RFID & NFC - Synchronizing Mobile Devices with Embedded Systems

David Tran - A00801942

9 Credit - COMP 8045 Set 8D

British Columbia Institute of Technology

Monday, January 5 2014

Table of Contents

Introduction

General Background of the Project

In business organizations, the use of card scanning as a means for authentication is common. The requirements of such a system involves a central server that can monitor and maintain access privileges, an integrated method of printing these identification cards, a protocol for authentication, card readers and of course, the cards themselves. Unfortunately, these cards are often made of plastic, and while businesses are not required to have to mass-produce these cards often, it is still not environmentally friendly.

A replacement would require some form of contact or wireless communication that is secure enough for means of authentication. Furthermore, the medium needs to be compliant with current technologies, or be capable to transmit a unique identifier that can quickly and reliably authenticate the user. And of course, the proposed solution needs to be cost-effective for both the user and the organization.

As technology advances in today's society, so too does the technology become readily available to consumers. Prime examples are today's smartphones. Many of today's smartphones come packed with Near-Field Communication (NFC) chips, a means of authentication. Many major banking institutions have adopted this technology to further their mobile banking experience to their users, as well as a means to attract customers to use mobile payment, simply by tapping their phone on tap-enabled electronic fund transactions (EFTs).

If banking institutions trust the technology enough to invest into it, then NFC technology should be secure enough for use by other businesses and by homeowners. At the moment, NFC has not been adopted as a means of security but the medium – the smartphone – has been used in conjunction with many other technologies such as WiFi, and Bluetooth. We want to discover if NFC is capable to provide the same – if not, better – means of security as the previously mentioned technologies.

Purpose of the Project & Components for Innovation

The primary purpose of the proposed study is to understand if NFC authentication is an attractive means for security. It is important to understand that this study will not be addressing the security risks between digital and physical authentication. The purpose of this research is to develop and integrate components for innovation that consists of smartphones, embedded systems, and the interrelationship between Radio Frequency Identification (RFID) and NFC.

As stated in the 9-credit COMP 8045 criteria, the project is required to be innovative as well as containing elements that are considered experimental, or exploratory in nature to meet the criteria of the COMP 8045 practicum. The project seeks to be innovative and explorative by attempting to integrate currently used means of encryption in the form of public key infrastructure, digital certificates and digital signatures with NFC technologies. The project also seeks to experiment with the security of the aforementioned implementation by conducting a series of penetration tests using the Kali Linux suite.

Firstly, the innovation criteria of the project can be justified by the fact that NFC is an emerging technology that only recently has been implemented in sensitive transactions. A prime example is the previously highlighted use of NFC and mobile banking. The project seeks to take the next step with NFC to use it as a means of secure authentication. This component also fulfills the criteria for innovation because NFC has yet to be used in place of Bluetooth and WiFi. With that being said, any form of security besides utilizing the mobile carrier's encryption methods shall also be innovative.

Secondly, the explorative criteria of the project is justified because of how NFC is an emerging technology, making any other integrated component to be a part of emerging technology. Therefore, while the general consensus regarding public key infrastructures, digital certificates and digital signatures are considered to be a staple in security and integrity, they become new technology when applied to other newly emerging technologies. The explorative component comes from researching and understanding the above-mentioned means of security, implementing them, and then ensuring that proper communication is ensued.

Finally, the experimental component of the project is achieved by conducting a series of penetration tests on NFC and RFID technologies. Ultimately this will highlight any drawbacks or downfalls of using NFC technologies as a means of security and authentication. By revealing these flaws, the project can then seek to patch these flaws, making NFC authentication that much more attractive. After achieving the above three criteria, the project seeks to continue innovation by utilizing popular and other emerging technologies. These technologies are highlighted below:

Utilizing Embedded Systems

As a proof-of-concept, the project shall implement its system using Raspberry Pi. The Raspberry Pi shall serve as the infrastructure's central server, in which it will process the communication between the RFID reader and the NFC-capable smartphone. The system is also beneficial due to its form factor and simplicity, making the development of a proof-of-concept much more feasible within the limited time frame of this project. The concepts of embedded systems can be applied to any similar embedded system in the present, such as Arduino chipsets, and in the future.

Combining RFID with NFC

While RFID has been in existence for a long time, NFC has only begun its emergence in popularity within the last few years. The idea between these two technologies is to allow current technology to coexist with new and upcoming technology. When NFC becomes more "mainstream", there will not be a need to introduce new proprietary systems, which makes NFC-based systems more attractive to implement.

Integration of Mobile Devices

The majority of NFC technologies reside within modern smartphone architecture. Therefore, the prime candidates to test NFC hardware and software would be to utilize smartphones. Unfortunately, at this time, only Android- and Windows OS-based smartphones are capable of NFC development; Apple iOS NFC technologies have been extremely limited to mobile payments. The smartphone of choice for this project shall be the Google Nexus 5 or the Samsung Galaxy Note 4; we have opted for an Android-based smartphone because of its availability to the researcher and due to its larger smartphone market share. The choice of either smartphone is dependent on the financial budget of the researcher.

Terms, Concepts, & Definitions

Throughout this paper, **“NFC”** will refer to the Near-Field Communication technologies that exist currently in smartphones and potentially other evolving technological devices. “NFC-enabled devices” will refer exclusively to smartphones that have NFC technologies in them.

“Security” refers to the concept of how information, especially identity, will be kept safe from data breaching. “Security systems” can refer to the currently existing identification systems that allow personnel to gain access through doors and area, as well as the new system proposed by this research proposal.

“Protocol” with respect to security, refers to the communication between NFC devices. The protocol will encompass the format the information between devices transfer to one another, as well as the sequence of the transfer between the two devices. Specifically, “NFC Protocol” will refer to the actual near field communication headers and packet transfer. “Systems” will refer to the security and authentication systems at the residential and/or organizational level.

“Radio Frequency Identification” (RFID) is a technology that incorporates the use of electromagnetic or electrostatic coupling in the radio frequency portion of the electromagnetic spectrum to uniquely identify an object, animal, or person.

“Concurrent Technology” refers to the technology that is used by home owners and business organizations with respect to security access. The research is mostly concerned with the systems that are currently in place at business organizations mainly because home owners still use physical objects such as keys. An example of concurrent technology in this research topic is the product, brand or system that maintains the organization’s access control, such as Avigilon Access Control systems and servers.

Problem Statements & Research Overview

How can we develop modern smartphones to become a digital representation of their owners? Which form of data security is secure enough for mobile authentication? Are these newly developed technologies susceptible to attacks that can compromise the integrity of the smartphone and its user(s)?

Sub-Problem I

The first obstacle of this project is to ensure that there is proper communication between the smartphone medium and the RFID reader. To do this, we shall configure the RFID reader with its embedded system and correlate its compatibilities with the smartphone and NFC technologies.

Pseudo-Problem I for Sub-Problem I

In order to address the needs of Sub-Problem I, the Raspberry Pi and the RFID reader need to be in working order. This means that the two hardware technologies must be able to communicate with each other through some form of software. This software may already exist or may need to be developed by the researcher using a language of their choice.

Pseudo-Problem II for Sub-Problem I

Once we address the first pseudo-problem for Sub-Problem I, the application that resides on the Android medium must be developed according to RFID standards and NFC capabilities. Using Java programming, we shall use Object-Oriented design to develop and design an intuitive graphical user interface that can control and administer the communication on the Android smartphone.

Sub-Problem II

The second obstacle of this research project is to develop data security features that can uniquely identify and authenticate NFC communication to the RFID reader. To do this, we shall reference our literature review for suggestions and attempt to implement as many data security features as possible to ensure the integrity of the NFC device.

Sub-Problem III

The final obstacle addresses the possibility of hacks that can be conducted on our system. We shall compare these attacks on raw systems (systems that do not have any security measures in place) and with systems that have security features. We shall conclude whether the systems were compromised to analyze the degree of security.

Preliminary Project Assumptions

1	NFC technologies are able to perform authentication, and are capable of using authentication protocols.
2	NFC and RFID technologies used in this research project shall not need any proprietary components.
3	The project shall only develop a proof-of-concept to determine concept feasibility.
4	NFC devices shall be at least be Android version 4.0.0 (Ice Cream Sandwich) for testing purposes.

Project Delimitations

The project shall develop the software technology that allows NFC devices to be able to communicate with RFID readers. The project shall develop some security measures, where possible, that can be implemented with the NFC device and RFID reader and then conduct penetration testing against these new security measures, if possible. The project shall document all exploratory outcomes, whether they had passed or failed testing criteria. Ultimately, the project seeks to establish the coexistence of current technologies (RFID) and new emerging technologies (NFC) while exploring alternative means of security.

The project shall not develop access control methods. The project shall not seek to create proprietary software or hardware. Also, the project shall not seek to deliver a finished product that is ready for market consumption.

Research Significance

The ultimate goal of this study is to provide the public with an alternative and secure method that can integrate with their daily lives. Through research, we can design and develop a means of gaining access using contact communication while giving device owners peace of mind. Currently, smartphones are the only devices with NFC technology that can provide security but this study can open doors for future technologies such as emerging smart watches as a means of access control and authentication. Trends have already started seeing the modularity of many common items such as calendars, credit cards, identification, etc. be integrated into one central device. The proposed study follows that trend and extends further to integrate a key mechanism for homeowners and for businesses and organizations.

Future Expansion for Innovation of Project

Due to financial restrictions and time constraints imposed on this project, the following components shall not be addressed. However, for expansion and implementation for future prospective researchers and students alike, these components may be considered innovative and can be included in the future.

Centralized Server Integration & Access Control Groups

While we have an embedded system that is a standalone server that works along side our RFID reader, we can “lighten the load” of the embedded system and have it forward the information to a centralized server. This centralized server will monitor locations for authorized access for example.

Once a foundation for a home network is established using a centralized server and multiple users, we can then begin to implement access control groups to allow only certain users access to certain places.

Include Email & SMS Notification

The inclusion of email and SMS notification can allow users, homeowners especially, to know whether there are suspicious activity occurring around areas where NFC authentication is in place. This is due to the fact that, once a centralized server is configured, networking notifications becomes a simple matter of connecting all NFC and RFID readers using our embedded systems together in a switch or wireless network.

However, it is unrealistic to configure a mail server for each embedded system; instead, it will be much easier to have one centralized mail server that resides on the centralized server that we have already mentioned. An SMS server can only be attained by enlisting the help of a designated telecommunications service provider.

Project Deliverables

All project deliverables, at the time of composing this documentation, shall be mostly software components and electronic copies of relevant documentation. Some components to note are:

1. RFID & Raspberry Pi Code Listings that works with NFC including:
    a. attempts at Public Key Infrastructure;
    b. attempts at Digital Certificates; and,
    c. attempts at Digital Signatures

2. NFC Application Code Listings that was developed on the Android OS including:
    a. attempts at Public Key Infrastructure;
    b. attempts at Digital Certificates; and,
    c. attempts at Digital Signatures

3. Links to any penetration testing tools used, if applicable

4. Electronic copies of documents including:
    a. Major Project Report in PDF
    b. Major Project Proposal in PDF
    c. Any other legal documents in PDF

Enhancing Expertise in Network Security Administration

We live in a society where technological advances occur at an exponential rate. With a keen interest in Android development, and emerging technologies such as NFC, it is imperative to be a part of the technology in its early years so that ideas for innovation can become a part of the technology's exponential growth.

Having a background in Computer Information Technology (CIT) from the British Columbia Institute of Technology, there were limited opportunities to be fully involved or exposed with Android development, and embedded systems. There was only once where there was exposure to Android: COMP 4900, whereby the project entails implementing multiplayer capabilities to an already existing game developed by its previous team in COMP 3900. The Android game utilizes WiFi-Direct technologies for its lobby room and uses WiFi connection for the actual game. These were all new concepts for CIT students but we were able to effectively execute and deliver the game with two components for multiplayer: turn-based and real-time options.

With nearly full control and almost no limitation for this upcoming project, it is appropriate to return to our roots, utilizing the popularity of Android OS, the emergence of NFC and the modularity of embedded systems such as the Raspberry Pi. Not only will the project include development of the system but it is also intended to perform penetration tests, which is currently covered by the Network Security Administration option of the Bachelor of Technology program. The scope, duration of project, and components for innovation is believed to be appropriate for enhancing learning, experience and most importantly, fun.

Literature Review

Researchers from various studies regarding NFC and its capabilities have confirmed three modes: peer-to-peer, card emulation and reader/writer mode. In addition, it seems that the most common uses of these three modes occur from card emulation, whereby the NFC device acts as a replacement of physical items such as credit cards and keys; and reader/writer mode where the device acts as access smart cards, RFID transponders and NFC tags. (Rowland & Langer, 2010, p. 71)

There have been numerous proposals for security implementation in the emerging technology. Such proposals refer to the use of digital signatures, borrowing the tried-and-true encryption and security algorithms of existing cellular 3G networks, offline tag authentication, and the use of stored tokenization methods.

Many of the studies have confirmed that the idea of using smartphone devices with NFC that are compliant with the NFC Data Exchange Format will be able to work concurrently with RFIDs. That means that already existing technology that uses integrated circuits and radio fields will be able to work cooperatively with each other. The issue is how to integrate the new technologies.

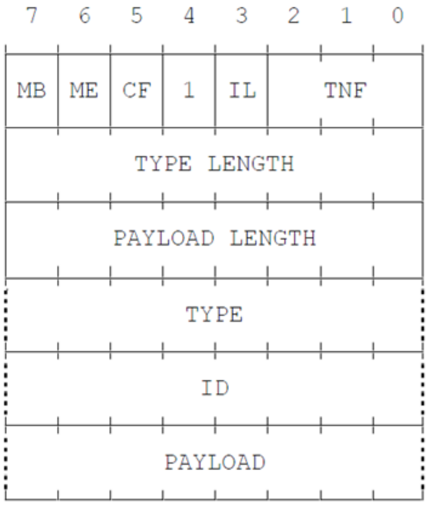

Figure 1 - The NFC Data Exchange Format

Firstly, Roland and Langer have proposed that the use of digital signatures be embedded inside the NFC Data Exchange Format to avert malicious users that will use these NFC readers or tags for phishing scams. It is important to note that Roland and Langer's proposal utilizes digital signatures in conjunction with public-key cryptography. When combined, the protocol reveals three critical traits with regards to security: its authenticity, where "the signing party can be determined unambiguously"; "unforgeability", where "only the holder of a secret signing key can create an authentic signature"; and non-reusability, where "a signature is bound to the signed data and cannot be used for any other data … [assuring] the integrity of the signed data." (Roland & Langer, 2010, pp. 73-74) However, some concerns arise with compatibility issues between NFC devices: those that follow the exchange format, and those that do not. There are also cases where some fields in the format cannot and should not be digitally signed or else further complications may arise.

Chen, Hancke, Mayes, Lien, and Chiu proposed a scenario of using cellular 3G networks for authentication, because banking institutions use them. Advantages of using the already-existing 3G networks allow developers to reuse algorithms that have been proven to be secure. It also reduces technical changes in the programming and allows flexible and broad scalability. (Chen, Hancke, Mayes, Lien, & Chiu, 2010, p. 447) However, these advantages require that the reader and the user must be both on the same Mobile Network Operator. Other requirements include no calls during the NFC communication, and a shared secret key. Therefore, visible disadvantages illustrate a dependency on functioning mobile networks, and cannot receive or make calls during the NFC transaction. (Chen et al. 2010, p. 447)

On the opposite end of the spectrum, Saeed and Walter had proposed an offline means of NFC authentication. (Saeed & Walter, 2012, p. 730) Their proposal, Tag Authentication Record, is an authentication protocol that contains parts of digital certificates. Combining ideas of Roland and Langer's ideas of digital signatures, a transfer of digital certificates attached to the payload of the NFC communication allows great compatibility with already existing devices and without the reliance on cellular coverage. To further add to their proposal, Saeed and Walter suggested using a challenge-response protocol in their proposal that includes the use of public key cryptography and public key infrastructure. (Saeed & Walter, 2010, p. 732)

Finally, Cha and Kim highlighted the use of tokenization with both card emulation and read/write modes. Simply put, tokenization can be embedded inside the NFC device which is generated from the server by a random seed, and the token is stored in the server database, where records could be checked. Their implementation is almost a hybrid of online and offline methods because if its non-reliance on 3G networks, but on the contrary, it relies on the local area network infrastructure instead. (Cha & Kim, 2013, p. 712)

The previous research material clearly identifies that smartphones with NFC capabilities are able to work as a card emulation mode, which is identical to how hotel rooms are accessed. Because we have grounds to confirm that NFC-enabled devices can work with RFID scanners, the next step in this research topic is to develop a tertiary program that can communicate with these systems on the smartphone, utilizing NFC. Once the foundation of an architecture is in place, it is imperative to test and compare as many of the above proposed means of security so see which is the most feasible while is offering the greatest means of security.

Research Methodology & Technologies Used

Strategies for Data Collection & Analysis

Much of the data collection shall pertain to answering whether or not the code or program works the way it is intended to. The data collection shall be comparing the actual outcome of test events with the expected outcome when such an event occurs. Proof of these test cases failing or passing shall be provided via screenshots of outputs, text dumps, or captures.

When collecting data during penetration testing, data collection will seek to determine whether the attacks were successful in compromising the system. Compromising the system includes masquerading of the legitimate user, interception of sensitive data, or phishing the RFID reader.

Intended Tools & Technologies to be Used

Hardware Components of the RFID Reader & NFC Medium

- Raspberry Pi B+ Model
- Google Nexus 5
- Parallax RFID USB Reader
- Samsung Galaxy Note 4
- RFID tags (for testing)

Hardware Components for Project Development

- MacBook Pro 15”
- Personal PC
- BCIT Lab PC

Software Components

- Android Development Environment
- Terminal Console
- Kali Linux
- Java / Python on Raspberry Pi
- Fedora 20 64-bit
- Apple iOS “Mavericks”
- Shell scripting
- Windows 8.1 64-bit
- Linux Debian “Wheezy”

Preliminary Test Cases for RFID Reader

Case #	Test Case	Tools Used	Expected Outcome
1	Placing an RFID tag in the vicinity of the RFID reader.	Terminal / “Notepad-equivalent”	There is some form of output that shows that the RFID reader recognizes the RFID tag.
2	Placing an NFC medium with NFC enabled in the vicinity of the RFID reader.	Terminal / “Notepad-equivalent”	If there is an output, it means that the RFID reader can already recognize the NFC device.
3	Placing an NFC medium with NFC enabled in the vicinity of the RFID reader.	Terminal / “Notepad-equivalent”	If there are no outputs, it means that the RFID reader have yet to recognize the NFC device.

Preliminary Test Cases for Various Security Measures

Case #	Test Case	Tools Used	Expected Outcome

1	Toggling a switch in the app of the medium to turn on NFC.	Android medium	NFC becomes enabled.
2	Toggling a switch in the app of the medium to turn off NFC.	Android medium	NFC becomes disabled.
3	When NFC is enabled, it is able to communicate with the RFID reader when placed in its vicinity.	Android medium, Terminal, “Notepad-equivalent”	The app responds with an appropriate message; the console shall output some message that is congruent with the app’s message.
4	When NFC is disabled, it is not able to communicate with the RFID reader when placed in its vicinity.	Android medium, Terminal, “Notepad-equivalent”	The app has no responses; the console shall not have any messages.

Preliminary Test Cases for Various Security Measures

Case #	Test Case	Tools Used	Expected Outcome
1	The Raspberry Pi is able to generate public key-pairs.	Java, Terminal, “Notepad-equivalent”	The Raspberry Pi can output public-key pairs.
2	The Raspberry Pi can authenticate the Android device using the device’s public key and the Pi’s private key.	Java, Terminal, “Notepad-equivalent”	The Raspberry Pi shall output the appropriate message when authentication is successful.
3	The Raspberry Pi can authenticate the Android device using the device’s public key and the Pi’s private key.	Java, Terminal, “Notepad-equivalent”	The Raspberry Pi shall output the appropriate message when authentication is not successful.
4	The Android medium is able to generate public key-pairs.	Android app	The Android device can display public-key pairs.
5	The Android medium outputs a message when authentication is successful.	Android app	The Android device shall display an appropriate message when authentication is successful.
6	The Android medium outputs a message when authentication is successful.	Android app	The Android device shall display an appropriate message when authentication is not successful.
7	The Raspberry Pi is given a payload with digital signature.	Java, Terminal, “Notepad-equivalent”	The Raspberry Pi can process RFID payloads with a digital signature to verify.
8	The Raspberry Pi can authenticate the Android device using the provided digital signature.	Java, Terminal, “Notepad-equivalent”	The Raspberry Pi shall output the appropriate message when authentication is successful.
9	The Raspberry Pi can authenticate the Android device using digital signatures.	Java, Terminal, “Notepad-equivalent”	The Raspberry Pi shall output the appropriate message when authentication is not successful.
10	The Android medium is able to provide a digital signature in its payload.	Android app	The Android device can provide digital signatures in the payload.

11	The Android medium outputs a message when authentication is successful.	Android app	The Android device shall display an appropriate message when authentication is successful using digital signatures..
12	The Android medium outputs a message when authentication is successful.	Android app	The Android device shall display an appropriate message when authentication with digital signatures is not successful.
13	The Raspberry Pi is given a payload with digital certificate.	Java, Terminal, “Notepad-equivalent”	The Raspberry Pi can process RFID payloads with a digital signature to verify.
14	The Raspberry Pi can authenticate the Android device using the provided digital certificate.	Java, Terminal, “Notepad-equivalent”	The Raspberry Pi shall output the appropriate message when authentication is successful.
15	The Raspberry Pi can authenticate the Android device using the provided digital certificate.	Java, Terminal, “Notepad-equivalent”	The Raspberry Pi shall output the appropriate message when authentication is not successful.
16	The Android medium is able to provide a digital certificate in its payload.	Android app	The Android device can provide digital certificates in the payload.
17	The Android medium outputs a message when authentication is successful.	Android app	The Android device shall display an appropriate message when authentication is successful using digital certificates..
18	The Android medium outputs a message when authentication is successful.	Android app	The Android device shall display an appropriate message when authentication with digital certificates is not successful.

Project Timeline

As per the project's guidelines, the minimum amount of hours spent on the project must be at least 405 man-hours. The project will begin on January 5th 2015 with an initial due date by May 1st 2015, and an extension lasting to January 1 2016. Below is a breakdown of the milestones that shall be achieved through this project, and their projected hours:

Milestone 1: Configuring Embedded Systems & RFID Reader

This project milestone includes the setup and familiarization of the Raspberry Pi, its operating system, and some preliminary form of RFID reader configuration. Some form of testing shall be conducted and the test cases and results shall be documented in the final report of the research project. For now, some example test cases can be referenced in the former of this document. After testing the waters with the Raspberry Pi and its RFID reader, we can move on to the next milestone.

Components	Description	Estimated Hours	Accumulated Hours
Familiarization of Raspberry Pi and "Wheezy" Operating System	Understanding the hardware limitations, how things are implemented, and where things should go. Understanding Debian environment over Redhat / SUSE / Fedora.	20 hours	20 hours
Installation and configuration of RFID Reader	Understanding the hardware with relation to software. Basically, a period to play around with the components of the system hardware architecture.	20 hours	40 hours
Testing RFID Reader with included RFID tags, cards, tokens, etc.	Testing the hardware components by verifying Raspberry Pi's software components. Results shall be documented as testing progresses.	20 hours	60 hours
Documentation of Project Report	An ongoing component of the research project, whereby each milestone shall be tested according to test cases. Test results shall be documented accordingly and to the best of the researcher's ability.	10 hours	70 hours

Milestone 2: Develop Android App to Communicate with RFID

Once we are done experimenting with the embedded systems, we can transition to working with our medium of choice. In this research project, we have delimited our medium to be an Android operating system, and to use either the Google Nexus 5 or the Samsung Galaxy Note 4. Using the Android Development Environment, we shall develop an app that can turn on NFC capabilities of the smartphone and to communicate using RFID standard protocols. Some preliminary test cases shall be applied to the app developed.

Components	Description	Estimated Hours	Accumulated Hours
Develop and design GUI and application core	Enlist some roommates that are good in design work and ask for ideas on how to make the app intuitive.	20 hours	90 hours
Program and code NFC and RFID-compliant components	Some preliminary coding that will allow the smartphone to be recognized by the RFID reader.	40 hours	130 hours
Test application and code to some degree	Testing to see that the RFID reader recognizes the smartphone. Using these “dumps” we can gauge how difficult the next milestone will be.	20 hours	150 hours
Document all preliminary findings	An ongoing component of the research project, whereby each milestone shall be tested according to test cases. Test results shall be documented accordingly and to the best of the researcher’s ability.	10 hours	160 hours

Milestone 3: Ensure Android App is RFID-Compliant

In this component, we refer to our literature review for ideas on improving security between the two components. We shall try to implement as many of the security features as possible between the application and the RFID reader, and then record if the attempts failed or passed. This component of testing and development is exploratory in nature and is used to see if other means of security can be used for authentication.

Components	Description	Estimated Hours	Accumulated Hours
Implement Public Key Infrastructure	Configuring between the Raspberry Pi and the Smartphone app, to adopt a Public Key Infrastructure.	40 hours	200 hours
Implement Digital Signatures	Configuring either the RFID reader or the Smartphone to provide correct and incorrect digital signatures.	40 hours	240 hours
Implement Digital Certificates	Configuring either the RFID reader or the Smartphone to provide recognized and unrecognized digital certificates.	40 hours	280 hours
Testing each security measure	Each security measure shall be tested against a series of test cases.	30 hours	310 hours
Penetration Testing (if possible) with Kali Linux	Using Kali Linux and its suite of penetration testing tools, to test our application.	30 hours	340 hours
Documentation of all security findings, lessons learned, and identification of weaknesses	An ongoing component of the research project, whereby each milestone shall be tested according to test cases. Test results shall be documented accordingly.	30 hours	370 hours

Milestone 4: Finalize Project Deliverables

Once we reach this milestone in the research project, it becomes a matter of finishing up the final project report and adding any missing components to the report. We shall use any time during this milestone to make adjustments to our project as necessary.

Components	Description	Estimated Hours	Accumulated Hours
Finish Project Report	Adding details, diagrams, etc. that are required as part of the final project deliverables.	15 hours	385 hours
Other miscellaneous components that have not been addressed.	Any component that have not been addressed by the project or have not been encountered by the researcher.	20+ hours	405+ hours

References

Cha, B., & Kim, J. (2013). Design of NFC Based Micro-payment to Support MD Authentication and Privacy for Trade Safety in NFC Applications. Complex, Intelligent, and Software Intensive Systems (CISIS), 2013 Seventh International Conference on, 710-713.

Chen, W., Hancke, G., Mayes, K., Lien, Y., & Chiu, J. (2010). Using 3G network components to enable NFC mobile transactions and authentication. Progress in Informatics and Computing (PIC), 2010 IEEE International Conference on, Volume 1, 441-448.

Roland, M., & Langer, J. (2010). Digital Signature Records for the NFC Data Exchange Format. Near Field Communication (NFC), 2010 Second International Workshop on, 71-76.

Saeed, M., & Walter, C. (2012). Off-line NFC Tag Authentication. Internet Technology And Secured Transactions, 2012 International Conference for, 730-735.

Appendix I – Researcher Resume

DAVID TRAN

136 8th Avenue West
Prince Rupert, BC V8J 2P3

E: david.tran_@outlook.com
T: 1.604.354.9326

RELEVANT SKILLS

Adobe Creative Suite • Microsoft Office • Java Programming • C# Programming
C Programming • Time Management • Team Leadership • Writing Proficiency

EDUCATION

BRITISH COLUMBIA INSTITUTE OF TECHNOLOGY, BURNABY, BC

Bachelor of Technology, Expected April 2015

Network Security Administration **GPA: 3.95**

- BCIT Legacy of Leadership Award
- Linda & Allan Stefanson Memorial – Excellence in Computing and Academic Studies

Diploma of Technology w. Distinction, May 2013

Computer Information Technology **GPA: 3.70**

- Industry Sponsor Student Projects 2012, 2013 – "Practicum" Project Leader

WORK EXPERIENCE

SUMMER STUDENT INTERNSHIP MAY 2014 – AUGUST 2014

Finance Dept. (IT) - Prince Rupert Port Authority, Prince Rupert, BC

- Trusted with off-hours office access during card access replacement resulted in fast, non-abrupt transition from old to new card access systems
- Cable installation and termination in cramped and tight areas allows installation of new technologies to occur at more convenient and better suitable locations whilst providing neat and clean cable installation
- WhatsUp Gold network monitoring system evaluation and implementation; finished evaluation in 1 week, implementation in 2 weeks ongoing; reduced troubleshooting time by 50% per downed device and allows graphical and statistical details at key locations to help make informed decisions for future technological installation
- "Transcribed" Microsoft Excel reports to SQL Server Reporting Services allows automated report generation and delivery while eliminating key person risks

SOLE-PROPRIETOR, WEB DEVELOPER JUNE 2011 – PRESENT

Prometheus Innovations, Prince Rupert, BC

- Applied schooling by developing websites implemented with industry standards, giving local businesses a chance to invest in a local IT business
- Giving back to community by providing fast and inexpensive IT solutions to local businesses, allowing them to pursue future IT endeavors

TUTOR, CAMP BUDDY, WEB MASTER SEPT. 2009 – PRESENT

PAC 10 Tutoring, Prince Rupert, BC

- Having an open mind through tutoring groups of four or one-on-one; adapts tutoring approaches for each student per subject
- Demonstrates role model and leadership qualities during Summer Camps; comfortable working with children grades Pre-K to Grade 7
- Maintaining website and provided continual website development, logo update, and social media integration as part of volunteer work, reducing costs of freelance design by nearly $2000

OTHER EXPERIENCE

KITCHEN & SERVICE CREW JULY 2008 – FEB. 2011

McDonald's Restaurant, Prince Rupert, BC

- Ability to plan ahead by managing quality control and daily product availability
- Demonstrated leadership and teamwork by leading teams of four during shifts; orders per second less than 1min
- Strong work ethics: youngest employee to close the restaurant alone at the age of 15