

SECURED AUTOMATED LOGON FOR WINDOWS
USING PRESENCE DETECTION

by

Azlyn Ab Manap

Dissertation submitted in partial fulfillment of
the requirements for the
Bachelor of Technology (Hons)
(Business Information System)

JULY 2010

Universiti Teknologi PETRONAS

Bandar Seri Iskandar

31750 Tronoh

Perak Darul Ridzuan

CERTIFICATION OF APPROVAL


Secured Automated Logon for Windows Using Presence Detection

by

Azlyn Ab Manap

A project dissertation submitted to the
Business Information System Programme
Universiti Teknologi Petronas
in partial fulfillment of the requirement for the
BACHELOR OF TECHNOLOGY (Hons)
(BUSINESS INFORMATION SYSTEM)

Approved by,



(YEUKWANG HOOI)

UNIVERSITI TEKNOLOGI PETRONAS

TRONOH, PERAK

July 2010

CERTIFICATION OF ORIGINALITY

This is to certify that I am responsible for the work submitted in this project, that the original work is my own except as specified in the references and acknowledgements, and that the original work contained herein have not been undertaken or done by unspecified sources or persons.

AZLYN AB MANAP

ABSTRACT

This report focuses on the research and development of a reliable automated logon and logoff to Windows using tag presence detection and voice command. This project was developed to overcome the common problem of unauthorized user who scrutinizes other's personal computer by providing a more effective way for the large number of computer users to logon and logoff automatically. The reader that had been setup shall capture the movement of a tag. Each tag had been designed to be detected by each personalized computer. The reader will capture the movement on real-time basis, capturing the time and date of the logon or logoff process. To attend to security concerns, voice recognition will be used in this project. The user is allowed to enter a voice command through a microphone to logon and logoff. The project should be reliable, speaker independent and has a low total hardware price tag. A noise reducing headset is used to increase recognition accuracy. Implementation of this project is aimed to introduce a new approach in logging on and off personal computers, yet safe and protected. This paper describes the capability and functionality of the whole application.

ACKNOWLEDGEMENT

All praise and thanks are due to Allah alone, the One, the All-High and All-Merciful. Blessings and peace be upon Prophet Muhammad, the last of His messengers and prophets, his family, companions and all those who follow in his footsteps till the end of time.

This project would not have been possible without the consent of the people that have guided me throughout the development of the system. It is a pleasure to convey my gratitude for the people who have given their heart whelming full support throughout the way.

I owe my deepest gratitude to my supervisor, Mr Yew Kwang Hooi, who has supported me throughout the development of this project with his assistance, support, patience, and insights, and also for spending a lot time sharing his knowledge and giving guidance on what should be completed. Your time spent had helped me understand the expectations needed to be achieved.

I would also like to thank Ms Amy Foong Oi Mean and Ms Penny Goh Kim Nee for assessing my project and giving motivating comments. Your reflections were much appreciated.

My heartfelt appreciation is also extended to my student colleagues who have been supportive and helpful throughout this project including Ms. Aini Farhana Asridin, Ms. Shafinaz Zulham and Mr. Muhd Hafiz. We have been through a lot of ups and downs together. Many thanks to others as well, who had helped me during the completion of the project. Without them, this journey would not be as wonderful.

Special thanks should be given to my parents who had encouraged and supported me financially. Finally, words alone cannot express the thanks I owe to Zairul Zahha, my other half, for his assistance, patience and understanding.

I apologize if I have unintentionally left out any individual who has helped me throughout this project. I thank you all. God bless.

Table of Contents

CERTIFICATION OF APPROVAL.....	ii
CERTIFICATION OF ORIGINALITY	iii
ABSTRACT	iv
ACKNOWLEDGEMENT	v
INTRODUCTION	1
1.1 BACKGROUND.....	1
1.2 PROBLEM STATEMENT	1
1.3 OBJECTIVES AND SCOPE OF STUDY	2
Objectives.....	2
Scope of Study.....	2
1.4 THE RELEVANCY OF THE PROJECT	2
LITERATURE REVIEW AND THEORY	3
2.1 Passwords	3
2.2 Windows Logon	3
2.3 Logon Security	4
2.4 Voice Recognition.....	5
2.5 Presence Detection	6
2.6 Other Applications	7
2.8 Windows GINA.....	8
2.9 Visual Basic.....	9
2.10 Phidgets	9
METHODOLOGY	10
3.1 Requirements Gathering.....	10
3.2 Development of SDLC Model	11
3.2.1 Planning.....	12
3.2.2 Analysis, Design and Implementation.....	12
3.2.3 Implementation.....	12
3.3 Tools.....	13
3.4 Gantt Chart	14

ANALYSIS AND DESIGN	15
4.1 Findings	15
4.2 Data Analysis	16
4.3 Project Deliverables	17
4.3.1 System Architecture	17
4.3.2 Flowchart.....	18
4.3.3 Use Case Diagram	19
4.3.4 Database Entity Relationship Diagram	20
4.4 Devices	21
4.4.1 RFID Reader.....	21
4.5 Phidget.....	24
4.7 Tag Testing Process.....	25
4.9 Authentication Process	26
4.10 Result Testing.....	30
4. 10.1 System Performance.....	30
4. 10.2 Time Testing.....	31
4.10.3 Proximity Testing	31
CONCLUSION AND RECOMMENDATION.....	32
5.1 Relevancy to the Objectives	32
5.2 Suggested Future Work for Expansion and Continuation.....	32
5.2.1 Improvised Hardware	32
5.2.2 Improvised Voice Command.....	32
5.2.3 Multiple User.....	32
5.2.4 Noise reduction.....	33
5.2.5 Voice Translation	33
5.2.6 Reader Proximity.....	33
REFERENCES	34
APPENDICES	36

List of Figures

Figure 1: System Development Life Cycle	11
Figure 2: System Architecture.....	17
Figure 3: Flowchart	18
Figure 4: Use Case Diagram	19
Figure 5: Database ERD	20
Figure 6: RFID Reader	21
Figure 7: Phidget Installation	22
Figure 8: Tag Information	23
Figure 9: USB Connector	23
Figure 10: RFID Tags	24
Figure 11: WinLogon for Logon Events	25
Figure 12: Tag Reading	25
Figure 13: Tag Count Function	26
Figure 14: Tag Authentication	27
Figure 15: Source Code Snippet for Loading the Tags	27
Figure 16: Add/Update Tag.....	28
Figure 17: Source Code Snippet for Add/Update Tag	29
Figure 18: Time Taken to Detect Tag	31
Figure 19: Time Taken to Load Windows	31

List of Tables

Table 1: Gantt Chart	14
Table 2: Survey Results	16
Table 3: RFID Reader	21
Table 4: System Performance Testing	30

CHAPTER 1

INTRODUCTION

1.1 BACKGROUND

This report described the project of developing “Secured Automated Logon for Windows Using Presence Detection” mainly use for computer users. Computer users usually leave their computer logged on even when the user is not in front of the computer. Since computers are used every day in daily life, there is a need to develop this project. In certain cases such as in an office or in a public places, this issue might become a threat to an individual or a company. This project is developed to create an automated process of logon and logoff windows.

The process of logging on and logging off is a normal security practice to secure an access to a computer or website. Usually, we would need to click the icon to logon to our personal computer. However, with this device, you may logon and logoff automatically using presence detection and voice recognition. Instead of having to click the icon and insert your password, a user will wear a tag, which is detected by the computer of its presence. The user may also speak or give instruction which is read by the computer microphone. When the authentication has been made, the computer will logon.

Later, if the user forgets to logoff, and went away from the computer, the computer will detect that the tag is nowhere near the set radius, it will logoff automatically. Comparing to the traditional way, this project may help keeping information and documents secured and no violation of stolen documents or information.

1.2 PROBLEM STATEMENT

There is a need to create an effortless and easy way to logon and logoff windows because of the many cases of illegal logins by other users.

1.3 OBJECTIVES AND SCOPE OF STUDY

Objectives

1. To develop an automated logon and logoff to Windows using ID detection and voice recognition.
2. To test security and reliability of using RFID technology and voice recognition for automated authentication.

Scope of Study

This project is focusing on the development of user interface that automates the process of logging on and off Windows system for users. Using the combination of several embedded applications provided from Windows with several additional devices so that the objectives are achieved, and yet security is not compromised.

The project does not cover the study of overcoming the issues of speech recognition. The project will only focus on the consistency of the combined process of proximity and speech recognition.

1.4 THE RELEVANCY OF THE PROJECT

The project is pertinence in a way that the security of one's personal computer is always at risk. Although it is password enabled, and it is true that longer and alpha numerical passwords are more secured but user tends to forget their passwords. To overcome to this, user uses a simpler easy to remember passwords like birthdays, partner's name and such. Some of the users write their passwords on a Post-it and stick it under the keyboard or drawer. Having said this, it is relevant to develop this project to overcome this problem.

CHAPTER 2

LITERATURE REVIEW AND THEORY

Personal computer has been the part and parcel of our everyday life. Some of us, may have kept important files or data in their personal computers. Some of us too, have jobs that require discretion of reports, files and such from unauthorized users. Logon and logoff process is a common security practice. Logging in and off your computer is part of the security measure so that your personal computer is not exposed to any unauthorized usage or breach. The process of logging in is to enable you to access your computer, and when the usage is done, logging off will get you or anyone else inaccessible of the computer. Therefore, there is a need to explore other simpler approaches to logon and logoff Windows but still putting security measures up front.

2.1 Passwords

Probably the most common technique employed for user authentication involves the use of passwords. However, the deficiency of traditional password-based access systems is well known and has even led some researchers to predict the disappearance of this kind of system. When people want to set their passwords to words they can easily remember, it is easy to crack by guessing or by simple brute-force dictionary attacks. Longer passwords are more secure, but harder to remember. In the event, stronger passwords cause more cost of maintaining help desk calls for forgotten passwords. There are two main reasons that make the situation worse as time goes on. The reasons are the ease of password sniffing and the difficulty of managing multiple passwords (Park, Hong, Oh, & Lee, One Touch Logon: Replacing Multiple Passwords with Single Fingerprint, 2006)

2.2 Windows Logon

The interactive logon process is the first step in user authentication and authorization. Interactive logon is mandatory in the Windows Server 2003, Windows XP, Microsoft Windows 2000, and Windows NT 4.0 operating systems. Interactive logon provides a

way to identify authorized users and determine whether they are allowed to log on and access the system. Windows interactive logons begin with the user pressing CTRL+ALT+DEL to initiate the logon process. The CTRL+ALT+DEL keystroke is called a secure attention sequence (SAS); Winlogon registers this sequence during the boot process to keep other programs and processes from using it. The GINA DLL generates the logon dialog box. A user who logs on to a computer using either a local or domain account must enter a user name and password, which form the user's credentials and are used to verify the user's identity. For smart card logons, a user's credentials are contained on the card's security chip, which is read by an external device, a smart card reader. During a smart card logon, a user enters a personal identification number (PIN) instead of a user name, domain, and password (Microsoft, 2009).

Probably the most common technique employed for user authentication involves the use of passwords. However, the deficiency of traditional password-based access systems is well known and has even led some researchers to predict the disappearance of this kind of system. When people want to set their passwords to words they can easily remember, it is easy to crack by guessing or by simple brute-force dictionary attacks. Longer passwords are more secure, but harder to remember. In the event, stronger passwords cause more cost of maintaining help desk calls for forgotten passwords. A lot of methods have been put into account for the logon process (Park, Hong, Oh, & Lee, One Touch Logon: Replacing Multiple Passwords with Single Fingerprint Recognition, 2006).

2.3 Logon Security

In Windows operation system, the access mechanism via end-user account and password authentication are vulnerable to attacks such as account and password theft or conjecture, and therefore doesn't meet the requirement for the higher security grade. In the existence logon models, the most of the password management are forced by some regulations and implemented by manual work. If there is something wrong with the operation, the system may attacked by the replay attack, dictionary attack or brute-force attack. Alternately, people use smart-card, fingerprint or iris-scan based biometrics or

the combination of these models to improve the security of the system access [1-2]. However, due to the restriction of the Windows operation system, the essential mechanism of all these logon models is to establish the mapping between the Windows password and the private information that customers have kept (smartcard, biometric information, or certification etc.) (Li, Wu, Guo, Li, & Niu).

2.4 Voice Recognition

This application uses voice recognition in order to login into Windows. Each computer is identified uniquely with one user (can be several users). This is possible with the Speech Recognition and Text-to-Speech provided in the Windows. The Voice Control application is a 32-bit windows application which opens a session with Microsoft's Text-To-Speech and Voice Command Recognition engines. The complexity of establishing and maintaining this interface is hidden from the Test Executive. The Voice Control system maintains the speech recognition grammar. When the Test Executive needs to modify the grammar, it sends a windows message to the Voice Control application. When a phrase from the current grammar is recognized, the Voice Control application sends a windows message back to the Test Executive (Evans, Tjoland, & Allred).

The phrase "automated methods" refers to three basic methods connected with biometric devices: (1) a mechanism to scan and capture a digital or analog image of a living personal characteristic; (2) compression, processing and comparison of the image to a database of stored images; and (3) interface with applications systems (Rashid, Mahalin, Sarijari, & Abdul Aziz, 2008).

For integration into an office environment the complexity of the voice recognition software necessitates for optimum performance a 450 Mhz machine with 250 MB Ram. A location away from windows, concrete walls (reflected sound can cause echoes) and the noise of co-workers and telephones is required. Research by Goette (1998) highlighted the problem of ambient noise seriously undermining voice recognition

performance and resulting in the unsuccessful implementation for some individuals, although more sophisticated systems can filter out background noise (Mills).

2.5 Presence Detection

RFID technology may be used in this project as it can be connected with the wireless technology embedded in the personal computer. RFID is a technology that uses electromagnetic transmission (i.e., radio waves) to store and retrieve data from an identification chip. This chip is called an RFID tag or transponder and is read by an RFID reader or transceiver without human interaction. An RFID system comprises five key components – RFID tag or transponder, reader/writer, encoder, middleware, and application software. The RFID reader/writer requests the identifying information contained in the microchip by sending an RF signal to the tag that then uses its antenna to transmit that information to the reader/writer. The reader then translates the received information into a digital form and sends it to the application software with the help of a middleware. The encoder, often the RFID reader/writer itself, encodes the data for storage in the tag once or many times, depending upon whether the RFID tag is a read-only tag or a read-write tag (Hossain & Prybutok, 2008).

RFID tags are used in this project because of its low consumption of energy. This is because it is planned not to store the captured data in the tag, it will be captured in the database developed later. This is shown by study performed before. For computational RFID tags, transmitting data consumes less energy than storing it locally. This observation motivates a new approach to protocol design in which tags outsource storage to readers. The challenge then is to enforce data integrity and confidentiality without negating energy savings. The EPC Gen-2 tags, the most prevalent form of barcode-type RFID, have a low-power regime that permits a conversion of the “kill” operation (a privacy feature) into a crude challenge-response protocol (Juels, 2009).

RFID is a not-contact technology that identifies objects attached with tags. Today RFID technology is widely used for various purposes. RFID has been widely applied to various areas such as railway transport monitoring, highway fees and charges, tracking of agricultural products, food, medicine, animal identification, anti-counterfeiting,

logistics transportation, etc. Nowadays, low-cost RFID has attracted more and more interests from both industry and academic institutes. In supply chain management, RFID tags are used throughout the supply chain to track products, from supplier, delivery, to warehouse stock and retail (Minbo & Chen, 2009).

2.6 Other Applications

Some other application using similar concept is the Security System using Biometric technology. Previously, the most popular methods of keeping information and resources secure are to use password and UserID/PIN protection. These schemes require the users to authenticate themselves by entering a "secret" password that they had previously created or were assigned. These systems are prone to hacking, either from an attempt to crack the password or from passwords which were not unique. A Biometric Identification system is one in which the user's "body" becomes the password/PIN. Biometric characteristics of an individual are unique and therefore can be used to authenticate a user's access to various systems (Rashid, Mahalin, Sarijari, & Abdul Aziz, 2008).

Another application that uses voice recognition can be seen in this journal. They try to build a system that can recognize spontaneous speech. How to automatically expand and adapt phonetic dictionaries for spontaneous speech recognition. Especially for spontaneous speech it is important to choose the pronunciations of a word according to the frequency in which they appear in the database rather than the "correct" pronunciation as might be found in a lexicon. Therefore, we proposed a data-driven approach to add new pronunciations to a given phonetic dictionary in a way that they model the given occurrences of words in the database. If phonological rules are used to derive pronunciation variants, the number of rules can vary between several dozens and more than thousand. Using only a few rules does not necessarily cover all spontaneous effects, using too many rules on the other hand results in too many possible variants. Even applying a few rules to a dictionary increases the number of pronunciations (and

therefore increase the computational cost) significantly. Expert knowledge is needed to restrict the application of rules; otherwise overgeneralization of rules *can* lead to bogus variants (Sloboda & Waibel).

2.7 Fingerprint

Whereas, this application is somewhat similar in terms of logging on and passwords authentication. Fingerprint is the most popular modality that is widely used in various authentication applications; PC logon, gate access control systems, and so on. The reason can be considered that fingerprint can achieve the best balance among authentication performance, cost, size of device, and ease of use. However, most of fingerprint authentication devices have some problems to be solved. One is that captured images are easily affected by the condition of finger surface and it can degrade authentication performance. The other is that the problem of impersonation by artificial gummy fingers has been pointed out. To solve those problems, we developed a new fingerprint authentication device that has a novel sensing principle. This device forms a image of fingerprint pattern based on optical characteristics of a finger's interior by scattered transmission light. The images so obtained are unaffected by the condition of finger surface such as dry or moist fingers or operating environment, and enable stable authentication processes. And it can differentiate between real fingers and fake gummy fingers made from gelatin or other material using optical characteristics (Sano, Maeda, Nakamura, & Shikai, 2006).

2.8 Windows GINA

GINA stands for Graphical Identification and Authentication. The GINA operates in the context of the Winlogon process and, as such, the GINA DLL is loaded very early in the boot process. The GINA DLL must follow rules so that the integrity of the system is maintained, particularly with respect to interaction with the user. The most common use of the GINA is to communicate with an external device such as a smart-card reader. It is essential to set the start parameter for the device driver to system (Winnt.h: SERVICE_SYSTEM_START) to ensure that the driver is loaded by the time the GINA is invoked. The purpose of a GINA DLL is to provide customizable user identification

and authentication procedures. The default GINA does this by delegating SAS event monitoring to Winlogon, which receives and processes CTL+ALT+DEL secure attention sequences (SASs). A custom GINA is responsible for setting itself up to receive SAS events (other than the default CTRL+ALT+DEL SAS event) and notifying Winlogon when SAS events occur. Winlogon will evaluate its state to determine what is required to process the custom GINA's SAS. This processing usually includes calls to the GINA's SAS processing functions. (Library, 2010)

2.9 Visual Basic

An Implementation of Microsoft's event-driven programming language Visual Basic, and associated integrated development environment (IDE), which is built into most Microsoft Office applications. By embedding the VBA IDE into their applications, developers can build custom solutions using Microsoft Visual Basic. (Wikipedia, the free encyclopedia, 2010)

2.10 Phidgets

Phidgets are a system of low-cost electronic components and sensors that are controlled by a personal computer. Using the Universal Serial Bus (USB) as the basis for all phidgets, the complexity is managed behind an Application Programming Interface (API). Applications can be developed in Mac OS X, Linux, Windows CE and Windows operating systems. Their usage is primarily focused to allow exploration of alternative physical computer interaction systems, but have most notably been adopted by robotic enthusiasts as they greatly simplify PC-Robot interaction. Phidgets are an attempt to build physical analogue to software widgets, allowing the construction of complex physical systems out of simpler components. Phidgets are designed and produced by the phidgets company. (Wikipedia, the free encyclopedia, 2010)

CHAPTER 3

METHODOLOGY

The research methodology for this project is aimed on how to gain knowledge required completing the project including literature review, study of previous projects and searching from the internet sources. The internet provides various sources by the search engines; Google and Yahoo which are vital because many developers share their findings and opinion in the forums. Books only provide the theoretical overview and concepts. Therefore, planning of the methodology is crucial in the process of developing this project.

3.1 Requirements Gathering

Requirement gathering is the first step in any project. There is a need to find out whether there is a market for the project being develop. Also, finding out whether there is a need for the project to be developed.

For this step, several methods are being used; interviewing and survey. Interview is done to random employees who use computers for their jobs. The interview includes questions that are based on security and ease of use. The interview also enlighten on computer user's behavior and habits on everyday life.

Surveys were given out to a range of computer users. The survey includes question on how often they use the computer. The survey also assesses what do the users think of the current process of logging on and logging off the computer. It also includes what do the user thinks of securing their personal computers.

The information; pros and cons are also evaluated from the literature review. Different opinions were assessed. Some improvements that are found to be crucial and helpful are

made. Thus, a few designs are being compared to get the best design out of the few selections being shortlisted.

3.2 Development of SDLC Model

The prototyping based technology is chosen for this project because of the suitability with the system to be developed. Other factors that this methodology was being chosen is because of time constraint and manpower. This methodology performs the three phases; Analysis, Design and Implementation in parallel. These phases are performed until the desired outcome has been achieved. After that, the implementation phase will be performed. This will allow several refinements to be made. This methodology is chosen because of the limited time frame given whereby if the project derails from the schedule, some functions may be adjusted. Also, this methodology allows a working prototype to be tested in shorter time.

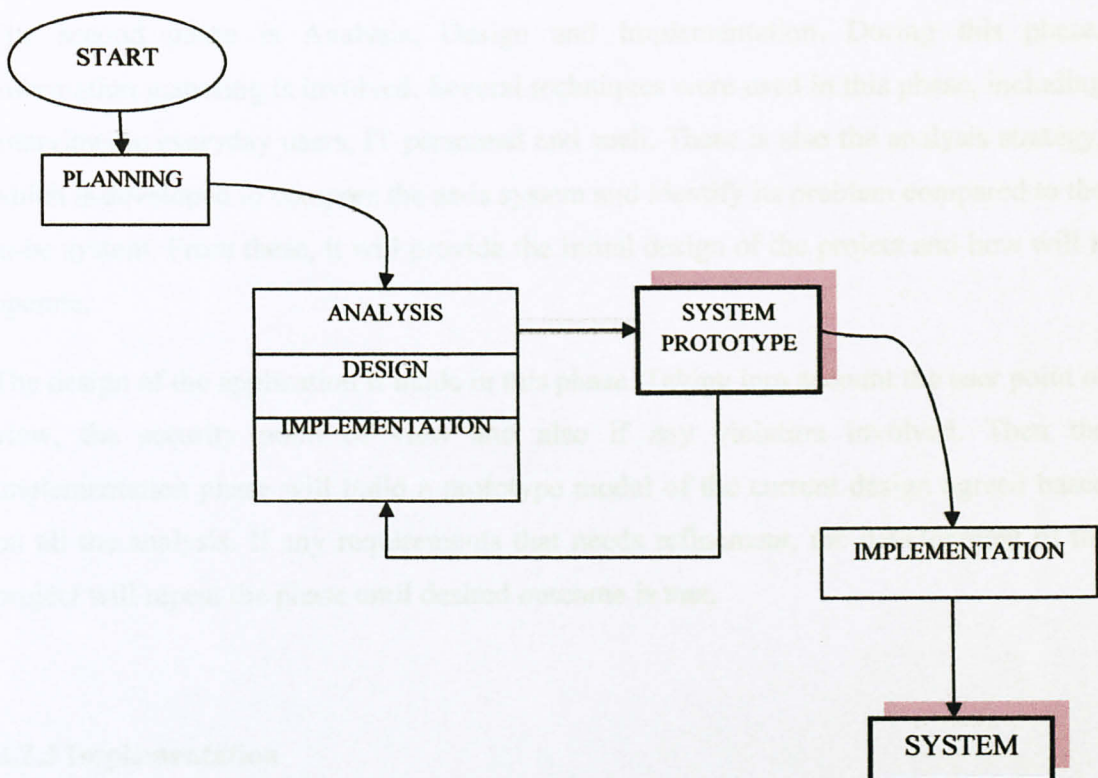


Figure 1: System Development Life Cycle

The methodology chosen has several phases as seen in Figure 1. The major milestone will be the accomplishment of certain features in the project as there is a need to ensure the components are working.

3.2.1 Planning

The first phase of this methodology is planning. This is when a feasibility analysis was made. This is to determine whether it will provide benefits and whether it can be build. Comparison was made between the existing products available in the market with the project planned. Information was also gathered from case studies, journals, books, websites and newspaper in relation of this project.

3.2.2 Analysis, Design and Implementation

The second phase is Analysis, Design and Implementation. During this phase, information gathering is involved. Several techniques were used in this phase, including interviewing everyday users, IT personnel and such. There is also the analysis strategy, which is developed to compare the as-is system and identify its problem compared to the to-be system. From these, it will provide the initial design of the project and how will it operate.

The design of the application is made in this phase. Taking into account the user point of view, the security point of view and also if any violation involved. Then the implementation phase will build a prototype model of the current design agreed based on all the analysis. If any requirements that needs refinement, the development of the project will repeat the phase until desired outcome is met.

3.2.3 Implementation

During this phase, the actual system is built from the prototype model. Hence, the final product will present the best designed prototype. Also, during this phase, after the

system is successfully installed, support plan is developed. This is the main deliverable of this project.

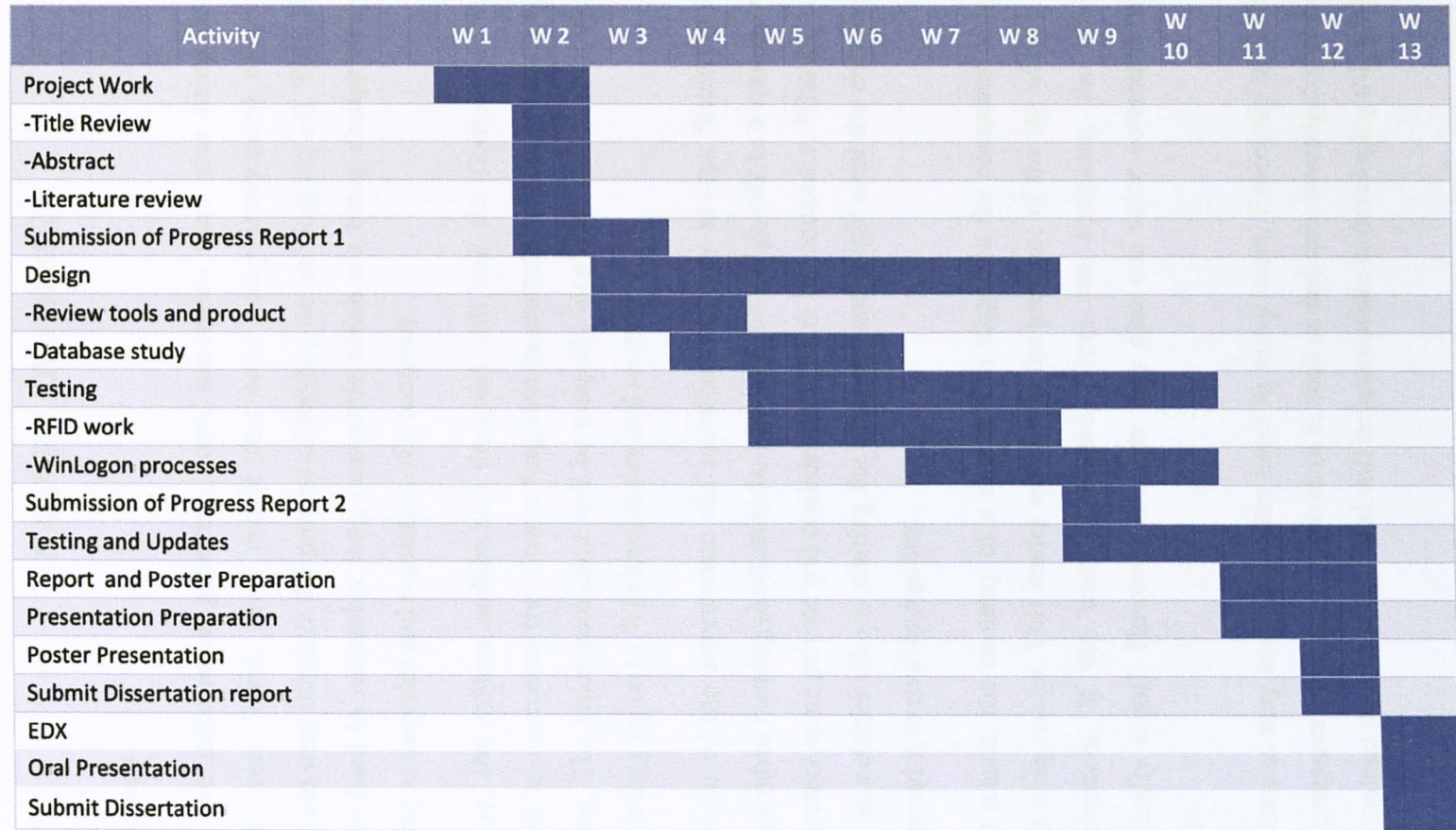
3.3 Tools

The tools and programs needed for this project may vary throughout the project. At this stage, the most needed tool is to have a computer with a PC soundcard and PCI audio card installed, most of the computers now have this pre-installed prior purchasing it. A noise cancelling headset with microphone might be a useful tool for the computer to capture the voice of the user. A tag reader is also needed to detect the presence of the unique tag.

The programs that will be involved in this project would be Windows Text to Speech. This is to convert the user's voice to text. This then will be compared to the pre-saved voice commands in the database (Microsoft Office Access). The interface will integrate all of these programs. This will be developed in JAVA language. An open source software, Phidgets is used to recognize the RFID reader, also to register the tag. Software called PollGina is used to modify the windows process logon events.

3.4 Gantt Chart

Table 1: Gantt Chart



CHAPTER 4

ANALYSIS AND DESIGN

4.1 Findings

During the information gathering, some interviews were also being done. Several findings were found. Most people that were being interviewed thinks that voice recognition may improve the process of logging on and logging off. They also mention that it is hard to remember long passwords which are being change every 3 months according to the rules and regulation of a company.

Therefore, the system architecture designed will suit the findings of the problem. Basically to overcome the always forgotten passwords will be replaced by the voice command. The voice command will be uniquely identified with a computer. This will make the logging on to Windows easier and secured.

Also, some of the interviewee did mention that they always forgot to logout their computer when running short errands. This may be a high risk to a company who really has to protect some private and confidential files in the computer. Who knows that there may be an outsider who is visiting the company and might steal the documents or even worst spread it to rival companies.

For that reason, the nametag of a user is also tagged to the computer which has been installed a tag reader. This reader will detect the presence of the tag when it is between the perimeters. If the user steps away from the computer, the computer will automatically logoff. However, the user may also use voice command to logoff the computer.

These features may assist computer users in many ways. Especially to jobs that really rely on computers and the documents in it, such as auditors, investigator and such. Thus, it is determined that the tools listed will be appropriate in developing this project.

4.2 Data Analysis

Based on the survey (refer to appendix I) done on 30 people, these are the results;

Table 2: Survey Results

No	Question	Percentage of YES (%)
1	Does your work require a computer?	93
2	Do you spend more than 5 hours a day in front of the computer?	86
3	Do you think that keying in your password to logon/logoff your computer a hassle?	60
4	Do you always forget your password?	73
5	Have you heard of voice recognition technology?	57
6	Do you think that logging on would be easier with voice recognition?	60
7	Do you think it is important to logout after using the computer?	53

From this survey, conclusion is made that security is the most important element in keeping your personal folders. We also know that nearly 95% of users use the computer each day. Many of the interviewee did mention that they are lazy to remember their ever changing passwords. The process of logon and logoff will automatically logon when your voice stored is being recognized.

4.3 Project Deliverables

4.3.1 System Architecture

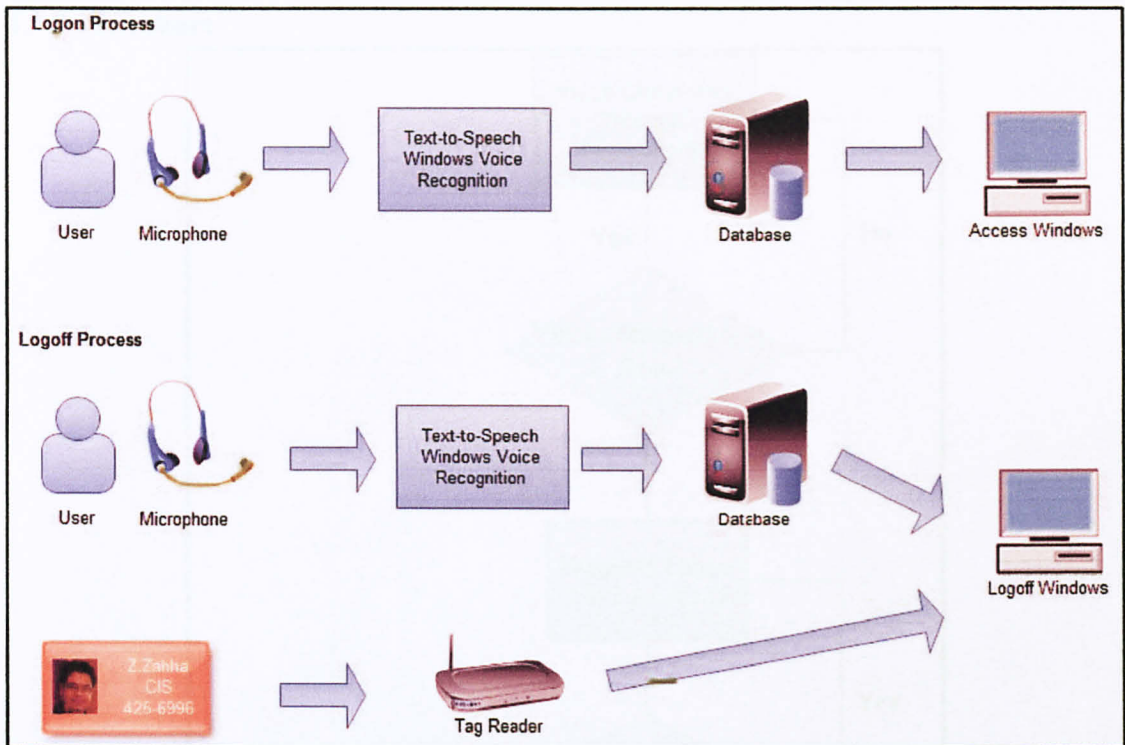


Figure 2: System Architecture

The system architecture of this project may be seen in this figure here. A user speaks a command into the microphone. Later this command will be transfer to the Windows Voice Recognition. Then when the voice has been converted into text, it will be compared in the database. If the voice command matches the one stored, Windows will logon automatically.

However, when the user is away from the computer, the tag reader will detect the tag that is being used by the user. The secured radius has been set. When the user steps away from the computer, it will automatically logout. The process of logging out may also be done manually by voice command.

The RFID tag is being used here as a security measures. For instance, if the user forgets to voice out the voice command to logout, the detection of tag may be used in order to

safely protect the files in the computer. This may come in handy when the user is always on the move.

4.3.2 Flowchart

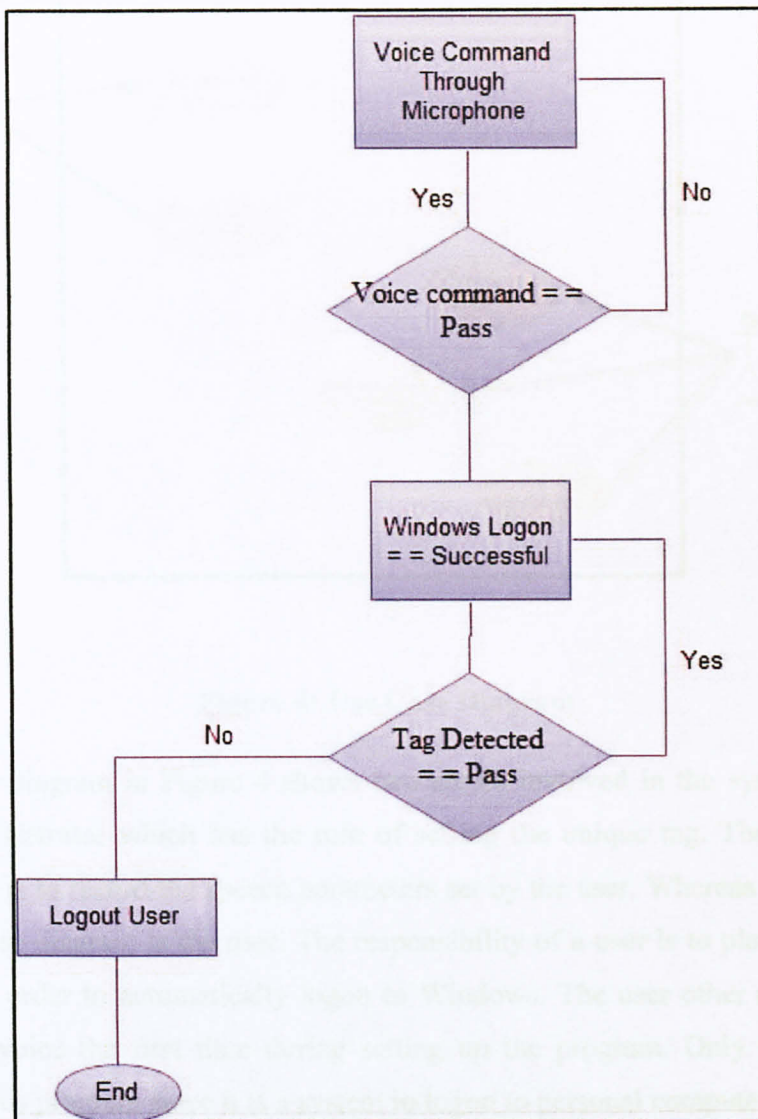


Figure 3: Flowchart

Figure 3 shows the flowchart of the application. When the voice is command through the microphone, the computer will check and compare the voice. If it passes the test then Windows will logon and the user will have access to it. Else, the user need to voice out the command again. If the user moves away from the computer, the tag reader will notify that the tag is not in the safe radius, therefore it will logoff automatically.

4.3.3 Use Case Diagram

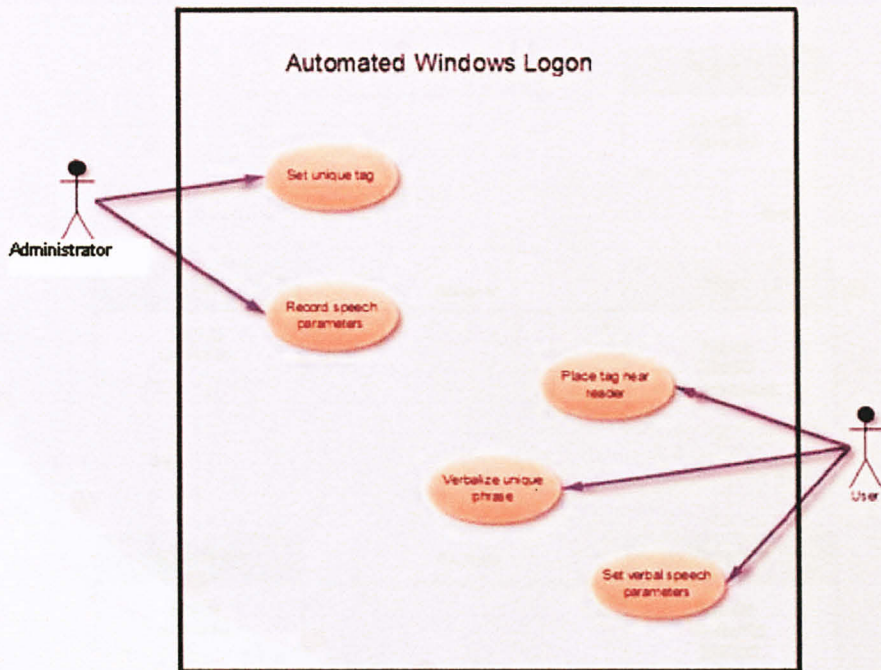


Figure 4: Use Case Diagram

The use case diagram in Figure 4 shows two actors involved in the system. The first actor is administrator which has the role of setting the unique tag. The other role of administrator is to record the speech parameters set by the user. Whereas the other actor in this use case diagram is the user. The responsibility of a user is to place the tag near the reader in order to automatically logon to Windows. The user other roles is also to record their voice the first time during setting up the program. Only two actors are involved in this program since it is a system to logon to personal computers.

4.3.4 Database Entity Relationship Diagram

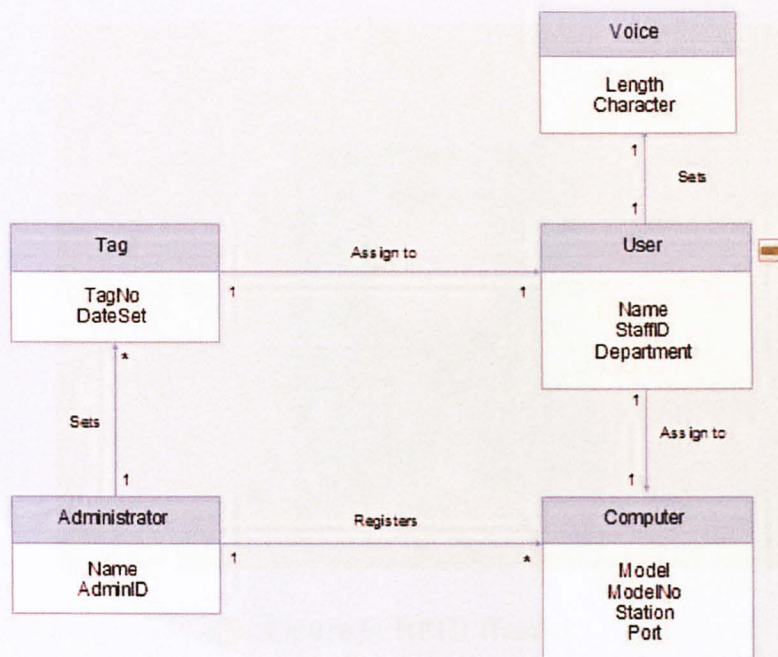


Figure 5: Database ERD

Figure 5 shows the database entity relationship diagram. This shows the parameters that will be captured in the database. The username, staffID and from which department the user is from will be stored for safety reasons. Also the computer where the system is installed will need to be recorded. Administrator here is the maintenance person who sets up the system and help with assembling the system. The tags are uniquely numbered and will be attach to one user only. The speech parameters will also be stored in the database.

4.4 Devices

4.4.1 RFID Reader

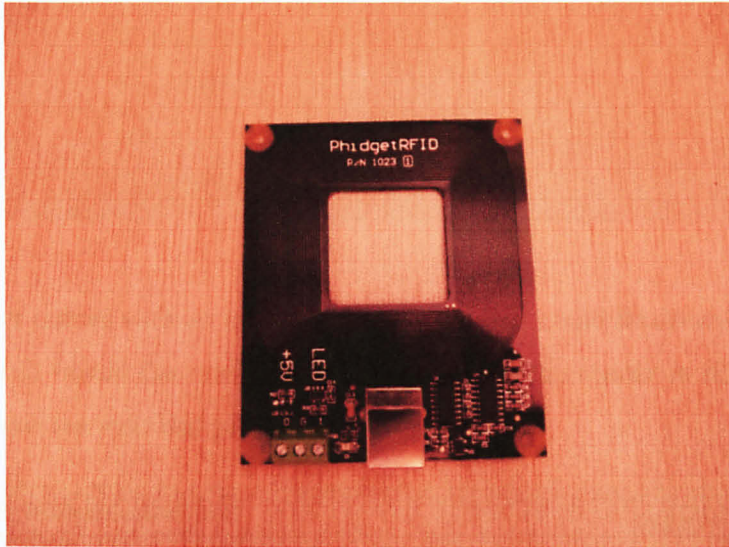


Figure 6: RFID Reader

The RFID reader is used to read the tag. The reader will be installed and programmed in the user's computer. When the reader detects the tag, it will trigger the program. However, due to the poor signal of wave, the tag needs to be near the reader to able the tag to be read. For the purpose of this study, this low cost RFID reader is used to prove that the study and research done is feasible. Therefore, a better reader should be more appropriate for this project. Nevertheless, the design and testing had proved it is usable.

The triggered program will be load and user will be logged on to Windows. Table 3 lists the details of the RFID reader.

Table 3: RFID Reader

Name	Phidget RFID reader
Serial Number	103402
Version	206
Reads	40-bit value contained in EM4102 RFID tags
Operating Systems	Windows 2000/XP/Vista Windows CE

	Linux Mac OS X
Languages	Visual Basic, VB.NET C, C++, C# Flash 9/Flex Java LabVIEW/Matlab

The RFID reader comes with an installation package that could be downloaded from the Internet. This will install the reader and check whether the reader is fully functioning. Figure 7 will show the installed program.

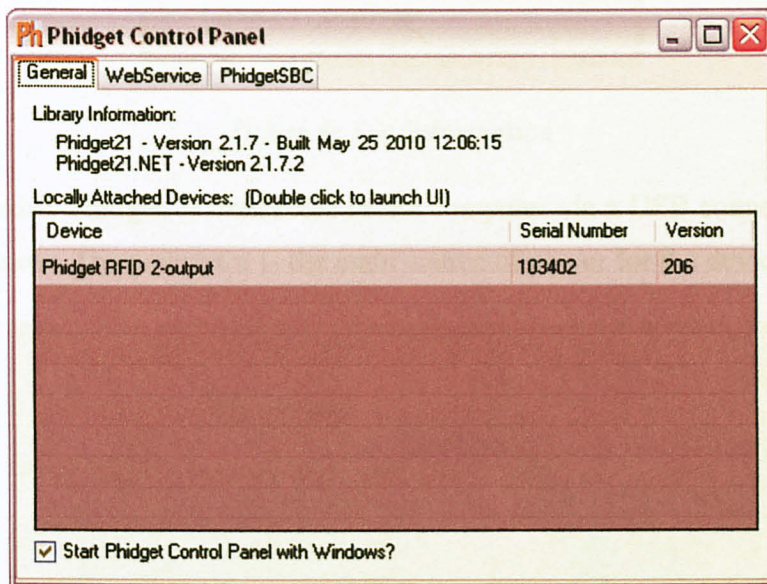


Figure 7: Phidget Installation

When the program had been successfully installed, it may read the unique tag number. This is shown in Figure 8 below.

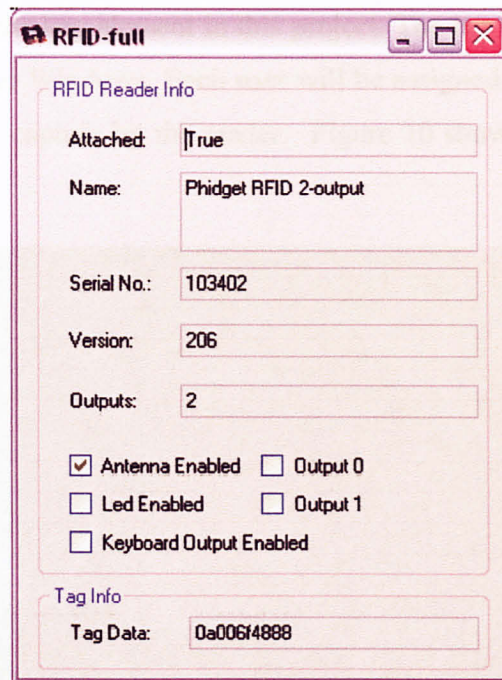


Figure 8: Tag Information

The RFID reader, Phidget, is connected to the computer via a USB connector as shown in Figure 9 below. The connector is the main source of power for the device.



Figure 9: USB Connector

The RFID tags will be the key element in this project. The tag will determine if the user may or may not logon to Windows. Each user will be assigned with one unique tag. All the information will be capture by the reader. Figure 10 shows a few EM 4102 RFID tags.



Figure 10: RFID Tags

4.5 Phidget

Phidget are a system of low-cost electronic components and sensors that are controlled by a personal computer, usually connected by a USB connector. This project uses open source software provided by Phidget. It uses the plug and play format for the RFID reader. The RFID reader is installed on to the computer. When the reader reads a tag, Phidget will compare the tag with the tag ID stored before. The software will also capture the time and date of the tag swiped on the reader.

4.6 PollGINA

GINA is an acronym for Graphical Identification and Authentication. It is a Windows component that manages the logon process of the computer. Basically it is the program

that runs during the boot of a computer, requiring username and passwords to log on. So PollGINA will instead allow all the standard Windows GINA functions to pass through to the original. Also, adds the ability for external applications to specify the logon account credentials. Figure 11 will show the difference between the original GINA and the PollGINA.

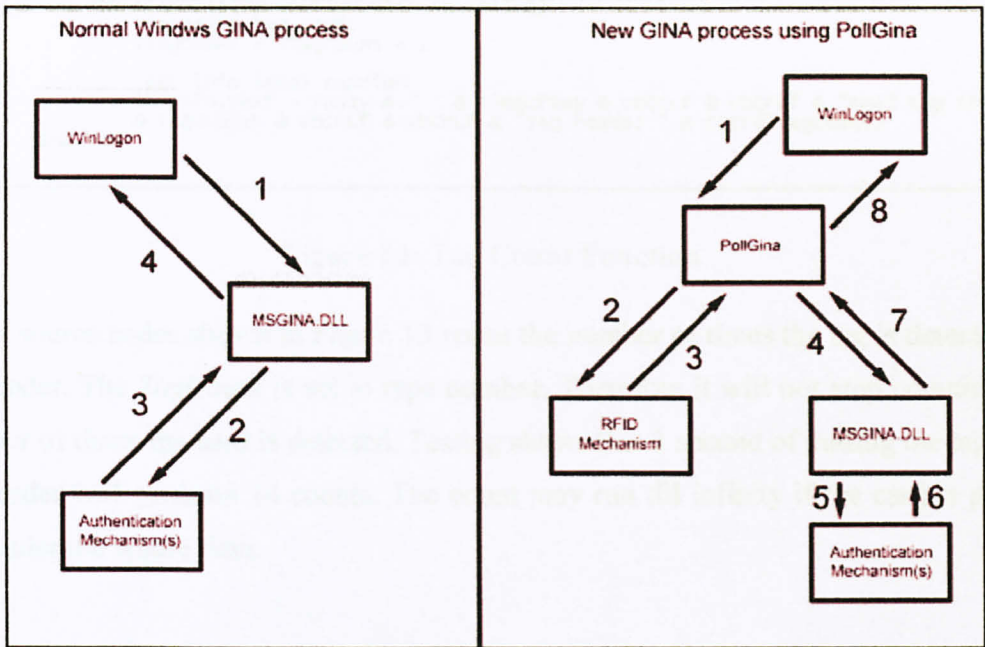


Figure 11: WinLogon for Logon Events

4.7 Tag Testing Process

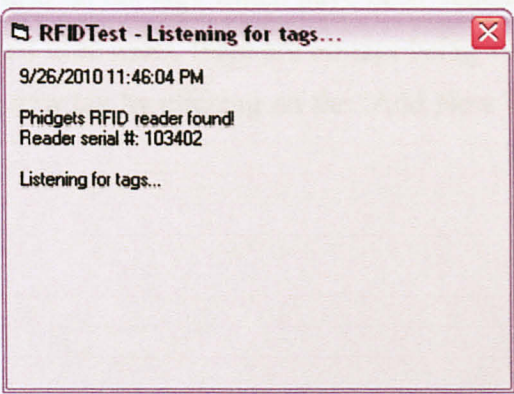


Figure 12: Tag Reading

The RFIDTest program is to detect the tags in close proximity to the RFID reader. It also detects the RFID reader itself whether it had successfully connected to the computer. The program detects how many times the tag had hit the reader.

```
Private Sub PhRFID_OnTag(ByVal TagNumber As String)
    'increase tag count
    lTagCount = lTagCount + 1

    'set info label caption
    lblInfo.Text = Today & " " & TimeOfDay & vbCrLf & vbCrLf & "Read tag ID: "
    & TagNumber & vbCrLf & vbCrLf & "Tag reads: " & CStr(lTagCount)
End Sub
```

Figure 13: Tag Count Function

These source codes shown in Figure 13 count the number of times the tag is detected by the reader. The *TagCount* is set to type number. Therefore it will not stop counting the number of times the card is detected. Testing shows that 1 second of putting the tag near the reader will generate 14 counts. The count may run till infinity if the card is put on the reader the whole time.

4.9 Authentication Process

The authentication process is where the program will validate the tags. When the program is open it will load all the tags which have been validated (source code shown in Figure 15). But, for first time users, there are no tags being validated by the program. User may need to add a new tag by clicking on the 'Add New Tag' button as shown in Figure 14.

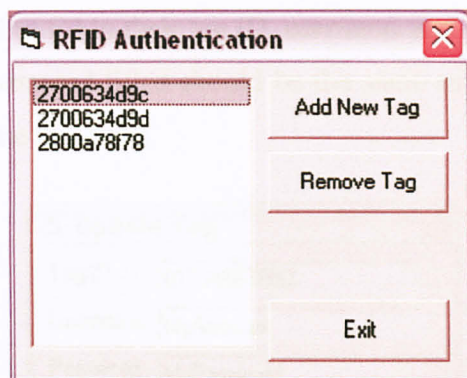


Figure 14: Tag Authentication

```

'clear list box
lstRFIDTags.Items.Clear()

'open registry key
lRetVal = RegOpenKeyEx(HKEY_LOCAL_MACHINE, "SOFTWARE\rfidPoll\" &
Chr(0), 0, KEY_ALL_ACCESS, hKey)

'check for errors
If lRetVal <> 0 Then
    MsgBox("There was an error opening the required registry
key.")
    Exit Sub 'could not open the registry key
End If

'itemize subkeys and load them into the listbox
Do 'loop until error
    strKeyName = Space(255) 'create space in the variable

    lRetVal = RegEnumKey(hKey, lKeyCount, strKeyName, 255)

    'check for errors
    If lRetVal <> 0 Then
        'exit loop, found all
        Exit Do
    End If

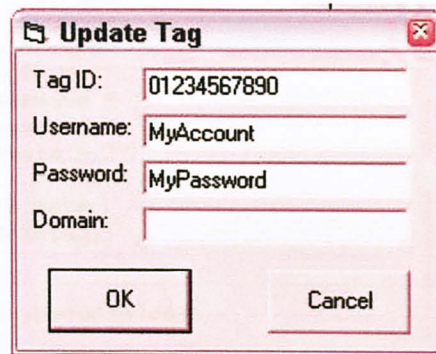
    'another key found, increase count and add to the listbox
    lKeyCount = lKeyCount + 1 'increase count
    strKeyName = Trim(Replace(strKeyName, Chr(0), "")) 'trim
spaces and remove NULL chars
    lstRFIDTags.Items.Add(strKeyName) 'add to listbox
Loop

'close the registry key
Call RegCloseKey(hKey)
End Sub

```

Figure 15: Source Code Snippet for Loading the Tags

Later, user may also need to fill in their tag ID, username and password shown in Figure 16. The username and password filled should be the same as the one saved to logon to Windows. This will also be validated.



The image shows a dialog box titled "Update Tag". It has a standard Windows window border with a title bar, a maximize button, and a close button. Inside the dialog, there are four text input fields arranged vertically. The first field is labeled "Tag ID:" and contains the text "01234567890". The second field is labeled "Username:" and contains "MyAccount". The third field is labeled "Password:" and contains "MyPassword". The fourth field is labeled "Domain:" and is currently empty. At the bottom of the dialog, there are two buttons: "OK" on the left and "Cancel" on the right.

Figure 16: Add/Update Tag

Then when user had clicked the 'OK' button, the new tag will be on the list of tags like the one shown back in Figure 14. Only the tags that are on the lists may be used to logon to Windows for that particular computer.

The source code shown in Figure 17 is the snippet of the function that adds or updates the tags. First it will clear all the strings in the list box. When the program had validated with the registry key, then the user may enter the fields. The fields that are entered by the user is saved in the registry.


```

Private Sub cmdAddNew_Click(ByVal eventSender As System.Object, ByVal
eventArgs As System.EventArgs) Handles cmdAddNew.Click
    Dim saKeyAttrib As SECURITY_ATTRIBUTES
    Dim lDisposition As Integer 'return code for key created or
existing key
    Dim lRetVal As Integer
    Dim hKey As Integer

    'clear public vars
    strUpdateTagID = ""
    strUpdateUsername = ""
    strUpdatePassword = ""
    strUpdateDomain = ""

    'load update form
    Load(frmUpdateTag)

    frmUpdateTag.ShowDialog()

    'form has returned, check public vars
    If strUpdateTagID = "" Then 'CANCEL is clicked
        Exit Sub
    End If

    'create key
    lRetVal = RegCreateKeyEx(HKEY_LOCAL_MACHINE, "SOFTWARE\rfidPoll\"
& strUpdateTagID & Chr(0), 0, Chr(0), REG_OPTION_NON_VOLATILE,
KEY_ALL_ACCESS, saKeyAttrib, hKey, 0)

    'check for errors
    If lRetVal <> 0 Then
        MsgBox("There was an error creating registry key")
        Exit Sub
    End If

    'set values
    lRetVal = RegSetValueExString(hKey, "Username", 0, REG_SZ,
strUpdateUsername, Len(strUpdateUsername))
    lRetVal = RegSetValueExString(hKey, "Password", 0, REG_SZ,
strUpdatePassword, Len(strUpdatePassword))
    lRetVal = RegSetValueExString(hKey, "Domain", 0, REG_SZ,
strUpdateDomain, Len(strUpdateDomain))

    'close registry key
    Call RegCloseKey(hKey)

    'reload tags
    Call LoadTags()
End Sub

```

Figure 17: Source Code Snippet for Add/Update Tag

Same goes to the 'Remove Tag' button. When the button is clicked, a window will appear asking whether the user is sure to delete the tag. If the user clicks 'OK', the tag will be deleted of the list. That particular tag may not be able to logon to Windows.

4.10 Result Testing

Several tests have been made to check the functionality of the project. Gathering information skills are important to get accurate data and to produce good system which is usable to all user; system administrator and computer user. The system had run a few testing to check the performance; the limitation and competency as well as for future references and expansions.

4. 10.1 System Performance

When talking about performance, response time should be considered. A Dell laptop was used and five tags were used in the testing; Tag 2700634d9c, Tag 2700634d9d, Tag 2800a78f78, Tag 3800030e5c and Tag 2700634d9e. Only the first 3 tags are stored as the unique tag for the computer. The five tags were swiipe at the RFID reader. Tag 3800030e5c and Tag 3800030e5c failed the logon process. The first 3 tags; Tag 2700634d9c, Tag 2700634d9d, Tag 2800a78f78 had successfully logon to Windows. Table 4 will show the testing results and simplify the explanation above.

Table 4: System Performance Testing

No	Tag Number	Stored	Success	Fail
1	2700634d9c	✓	✓	
2	2700634d9d	✓	✓	
3	2800a78f78	✓	✓	
4	3800030e5c	x		✓
5	2700634d9e	x		✓

4.10.2 Time Testing

During the test, time was clocked by a stopwatch. It took 0.66 seconds for the reader to detect tags; Tag 2700634d9c, Tag 2700634d9d, Tag 2800a78f78 and to logon to Windows as shown in Figure18. The loading of windows depends on the computer specification. On the computer tested, it took 6.8 seconds to load Windows and the desktop of the computer. Figure 18 and 19 shows the time taken by the stopwatch.



Figure 18: Time Taken to Detect Tag



Figure 19: Time Taken to Load Windows

4.10.3 Proximity Testing

The reader works as the tag detector. Therefore, the closeness of the tag to the reader should be tested. Based on the testing, the reader may read the tag 5 inches in distance from top or bottom of the reader. Whereas, when the distance is calculated from the sides of the reader, it may read the tags one inch away. This is seen as a drawback as the user needs to be closed to the reader for it to detect.

CHAPTER 5

CONCLUSION AND RECOMMENDATION

5.1 Relevancy to the Objectives

The objectives set earlier may be achieved with the success of this project. Developing an automated logon and logos for Windows may be achieved. This is proven at this point in time based on the literature reviews and the scope of study. The design of the system architecture is in line with the objectives set. It is relevant based on the specific requirements set. Security measures are not neglected. However, integration with voice recognition is still in progress. The application may improve the existing system.

5.2 Suggested Future Work for Expansion and Continuation

5.2.1 Improvised Hardware

An advancement that can be made with this project is that the RFID reader can be hid in a keyboard or speaker instead of having it outside of the CPU. This will free one of the USB port if the RFID reader is connected via the keyboard or speaker. This will also look neater.

5.2.2 Improvised Voice Command

Further continuation of this project may be the voice command for other purposes. For example, to open an application in the computer, voice command may be used here. Another example is that when a user needs to maximize a window, show desktop and such. This can help the disabled to use the computer efficiently. It is also useful for jobs which require the user to multitask such as Air Traffic Controller.

5.2.3 Multiple User

Another enhancement may be that one computer does not only unique for one user. The voice database may store a few voice. This way, the computer may be shared with colleagues with business purposes. Also can be used for a factory or warehouse which have few employees using the same computer.

REFERENCES

- [1] (2010). Retrieved September 2010, from Wikipedia, the free encyclopedia:
<http://www.wikipedia.org>
- [2] Bekkali, A., & Matsumoto, M. (2007). RFID Indoor Tracking based on Inter-tags Distance Measurement.
- [3] Evans, J. R., Tjoland, W. A., & Allred, L. G. (n.d.). Achieving a Hands-Free Computer Interface using Voice Recognition and Speech Synthesis.
- [4] Finkenzeller, K. (2003). *RFID Handbook*. West Sussex: John Wiley & Sons.
- [5] Hossain, M. M., & Prybutok, V. R. (2008). Consumer Acceptance of RFID Technology: An Exploratory Study.
- [6] Hunt, V., Puglia, A., & Puglia, M. (2007). *RFID A Guide To Radio Frequency Identification*. New Jersey: John Wiley & Sons.
- [7] Juels, A. (2009). Power Games in RFID Security.
- [8] Li, L., Wu, J., Guo, X.-w., Li, M., & Niu, X.-m. (n.d.). Framework for Windows password Function Security Enhancement.
- [9] *Library*. (2010). Retrieved July 2010, from MSDN Microsoft:
<http://msdn.microsoft.com/>
- [10] Lieckfeldt, D., You, J., & Timmermann, D. (n.d.). Characterizing the Influence of Human Presence on Bistatic RFID-System. 1-6.
- [11] Microsoft. (2009, January 22). *How Interactive Logon Works*. Retrieved April 2010, from <http://technet.microsoft.com>.
- [12] Mills, S. (n.d.). Is Voice Recognition the Solution to Keyboard-Based RSI?

- [13] Minbo, L., & Chen, C. (2009). RFID Complex Event Processing Mechanism for logistics Tracking and Tracing. 44.
- [14] Ni, L. M., Liu, Y., Yiu, C. L., & Patil, A. P. (2004). Indoor Location Sensing Using Active RFID. *Kluwer Academic Publisher* , 1-10.
- [15] Noor, M. Z., Ismail, I., & Saaid, M. F. (2009). Bus Detection Device fir the Blind Using RFID Application.
- [16] Park, B., Hong, S., Oh, J., & Lee, H. (2006). One Touch Logon: Replacing Multiple Passwords with Single Fingerprint.
- [17] Park, B., Hong, S., Oh, J., & Lee, H. (2006). One Touch Logon: Replacing Multiple Passwords with Single Fingerprint Recognition.
- [18] Rashid, R. A., Mahalin, N. H., Sarijari, M. A., & Abdul Aziz, A. A. (2008). Security System Using Biometric Technology: Design and Implementation of Voice.
- [19] Sano, E., Maeda, T., Nakamura, T., & Shikai, M. (2006). Fingerprint Authentication device based on characteristics inside a finger.
- [20] Siadat, S. H., & Selamat, A. (2008). Location-Based System for Mobile Devices Using RFID. 1-6.
- [21] Sloboda, T., & Waibel, A. (n.d.). Dictionary Learning for Spontaneous Speech Recognition.
- [22] Wexler, J. (2004, April 27). Legoland tracks children with Wi-Fi based RFID.

APPENDICES

Appendix I – Survey Form

The purpose of this survey is to observe the usage and behavior of computer users on logon and logoff Windows process. This survey is used to enlighten on how this process may be easier to perform and secured.

Kindly tick your answers in the box.

- 1. Does your work require a computer?**
[] YES [] NO
- 2. Do you spend more than 5 hours a day in front of the computer?**
[] YES [] NO
- 3. Do you think that keying in your password to logon/logoff your computer a hassle?**
[] YES [] NO
- 4. Do you always forget your password?**
[] YES [] NO
- 5. Have you heard of voice recognition technology?**
[] YES [] NO
- 6. Do you think that logging on would be easier with voice recognition?**
[] YES [] NO
- 7. Do you think it is important to logout after using the computer?**
[] YES [] NO

~Thank you for your time~