to the public.
- Since all the system components can be easily bought from online stores, and we made the code open source, any user that wants to try out the system can build the system for themselves.

Conclusion(1 of 2)

- Our system aims to provide cost-effective security to the public.
- Since all the system components can be easily bought from online stores, and we made the code open source, any user that wants to try out the system can build the system for themselves.
- While the door lock has not yet been integrated into the system, all other major functions are already in place, like determining whether to allow a user based on their input credentials, managing user permissions, and viewing and exporting logs.

Conclusion(2 of 2)

- Communications are encrypted, and additional features such as lockouts are implemented in order to defend against attackers.

Conclusion(2 of 2)

- Communications are encrypted, and additional features such as lockouts are implemented in order to defend against attackers.
- When we presented the system, it was well-received, whether the person had prior experience with similar systems or not.

Conclusion(2 of 2)

- Communications are encrypted, and additional features such as lockouts are implemented in order to defend against attackers.
- When we presented the system, it was well-received, whether the person had prior experience with similar systems or not.
- We have shown that the system is both acceptably secure, and easy to understand and operate, while still costing less than most commercial products currently available in the market.