Authentication Mechanisms Using Raspberry Pi

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

Matthew Kendrick D. Co
matthewdeco@gmail.com

October 2, 2014

Abstract

1 Introduction

2 Literature Review

2.1 Identification and Authentication

Authentication generally comes in two parts. The first step, **identification**, is the act of claiming an identity, a set of attributes that describes an entity (e.g. a user is identified by its username, a person is identified by their fingerprint). Once the entity is identified, **authentication** is done to verify that the entity is indeed who it says it is [10]. Authentication is performed using various **factor**s, 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)

2.2 Types of Authentication Systems

1. **Hardware-based** authentication systems secure tangible resources such as rooms and valuables.
2. **Software-based** authentication systems secure digital resources such as databases.

2.3 Hardware-based Authentication

2.3.1 Disadvantages of Hardware-based Authentication

The hardware used in hardware-based authentication has to be manufactured, shipped, inventoried, distributed and tracked. It also has a higher maintenance cost because it has a vendor-defined lifetime and a lengthy replacement process. Software, on the other hand, can be created as needed on the fly. It also has a customer-specified lifetime and a faster replacement or renewal process. As a result, reports have shown that software-based authentication is 95 percent cheaper than hardware-based authentication [7].

2.3.2 Advantages of Hardware-based Authentication

While software has many advantages over hardware in terms of authentication, a lot organizations still prefer hardware tokens because they feel that their keys are more secure with a physical layer of protection. There are also instances where hardware-based authentication is the only applicable scenario. These scenarios include physical protection such as doors and safes.

2.4 Factors in Hardware-Based Authentication Systems

1. **PIN**s are the most commonly used knowledge-based authentication method. Longer PINs mean better security since it takes more time to guess by brute force.

2. **Smart cards** contain cryptographic keys that are based on the public key infrastructure (PKI) [11]. They are considered to be very secure and can hold a lot of useful information. Since smart card security also usually involves entering a PIN, security is not entirely breached should the card fall into other people's hands.

3. **Radio-frequency identification tags** are typically attached to objects which they identify and transfer information using electromagnetic or radio waves. They are usually cheaper than smart cards but hold less information. Like smart cards, much of the security they provide is lost when stolen.

4. **Biometrics** such as fingerprint, voice, iris or face patterns uniquely identify individuals and are more secure than possession-based factors in the sense that they are difficult to steal or replicate, but less secure in that they can generate false positives and false negatives [11].

2.5 Cost of Hardware-based Authentication Systems

2.5.1 PIN-based

PINs see use mostly in multi-factor hardware-based authentication systems, but they are also viable for single-factor if the system is small or for personal use only, like safes or lockers. For example, the REL.RB3002 Series PIN Locks that are used to provide extra security to doors cost $265.71 per lock. [5]

2.5.2 RFID-based

The two main components of RFID systems are tags and readers. There are two kinds of tags – active and passive, with active tags are more expensive than passive tags. The cost of passive tags are typically at around twenty cents when purchased en masse, while the cost of active tags range from ten to fifty dollars each, even when purchased en masse. The cost of UHF (Ultra High Frequency) readers range from $500 to $3000, depending on their functionality [12].

2.5.3 Smart card-based

The AL5H is a door locking authentication system which is designed for use by hotels [1]. It has undergone vigorous test installations at the Essex Inn, Chicago, and at the Hyatt and ANA Hotels, Tokyo, and at the Bay Landing Hotel, San Fransisco. It is capable of reading both Magstripe and smart cards. The system is available for $229 each at LodgeMart [4].

2.5.4 Biometric-based

When authenticating using biometrics, it is important to minimize two errors: the false acceptance rate and the false rejection rate. False acceptance rate is the probability of unauthorized users being granted access to the system. False rejection rate is the probability of authorized users being denied access to the system.

The MegaMatcher biometric software engine can authenticate users based on various biometrics. When authenticating using a single fingerprint, the false rejection rate is 0.174% at a fixed false acceptance rate of 0.0001%[3]. The components of the fingerprint module cost $222.49 in total[8].

2.5.5 Barcode-based

ChurchTrac, a church database system, uses ID cards or tags with printed barcodes for checking in members and guests. These tags are also used to determine which individuals are allowed to pick-up children from the church.

For small churches (up to 100 people), the Windows version is free while the online version costs $1.35 a week [2].

2.6 Possible Cost of Authentication Using Raspberry Pi

Having Raspberry Pi as the target platform in developing authentication systems seems to significantly reduce the cost. For example, Pi Lock is an open-source authentication system built on the Raspberry Pi and uses RFID and PIN technologies to secure doors. It also provides means to monitor all secured doors and manage user permissions within a network. The fundamental components cost around $85 in total [9], which is relatively cheap compared to other RFID authentication systems.

After evaluating the trade-offs between security, cost and usability, it was decided that PINs, RFID tags and fingerprints would provide the best security at a reasonable cost. Smart cards are quite expensive to produce, costing $2 to $10 [6]. On the other hand, barcodes are inexpensive but the patterns are easy to forge or replicate. For the biometrics, there are many different types, but from the tests conducted by MegaMatcher, fingerprints seem to have the lowest false acceptance and false rejection rates [3].

Regardless of the factor/s to be used used, three components will be needed, namely a Raspberry Pi Model A ($25), an OLED Graphic Display ($17.50), and a Solenoid Lock ($14.95). Prices were taken from Adafruit's online store.

If single-factor PIN is used, a $3.95 keypad will be needed, putting the final price at **$61.40**. This is 77% less expensive than the previously mentioned REL.RB3002 Series PIN Locks.

If RFID is used alongside PIN, additional components would be needed, namely the PN532 NFC/RFID controller breakout board ($39.95) and the Adafruit Assembled Pi Cobbler Breakout + Cable for Raspberry Pi ($6.50), which puts the final price at **$107.85**. The RFID MiFare tags would cost $2.50 each. The reader is at least 78% less expensive than its UHF counterparts. The tags are about $1.6 more expensive, but the system should still be cheaper as a whole provided that only a few tags (around 200) will be used. However, note that UHF readers can detect tags at much larger distances.

If fingerprint authentication is used instead of RFID, a fingerprint scanner costing $49.95 would be needed, putting the final price at **$111.35**, which is 50% less expensive than MegaMatcher's fingerprint authentication system.

If all three factors are to be used, the total cost would be **$157.80**, not including the cost of each RFID tag.

3 Problem Statement

Based on research, secure hardware-based authentication systems are still inaccessible due to their high cost. As a result, such systems are currently confined in the business setting. The goal of this study is to make a hardware-based authentication system that is more accessible to the public by lowering the cost of setup while maintaining or surpassing the security features of existing hardware-based authentication systems. In this study, three authentication factors will be considered: PIN, RFID and fingerprint. CD-R King's Fingerprint Time Attendance System combines all three factors, making it an ideal point of comparison for this study. This study will compare single and multi-factor authentication mechanisms involving the three factors in terms of security, usability and cost in order to determine the combination to be used.

4 Methodology

5 Conclusion

References

[1] AL5H hotel lock system. http://www.miwalock.com/product/al5h/. Last accessed 25 September 2014.

[2] Barcode check-in and child security. http://www.churchtrac.com/knowledgebase/checkin_child_security.htm. Last accessed 24 September 2014.

[3] Megamatcher algorithm features and capabilities. http://www.neurotechnology.com/megamatcher-technology.html. Last accessed 26 September 2014.

[4] Miwa AL5H hotel lock. http://www.lodgemart.com/mialholo.html. Last accessed 25 September 2014.

[5] PIN code locks – REL.RB3002 series pin locks. http://www.keylex.co.uk/acatalog/Pin-Code-Locks.html. Last accessed 26 September 2014.

[6] Smart card technology. http://www.cardwerk.com/smartcards/smartcard_technology.aspx. Last accessed 26 September 2014.

[7] Software-based authentication 95% cheaper than hardware-based authentication, report shows, July 2012. http://www.infosecurity-magazine.com/news/

software-based-authentication-95-cheaper-than/. Last accessed 13 September 2014.

[8] Prices for megamatcher, March 2014. http://www.neurotechnology.com/prices-megamatcher.html. Last accessed 26 September 2014.

[9] Paolo Bernasconi. Raspberry pi RFID door lock. http://www.pi-lock.com. Last accessed 24 September 2014.

[10] Vijayakrishnan Pasupathinathan. *Hardware-based Identification and Authentication Systems*. PhD thesis, Macquarie University, 2009.

[11] CA Technologies. Advanced authentication methods: Software vs. hardware, 2011. http://www.ca.com/~/media/Files/whitepapers/ebook-advanced-authenticaiton-methods.pdf. Last accessed 13 September 2014.

[12] Bob Violino. RFID system components and costs. *RFID Journal*, January 2005.