Fourth Year Project Proposal

Craig Shorrocks 100887781
Jessica Morris 100882290
Richard Perryman 100887250

September 15, 2016

Supervisors: Shikharesh Majumdar and Chung-Horng Lung

Contents

1 Objective

As technology becomes more and more prevalent in our lives, our identities become more and more intertwined with the technologies that we use daily. This melding has become extremely prevalent in some areas. Some such areas are professional networking with LinkedIn, or banking with the advent of online account management. Over half of all smartphone users have used mobile banking [1]. This popularity may be derived from how convenient and secure handling money online is. However, certain aspects of our day to day lives haven't yet been graced by the benefits of electronic security and automation.

Physical locks and keys are still widely used for several tasks where electronic locks could be used instead. House locks, bicycle locks, and locker locks are frequently physical locks. Changing to electronic locks could help streamline all of these locks, reducing the number of keys to remember and improving security by reducing the likelihood that the key could be faked by an attacker. Some applications for this have already been found: for example, Walmart has a system where customers can order products to be placed in lockers with electronic keys called Grab-and-Go [2]. Such a system greatly reduces the work involved in getting a key (in this case, a PIN instead of a physical key or combination) to the customer and increases the security of the lockers by reducing the number of points of failure.

This proposal outlines a system that will expand upon such a concept to further tie security and identity to the electronics we use most: our phones. Using technologies like near-field communication (NFC) sensors and quick response (QR) codes, the identity associated with a phone can be used as identification for anything. This represents a huge advantage with respect to convenience, and it would even further lower the number of possible failure points in security.

2 Background

NFC is a form of short-range, low-power communication used by devices such as smartphones, and tablets. NFC is a fast and convenient method to exchange small amounts of data, as it does not require any steps to set up a connection. One device, the active device, uses magnetic induction to induce a current in the information-holding "passive device". The passive device responds by modulating the EM field coming from the active device, and the active device converts the modulations into useful data [3]. This scenario is a NFC communication in passive mode. Two smartphones may both act as passive and active devices, allowing them to exchange data through a call-and-response procedure, also known as communication in active mode.

NFC is being increasingly used to "smarten up" passive information delivery systems such as business cards, and posters. Information such as contact information, URLs, or credentials may be written to a passive NFC device, such as a smart tag [4], and read by any NFC-enabled mobile device. These mobile devices can also be used to replace credit cards in contactless exchanges. In fact,

NFC payments may be more secure than payment with a card, as each point in the transaction requires the device and the reader to exchange an encrypted password, and the transactio must be approved by the device's user before the device sends payment information [5].

Because of the close range required for an exchange, NFC has inherent protections against attackers. An NFC exchange can only be reliably eavesdropped from a distance of approximately 10 m or less if the interaction is between two active devices, dropping to 1 m if the interaction is a passive communication; and a man-in-the-middle attack is nearly impossible to accomplish in a real-world scenario [6]. These attacks may be protected against by establishing a secure channel, by using symmetric-key encryption or other secret-sharing method. For these reasons, NFC is a reliable method to pair a smart device with an electronic lock.

3 Methods

Lorem ipsum dolor sit amet, consectetuer adipiscing elit. Ut purus elit, vestibulum ut, placerat ac, adipiscing vitae, felis. Curabitur dictum gravida mauris. Nam arcu libero, nonummy eget, consectetuer id, vulputate a, magna. Donec vehicula augue eu neque. Pellentesque habitant morbi tristique senectus et netus et malesuada fames ac turpis egestas. Mauris ut leo. Cras viverra metus rhoncus sem. Nulla et lectus vestibulum urna fringilla ultrices. Phasellus eu tellus sit amet tortor gravida placerat. Integer sapien est, iaculis in, pretium quis, viverra ac, nunc. Praesent eget sem vel leo ultrices bibendum. Aenean faucibus. Morbi dolor nulla, malesuada eu, pulvinar at, mollis ac, nulla. Curabitur auctor semper nulla. Donec varius orci eget risus. Duis nibh mi, congue eu, accumsan eleifend, sagittis quis, diam. Duis eget orci sit amet orci dignissim rutrum.

4 Time Table

Lorem ipsum dolor sit amet, consectetuer adipiscing elit. Ut purus elit, vestibulum ut, placerat ac, adipiscing vitae, felis. Curabitur dictum gravida mauris. Nam arcu libero, nonummy eget, consectetuer id, vulputate a, magna. Donec vehicula augue eu neque. Pellentesque habitant morbi tristique senectus et netus et malesuada fames ac turpis egestas. Mauris ut leo. Cras viverra metus rhoncus sem. Nulla et lectus vestibulum urna fringilla ultrices. Phasellus eu tellus sit amet tortor gravida placerat. Integer sapien est, iaculis in, pretium quis, viverra ac, nunc. Praesent eget sem vel leo ultrices bibendum. Aenean faucibus. Morbi dolor nulla, malesuada eu, pulvinar at, mollis ac, nulla. Curabitur auctor semper nulla. Donec varius orci eget risus. Duis nibh mi, congue eu, accumsan eleifend, sagittis quis, diam. Duis eget orci sit amet orci dignissim rutrum.

5 Components

- Raspberry Pi 3 Model B with 5V power supply and microSD card
- Rasperry Pi Camera NoIR Board Add-on
- Adafruit Feather 32u4 FONA with prototyping board
- Starter Pack for Arduino (with Arduino Uno R3)
- Adafruit PN532 NFC shield
- Soldering tools in ME4135
- Amazon Web Services - Amazon API Gateway, Amazon RDS

Appendices

Appendix A UML

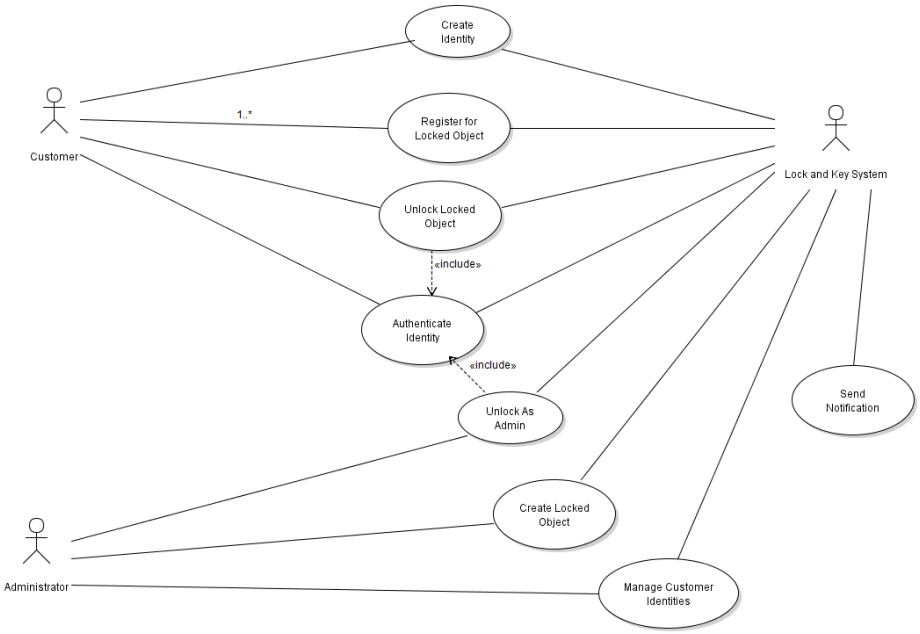

Figure 1: Use case diagram

References

[1] Board of Governors of the Federal Reserve System. *Consumers and Mobile Financial Services*. 2015. URL: http://www.federalreserve.gov/econresdata/consumers-and-mobile-financial-services-report-201503.pdf (visited on 09/15/2016).

[2] Walmart. *Grab And Go*. 2016. URL: http://www.walmart.ca/en/help/checkout/grab-and-go (visited on 08/19/2016).

[3] NearFieldCommunications.org. *About Near Field Communication*. 2016. URL: http://nearfieldcommunication.org/about-nfc.html (visited on 09/08/2016).

[4] NFC Forum. *What is NFC? About the Technology*. 2016. URL: http://nfc-forum.org/what-is-nfc/about-the-technology/ (visited on 09/11/2016).

[5] qrscanner.us. *Near Field Communication Payment and NFC Payment*. URL: http://www.qrscanner.us/nfc-payment.html (visited on 09/11/2016).

[6] Ernst Haselsteiner and Klemens Breitfu. *Security in Near Field Communication (NFC)*. 2006. URL: http://events.iaik.tugraz.at/RFIDSec06/Program/papers/002%20-%20Security%20in%20NFC.pdf (visited on 09/11/2016).