Available Online at www.ijcsmc.com

International Journal of Computer Science and Mobile Computing

A Monthly Journal of Computer Science and Information Technology

ISSN 2320–088X

IJCSMC, Vol. 3, Issue. 3, March 2014, pg.1095 – 1126

RESEARCH ARTICLE

IMPROVING THE WINDOWS PASSWORD POLICIES USING MOBILE BLUETOOTH AND RIJNDAEL ENCRYPTION

Pharaoh Chaka[1], Hilton Chikwiriro[2], Clive Nyasondo[3]

[1]Computer Science Department, Bindura University of Science Education, Zimbabwe

[2]Computer Science Department, Bindura University of Science Education, Zimbabwe

[3]Computer Science Department, Bindura University of Science Education, Zimbabwe

[1] pchaka01@gmail.com; [2] hchikwiriro@gmail.com; [3] clivenyasondo@gmail.com

ABSTRACT

Security in computers has been the core issue when it comes to the operation of computer systems. To safeguard data, organizations impose password policies that in way ascertain that there is a degree of security on files that may be sensitive in nature. These policies differ in different organizations and the effectiveness depends on the success of those password policies. A successful policy mainly depends on the behavior of the users and how they follow it to the book. This research focuses on this aspect and will try to address the end user acceptance and will attempt to improve these policies by introducing the use of mobile phone tokens using the Bluetooth and Rijndael encryption. This would ensure that the users get authenticated by the windows password login and then further authenticated to gain access to their most private files using their Bluetooth enabled mobile phones. In this way we can have less frequent password changes or have less strict policies that the users are resistant to and they can and provide an extra feature that would allow for an automated environment using the proximity sensor to verify if your mobile token is in range or not. This paper will try to assess whether an implementation of this system will provide extra security to files and also improve password policies.

Keywords: - Security; Bluetooth; Mobile phone; Rijndael; Password

1.1 Introduction

In today's world of increasing dependence on computers and computer systems, it is imperative that we be able to rely on secure and confidential connections to the computers. Traditionally, this has been by authentication with usernames and passwords. "A *password* is information associated with an entity that confirms the entity's identity." (Bishop M. 2003). The password is a string of characters that can either be automatically generated by the system or selected by the entity or user. Passwords can range from a single character to passphrases, which can be hundreds of characters in length and be comprised of series of words and phrases. The goal of a password is to authenticate a user. It is a piece of information that the user knows. However, this is a weak method of authentication because users tend to generate passwords that are easy to remember but also easy to crack (Kim-Phuong L. et al (2007). Passwords provide a first line of defense in most cases, but there is much more. If someone can guess a user's password, they can impersonate the user.

Chapter 2: LITERATURE REVIEW

2.1 Introduction

The aspect of protecting data has been the primary concern for computer users all over especially those who are entrusted with sensitive data. Windows password policies can be invoked in different ways as deemed necessary by relevant authorities in an organization and it is therefore imperative that these be followed to the book to ensure that none of the data is violated. However, some of the policies are not enough to guarantee security over personal or organizational data, hence the need for other stronger or foolproof solutions to ensure protection. Having (and enforcing) a strong password policy is a basic step that is often overlooked. In random audits of corporate networks, about 30% of user passwords are ridiculously easy to guess and appear in any hacker's dictionary. Strict password policies can also be a double edged sword - make them too strong and your users will begin writing their passwords on sticky notes and keeping them in their desk drawers, under mousepads, or taped to the bottom of the keyboard.

They can also flood your help desk with requests to reset forgotten passwords (Summers et al, 2004).

2.2 Windows password security

The windows security feature has been the most important issue ever since the beginning of the windows systems. The password feature is tied to user accounts and users can create or modify accounts, if they have administrator privileges. The general drawback was that there was no guarantee that the set passwords are strong or perhaps follow some guideline to make sure that they are secure enough. The existence of password policies made certain that the systems were protected using certain guidelines either set in the system itself or imposed by organizations so that users follow these rules to ensure that the systems were secure. Even then the general acceptance of these policies was not wide. Some policies became more and more forced through system configuration and some were based on the user abiding by them, for example, other policies require password change at the end of each work day or even once a week.

2.3 Password policy implementation in organization

Philip Inglesant et al [2] explored the use of password policies in organizations and also to understand more about specific problems faced by users in conforming to password policies, and the strategies which they adopt to cope with these issues. In their research they discovered that Conflict between password policies and the capabilities of users, and the problems this creates, the ways users find to cope with this conflict and the impact on security of different contexts of use. The results showed that users tend to feel that some policies imposed by their organizations are too difficult to follow [2]. In the study, they realized that the idea of devising complex passwords was a direct interruption of user's activities and also the need to change passwords after a short while. Even if users understand the importance of such a policy, the impositions themselves are a burden and will prompt the user to resist. In this light, a more versatile solution must be implemented that will ensure that the needs of the organizations and of the users are met. Users just do not want the burden of having to be alert when conforming to policies that require too much of them. Thus they end up creating simpler solutions and probably create simpler passwords [2].

"Computer passwords are supposed to be secret. But psychologists say it is possible to predict a password based on the personalities of users or even what is on their desks…." In their discussion they indicate that a stronger measure must be in place. They advise on implementing a stronger and more feasible password policy that ensures that data is secure, especially for organizations. But the ultimate challenge is that users tend to be tempted to create passwords that are easier to remember thereby playing directly into the hands of the hacker. In light of this discovery, a stronger but easily adaptable measure is not far off and should be employed in order to warrant the continued protection of data with minimal participation on the part of the user. Users then tend to create passwords that are easier to remember because they do not want to deal with complication [1]

Results of a National Survey on Data Security Breach Notification by the Ponemon Institute LLC (2006) in 2005, show that nearly 12% of the respondents reported that they had received notification of a data security breach in the last year, suggesting that more than 23 million adult Americans may have received a breach notification (Durrett, 2006)." According to this extract, it is inevitable that breaches will eventually occur and what is needed is therefore a way to make sure that they are minimized as much as possible. If not, users and organizations tend to lose more when their personal or organizational sensitive information is breached.

Some of the results of the questionnaires that were given to quite a number of users showed Eighteen percent of the respondents always use the same password to access the different computer systems, application or websites, 50% sometimes use the same password and sometimes another password, and 31% always use different passwords. Also on an average, respondents change their password 7 times a year, almost always prompted (96%) by their department.

This again confirms that users tend to sway from the requirements of password policies and eventually fall prey to attacks all because they forgot to change their password as required. This is a common human trait that people are forgetful and are most of the time tend to forego what they are required to do and in turn try their own "unpainful" ways to get around the system. So

the question still remains, what can be done to alleviate these issues and still provide airtight security, a solution that will be beneficial to all parties? This research focuses on this question.

2.4 Security weakness of windows password authentication

We can also take a look at the paper by Danuvasin Charoen et al, 2007. The paper is about the design and implementation of techniques and strategies to improve end user behavior in the utilization of passwords within a formal setting.

There is also mention of a program called LC5 that is capable of cracking simple passwords with eight characters in a matter of seconds. In the region of 5-8 characters is where most of the user's password length resides. "According to classical cognitive research, humans can memorize only seven plus or minus two chunks of information (Miller 1956). Not surprisingly, a set of preliminary interviews showed that most users within the Client organization had difficulty remembering strong passwords. As a result, the users often wrote down their passwords. These written passwords are often kept in insecure locations and were subject to misuse" (Danuvasin Charoen et al, 2007).

It can be argued that password management on the part of the user is a very difficult task and should be duly noted. As has been already established, users tend to take the easy path when it comes to dealing with hard to grasp password policies and in the end open up gap that allows for breach of security. The primary concern hereby lies on the issue of password and this has to be dealt with swiftly. The authors here focus on user training and strengthening user policies and at the end they expect the user training in password management to be accepted and utilized

Password Authentication from a Human Factors Perspective: Results of a Survey among End-Users, by Peter Hoonakker et al take a look at the human factors that affect their behavior when it comes to passwords. They undertook a survey based on various focus groups and came up with deviations from Computer and Information Security (CIS) best practices with respect to password use. It is also mention that, according to Computer Security Institute (2007) the survey show that the average losses per company participating in their survey, was nearly $350,000 and this is the most reliable estimate of computer security breaches based on the CSI/FBI Computer

Crime and Security Survey. "Some states in the U.S. have made it mandatory for organizations to disclose data security breaches, if personal information was, or is reasonably believed to have been acquired by an unauthorized person.

While studying password policies we may also look at paper by Richard Shay et al (2009). The primary focus of the paper is a simulation model for a password policy. The model considers technical factors and human factors essential to the creation of a successful password policy that is enough to be a safeguard against a security breach. The researchers took a look at the interaction of three types of components in a computer system namely Users, Accounts and Services. The author discovered that, "At any point in time, each Account and each Service is either Compromised or not Compromised. All Accounts and Services start as not Compromised.

An Account is considered to be compromised if and only if a malicious entity knows its password. A Service is considered to be compromised if and only if there is a Compromised Account which accesses it. In this model, a User is never Considered Compromised. A Compromised Account is no longer compromised when it receives a new password. A Compromised Service is no longer compromised when none of the Accounts accessing it are compromised. They also talk about vulnerabilities that arise when passwords are not complex enough and state that the accounts are daily subject to a specified number of brute force attacks. Strengthening one's policy has the effect of militating against security intrusions but it is in the organization's interests to ensure that users adhere to the instigated password policy. (Richard Shay and Elisa Bertino, 2009)

In the journal by Fernando Alonso 2008, it is analyzed that passwords have become extinct and quoting this statement: "In the near future, password authentication will become either extremely insecure or extremely difficult to implement among human users." The author exposes the password authentication mechanism and reveals hashing and how passwords are not stored in plain text. As with passwords being weak, the author discusses about password cracking and mentions two known methods that are used namely, Dictionary attack - Based on known possible passwords, such as dictionary words, names, calendar, dates, etc. and Brute force - Trying all the possible character combinations based on known parameters. The author also talks about the

evolution of CPUs and how their ever improving speed, growing at an exponential rate can be used to crack passwords in the shortest amount of time due to cycle speeds (Fernando Alonso, 2008).

So eventually we will ask ourselves, can we still rely on password authentication alone or should we start adopting other methods of security? Other authors such as Danuvasin Charoen et al, (2007), believe that we just need to strengthen our current password policies. These authors talk about user awareness and training of users to adapt to password changing but Fernando Alonso (2008) believes that it is time to shift gears and take notice of other ways that data can be kept safe. The author also says that, "even considering policies forcing users to change them every 10 days, the time will come when they will be cracked in less than one day, obtaining nine days to develop the silent attack without being discovered by intrusion detection tools due to its "legitimate user" natural behavior." This is a quote from the conclusion by Fernando Alonso (2008) which really suggests that soon other methods will be necessary. And so another question is, should we wait until this has happened or should we start investing in other methods such biometrics and tokens.

2.5 Token Authentication as a security measure

The paper, Guide to Enterprise Password Management by Karen Scarfone Murugiah Souppaya (2009), the mention of single factor, two factor and three factor authentication arises. According to the research, authentication can involve something the user knows, for example a password and something the user has possibly a smartcard or any other token and finally something the user "is" for example a fingerprint or voice pattern.

Single factor authentication uses one of the mentioned forms, while Two Factor Authentication uses any two and three factor authentication uses all three. The authors acknowledge that using more factors makes it difficult for someone to gain access to the system. This is in contrast to just using single factor in the form of password authentication. This research focuses on two factor authentication (2FA) and attempts to strengthen the already available policies. Karen Scarfone Murugiah Souppaya also explains that it is difficult for an unauthorized user to steal the

user token and also discover the users' password at the same time. The two also tackle the password management difficulties that arise in many organizations.

As with Philip Inglesant and M. Angela Sasse (2007), the authors acknowledge that users tend to have difficulties following policies set by their organization manly due to the requirements that they feel, are a constant pressure on their day to day operations. Now this has been a major observation, even Dr. Wayne C. Summers et al (2004) take note of this behavior in users and according to them users then turn to more vulnerable methods that will expose them to numerous attacks and dangers of being hacked. This again confirms that a more robust method of authentication be invoked by organizations as a way to combat such important concerns and make the users a bit more comfortable.

As with an ATM card that has to be inserted into the machine and verification through a PIN number to ascertain the identity of the person making the transaction, then this is ultimately two factor authentication. Fadi Aloul, Syed Zahidi et al (2009) introduce a two factor authentication method using mobile phones. "The proposed system involves using a mobile phone as a software token for One Time Password generation. The generated One Time Password is valid for only a short user defined period of time and is generated by factors that are unique to both, the user and the mobile device itself. Additionally, an SMS-based mechanism is implemented as both a backup mechanism for retrieving the password and as a possible means of synchronization." The authors noted that static passwords provide a security concern in safekeeping data. They also acknowledged that users tend to use easy to guess passwords, write the passwords down or store them on their machines. This discovery also made by Dr. Wayne C. Summers et al, (2004) among other several authors in this document.

Fadi Aloul et al, (2009) also cite that the proposition of strategies such as the use of tokens or tokens have proven to be difficult to hack. The idea itself is not without its cons and the authors acknowledge that it can be expensive to purchase tokens to be distributed among several users, manage them. Ultimately, the cost of losing sensitive data by employing the old one factor password authentication to hacking outweighs that of the cost of such tokens. The authors have already implemented and tested their proposed authentication method to great success. Our research takes a similar idea and uses it to combat localized attacks by initiating a two factor

authentication system using mobile phones with their Bluetooth and the Bluetooth installed on a workstation.

2.6 Encryption of files to preserve confidentiality

As an extra added feature but highly effective, to enhance security, encryption of files seems best as this preserves the confidentiality of most sensitive files. They are many competitive encryption algorithms out there and they differ on their efficiency, speed and complexity.

The encryption method adopted for this research is the Rijndael cipher which is an Advanced Encryption Standard (AES). AES is based on a design principle known as a substitution-permutation network, and is fast in both software and hardware (Bruce Schneier et al, 2000). Unlike its predecessor DES, AES does not use a Feistel network. AES is a variant of Rijndael which has a fixed block size of 128 bits, and a key size of 128, 192, or 256 bits. By contrast, the Rijndael specification per se is specified with block and key sizes that may be any multiple of 32 bits, both with a minimum of 128 and a maximum of 256 bits.

The Rijndael encryption in overall performance, based on the speed of encryption and decryption and on key set-up time, the algorithm has attained top scores in tests conducted by National Institute of Standards and Technology (NIST). The belief is that almost all US government agencies will shift to the AES algorithm for their data security needs in the next few years. Also, that the algorithm will find its way in smart cards and other security-oriented applications used for safely storing private information about individuals.(T Jamil, 2004)

In terms of performance, High speed and low RAM requirements were criteria of the AES selection process. Thus AES performs well on a wide variety of hardware, from 8-bit smart cards to high-performance computers. On a Pentium Pro, AES encryption requires 18 clock cycles / byte, equivalent to a throughput of about 11 MiB/s for a 200 MHz processor. On a Pentium M 1.7 GHz throughput is about 60 MiB/s. On Intel i3/i5/i7 CPUs supporting AES-NI instruction set extensions, throughput can be over 700MiB/s per thread (A Nadeem, 2005).

If files are encrypted and the cipher used is commendable, then we can at least ensure that if we are hacked, the hackers will have a difficult time cracking the algorithm. At the end of the day

files are in a secure state and the most important factor to almost all organizations, Confidentiality, is preserved.

2.7 Conclusion

In conclusion, considering what all the articles indicate, passwords have been thought to be the last line of defense but various factors allow for hackers to infiltrate past computer security. Surely some strong password policies can ensure that data is protected, especially in corporate world as companies deem it necessary. The drawback has always been user participation in these policies, lest they are worthless and as we have discovered in the articles above, especially when Dr. Wayne C. Summers (2004) noticed that users tend to write their passwords somewhere so that they may remember. This ultimately leads to vulnerability and could result in breach of security. As this research focuses on establishing a way to make sure that a policy is adhered to, it follows the steps in which Token-less 2FA is established. Therefore people will not have to make excuses and eventually lead a foolproof secure environment. Even Fernando Alonso (2008) says that the use of Passwords is coming to an end which suggests that more and more secure ways of protecting data are slowly emerging and some of them include Token 2FA(two factor authentication) and biometrics.

Chapter 3: RESEARCH METHODOLOGY

3.1 Introduction

The Mobile Bluetooth token and the Rijndael security extension was used to shield sensitive files from perpetrators by ensuring that they are not breached of their confidentiality. Interviews and questionnaires were used to analyze the effectiveness of this tool in securing files and improving the password policies as compared to the windows password login alone.

3.2 Data Collection Approaches

Data was collected using different approaches and tools such as questionnaires, interviews and observation.

3.3 Design Methods

In order to implement and build a working model of a Bluetooth token to work with a Bluetooth enabled Computer; there was need for a framework that would allow for the fluent communication between the Bluetooth devices without worrying about vendor origin. The Bluetooth client system was designed using:-

- Microsoft Visual C# language
- Microsoft based IDE Visual Studio 2010
- 32feet.Net Bluetooth library for manipulation of the Bluetooth API – this includes wrapper classes necessary to interact with Bluetooth devices from a variety of vendors.

Hardware

- Mobile Phone with Bluetooth

  The phone should be Bluetooth enabled and OS specifications are not an issue as the system only operates at hardware level with the mobile Bluetooth. The 32feet.Net library is responsible for the manipulation of this hardware. The Bluetooth has a unique MAC

address hardcoded into the hardware and this is used to identify the phone as a token in conjunction with a password on authentication.

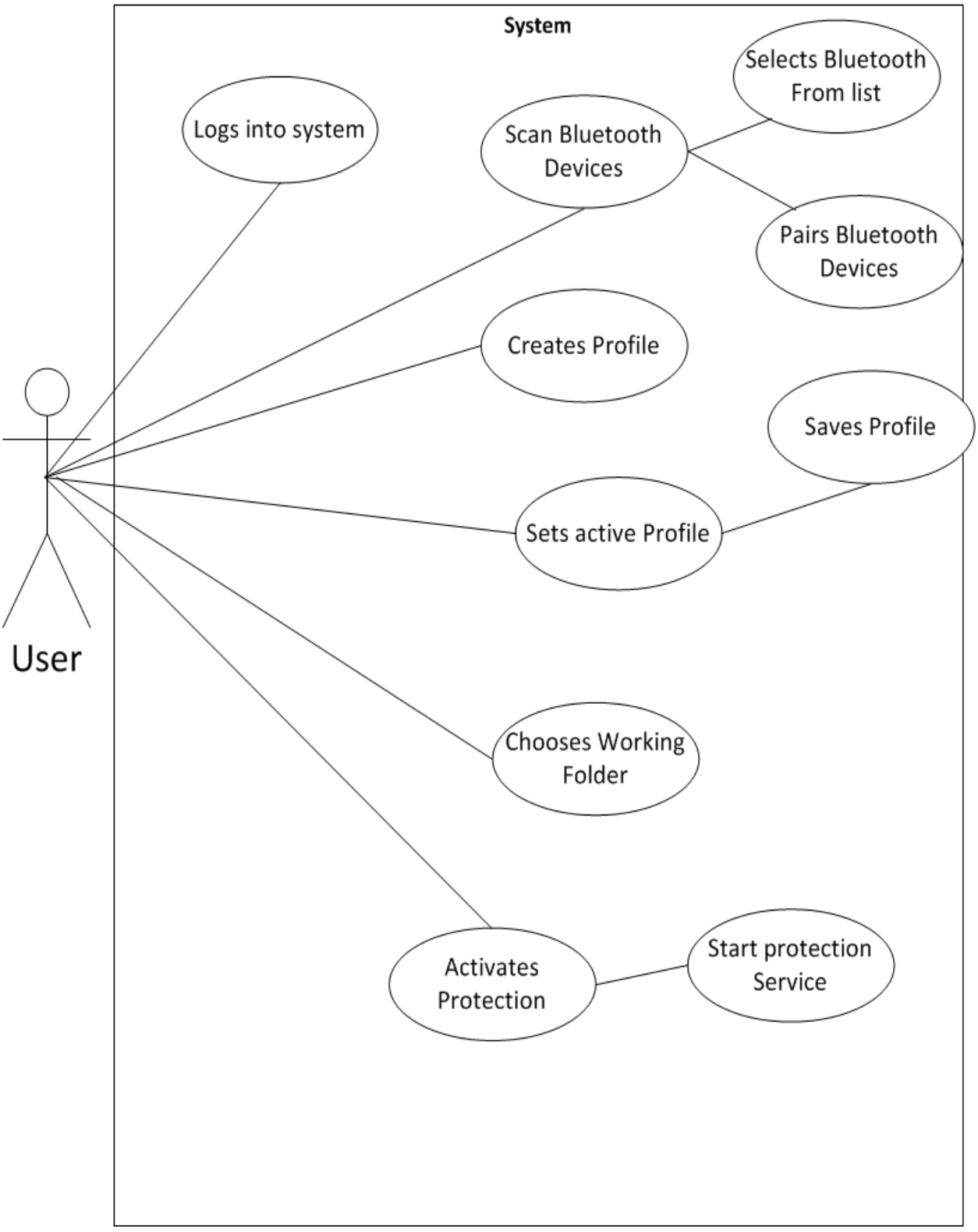
- Bluetooth dongle Plug'n'Play for one's desktop computer or laptop(If the laptop does not already have one built in)
- PC or Laptop

This is the host for the client software. The system will include client software and a windows service. These two will run on the computer that is to be secured with the service running as long as the system is running.

3.3.1 System design

3.3.1.1 Use case diagrams

Use-case modeling is a technique used to describe the functional requirements of a system. It makes it easier to show the functional requirements in an abstract way that can easily be understood even by the stakeholders of the system, therefore acting more like a communicating tool between the stakeholders and the developers.



3.3.1.2 Requirements Specification

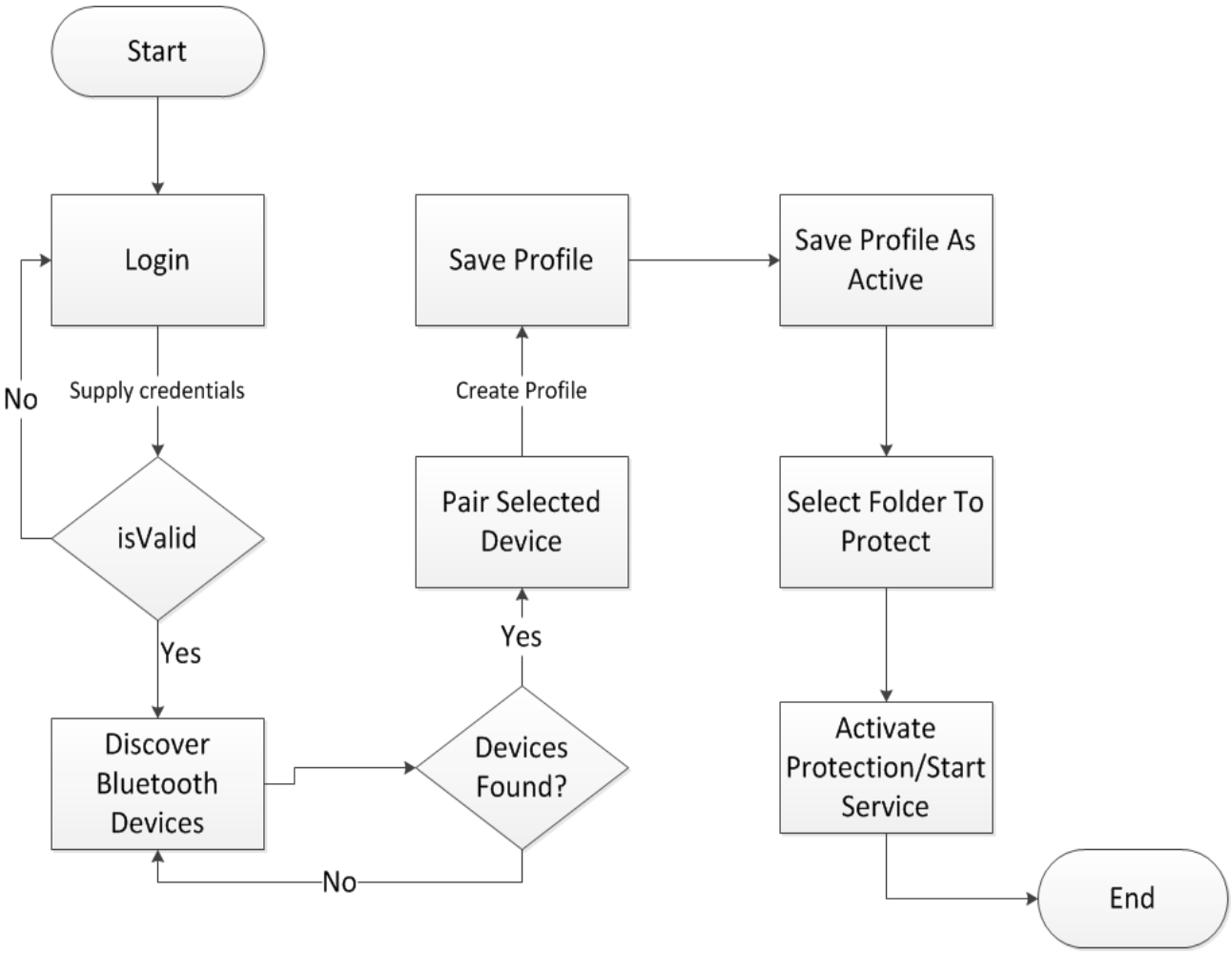
Windows Service

This is the service that runs in the background for the lifetime of the computer system runtime and will automatically be started when the computer boots. This service has functional requirements that it has to fulfill in order to be fully operational.

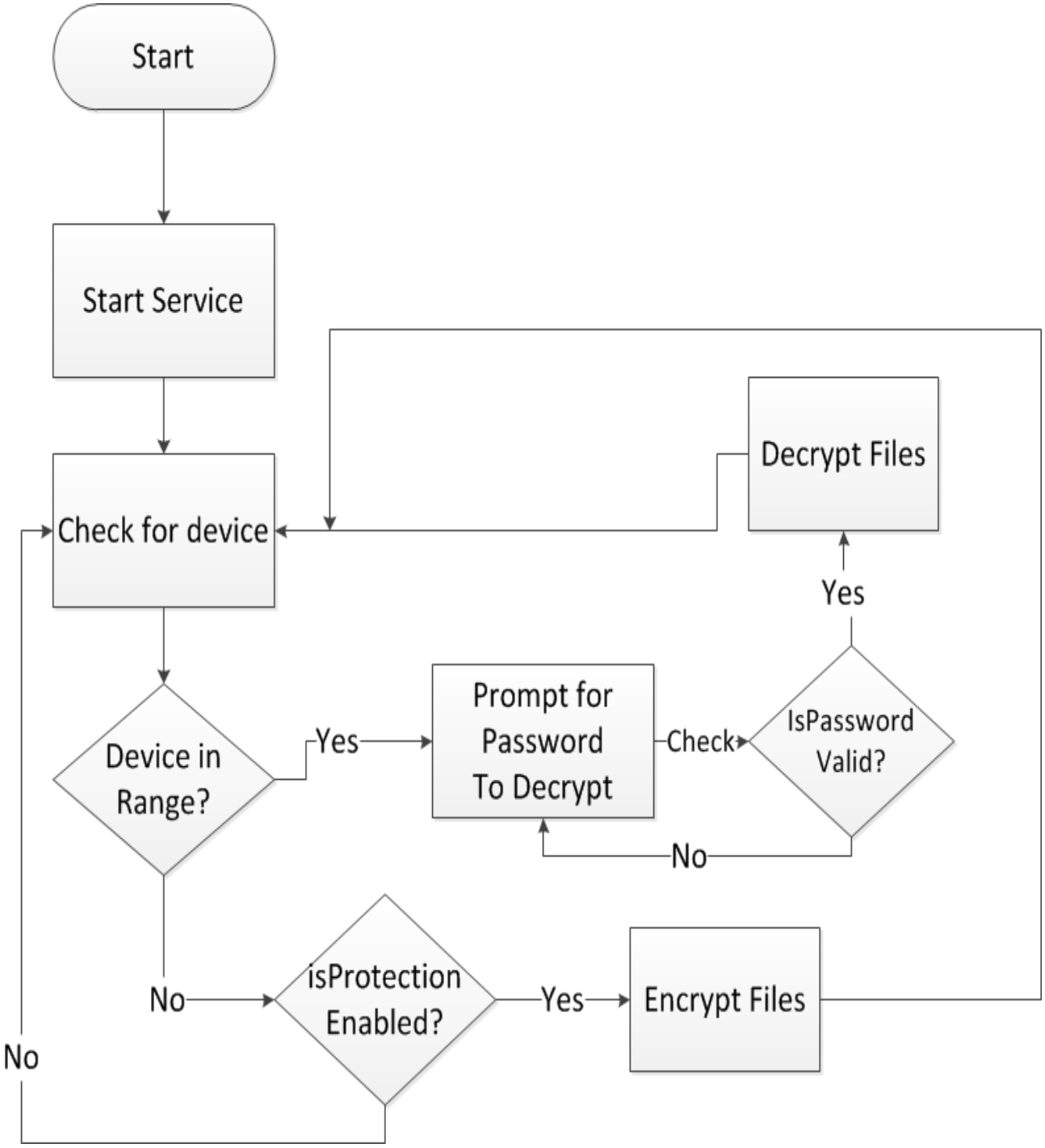
- Lifetime service – Service must run for the whole time the windows system is running.
- Scan Bluetooth Proximity – Service should be able to recognize when a particular Bluetooth device is range. This particular device is the one that is saved in the database as the active profile. It should match the service records of the Bluetooth that match the MAC address of that device.
- Encrypt Files – Should be able to encrypt files in the working folder whenever the Bluetooth device goes out of range.
- Lock workstation – The service should automatically lock the windows workstation when the authenticated Bluetooth device is out of range.

3.3.1.4 Process Flow Charts

Windows Form Application:



Windows Service:



4.1 Data Presentation and analysis

As mentioned in the previous chapter, the questionnaire was the main research instrument used by the researcher backed up by observations and mock tests. Presentation and analysis of data will therefore incline more towards questionnaire responses and observation results. The quantitative data was edited for completeness, consistency, and duplication, and then organized into graphs and charts. These were then analyzed using Microsoft Excel sheets. A quantitative research design method was used using descriptive statistical analysis. Statistical power and effect size was calculated to understand sample size and its relationship to power the tables, charts and graphs were used by the researcher to come up with or devise strategies to display meaningful research findings.

4.2 Questionnaire Responses

4.2.1 Questions and Responses

Questionnaires were distributed to those participants who had taken up in using the system for two weeks during this time they had time to notice and understand how the system worked. The response rate results are tabulated below showing the quantity of questionnaires responded As illustrated in fig 4.1 below of the thirty-six questionnaires sent to respondents thirty-four out of thirty-six were returned. A summarized illustration of the questionnaires distributed and received and the respective percentages is shown in Table 4.1 below. This table will complement with the graph illustrated later on fig 4.1.

Target Group	Number of Questionnaires sent	Number of Responses Received	Response Percentage
Government workers	36	34	94

Table 4.2.1 Responses to Questionnaires

A total of 94% was the percentage representing the respondents since 34 out of an overall 36 responded to questionnaires sent after using the system for two weeks. The researcher targeted the corporate group of people who have an obligation to safeguard company data and who have certain password policies set for them. This target group is enough to analyze the effectiveness of the system in terms of improving the password policy and generally keep the data safe. Fig 4.2.1.1 shows the response data in a chart and showing the overall distribution of the respondents.

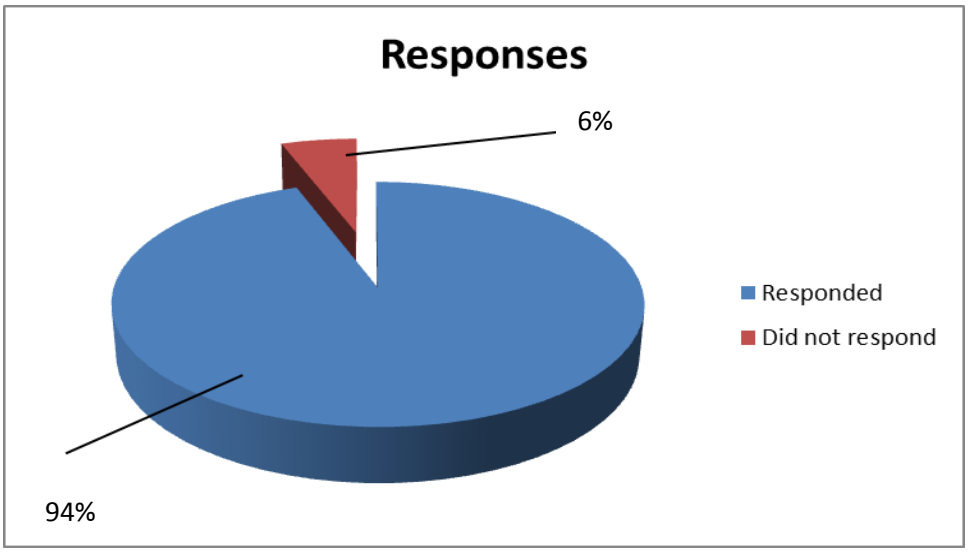


Fig 4.2.1.1 Respondents Data

The first question in the questionnaire needed to ask respondents if they thought that their data is secure when using the windows password login alone. This question was to allow respondents to first give their view on this authentication mechanism before asking them about the Bluetooth system to see if it would further improve the security. Fig 4.2.1.2 shows responses for **Do you think that the existing windows password login is enough to secure your files?**

Do you think that the existing windows password login is enough to secure your files?

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Strongly Agree	1	2.9	2.9	2.9
	Agree	6	17.6	17.6	20.6
	Undecided	13	38.2	38.2	58.8
	Disagree	8	23.5	23.5	82.4
	Strongly Disagree	6	17.6	17.6	100.0
	Total	34	100.0	100.0	

Table 4.2.1.2

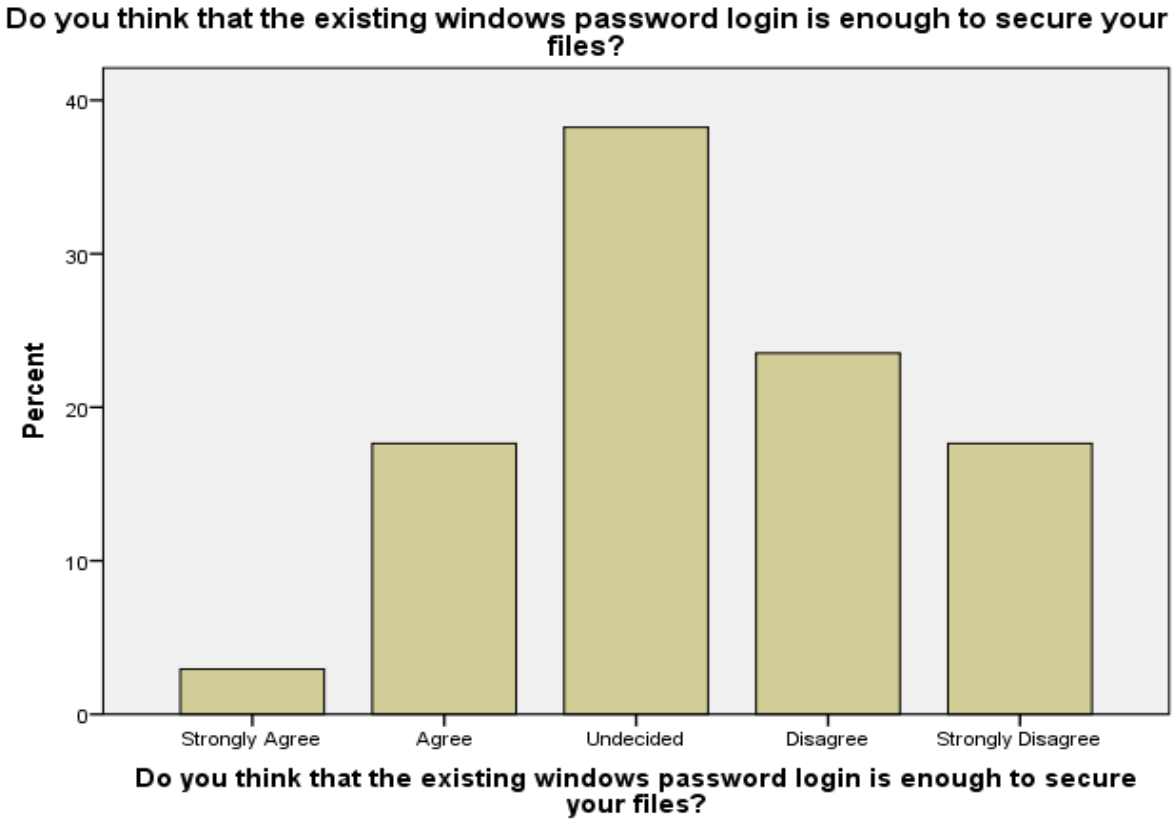


Fig 4.2.1.3

In the above graph, it is noted that about 1(3%) responded strongly agreed, 6(18%) respondents agreed, about 13(38%) were undecided, 8(24%) disagreed and 6(18%) strongly disagreed when they were asked if the existing windows password login was enough to secure their files. This was to get an insight into how secure users felt with the current windows password system alone. From the response distribution, a lot of users were undecided.

Certain policies require the user's participation and may require the user to change their password, some on a day to day basis and this has been a major job for the user. The researcher asked if they would agree with such a policy and the pie chart below shows the responses shows how the users feel.

There are certain password policies that require you change your password almost every day? Do u agree with such a policy??

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Strongly Agree	3	8.8	8.8	8.8
	Agree	5	14.7	14.7	23.5
	Undecided	9	26.5	26.5	50.0
	Disagree	11	32.4	32.4	82.4
	Strongly Disagree	6	17.6	17.6	100.0
	Total	34	100.0	100.0	

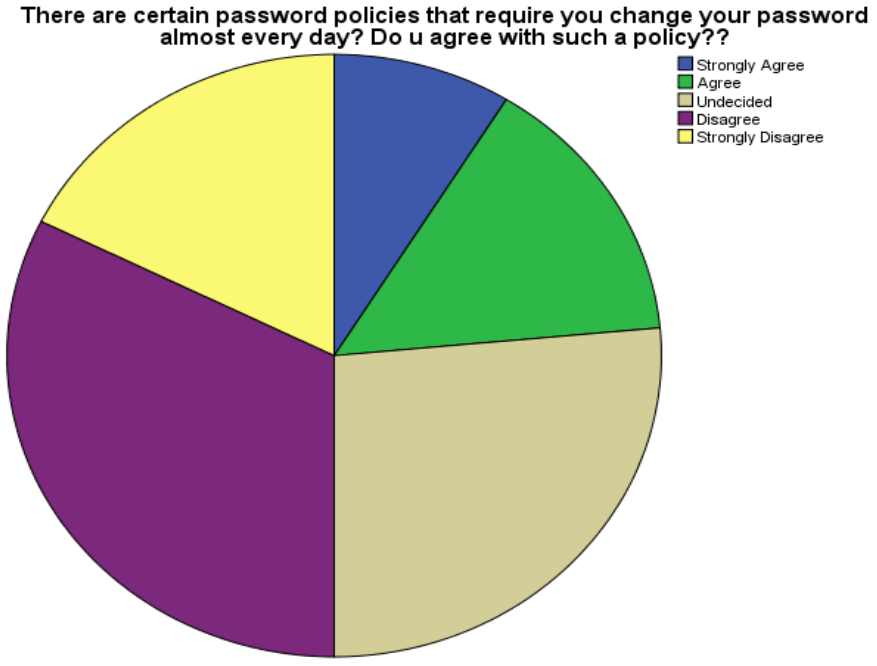


Fig 4.2.1.4

The responses show that a greater number (32%) disagreed with such policies. Again a substantial number (26%) were undecided while small numbers agreed with such a policy.

Do you think certain security measures must be in place to strengthen the existing windows authentication system?

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Strongly Agree	9	26.5	26.5	26.5
	Agree	18	52.9	52.9	79.4
	Undecided	3	8.8	8.8	88.2
	Disagree	3	8.8	8.8	97.1
	Strongly Disagree	1	2.9	2.9	100.0
	Total	34	100.0	100.0	

Table 4.2.1.5

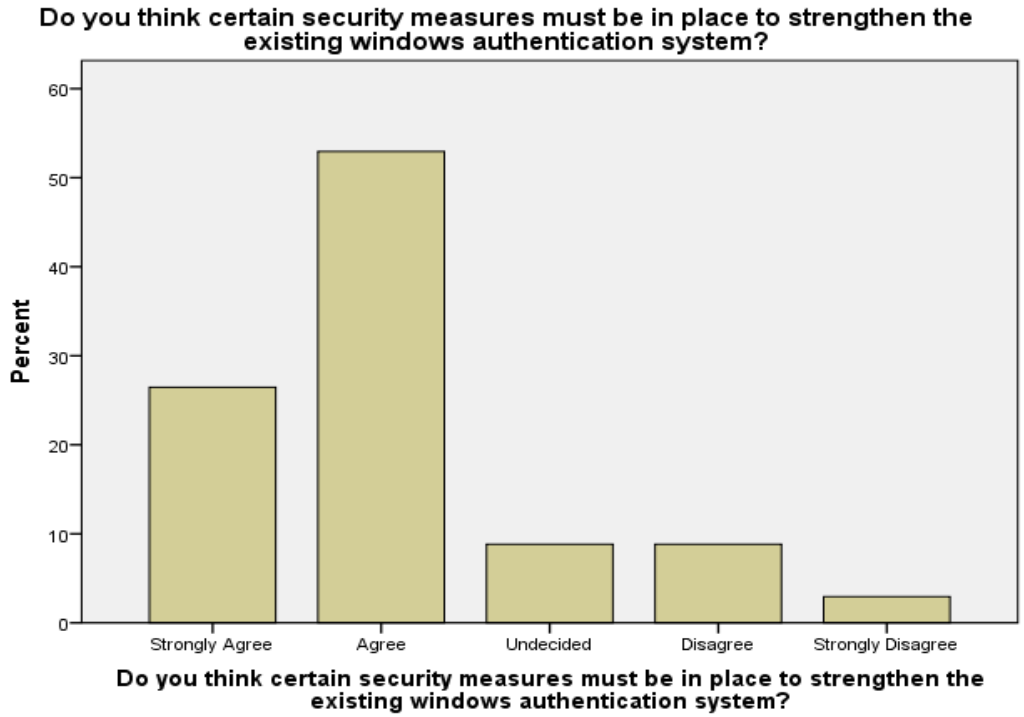


Fig 4.2.4

Fig 4.2.4 illustrates the responses from the users pertaining to their opinion if they thought if another measure should be introduced to enhance the existing windows password authentication mechanism. It can be duly noted that a greater number had strong feelings in agreeing and

supported the idea of another secondary mechanism to safeguard data. The researcher needed the confidence of people in believing that another mechanism would surely enhance security in windows systems. Therefore a whopping 53% of the respondents agreed to the idea while an extra 26% had strong feelings towards security enhancement.

4.2.2 System Effectiveness

The system effectiveness is perhaps the most important question that can be asked and the researcher needed to know how people felt about the protection that the system provided when they were done using it. At first, before the actual usage of the system, the researcher explained briefly how it works and gave the users an understanding into how encryption protected their files. After that the two weeks of system usage commenced during which the users had a firsthand look at the system as it functioned. Fig 4.2.5 shows the responses of the question – **After using the Bluetooth Secure System, do u think it is an effective system?**

Effectiveness

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Strongly Agree	16	47.1	47.1	47.1
	Agree	10	29.4	29.4	76.5
	Undecided	5	14.7	14.7	91.2
	Disagree	2	5.9	5.9	97.1
	Strongly Disagree	1	2.9	2.9	100.0
	Total	34	100.0	100.0	

Table 4.2.2.1

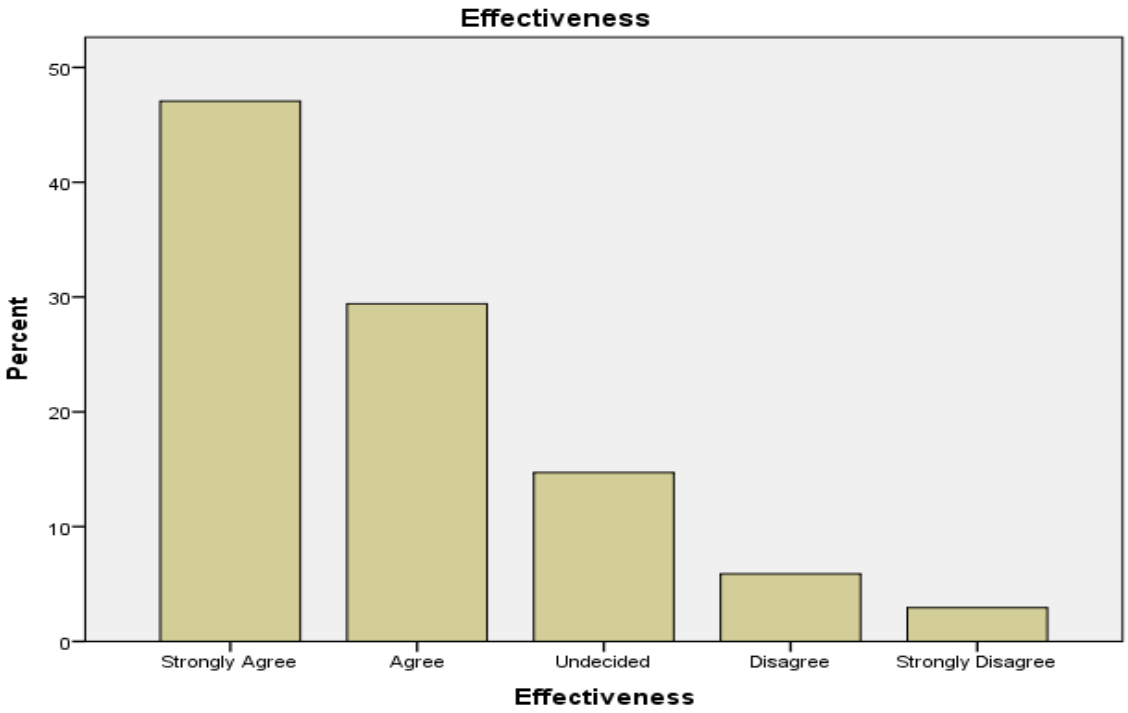


Fig 4.2.2.2

The responses pertaining to the effectiveness of the system have more favor than disfavor as seen in the graph. Most users thought that the system had been effective in protecting their files and generally making their jobs easier due to its automation. In the graph it can be noted that 47% strongly agreed that the system was effective and 6% disagreed. About 14% were generally undecided with the system.

Do you think it has simplified the problems associated with other policies that require more participation from you in ensuring that your system is secure?

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Strongly Agree	9	28.1	28.1	28.1
	Agree	20	62.5	62.5	90.6
	Undecided	2	6.3	6.3	96.9
	Disagree	1	3.1	3.1	100.0
	Total	32	100.0	100.0	

Table 4.2.2.3

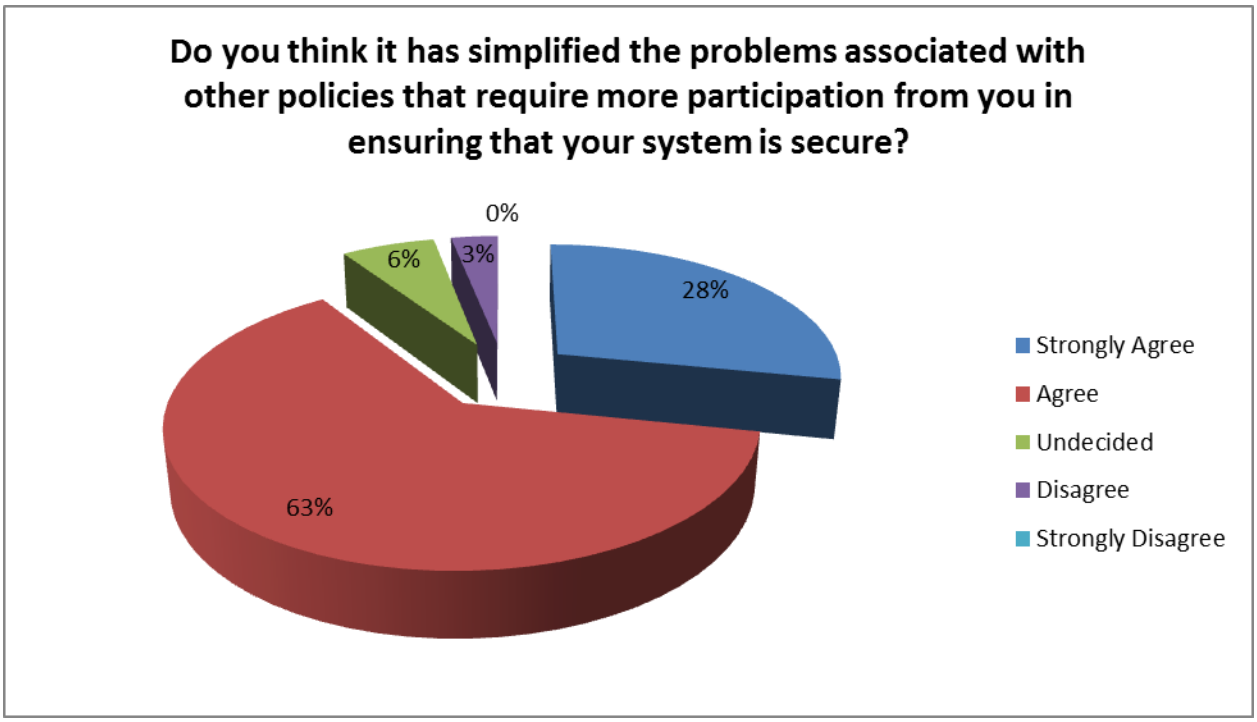


Fig 4.2.2.4

The above pie chart shows the distribution of responses from users when they were asked if they agree that the system had simplified associated with other policies that require more participation from them in ensuring that their systems were secure. The researcher needed to know if the variety of issues like changing passwords on a daily basis or having passwords that had all sorts of characters in them had been alleviated by the system. A lot of users (62.5%) agreed that the system had indeed simplified the problems and a small amount (3.1%) disagreed. The pie chart shows more favor in users agreeing and less users in the undecided region and disagreeing.

4.2.3 Token Authentication

The Bluetooth security follows the idea of token authentication to enhance the windows security mechanism. Since it is part of the system and makes up the secure part, the researcher needed to know if users would consider having token authentication as part of security for every workstation. The responses to such a question are shown in Fig 4.2.7 below.

Do you think token authentication using mobile phones for example should be the hub of every workstation for security purposes?

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Strongly Agree	16	47.1	47.1	47.1
	Agree	12	35.3	35.3	82.4
	Undecided	2	5.9	5.9	88.2
	Disagree	2	5.9	5.9	94.1
	Strongly Disagree	2	5.9	5.9	100.0
	Total	34	100.0	100.0	

Table 4.2.3.1

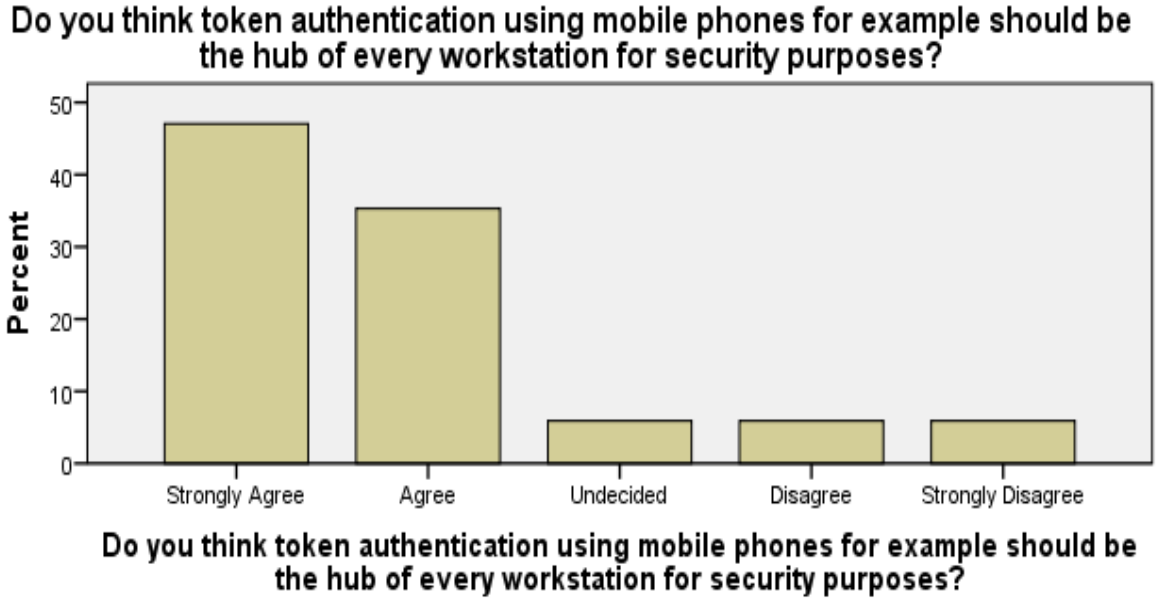


Fig 4.2.3.2

From the graph, it can be seen that a lot of respondents (82.4%) would consider token authentication and that it should be implemented in security mechanisms that uses passwords.

4.2.4 Effectiveness of encryption in securing files

Do you think encrypting files specifically hinders unauthorized users from violating your files?

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Strongly Agree	16	50.0	50.0	50.0
	Agree	11	34.4	34.4	84.4
	Undecided	4	12.5	12.5	96.9
	Disagree	1	3.1	3.1	100.0
	Total	32	100.0	100.0	

Table 4.2.4.1

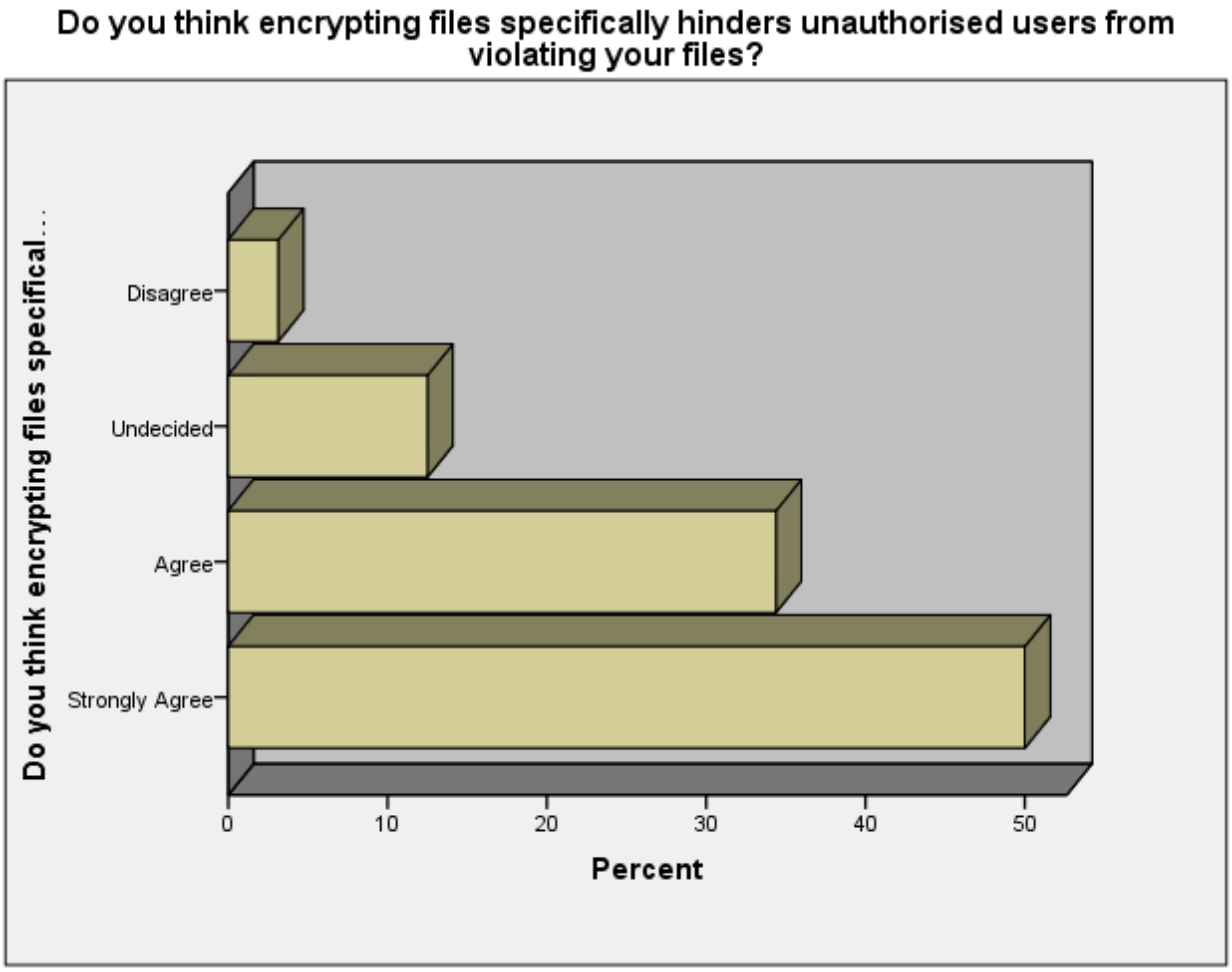


Fig 4.2.4.2

The graph shows that 50% of the respondents strongly agreed when asked if the thought that encryption in securing files makes it harder for hackers to access those files. 12.5% were

undecided with the question and 3.5% disagreed with the idea. The larger number who agreed had time to use and understand the system as it employs encryption when securing files. The numbers of people who are undecided probably do not understand the idea of encryption and how it enhances security.

4.2.5 System usability

The system usability is another important factor to consider and the questionnaire asked users if the system was usable after using it. Several responses have shown that most were in favor with the system usability.

Overally, do you think the system is usable?

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Strongly Agree	10	29.4	29.4	29.4
	Agree	17	50.0	50.0	79.4
	Undecided	5	14.7	14.7	94.1
	Disagree	2	5.9	5.9	100.0
	Total	34	100.0	100.0	

Table 4.2.5.1

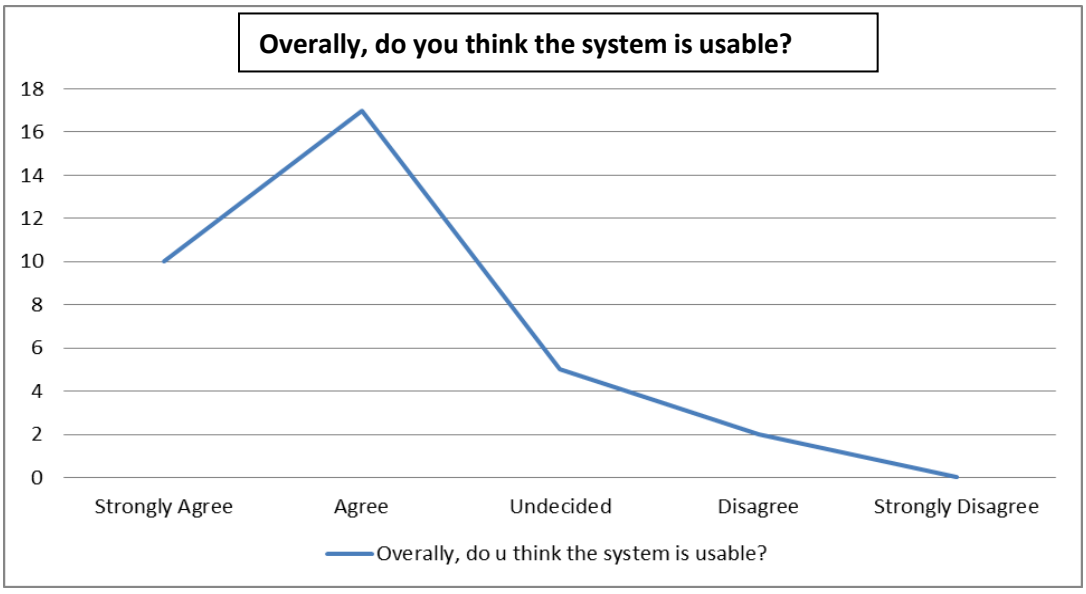


Fig 4.2.5.2

The respondents' data in the pie chart shows that about 50% and 29.412% agreed and strongly agreed respectively in support of the system usability. About 14% remained undecided after using the system and could not decide whether the system was usable or not. The researcher posed this question to better understand how the system was accepted by the users and the data distribution from the respondents firmly proves that the system is indeed usable.

4.2.5 Analysis of independent variables

One standard questionnaire was distributed to the sample selected of 34 users from the public works and local government (Bindura, Mashonaland Central, Zimbabwe). The questionnaires were distributed targeting people with different roles in the company and who handle different files, some of which are not supposed to be seen by other people. The researcher also used observations as a way of investigating how the users rated or viewed the system, how they took the system and how they used it.

4.3. Questionnaire Responses

The responses that the researcher obtained for all the evaluating factors (system effectiveness, user satisfaction, usability) were overwhelming as most of the users all agreed or strongly agreed with the implementation of the system. .The cross-section of respondents is wide enough to warrant reliable findings and conclude that most of the respondents felt strongly for the system and found it as a tool against vigorous password policies and as a protection mechanism for data and files. All the questionnaires were distributed to that sample population since they are the final users of the system and are somehow directly affected by the system.

4.3.1 Perception of users towards mobile Bluetooth driven security system?

The perceptions of the users were centered on three factors usability, effectiveness and security as they are the underlining pillars of a successful security system. Because this system main aim is to offer a possible solution to the difficulties being faced by the users who have difficulties abiding by some password policies and who are also conscious on securing their files. It was noted earlier that when asked if the system was effective, a lot of respondents agreed that the system is indeed effective. When asked if they were satisfied with the system and that it is usable, again more users stuck to that belief and most of them agreed to that.

4.4 Key findings and conclusions

The main finding from the implementation of the Bluetooth driven security system was successful enough to warrant a permanent implementation of the system. The behavior of users in security has changed dramatically and more respondents were impressed with the easiness associated with the system. So in a way it has been noted that the system has simplified the daily work lives of several people due to its simplicity and automated protection mechanism. It is therefore safe to say the system is indeed effective in protecting files and also in improving password policies.

References

1. Wayne C. Summers and Edward Bosworth, Columbus State University (2004). Password policy: The Good, the Bad and the Ugly

2. Philip Inglesant & M. Angela Sasse, Department of Computer Science University College London (2010), the True Cost of Unusable Password Policies: Password Use in the Wild

3. Karen Scarfone Murugiah Souppaya (2009). Guide to Enterprise Password Management

4. Peter Hoonakker, Nis Bornoe and Pascale Carayon (2009). Password Authentication from a Human Factors Perspective: Results of a Survey among End-Users

5. Danuvasin Charoen, Murali Raman and Lorne Olfman (2007). Improving End User Behavior in Password Utilization: An Action Research Initiative

6. Richard Shay and Elisa Bertino, Published in International Journal of Information Security; Volume 8, Number 4 (2009). A Comprehensive Simulation Tool for the Analysis of Password Policies

7. Fernando Alonso, ISSA Journal December 2008. The Extinction of Password Authentication

8. Fadi Aloul, Syed Zahidi, Department of Computer Science & Engineering, American University of Sharjah, UAE and Wassim El-Hajj, College of Information Technology UAE University (2009). Two Factor Authentication Using Mobile Phones.

9. National Survey on Data Security Breach Notification by the Ponemon Institute LLC (2006)

10. Bishop M. (2003). *Computer Security Art and Science,* Addison Wesley.

11. A Nadeem, Information and Communication Technologies, 2005, ICICT 2005. First International Conference

12. T Jamil - Potentials, IEEE, 2004 - ieeexplore.ieee.org

13. Bruce Schneier, John Kelsey, Doug Whiting, David Wagner, Chris Hall, Niels Ferguson, Tadayoshi Kohno, Mike Stay (May 2000). The Twofish Team's Final Comments on AES Selection

Appendix

Questionnaire

Improving windows password policies using mobile Bluetooth and Rijndael Encryption

1. Do you think that the existing windows password login is enough to secure your files?

Strongly disagree ☐ disagree ☐ undecided ☐ agree ☐ strongly agree ☐

2. There are certain password policies that require you change your password regularly? Do you agree with such a policy?

Strongly disagree ☐ disagree ☐ undecided ☐ agree ☐ strongly agree ☐

3. Do you think certain security measures must be in place to strengthen the existing windows authentication system?

Strongly disagree ☐ disagree ☐ undecided ☐ agree ☐ strongly agree ☐

4. After using the Bluetooth Secure System, do u think it is an effective system?

Strongly disagree ☐ disagree ☐ undecided ☐ agree ☐ strongly agree ☐

5. Do you think the system has simplified the problems associated with other policies that require more participation from you in ensuring that your system is secure?

Strongly disagree ☐ disagree ☐ undecided ☐ agree ☐ strongly agree ☐

6. Do you think token authentication using mobile phones for example should be the hub of every workstation for security purposes?

Strongly disagree ☐ disagree ☐ undecided ☐ agree ☐ strongly agree ☐

7. Do you think encrypting files specifically hinders unauthorized users from violating your files?

Strongly disagree ☐ disagree ☐ undecided ☐ agree ☐ strongly agree ☐

8. Overally, do u think the system is usable?

Strongly disagree ☐ disagree ☐ undecided ☐ agree ☐ strongly agree ☐

Comments……
……
……

