Conference Paper

Usability, Encryption, and the User Experience

Hesham Al-Ammal and Lamya Aljasmi

College of Information Technology, University of Bahrain, P.O.Box 320328, Sakheer, Kingdom of Bahrain

Corresponding Author:
Hesham Al-Ammal
halammal@uob.edu.bh

Received: 18 September 2018
Accepted: 10 October 2018
Published: 15 October 2018

Publishing services provided by Knowledge E

Selection and Peer-review under the responsibility of the Sustainability and Resilience Conference Committee.

Abstract

Security and usability have been considered to be at odds with each other by many researchers, who held the view that improving one affects the other in a negative way. Encryption is a ubiquitous technology in cyber-security and is an essential part of the hardening and resilience of any service. The security community have repeatedly advocated the use of encryption for ensuring privacy and integrity of the user's data and communications. However, many studies have shown that users either lack an understanding of encryption or the knowledge of its features. Several parameters such as key length, key management, etc., may affect the usability of encryption techniques. Furthermore, many users think that the usability of these encryption applications is poor. This is a serious issue as their attitudes toward usability may seriously affect the user's and the organization's security and privacy, while the installation of the encryption software leads to a false impression of security. The aim of this article is to investigate the usability of several popular encryption products and study the effects of usability on user's adoption of these tools. The study adopts a suitable cognitive model for the problem, and presents a study on a group of users that was conducted to discover the different factors that affect the usability of encryption in everyday life. The article will investigate security usability design guidelines and models that lead to better usability for encryption software. Several recommendations and practical guidelines are outlined that can be used by practitioners to make encryption more usable and thus increase the resilience of software systems.

Keywords: Usable Security, Software Resilience, Encryption, Usable Security Models

1. Introduction

Ever since the introduction of computers and communication devices we have seen an increasing dependence on digital media and the need for privacy, confidentiality and authentication. The digital transformation of every aspect of life from personal files

How to cite this article: Hesham Al-Ammal and Lamya Aljasmi, (2018), "Usability, Encryption, and the User Experience" in *Sustainability and Resilience Conference: Mitigating Risks and Emergency Planning*, KnE Engineering, pages 71–91. DOI 10.18502/keg.v3i7.3073

to official documents, made it necessary to use tools such as cryptography to protect these documents. However, for this very technical tool, there is a human element.

Our digital infrastructure’s resilience depends on the correct use of encryption. A powerful military-grade cryptosystem can be compromised if the human using it is not willing or able to use it properly. Throughout the history of computing and the Internet, we have seen cases where a security system is compromised due to human negligence or misuse [1, 2]. In this paper, we will examine some aspects of usability for encryption, which contributes directly to the resilience of our digital society.

Resilience according to the Oxford English Dictionary refers to “the capacity to recover quickly from difficulties”. While it defines cryptography as “the art of writing or solving codes.” Although this might be historically accurate it does not define the breadth of the field and its relationship to resilience.

Within the field of cyber security there are three main objectives that are vital for a system to be secure: confidentiality, availability, and integrity [3]. The latter two objectives are vital for resilience of our data and most systems controlled by ICT in this information age. Providing availability of the data and its integrity using the various tools will ensure resilience, which is the basis for a stable and secure society. Confidentiality also contributes to resilience by making attacks harder on data and information. A common tool for the three objectives is cryptography, and whatever the strength of a cryptographic cipher, usability by the public is vital to resilience.

2. A Review of Usability and Security in Software Systems

For the past three decades, researchers have studied usable computer security using concepts from Human Computer Interaction as well as other novel tools related to security [4]. Developers and researchers addressed usability among many different topics within cybersecurity, including: user authentication, access control, email encryption, among others [4].

Early research looking at usability of secure systems suggested that the satisfying the goals of usability might necessarily be counter-productive to security. Intuitively, usability aims at making life easier for the user, while security aims at making it hard (for malicious or unauthorized) users to access information. However, this over-simplistic approach was then dismissed by researchers with the introduction of several models that combine the goals of both usability and security [4]–[7].

The design of security-sensitive software applications involves a trade-off between achieving strong security and making the software easy to use. Security and usability have frequently been viewed as competing system goals [8], [9]. There was always an impression among practitioners that enforcing usability characteristics produces more easily compromised software; and that security measures make software tedious to use or hard to understand.

Some examples of usability and security features in applications and systems include: word processing software with tasks such as adding digital signatures to facilitate subsequent document authentication, document readers which allow setting viewing, access and printing permissions, personal devices with activities such as applying security pins and locks to mobile phones, personal security firewalls and email encryption tools. [9].

Poor usability in a security environment normally leads to incorrect or insufficient configurations of security tools and functionality such as access controls, firewalls, encryption mechanisms and routers. In addition, users may (through misuse or ignorance) weaken security features all together [10]–[12].

Conflicts between security and usability can often be avoided by taking a different approach to security in the design process and the design itself. As John Viega and Gary McGraw [13] wrote, "Bolting security onto an existing system is simply a bad idea. Security is not a feature you can add to a system at any time." The most successful designs find ways to achieve multiple goals simultaneously that is to bring security and usability into alignment through many points that consider satisfying both aspects [5]. Many researchers [6], [9] emphases that security and usability are vital, and the goal should be to consider them early on, iteratively and in concert. Fidas et al. [6] value a user-centric design approach to usable security.

3. Aligning Security and Usability: A Model

Kainda et al. [7] developed a Security-Usability Threat Model which specifies the critical characteristics that require examining during the evaluation of usability and security. Those characteristics are related to usability, security, or both. Figure 1 depicts the Security-Usability Threat Model. It shows that the model is centered around the user. Nielsen [14] defined usability as a quality characteristic that evaluates how easy user interfaces are to use. Usability also relates to means for improving ease-of-use during the design process. The usability quality characteristics to be considered are effectiveness, satisfaction, accuracy, and efficiency. The security characteristics are attention, vigilance, conditioning, motivation, and social context. Other characteristics that belong to both usability and security are memorability and knowledge/skill.

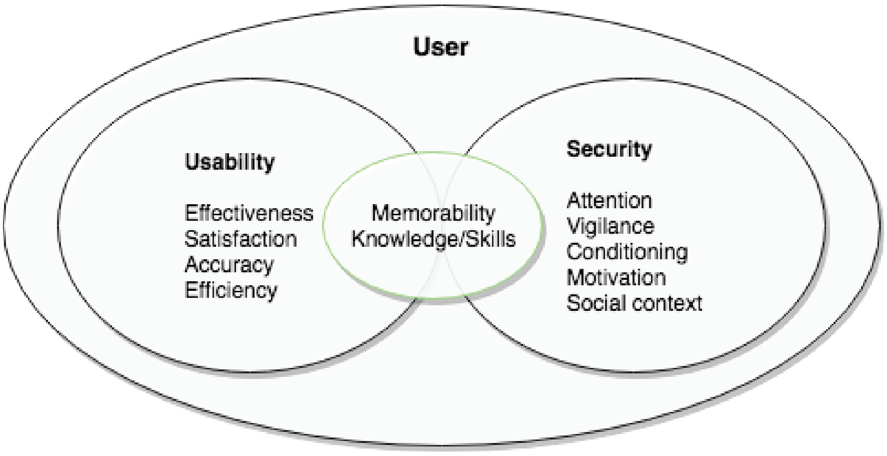

Figure 1: Usability Security Threat Model (adopted from Kainda et al. [6]).

The following is a discussion of the usability and security metrics/characteristics from the model suggested by Kainda et al. [7]. This was the model adopted by the study for the purposes of constructing the survey instrument.

3.1. Usability metrics

1. *Effectiveness* refers to how good a system at going what it supposed to do [15]. A system is only usable if its users are able to accomplish their planned goals. Effectiveness is measured by whether users are able to complete a particular task or not.

2. *Satisfaction* refers to how pleasant is to use the system [14]. Users should accept and like the system. Important indicators to measure users' satisfaction are if users well to continue to use a system and a higher degree of assessment is to recommend it to others. User satisfaction can be assessed through interviews and rating scales.

3. *Accuracy* as a factor was identified in authentication and device pairing studies. In many cases, authentication systems require users to enter passwords with 100% accuracy while certain mechanisms in device pairing require 100% accuracy when entering or comparing short strings [16]. Accuracy requirements on users are affected by other requirements such as recall of required information, environmental, or personal factors.

4. *Efficiency* refers to when a system supports users in carrying out their tasks and achieving their goals in a way to save time and effort [15]. So, once users have learned how to use the system, how quickly they can perform their desired tasks

[14]. Efficiency is captured by measuring the time to complete a task or the number of clicks/buttons pressed to achieve required goals.

5. *Memorability* refers to how easy a system is to remember how to use and maintain once learned [15]. Many verification systems demand that users remember secrets and then recall them when they want to be validated by a system. The number of secrets a person needs to memorize increases with the number of different validation systems that a specific person interacts with. This causes memorability difficulties and thus has a negative impact on usability. Users face problems in validating themselves on various systems and often their attempts end in demands to reset those secrets [17].

6. *Learnability* refers to how easy a system is to learn and to use [15]. This depends on the assumption that users attempt to learn and understand the system. This assumption is imperfect especially in personal secure systems. Many studies specified that despite using a system, users only care about those parts that they think are important to specific operations they need, however in many cases *security tasks are not seen to be important*. For instance, a study of a P2P system found that users did not know that the system shared folders on their local drives that were viewable on the internet [18]. Furthermore, it was found that users of banking websites cannot distinguish between a padlock at the bottom of a browser window or one displayed as an image on a web page [19]. Previous studies have also found that training users in using secure systems is unsuccessful [20]. This can be due to fact that tasks such as sharing folders, checking presence of padlock and learning about good security practices are not the goals of the users in many situations.

3.2. Security metrics

1. *Attention* allows us to focus on information that is related to what we are doing [15]. It is known that users can easily be distracted, triggering them to change their attention from the original and aimed task. Security tasks should not request exclusive attention from users as this will cause annoyances and frustrations, and probably security failures. Users have an impression that secure systems are disruptive because secure systems frequently disrupt user’s attention for the purpose of attending security prompts. Disruptive and passive methods to gain users’ attention such as certificate prompts and browser padlock are generally ignored by the users [7].

2. *Vigilance* is a state of watchfulness, the force for which maps directly to perceived consequence of missing out on possible observations [21]. Secure systems expect users to be alert and proactive in evaluating the security status of a system.

   However, studies have indicated that even experts are not constantly alert. For example, [22] discovered that experts on web site security indicators did not look in places where those indicators were, therefore they fall into simulated phishing attacks that they would have avoided if they looked and noticed the absence or presence of indicators. Tasks that carry this security risk were those that require users to divert their attention from a primary task to attend to a security task.

3. *Motivation* can be described as the influences that account for the initiation, direction, intensity, and persistence of behavior [23]. According to professor of psychology J. Nevid "The term motivation refers to factors that activate, direct, and sustain goal-directed behavior" [24]. Users have different levels of motivation to perform security tasks in different situations. Participants in a study in [16] specified that they would prefer typing passkeys longer than 6 digits for financial transactions exceeding a certain monetary value. Thus, in this situation, the participants saw the risk to be more direct to them because they will lose money than in a situation where risk is perceived to be low or directed at someone else [7].

4. *Memorability* is necessary as authentication systems need users to memorize secrets that are difficult for someone else to guess or attack. Passwords present an essential tension between usability which is supported by having short, easily memorable passwords and reusing them across multiple systems and security which requires longer and distinct passwords that are difficult to crack for each system [4]. As the number of secrets to be memorized increase, it become hard to recall a particular secret when it is required by a system especially if the system is not used frequently. Users write down these secrets to prevent forgetting and resetting. This effect the security of the system because written secrets can be found by others who might use them for malicious purposes [7].

5. *Learnability*–the ability of the users to learn and gain knowledge or skills about a security of a system support and preserve the security of the system. Many users enter sensitive information on unprotected websites because they lack the knowledge or skill to distinguish between a secure and an insecure website [19]. Users also share sensitive information using P2P software unknowingly because they lack knowledge about the operation of P2P software.

6. *Social context* is vital, as humans are social beings. They live together, help each other, and share many stuffs. Usually sharing is a good practice, however, it is not for security users when they share their security secrets. Researchers [25] found that users working on a particular project shared one digital certificate rather than each having their own as intended by system designers. Also [26] found that users shared passwords for various social reasons. Users also share secrets because someone is offering to help them if they disclose the secret. This has been exploited in many situations [27] and that is why it has been named social engineering.

7. *Conditioning* which involves repetitive security tasks that lead users to guess a result can be a threat to the security of a system. This can be seen in pop-up messages that ask users if a particular certificate should be trusted or not. A few exposures to those pop-up messages allow the user to understand that clicking a specific button will make the pop-up disappear and to proceed with a task [7].

4. Study Methodology

The aim of this paper is to investigate the users' attitudes toward disk and file encryption software. These utilities are used for protecting private files and data within the operating system, and some of them are native to the operating system (such as Microsoft's BitLocker, Apple's FileVault) or software utilities for encrypting email or files (such as PGP, Veracrypt, AxCrypt, GNU Privacy Guard, etc.).

The model that was adopted was the Usability-Security Threat Model proposed by Kaninda et al. [7] (shown in Figure 1) and discussed in the previous section. This seems like a simple model that encapsulates most of the required metrics and aligns both the usability and security metrics. A survey was prepared and administered on a sample of N=34 persons (17 males and 17 females).

The survey included introductory questions regarding gender, age, profession, and IT experience. The following Figures show the composition of the selected sample. The sample was chosen from both private and public sector and covered a wide range of professions and qualifications as can be seen from the charts. The survey questions covered the model metrics, and a Likert-type scale of 5 was used with choices ranging from Strongly Agree to Strongly Disagree. For the responses on the survey the sample size was reduced to N=27 sue to the fact that 7 respondents had no experience using encryption software.

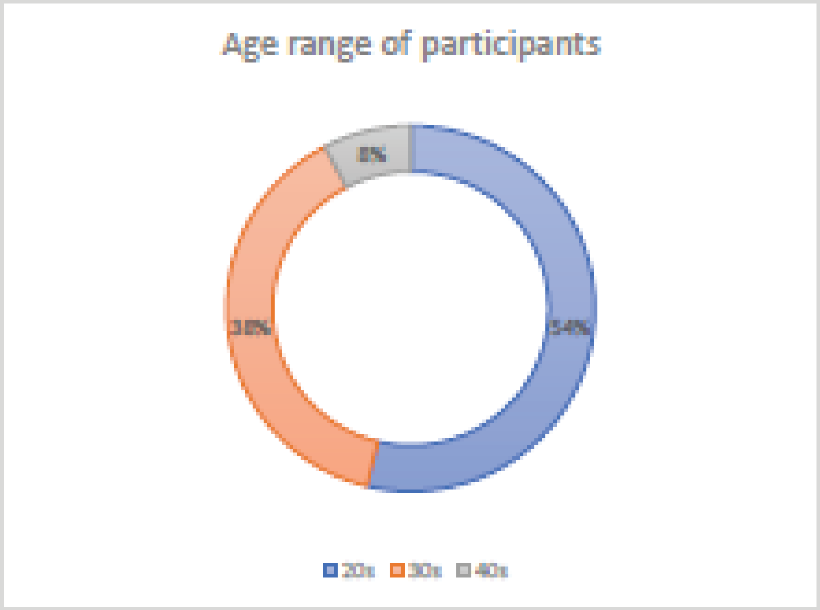

Figure 2: Age range of the participants (N=34).

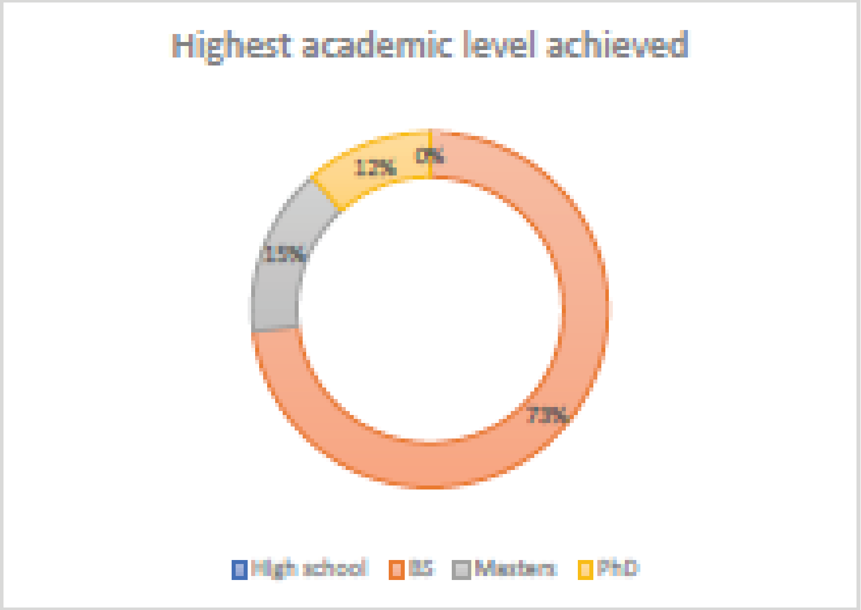

Figure 3: Academic qualifications.

5. Results and Analysis

The following are the results for section I regarding Usability of these encryption tools. Note that the sample size for the following analysis is N=27 and includes only respondents with experience with encryption software.

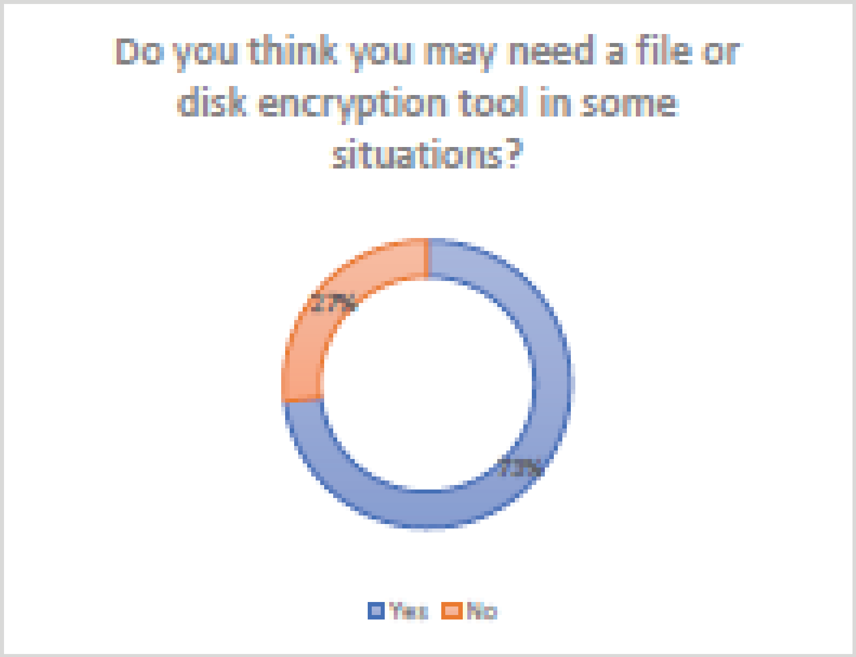

Figure 4: User's perception of the need for encryption tools.

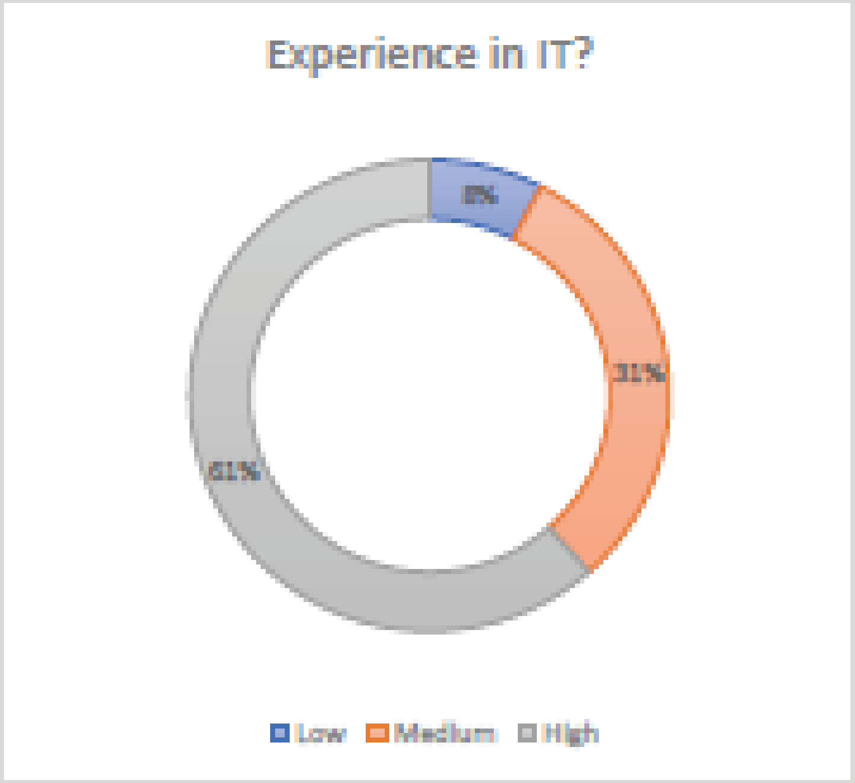

Figure 5: Respondent's experience in IT (N-34).

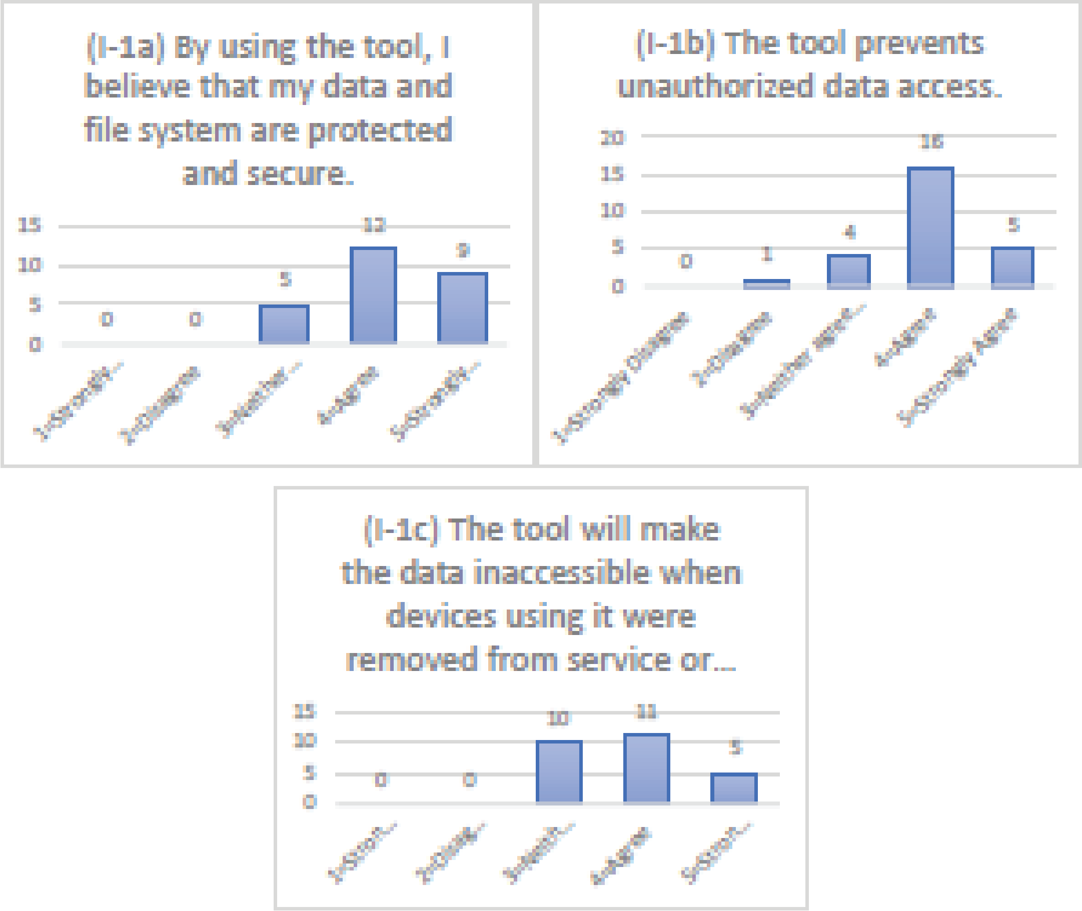

Figure 6: Usability -Effectiveness.

5.1. Usability component

The mean value of effectiveness (Figure 6) is 3.97 which is above our target. This indicates that the encryption tools were effective. 80% of the respondents agree that they were able in accomplish their planned goals by using the encryption tools to secure their data and file systems and to prevent unauthorized data access. The mean of the responses for the tool will make the data inaccessible when devices using it were removed or recycled is 3.8. It should be noted that 60% of the respondents agree with the question but 38% (more the third) were not sure or able to decide about this issue.

The mean value for the questions related to satisfaction (Figure 7) is 4.24. This means that the respondents liked the tools and are highly satisfied from using them to protect their data. Around 80% of the respondents will continue using the tool to protect their data. While 92% of the respondents indicated that they will recommend using the tool to others which indicates a higher level of satisfaction than just using it individually.

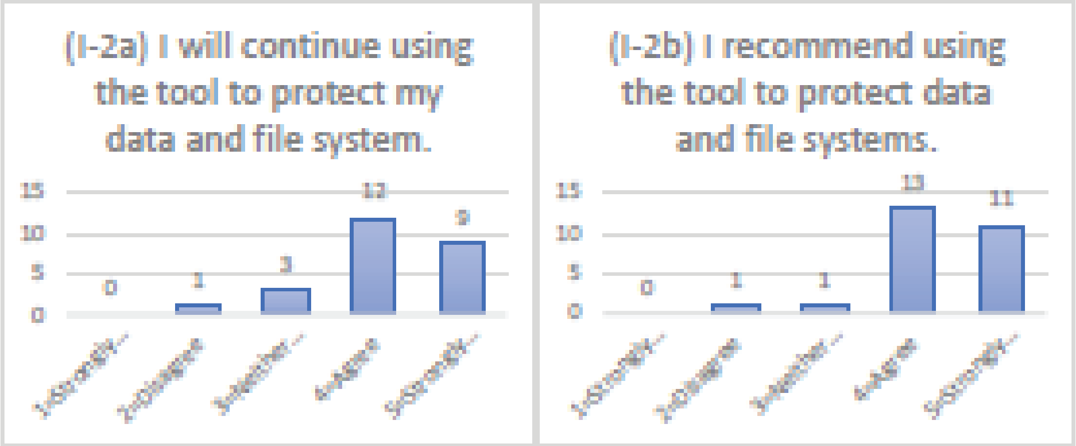

Figure 7: Usability – Satisfaction.

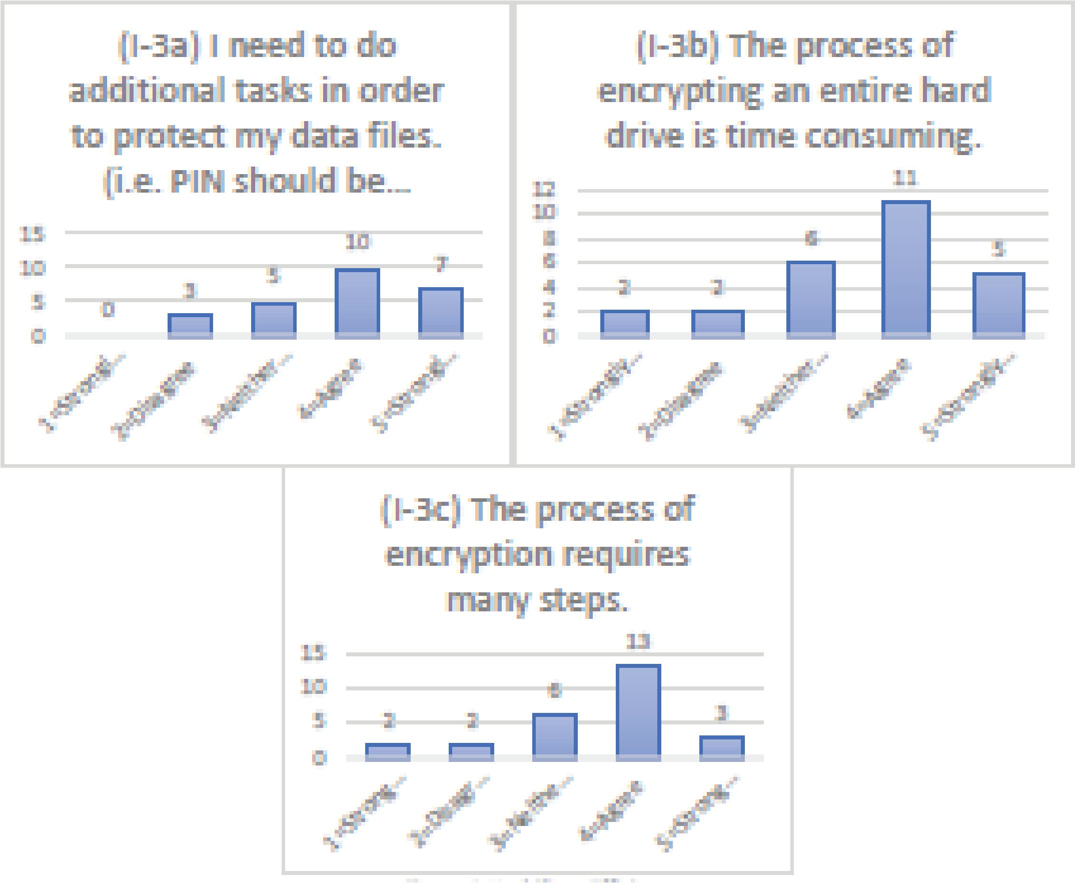

Figure 8: Usability - Efficiency.

The mean value of the indicators related to efficiency (Figure 8) is 3.46, which is slightly below our target of 3.5. This means that the respondents feel that the tools require additional tasks or many steps and time consuming. The number of respondents who agreed that the security features of the tools were enabled by default almost equal to those who did not agree and also those who are not sure which resulted to get a mean of 2.92. When the security features are enabled by default, the number of steps to complete the tasks will be reduced, which will increase the efficiency of the tools.

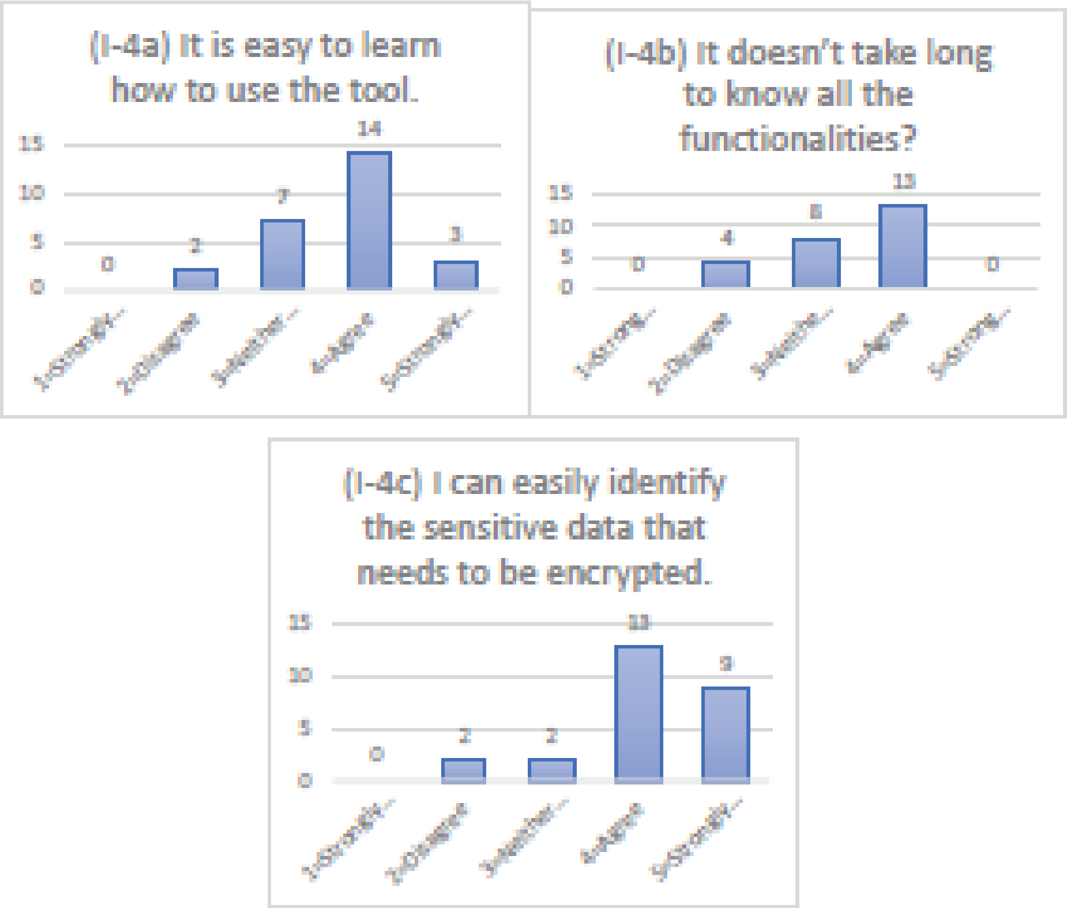

Figure 9: Usability - Learnability.

The mean value of the indicators related to learnability (Figure 9) is 3.73 which is above our target. Around 84% of the respondents agreed that it is easy to identify the sensitive data that needs encryption (4.1). However, only 65% of the respondents agreed that the tools are easy to use (3.7) and 50% of the respondents agreed that it does not take long time to know all the functionalities (3.36) which is below the target.

The mean value of the memorability indicators (Figure 10) related to usability is 3.45 which is below our target. The majority of the respondents agreed that the tools require memorizing additional secrets, and wrote those secrets whenever not able to recall them. Around 54% of the respondents agreed that it is easy to remember additional secrets.

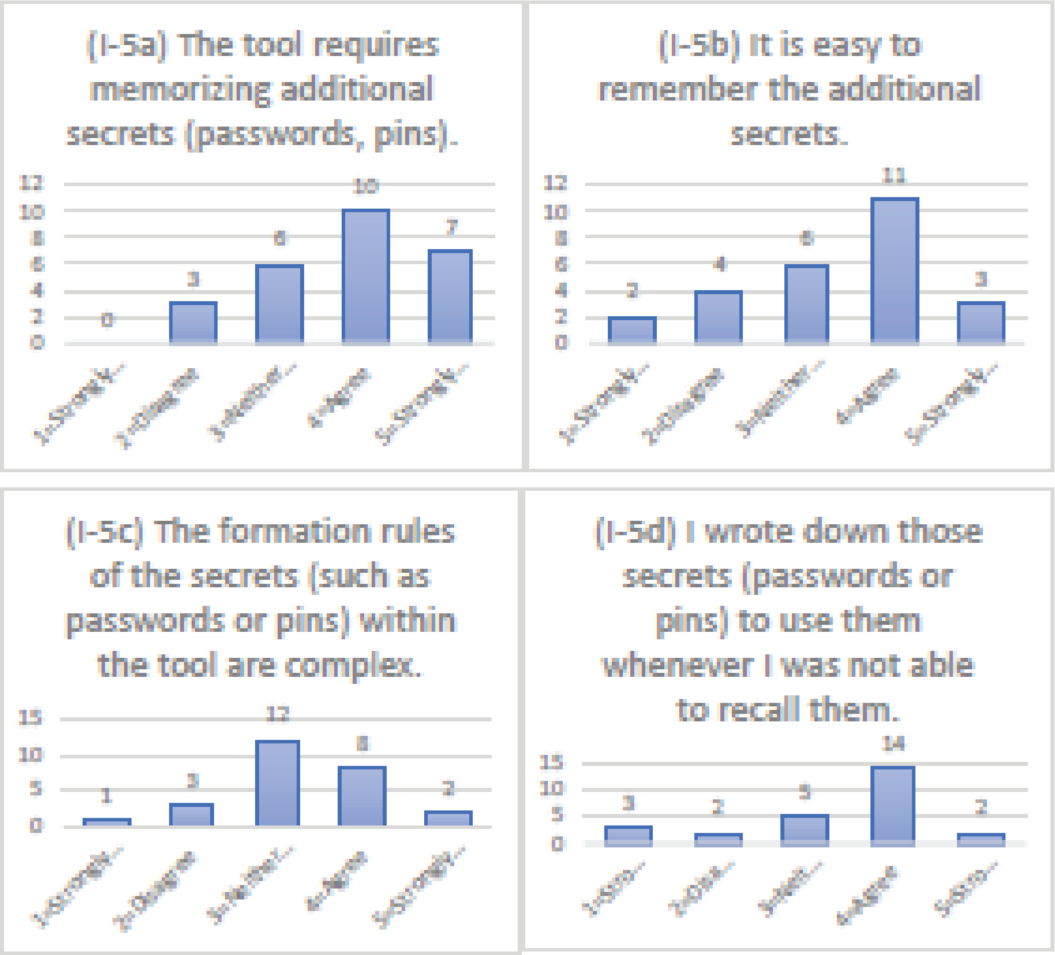

Figure 10: Usability - Memorability.

Figure 11 shows a summary of the means for Usability metrics. Note that the internal consistency measure selected was the Cronbach's alpha, and its value for the usability part was 0.7, which is within range.

5.2. Security component

The following are the results for assessing the security characteristics among the sample who had experience with encryption software (N=27). Note that the Cronbach's alpha for this part was 0.75 which shows good internal consistency and is within the target.

Although, the mean value of the attention indicators (Figure 12) turned out to be 3.45 which almost reached our target, the mean values of all three indicators related to that the security tasks are done automatically reached the target (3.53-3.69).

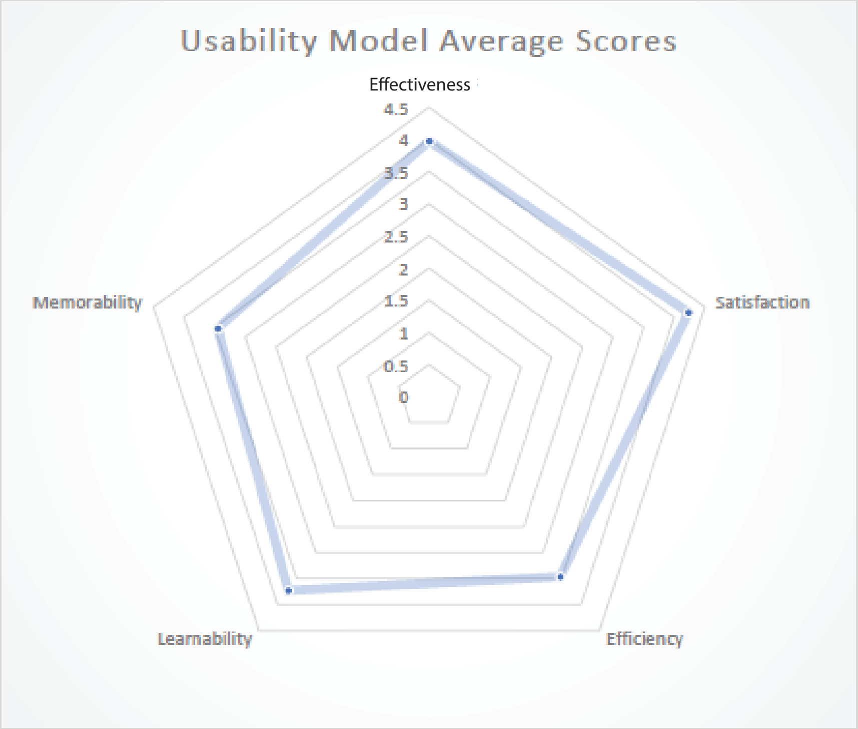

Figure 11: Average scores for various metrics in the Usability component.

However, the mean value of the indicator states that encryption and decryption distract from completing the aimed tasks is 3.0 which is below the target. Furthermore, 42% of the respondents neither agree nor disagree, 31% of the respondents agree that the tasks distracted them, and only 27% disagree that the tasks distracted them.

The mean value of the indicator related to Vigilance (Figure 13) reached the target which is 3.81. The majority of the respondents agree that they have to be alert to determine the security state of the system even though they use an encryption tool.

The mean value of the motivation indicators is 4.5. This indicates that the respondents are highly motivated to use encryption tools.

The mean of the social context indicators (Figure 15) which are related to sharing passwords and digital certificates with other is 3.05 and is far below the target. This indicates that around quarter of the respondents share their passwords and digital certificates with others, which is a very dangerous practice.

The mean to the first indicator “repetitive security tasks for which users can predict an outcome can become a threat to the security of a system” is 3.69 which is slightly above the target (Figure 15). It means that the respondents have an acceptable awareness regarding the condition of repetitive security tasks. The mean of the second indicator is 2.38 which is far below the target. This indicates that the respondents do

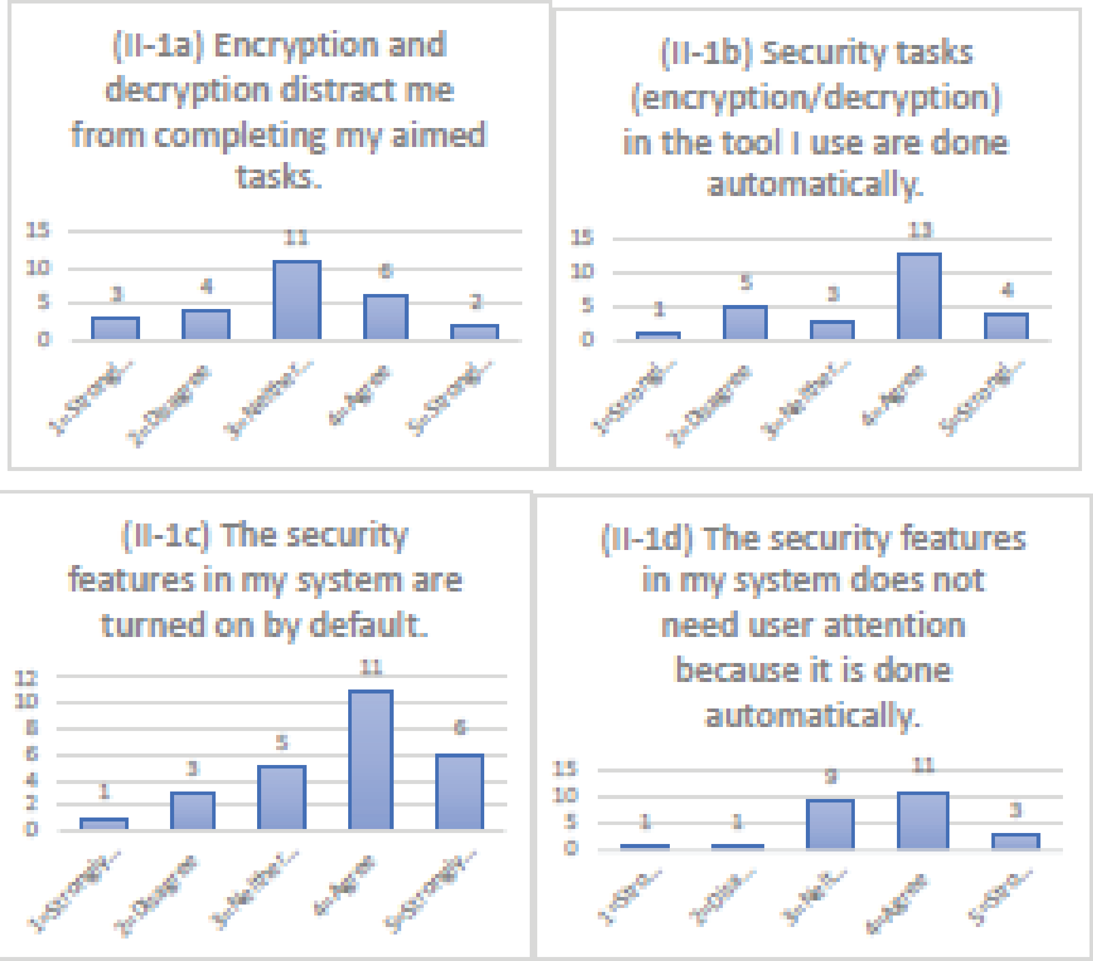

Figure 12: Security - Attention.

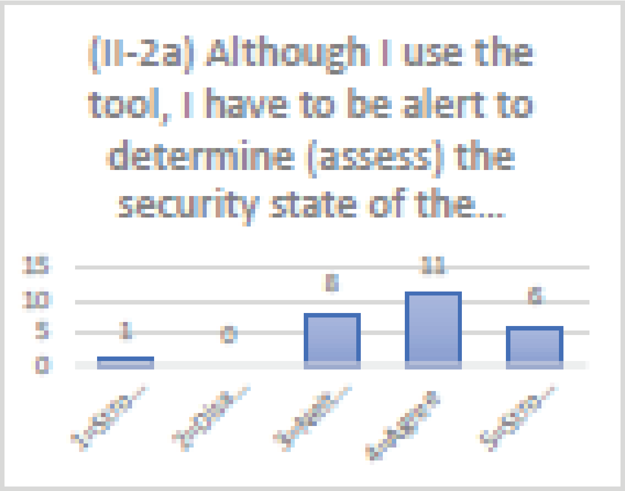

Figure 13: Security - Vigilance.

not trust the software used to save and fill the password even it can be a solution for the difficulty of memorizing passwords or reduce the efforts needed to deal with

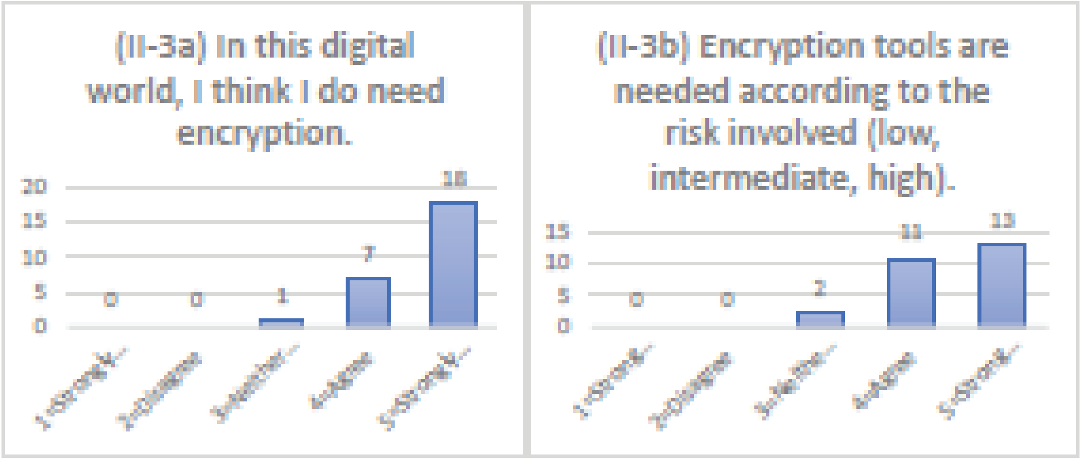

Figure 14: Security - Motivation.

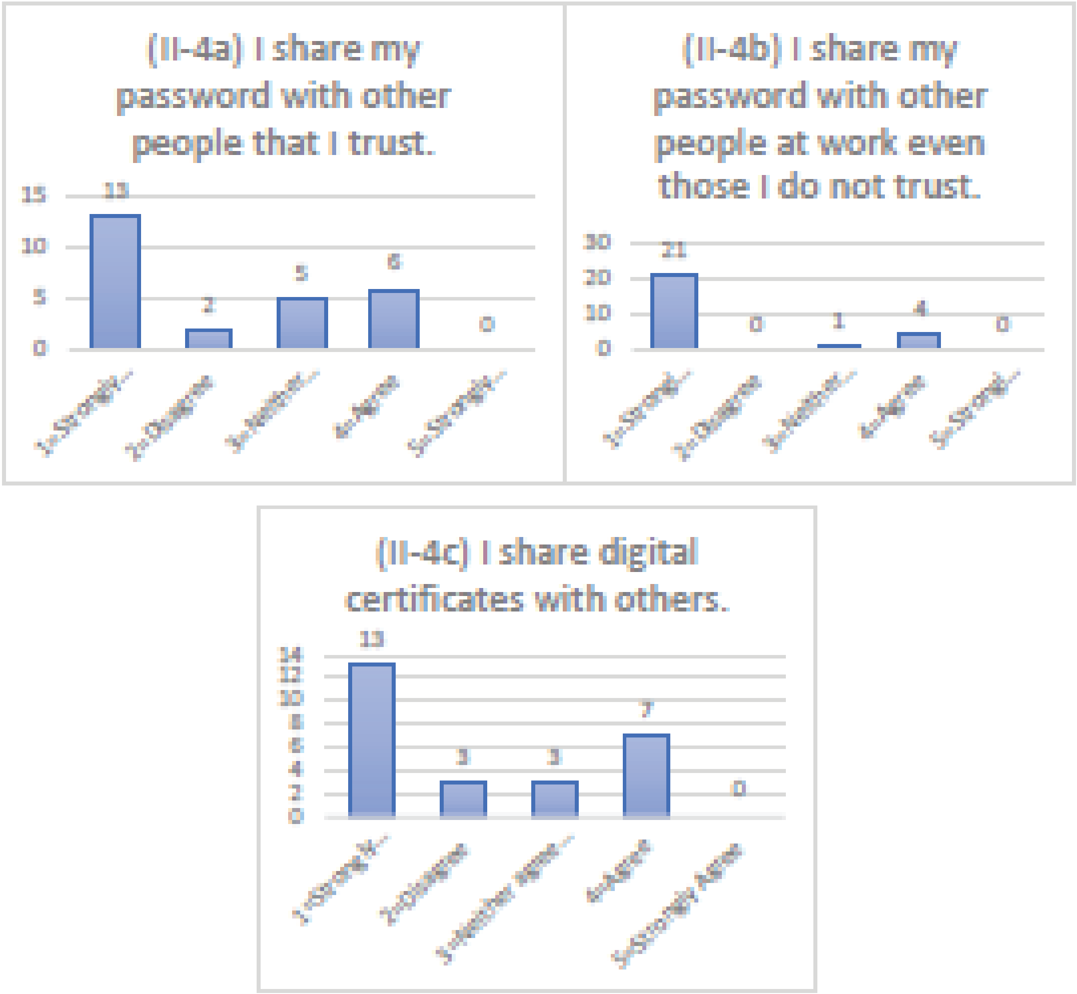

Figure 15: Security - Social Context.

security issues. The mean of the third indicator is 2.65 which is also below the target.

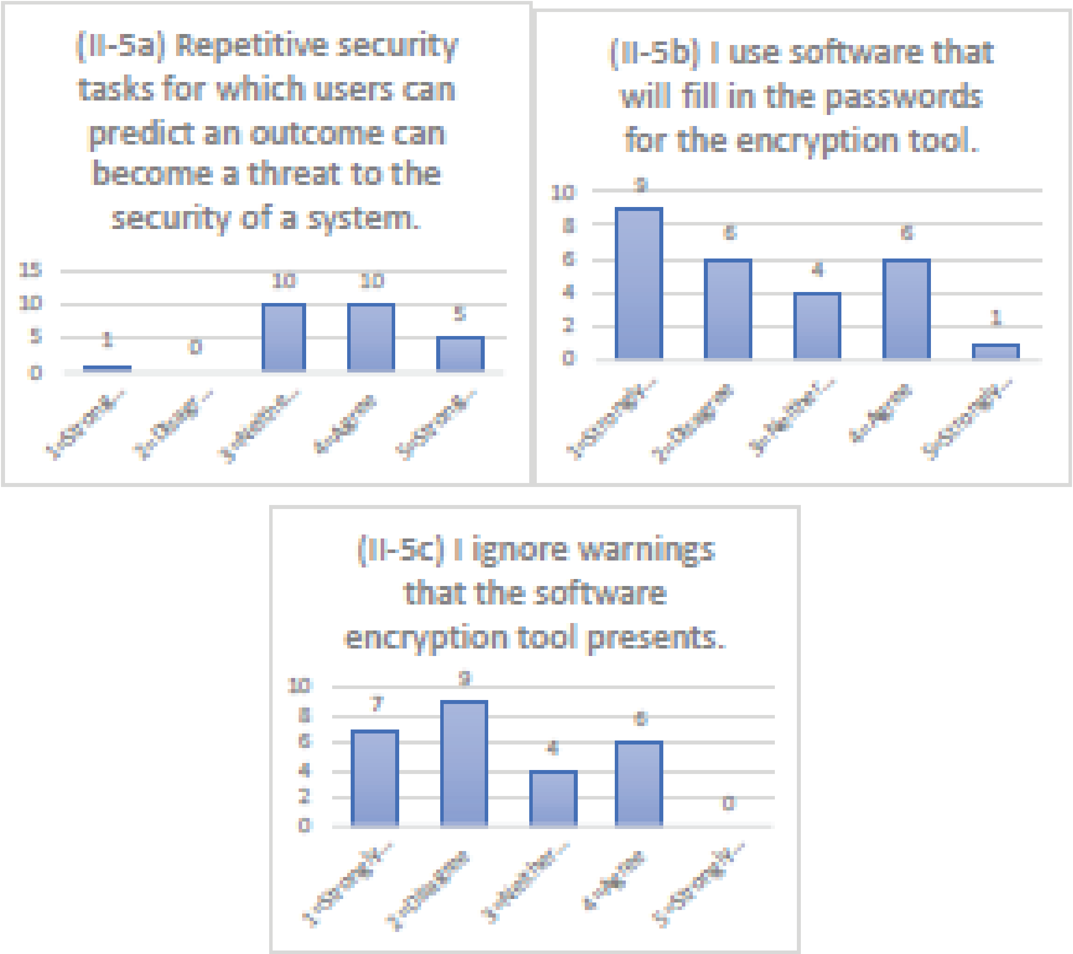

Figure 16: Security -Conditioning.

Only 61% of the respondents refuse to ignore warnings presented by the encryption software.

Figure 17 shows a summary of the means for the security component.

6. Conclusions

Resilience of our data and software resources depends on many factors, one of which is encryption technology. Encryption is the single most widely used method for both access control and authentication, leading to the resilience of our data resources. Even though awareness of this fact has been strengthened by the occasional attacks on data and systems, as well as public awareness and training campaigns; there is still a need to increase the awareness of professionals to adopt encryption tools for protecting their data.

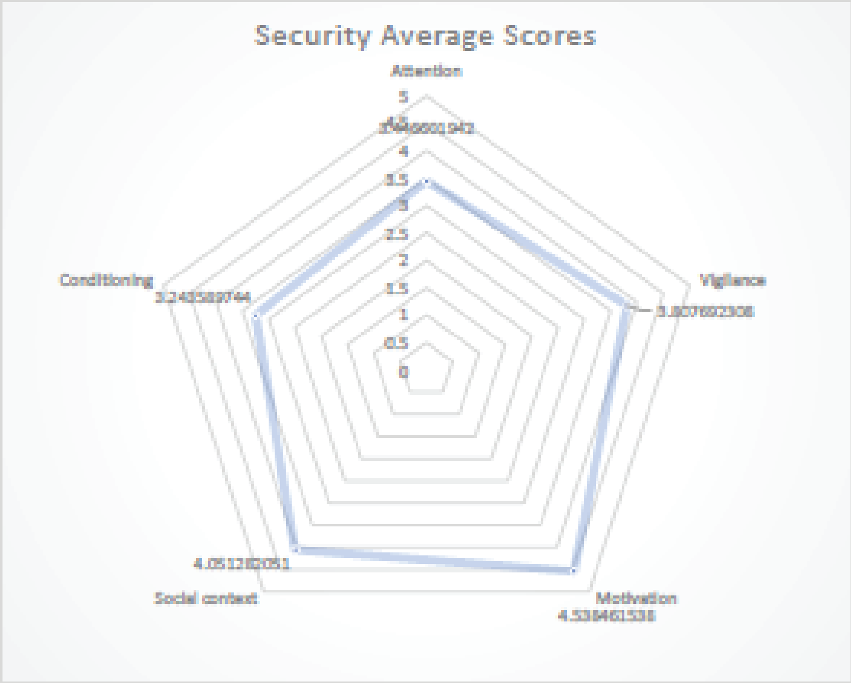

Figure 17: Mean scores for the Security component of the model.

Cryptography has always been associated with applications in the military or espionage. Thus, most normal users do not think that it is of vital importance for protecting their data. Furthermore, the various cryptographic techniques have mathematical background that is somewhat archaic and is not accessible to normal citizens.

In this study a model was adopted to assess both the usability and security of file and disk encryption software on a sample of professionals in the Kingdom of Bahrain. The model adopted was developed to unify both usability and security concerns, which were thought to be contradictory in some of the literature [7]. The sample included N=27 professionals of different positions and qualifications, all of which had experience working with encryption software. The internal consistency of the survey, measured using Cronbach's alpha was acceptable.

Within the *Usability* component, the indicators for Effectiveness, Satisfaction, and Learnability were high. However, Efficiency and Memorability were below the target. This may be affected by the design of these encryption tools or may be the result of the inaccessibility of cryptography as a concept. More capacity building is needed in this regard.

On the other hand, for the Security component, the Vigilance, Motivation, and Social Context indicators were above the target level. While Conditioning and Attention were relatively low. This is expected, as one of the biggest problems with such software has been repetitive tasks that lead to humans exposing the process steps, or sharing passwords or secret keys with others. Perhaps the most striking result was in the conditioning metric, as the mean for the second indicator regarding the trust of the password saving tools was below 2.5. Furthermore, around 39% ignored security warnings from encryption software.

This is something that needs to be ameliorated by capacity building and education. Hiding the complexity of encryption by automating it to make it seamless, such as the process done in browsers and other devices, may also be a solution to such user behavior. The adoption of biometrics and other techniques that simplify the encryption decryption process is another good option for making the process more seamless and reducing complexity related to secret key memorization. As was stated earlier, successful designs find ways to achieve multiple goals simultaneously that is to bring security and usability into alignment through many points that consider satisfying both aspects.

References

[1] C. Stoll, *The cuckoo's egg: tracking a spy through the maze of computer espionage*. Simon and Schuster, 2005.

[2] D. Kahn, "The codebreakers–The comprehensive history of secret communication from ancient times to the Internet–Revised and updated," *N. Y. NY Scribner*, 1996.

[3] R. Von Solms and J. Van Niekerk, "From information security to cyber security," *Comput. Secur.*, vol. 38, pp. 97–102, 2013.

[4] B. D. Payne and W. K. Edwards, "A Brief Introduction to Usable Security," *IEEE Internet Comput.*, vol. 12, no. 3, pp. 13–21, May 2008.

[5] K.-P. Yee, "Aligning security and usability," *IEEE Secur. Priv.*, vol. 2, no. 5, pp. 48–55, 2004.

[6] C. A. Fidas, A. G. Voyiatzis, and N. M. Avouris, "When security meets usability: A user-centric approach on a crossroads priority problem," in *Informatics (PCI), 2010 14th Panhellenic Conference on*, 2010, pp. 112–117.

[7] R. Kainda, I. Fléchais, and A. W. Roscoe, "Security and Usability: Analysis and Evaluation," in *2010 International Conference on Availability, Reliability and Security*, Krakow, Poland, 2010, pp. 275–282.

[8] Nicholas A. Sherwood, *Enterprise security architecture: a business-driven approach*. CRC Press, 2005.

[9] J. R. Nurse, S. Creese, M. Goldsmith, and K. Lamberts, “Guidelines for usable cybersecurity: Past and present,” in *Cyberspace Safety and Security (CSS), 2011 Third International Workshop on*, 2011, pp. 21–26.

[10] S. W. Smith, “Humans in the loop: Human-computer interaction and security,” *IEEE Secur. Priv.*, vol. 99, no. 3, pp. 75–79, 2003.

[11] A. L. Stephano and D. P. Groth, “Useable security: interface design strategies for improving security,” in *Proceedings of the 3rd international workshop on Visualization for computer security*, 2006, pp. 109–116.

[12] C. Kuo, A. Perrig, and J. Walker, “Security Configuration for Non-Experts: A Case Study in Wireless Network Configuration,” in *Social and Human Elements of Information Security: Emerging Trends and Countermeasures*, IGI Global, 2009, pp. 179–195.

[13] G. McGraw and J. Viega, *Building Secure Software: How to avoid security problems the right way*. Addison-Wesley Professional, 2002.

[14] J. Nielsen, *Usability 101: Introduction to usability*. 2003.

[15] J. Preece, Y. Rogers, and H. Sharp, *Interaction design: beyond human-computer interaction*. John Wiley & Sons, 2015.

[16] R. Kainda, “Human Factors in HCBK Protocol,” PhD Thesis, University of Oxford, 2007.

[17] S. Brostoff and M. A. Sasse, “‘Ten strikes and you’re out’: Increasing the number of login attempts can improve password usability,” 2003.

[18] N. S. Good and A. Krekelberg, “Usability and privacy: a study of Kazaa P2P file-sharing,” in *Proceedings of the SIGCHI conference on Human factors in computing systems*, 2003, pp. 137–144.

[19] S. E. Schechter, R. Dhamija, A. Ozment, and I. Fischer, “The emperor’s new security indicators,” in *Security and Privacy, 2007. SP’07. IEEE Symposium on*, 2007, pp. 51– 65.

[20] M. A. Sasse, “Computer security: Anatomy of a usability disaster, and a plan for recovery,” 2003.

[21] M. Kurosu, *Human-Computer Interaction Theories, Methods, and Tools: 16th International Conference, HCI International 2014, Heraklion, Crete, Greece, June 22- 27, 2014, Proceedings*, vol. 8510. Springer, 2014.

[22] R. Dhamija, J. D. Tygar, and M. Hearst, “Why phishing works,” in *Proceedings of the SIGCHI conference on Human Factors in computing systems*, 2006, pp. 581–590.

[23] P. W. Nash and D. A. Bernstein, *Essentials of psychology*. Houghton Mifflin, 2008.

[24] J. Nevid, *Psychology: Concepts and applications*. Nelson Education, 2012.

[25] B. Beckles, V. Welch, and J. Basney, “Mechanisms for increasing the usability of grid security,” *Int. J. Hum.-Comput. Stud.*, vol. 63, no. 1–2, pp. 74–101, 2005.

[26] M. A. Sasse, S. Brostoff, and D. Weirich, “Transforming the ‘weakest link’—a human/computer interaction approach to usable and effective security,” *BT Technol. J.*, vol. 19, no. 3, pp. 122–131, 2001.

[27] K. D. Mitnick and W. L. Simon, *The art of deception: Controlling the human element of security*. John Wiley & Sons, 2011.