2014

Persistent issues in encryption software: A heuristic and cognitive walkthrough

Jad El-Abed
Edith Cowan University

Patryk Szewczyk
Edith Cowan University, p.szewczyk@ecu.edu.au

Recommended Citation

El-Abed, J., & Szewczyk, P. (2014). Persistent issues in encryption software: A heuristic and cognitive walkthrough. DOI: https://doi.org/10.4225/75/57b66416343d5

DOI: 10.4225/75/57b66416343d5

12th Australian Information Security Management Conference. Held on the 1-3 December, 2014 at Edith Cowan University, Joondalup Campus, Perth, Western Australia.
This Conference Proceeding is posted at Research Online.
https://ro.ecu.edu.au/ism/174

PERSISTENT ISSUES IN ENCRYPTION SOFTWARE: A HEURISTIC AND COGNITIVE WALKTHROUGH

Jad El-Abed[1], Patryk Szewczyk[1,2]
[1]Edith Cowan University, Perth, Australia
[2]Security Research Institute, Perth, Australia
p.szewczyk@ecu.edu.au

Abstract

The support information accompanying security software can be difficult to understand by end-users, who have little knowledge in cyber security. One mechanism for ensuring the integrity and confidentiality of information is encryption software. Unfortunately, software usability issues can hinder an end-user's capability to properly utilise the security features effectively. To date there has been little research in investigating the usability of encryption software and proposing solutions for improving them. This research paper analysed the usability of encryption software targeting end-users. The research identified several issues that could impede the ability of a novice end-user to adequately utilise the encryption software. A set of proposed recommendations are suggested to improve encryption software which could be empirically verified through further research.

Keywords
security software usability, encryption, cyber security, heuristic evaluation, cognitive walkthrough

INTRODUCTION

The Australian Bureau of Statistics revealed that there were approximately 12.5 million internet subscribers in Australia as of June 2014 (ABS, 2014). This number is expected to rise as a result of the Australian Government, National Broad Network (NBN), which will provide consumers, with high-speed internet through fibre optic cabling or fixed wireless systems (Mani, Choo, & Mubarak, 2014; NBNCo, 2014; Szewczyk, 2012). Internet communication is an integral part of society that has replaced legacy forms of communication. Unfortunately, there is a downside to embracing the benefits of the Internet in the form of online threats (Szewczyk, 2012). It has become necessary to safe guard the privacy and confidentiality of personal information through the use of cyber security software. One such security mechanism is encryption software.

There are many documented cases of cyber related crimes on businesses that have had their confidential and unencrypted information stolen. In 2010, an employee from A4E Limited had their laptop stolen (Turner, 2011). Stored on it was the unencrypted confidential information of approximately 24,000 users. As a result of the company's negligence, they were fined $108,000 by the UK Information Commissioner. In 2013, Hospice of North Idaho had a laptop which encompasses unencrypted records of 441patients (Senft, 2013). In 2013, Horizon Blue (a health insurance provider) had two laptops stolen from its main office. The laptops contained unencrypted data on 840,000 of their customers' medical records ("Horizon Blue", 2013). According to the 2014 incident report by Symantec (2014), approximately 552 million records were exposed due to data breaches and a lack of cryptographic practices.

End-users are typically unaware of the benefits and requirements for using encryption software. In 2010, an international research study by LMRMC (2010) surveyed over 3250 office workers across six countries. The research revealed that forty-two percent of employees, would copy confidential documents onto unencrypted storage media (Wall, 2013). In a separate study, Gujrati and Vasserman (2013) revealed that of the 54 respondents they surveyed, 93 percent had no understanding of disk encryption or its purpose. Unfortunately, despite the lack of knowledge and awareness, software usability issues such as poor interface design and difficult terminology can further hinder an end-user's ability to use encryption software effectively (Furnell, 2010; Whitten & Tygar, 1999; Gujrati & Vasserman, 2013). In addition, performance degradation and coding errors can subsequently affect the reliability of the software.

RELATED WORKS

Encryption Software Usability Research

Perhaps one of the most influential papers associated with security software usability research is through Whitten and Tygar's (1999) evaluation of PGP 5.0 encryption software. Their work included using a cognitive walkthrough and laboratory experiment as part of their analysis methodology. The cognitive walkthrough involved assessing the software with regards to four usability guidelines the authors had created. These guidelines were proposed definitions for good design properties, which meant not adhering to them would yield usability issues. The laboratory experiment, which involved participants performing general encryption tasks, was conducted in order to confirm what they had identified during their evaluation process. From the collective results, their first conclusion was that the software suffered sufficient usability issues that it was considered unsuitable for most end-users. Their second conclusion was identifying that PGP 5.0's interface design philosophy, mismatched the end-users' ability to accomplish encryption tasks effectively (Whitten & Tygar, 1999).

Gujrati and Vasserman (2013) examined the usability of TrueCrypt and then proposed a modified interface based on their analysis. Their first goal was to improve a novice end-user's experience without affecting the functionality and capability of the software. While their second and broader goal, was to prove that modifying existing source code for a piece of software, in order to improve usability, was not a strenuous task. They conducted two types of studies, a cognitive walkthrough and an empirical end-user study. The walkthrough focused on identifying usability issues within TrueCrypt using Wharton, Rieman, Lewis and Poison's (1994) outlined usability properties as a guide.

The research process divided forty-four participants into either a treatment or control group. Participants were expected to perform general tasks with the software they were assigned. In this case, the control group used the original TrueCrypt, whilst the remaining group used the modified version. During the experiment, participants were continually observed. A post-study questionnaire was then administered in order to collect feedback on their experiences. The results from both studies identified similar issues. Specifically it was revealed that TrueCrypt suffered from non-intuitive visuals, using difficult terminology, providing an illogical flow of tasks, and being unnecessarily complex. As a result, the authors' concluded that the identified usability issues may impede on an end-user's ability to use the software correctly. Thereby, becoming sufficiently frustrated to the point where they would abandon its use (Gujrati & Vasserman, 2013).

Security Software Usability Research

Furnell, Jusoh and Katsabas (2006) conducted an end-user study to examine the usability of the security features within Microsoft Windows XP's 'security centre', Internet Explorer (IE), Word and Outlook Express. This was performed by screen capturing interfaces end-users may have encountered when using the programs, and embedding them within an online survey. The authors' goal was to better understand the end-users' perception and understanding of the security features within commonly used programs. During the survey period they had collected 342 responses. The survey findings showed that usability issues were identified among the basic and advanced security options. These issues mainly involved convoluting controls, and difficult to understand technical and security terminology (Furnell *et al*, 2006).

Agashe, Jaferian and Shamji (2007) evaluated the usability of Microsoft Vista's firewall through an end-user study. They performed a sample survey to collect the participant's general understanding about the firewall. Afterwards, they conducted an experiment involving participants completing several tasks. A post-study questionnaire was administered to obtain information on their experiences. The authors' concluded that the firewall suffered from a number of usability issues, including difficulty navigating the software, weak in-built help feature, and the advanced firewall system not being readily accessible (Agashe *et al.,* 2007).

Similarly, Arjmandi, Boeck, Raja and Viswanathan (2008) performed a heuristic evaluation followed by a laboratory experiment to examine the usability of Microsoft Vista's firewall. Before they attempted their end-user study, a heuristic evaluation was conducted to identify usability issues within the software. This was done by performing several representative tasks through the perception of a novice end-user. Subsequently, this allowed the experimenters to anticipate and record usability issues that may come up during the end-user study. Thus, from the evaluation several tasks were created for the participants to complete during their laboratory exercises. Afterwards, participants were questioned about their experiences using the software. The authors identified several usability issues, including the lack of end-user freedom, poor placement of controls, difficulty locating the firewall in advanced security, and an ineffective supportive documentation (Arjamandi *et al.,* 2008).

Alfayyadh, Ponting, Alzomai and Josang's (2010) research focused on observing the usability of four popular personal firewalls from the perspective of a 'normal' end-user. This was performed using a cognitive walkthrough approach, whereby usability issues would be identified if they violated any of Josang *et al.'s* (2007) eight usability principles. Issues that were highlighted during the evaluation process included difficult terminology, poor visibility of alerts, and a lack of information. As a result, the personal firewalls were all deemed unsuitable for novice end-users. Fortunately, the authors noted that configuring the firewalls correctly would provide effective and efficient security protection (Alfayyadh *et al.*, 2010).

RESEARCH DESIGN

Purpose and Aim

The purpose of this research is to assess whether the selected encryption software products are appropriately suitable for end-users. The research encompasses a heuristic evaluation and cognitive walkthrough of each encryption software; identifying usability and performance issues. The aim of this paper is to identify and subsequently raise awareness of the problems that exist within encryption software. Eventually, the hope is that improvements will be made to increase the usability of the software products amongst end-users. As such, this paper outlines a list of recommended changes based on the outcomes of this research.

The following are the encryption software products that were examined:

- *Advanced Encryption Package 2014* was selected for being ranked second in the top ten reviews website (Carlsen, 2014), and claiming to be 'award-winning easy-to-use file encryption software' as stated on their official website (www.aeppro.com).
- *Cryptainer LE 10* was selected as the official website claims it has 8 million end-users worldwide using their product. In addition, they claim their 'world-class encryption software package' is one of the most used in the world (www.cypherix.com).

Data Collection and Analysis Method

This research examines the usability of popular encryption software marketed to end-users. Qualitative techniques were used for collecting and synthesising data gathered, often useful for describing phenomena amongst results (Trochim, 2001). The software selected went through a heuristic evaluation and cognitive walkthrough, carefully examining their end-user interface design, performance, and ease of use. To help identify any possible usability issues, a list of usability criteria from various publications shown in Table 1, were used as an integral part of the evaluation process.

There are two main types of usability inspection methods that require no end-user participation. Firstly a heuristic evaluation, which examines the software against a set of established usability criteria, also known as heuristics. These heuristics were developed to help indicate problems end-users may encounter with the software (Nielsen, 1994). In contrast, a cognitive walkthrough involves an experimenter performing tasks with the software by assuming the position of a novice end-user. The goal here is to identify any possible difficulties the experimenter believes a novice end-user may encounter (Nielsen, 1994). As such, this research performs both usability inspection methods in order to produce meaningful results, similarly to Whitten and Tygar's (1999) research. The examination of the software analysed the main end-user interfaces, configuration settings, and the process of encrypting and decrypting the same MD5-hash checked image file (.jpg).

Table 1 Summary of usability criteria

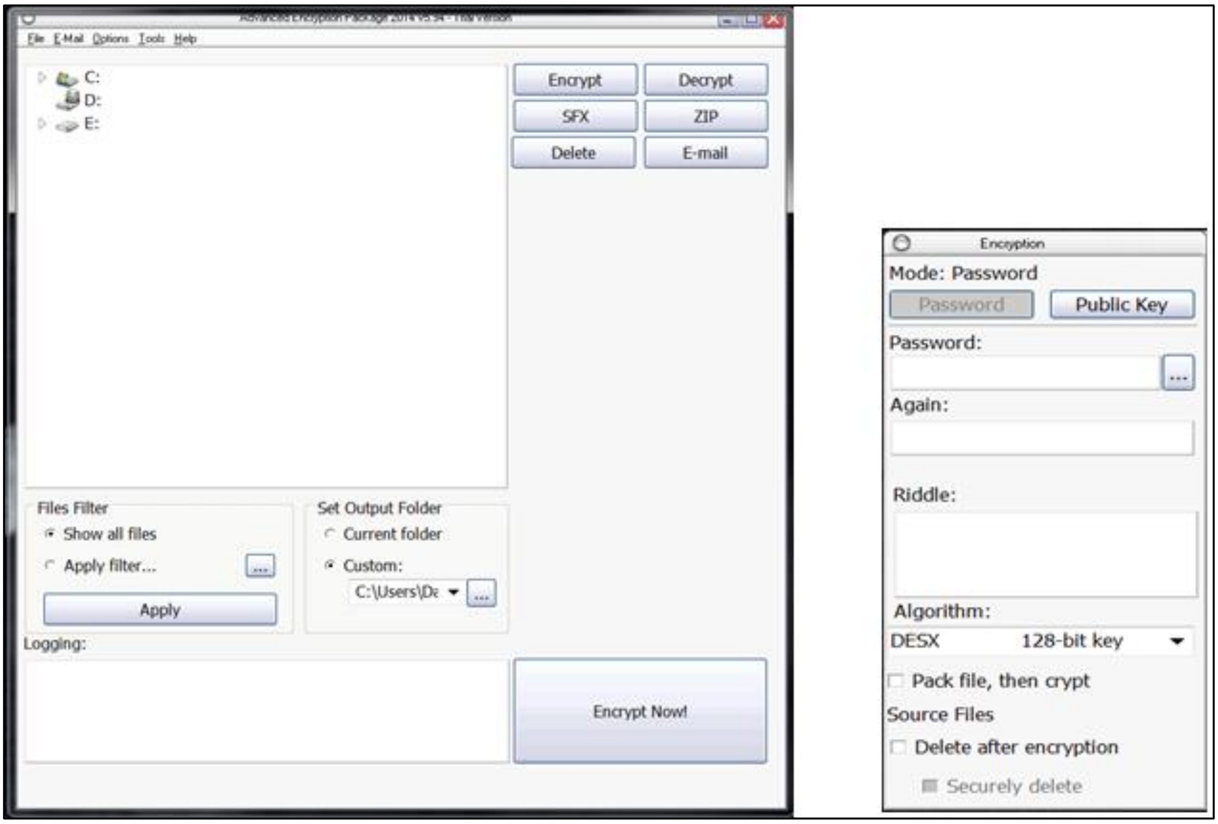
Criteria	Description
Aesthetic and minimalist design	The interface should only include relevant information and have an aesthetic design
Learnability and efficiency of use	The interface should be easy to learn, and include helpful explanatory links to security terms
Meaningful vocabulary and terminology	The information presented should match the end-user's language rather than use IT and security related terminology
Convey features	The interface should communicate the available security features to the end-user efficiently
Supportive documentation	The interface should include help documentation that relates to the end-users' task, with a step-by-step guide that is not too long

DISCUSSION

Advanced Encryption Package 2014

Main End-user Interfaces

The main end-user interface for Advanced Encryption illustrated in Figure 1(a), presents the end-user with a range of security controls. In addition to opening the application, a separate interface titled ‘Encryption’ appears overlapping the main end-user interface shown in Figure 1(b). The second interface’s purpose is to present controls that are relevant with each security utility selected on the right of the main end-user interface. For example, when an end-user presses the ‘Encrypt’ button, several controls to set the password and encryption algorithm appear on the second interface. Moreover, the ‘Encryption’ interface can be switched between two modes by pressing either one of the top buttons shown in Figure 1(b). Unfortunately, the purpose of doing so is unknown to first time end-users. For this evaluation, only the encryption and decryption interfaces were examined.



Mode: Password

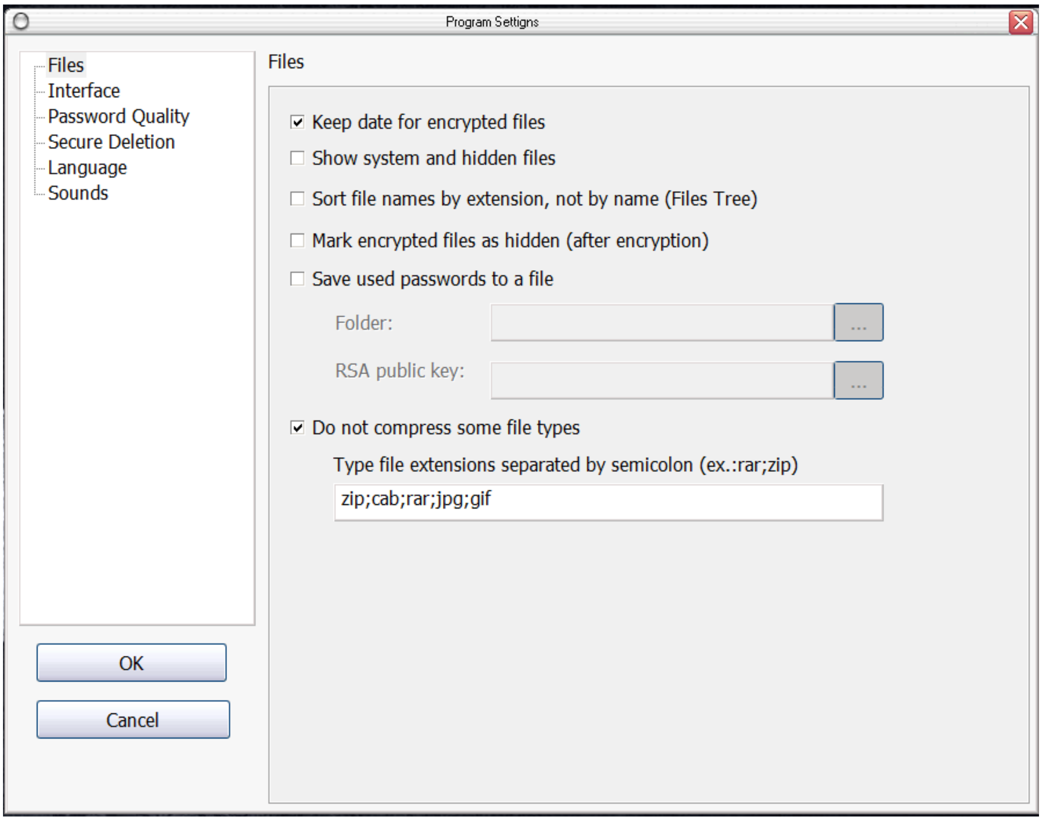
Algorithm: DESX 128-bit key

Figure 1a Main end-user interface and Figure 1b Encryption interface

An immediate problem identified upon executing the application, is that these interfaces appear without relevant information explaining to the end-user about their controls. This may potentially intimidate first time end-users and possibly frustrate them to the point of not using the software (Furnell *et al.*, 2003). Furthermore, the controls are labelled with terminology that may confuse end-users that lack the necessary security knowledge. For instance, the main end-user interface uses terms such as ‘encrypt’, ‘decrypt’, and ‘logging’. Additionally, terms that are abbreviated such as ‘SFX’ and ‘ZIP’ can be puzzling without context. The ‘encryption’ and ‘decryption’ interfaces also present the same issues, with labels such as ‘source file’, ‘pack file, then crypt’, ‘public key’, ‘compress’, and ‘priv key’. There is also the ‘algorithm’ section of the ‘Encryption’ interface, which presents a drop down list of algorithms without providing further explanation or guidance. Unfortunately, the lack of context-sensitive help is also present throughout the entire application, which may leave first time end-users confused on some of the important controls.

Settings Interface

The ‘Program Settings’ interface, accessible from the menu bar under the heading ‘tools’, provides end-users with six interfaces each with their own settings. In this example, the ‘Files’ interface illustrated in Figure 2 was examined. Immediately, there is a noticeable lack of context-sensitive help and instructions being provided on the interface. As a result, novice end-users may have difficultly interpreting their options with terms such as ‘system and hidden files’, ‘file extension’, ‘files tree’ and ‘RSA public key’ being used. For example, end-users that are unfamiliar with the term ‘file extension’ will likely have difficulty interpreting the third and last options shown on the interface. Further investigation into the remaining five interfaces reveals a number of additional issues similarly identified within the ‘Files’ interface. Figure 2 shows the names of those interfaces on the left hand side. For example, terms and phrases such as ‘crypto operations’, ‘allocated disk space’, ‘NTFS compressed’, ‘sparsed’, ‘multi-streamed files’, ‘alternate streams’ and ‘tray agent (clipboard encryptor)’ were used amongst the settings within those interfaces, to name a few. Unfortunately, these terms are more commonly identified within IT and cyber security related literatures. Therefore, novice end-users that lack sufficient knowledge and experience may not understand their choices. Another issue was the lack of explanatory text and assistance provided to educate end-users on the ‘wipe algorithms’ shown in the ‘Secure Deletion’ interface.



Files

☑ Keep date for encrypted files

☐ Show system and hidden files

☐ Sort file names by extension, not by name (Files Tree)

☐ Mark encrypted files as hidden (after encryption)

☐ Save used passwords to a file

Folder:

RSA public key:

☑ Do not compress some file types

Type file extensions separated by semicolon (ex.:rar;zip)

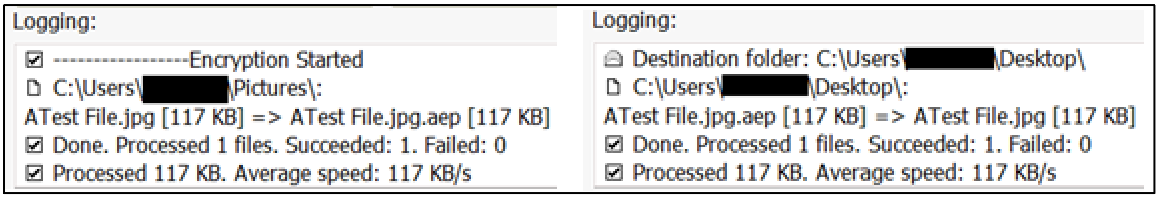
zip;cab;rar;jpg;gif

Figure 2 Programs settings interface

Software Operations

The first step to encrypting a file is selecting the ‘Encrypt’ button located on the right hand side of the main end-user interface. This will concurrently set the second interface to the ‘Encryption’ utility along with its relevant controls. The end-user now has two modes that they can select between, ‘password’ and ‘public key’. The first mode allows the end-user to encrypt a file with a password lock, while the second mode encrypts a file using a public key already stored on the computer. Unfortunately, both modes lack context-sensitive help, and neglect to provide assistance on how to perform the steps thus far.

For the purpose of this evaluation, the password mode was chosen and the default algorithm was used, which was DESX 128-bit key. The options ‘pack file, then encrypt’ and ‘delete after encryption’ were not selected. Locating a file to be encrypted is fairly straight forward and is accomplished by using the file explorer window on the main end-user interface. Upon selecting the desired file, the end-user has to switch back to the main end-user interface and select the large button labelled ‘Encrypt Now!’ Once encryption has initiated, the information on the process is recorded under the label ‘Logging’ shown in Figure 3 (a).



```
Logging:
☑ -----------------Encryption Started
🗋 C:\Users\[redacted]\Pictures\:
ATest File.jpg [117 KB] => ATest File.jpg.aep [117 KB]
☑ Done. Processed 1 files. Succeeded: 1. Failed: 0
☑ Processed 117 KB. Average speed: 117 KB/s
```

```
Logging:
Destination folder: C:\Users\[redacted]\Desktop\
🗋 C:\Users\[redacted]\Desktop\:
ATest File.jpg.aep [117 KB] => ATest File.jpg [117 KB]
☑ Done. Processed 1 files. Succeeded: 1. Failed: 0
☑ Processed 117 KB. Average speed: 117 KB/s
```

Figures 3a Encryption process details and Figure 3b Decryption process details

In order to decrypt a file, the end-user has to select the 'decypt' button on the main end-user interface then search for the relevant file using the file explorer window, similarly to the above explanation. The decryption interface presents two modes for the end-user to select from, 'password' and 'privkey'. As already stated, the application unfortunately fails to provide further assistance on these options. In particular, the term 'privkey' may confuse novice end-users that are unaware it stands for privatekey. Unfortunately, the concept of private and public may be lost on novice end-users that have little security knowledge or experience, considering the application fails to provide a sufficient description on the process. Once the file has been selected and the password is typed in correctly, the end-user only has to select the 'Decrypt Now!' button located on the main end-user interface. Similarly to the encryption process, the relevant information is recorded under the label 'Logging' shown in Figure 3 (b). Overall, an issue that was identified with the encryption and decryption processes is the illogical flow between tasks. Having to switch between the main end-user interface and the second interface breaks the continuity of having to only focus on one end-user interface and its controls.

Cryptainer LE 10

Main End-user Interface

The main end-user interface for Cryptainer illustrated in Figure 4, presents a range of controls and features that may seem confronting for first time end-users. Fortunately, after installing the application and creating a volume disk, discussed in detail below, the application does present the end-user with a dialog window of 'did you know' information. Nonetheless, the interface includes controls that without context have little meaning to first time end-users. For example, the buttons 'View in explorer, 'load', and 'unload'. In addition, the terms 'volume' and 'drive' may only be understood by end-users with sufficient IT knowledge. Furthermore, the icons displayed on the buttons could be slightly confusing or misinterpreted, especially considering they are relatively small in size. For instance, the load and unload icons show a yellow lock next to a file cabinet with an arrow pointing up and down respectively. Unfortunately, the meaning behind these controls may be lost on first time end-users that fail to understand the volume disk can either be locked (hidden) or accessible (unhidden).

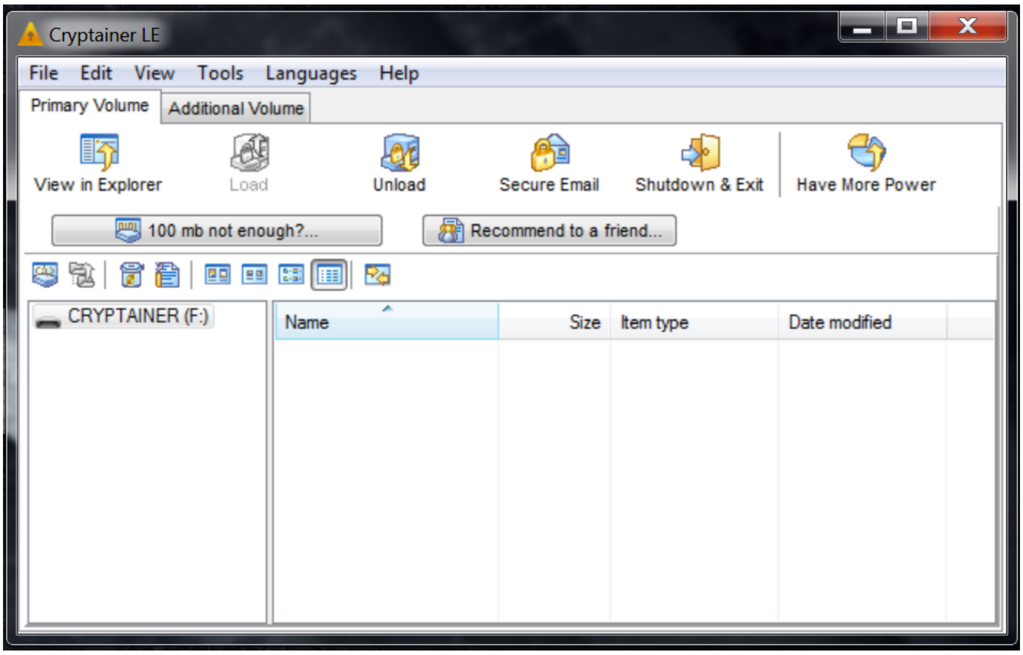
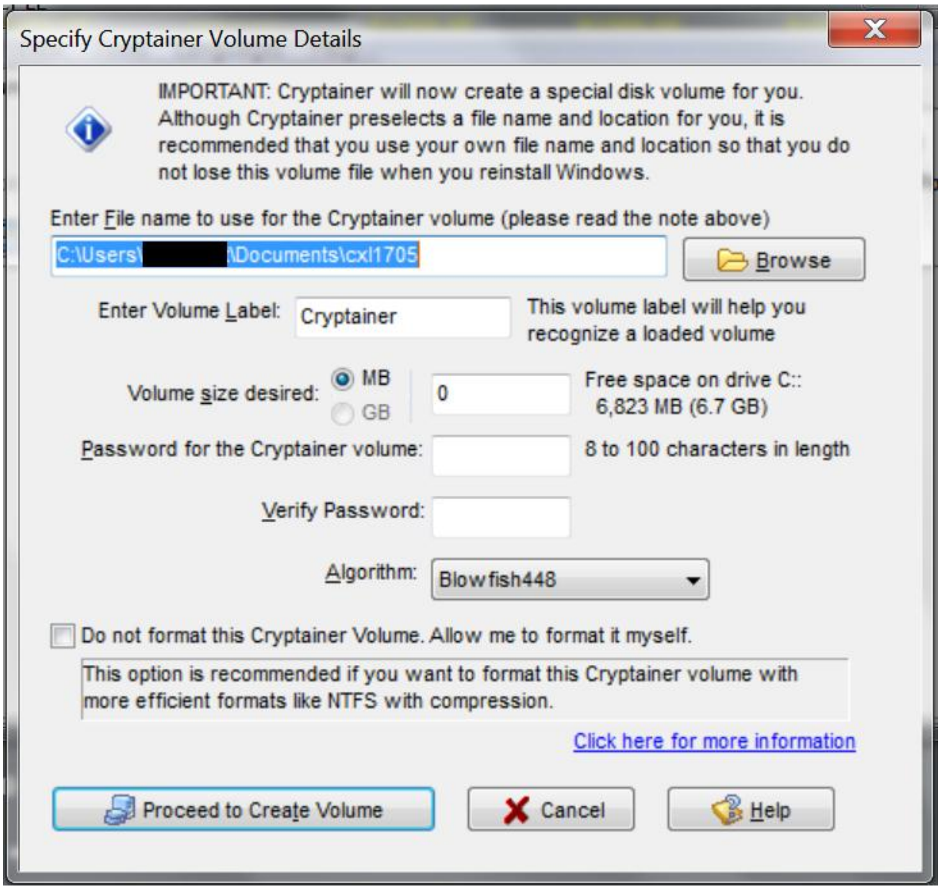


Figure 4 Main end-user interface for Cryptainer LE 10

Settings Interface

The ‘Specify Cryptainer Volume Details’ interface illustrated in Figure 5, appears with various controls and information that may at first instance be confusing for novice end-users. For example, the important notice indicates to end-users that the interface is for creating a ’special disk volume’. Unfortunately, this term may be difficult to interpret by novice end-users that have little IT knowledge. In fact, without understanding what ‘volume’ means, the entire interface can be difficult to interpret as it reuses the term several times without a meaningful explanation.

Pressing on the text field labelled ‘Volume size desired’ yields a temporary dialog help message. However, it only lasts five seconds and given how much information is presented, it can be difficult to read in one session. The only method of retrieving the information again is to click away and then click back onto the text field. Essentially, this issue can possibly provide another frustrating experience for the end-user among the already mentioned problems thus far. In addition, the information presented could be considered cryptic for novice end-users that have little IT knowledge. For instances, the term ‘drive size’ and the premise of increasing storage space may not be understood correctly.



Specify Cryptainer Volume Details

IMPORTANT: Cryptainer will now create a special disk volume for you. Although Cryptainer preselects a file name and location for you, it is recommended that you use your own file name and location so that you do not lose this volume file when you reinstall Windows.

Enter File name to use for the Cryptainer volume (please read the note above)

C:\Users\[redacted]\Documents\cxl1705

Enter Volume Label: Cryptainer

This volume label will help you recognize a loaded volume

Volume size desired: ● MB ○ GB 0

Free space on drive C:: 6,823 MB (6.7 GB)

Password for the Cryptainer volume:

8 to 100 characters in length

Verify Password:

Algorithm: Blowfish448

□ Do not format this Cryptainer Volume. Allow me to format it myself.

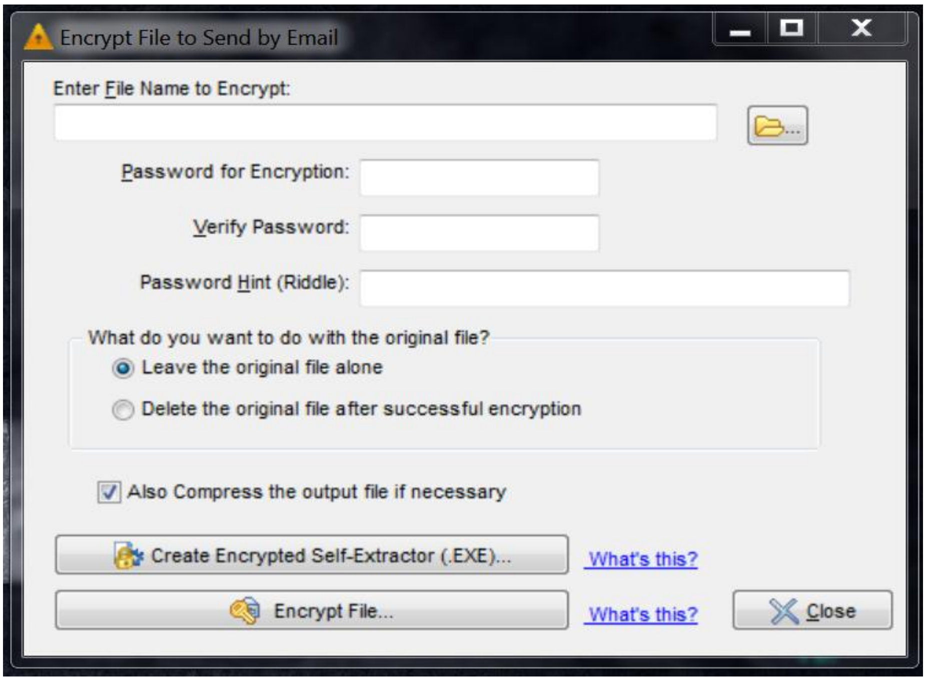
This option is recommended if you want to format this Cryptainer volume with more efficient formats like NTFS with compression.

Click here for more information

Figure 5 Volume creation interface for Cryptainer LE 10

Moreover, the ‘Algorithm’ drop down list provides the end-user with no explanation to what the feature is for, which can be confusing for end-users with little knowledge in cryptography. Lastly, the bottom section of the interface where it presents the end-user the opportunity to format their ‘cryptainer volume’, fails to provide a sufficient explanation on the process. Indeed, the idea of using an NTFS format for the volume may confuse novice end-users with little knowledge in IT. Unfortunately, by not selecting this option, files four gigabytes or larger cannot be stored on the default FAT 32 format, thus the volume’s storage capability is effectively reduced.

The first step to encrypting a file is either clicking on the ‘Secure Email’ option on the main end-user interface, or selecting tools in the menu bar and then on the option ‘Encrypt File to Send by Email…’ Selecting either one will result in the same interface appearing as illustrated in Figure 6. However, the labels for both options and the interface itself are slightly misleading, considering the feature has nothing to do with sending an email, rather just encrypting a file. Additionally, labels such as ‘Encrypt’, ‘Compress’ and ‘Create Encrypted Self-Extractor (EXE)’ may not be interpreted correctly by novice end-users based on their use of technical terms.


Encrypt File to Send by Email
Create Encrypted Self-Extractor (.EXE)...
What's this?
Encrypt File...
What's this?
Close

Enter File Name to Encrypt:

Password for Encryption:

Verify Password:

Password Hint (Riddle):

What do you want to do with the original file?

● Leave the original file alone

○ Delete the original file after successful encryption

☑ Also Compress the output file if necessary

Figure 6 File encryption interface for Cryptainer LE 10

Furthermore, the ‘What’s this?’ help links also suffer from using difficult terminology and providing information that may confuse novice end-users. For example, the links use terms such as ‘self-extractor’ and ‘email module’ that novice end-users may find difficult to interpret. In addition, the second link tells the end-user that selecting the ‘Encrypt File’ option will reduce a file’s size, which may be a deterrent for end-users that believe their file may undergo unwanted and irreversible change. However, despite these issues the encryption process is simple and straight forward. After filling out the relevant information on the interface and selecting the encrypt file button, a dialog box appears stating that the encryption process was successful, along with the newly created files location.

The decryption process is similarly simple and straight forward. However, there is an immediate issue of locating the ‘Decrypt File…’ button hidden under the tools section on the menu bar. Moreover, if the end-user selects ‘Secure Email’ on the main end-user interface, an option to ‘Decrypt a SIT file…’ appears. Unfortunately, novice end-users may avoid this option due to the ambiguity of the term ‘SIT file’. Otherwise, once selected a simple interface appears asking the end-user for the files location, its password and the path to extract the file. After performing the operations, a dialog box appears stating that the decryption process was successful, the location it was decrypted, and if the end-user wants to retain or delete the original encrypted file.

If the end-user decides to only encrypt files on their computer, and have successfully created a volume disk by filling out the information in Figure 5. Then they can simply ‘drag and drop’ a file onto the main end-user interface. Unfortunately, the application fails to specify that ‘dragging and dropping’ a file will in affect copy the original. This means that the file can still be accessed by anyone if not previously removed or deleted. In addition, the end-user is not notified that selecting the close button on the top right hand corner of the main end-user interface, only minimises the application into the system tray. They must select the ‘Shutdown & Exit’ button if they want to ensure their confidential volume is hidden from the computer and can only be accessed by password validation. Consequently, these issues can lead to the misfortunate use of the software and thus potentially put at risk confidential information being accessed by unauthorised parties

Recommended Changes

Several usability issues were identified that may adversely impact an end-user's ability to utilise encryption software. The following list portrays potential solutions that may improve the usability of the software.

1. *Non-technical terminology*: Information presented by security software should be clearly stated in a language that end-users of varying technical competency can interpret correctly (Nielsen, 1994). One of the main issues identified was the use of wording commonly associated within IT and security literature.

2. *Context-sensitive help*: Helpful information should be presented in a readable format without being obtrusive, and relate to the end-users task (Johnston *et al.*, 2003). One of the helpful features in Advanced Encryption was when the end-user selected a text-field a message would appear to give advice. Unfortunately, it was temporary and did not allow sufficient time for it to be read entirely.

3. *Appropriately placed controls*: Controls, especially ones that will be repeatedly used by the majority of end-users, should be clearly displayed on the main end-user interface and made readily available. An issue that was identified in Cryptainer was the decryption button being hidden under the tools section of the menu-bar.

4. *Icons and pictures*: The use of images is an effective way to convey security features on interfaces, especially amongst end-users who are not technically competent (Ibrahim *et al.*, 2010; Johnston *et al.*, 2003). Unfortunately, Advanced Encryption neglected to incorporate any images in its interface design to aid end-users into interpreting the functionality of its controls correctly.

5. *Consequences of actions*: It is essential that security software communicates to end-users that a specific action may result in detrimental consequences (Gujrati & Vasserman, 2013). For example, Cryptainer neglects to notify the end-user that pressing the close button at the top right hand corner of the application only minimises it into the system tray. As a result, confidential information is exposed within the volume disk, unbeknownst to the end-user having believed they successfully closed the application.

6. *Use colours to attract end-user attention*: Colours can help convey the controls of the software more clearly and make them more recognisable to end-users. Ibrahim *et al.*, (2010) states that end-users are most attracted to the use of colours in interfaces. Unfortunately, Cryptainer and Advanced Encryption neglect to incorporate any or very little colour in their respective interfaces, which if implemented, could make their software more appealing and inviting (Arnowitz, Priester, Willems, & Faber, 1997).

CONCLUSION

The increasing dependency on the Internet has replaced traditional means of exchanging sensitive information, and transformed how companies conduct business. In hindsight, it has become essential to ensure information is protected against the vast amounts of threats online and from physical theft. One such means is through the use of encryption software, which is developed to hide information in an unreadable format for unauthorised parties. This paper examined the usability of popular encryption software marketed to the general public and assessed whether novice end-users can properly use them. The methods used for conducting the analysis included a heuristic evaluation and cognitive walkthrough. In addition, a set of established heuristics from various publications were used to help identify any usability issues or problems.

From the findings, several usability issues were identified that could potentially impede on a novice end-user's ability to properly manage the software. These issues included poor interface design, lack of context-sensitive help, confusing controls for first time end-users and, the use of security and technical related terminology. Taking into consideration the underlining deficiencies present, experienced end-users would likely be capable of using the software properly, whilst novice end-users less experienced in security technology will encounter difficulty. In conclusion, this study has identified that to date, there is little research being done in the area of encryption software usability. As a result, further research is needed to better understand the end-users' ability, perceptions and views on the usability of encryption software, and to investigate alternative solutions for improving interface design.

REFERENCES

ABS. (2014). Australian Bureau of Statistics Type of Access Connection. Retrieved from http://www.abs.gov.au/ausstats/abs@.nsf/mf/8153.0/

Agashe, G.., Yu, S., Jaferian, P., & Shamji, F. (2007). Usability study of Vista's firewall using respondent methods. Retrieved from: http://courses.ece.ubc.ca/412/term_project/reports/2007-fall/Usability_study_of_Vista_firewall_using_respondent_methods.pdf

Alfayyadh, B., Ponting, J., Alzomai, M., & Josang, A. (2010). Vulnerabilities in personal firewalls caused by poor security usability. *Information Theory and Information Security (ICITIS), 2010 IEEE International Conference*.

Arjmandi, P., Boeck, R., Raja, F., & Viswanathan, G. (2007). Usability of Windows Vista Firewall: A Laboratory User Study. *EECE 412 Term Pape*r. Retrieved from: http://lersse-dl.ece.ubc.ca/record/172/files/172.pdf

Arnowitz, J. S., Priester, R., Willems, E., & Faber, L. (1997). Mahler, Mondriaan, and Bauhaus: using artistic ideas to improve application usability. In *Proceedings of the 2nd conference on Designing interactive systems: processes, practices, methods, and techniques* (pp. 13-21). ACM.

Australian Bureau of Statistics (ABS). (2012) *Internet Activity, Australia, December 2012* (Cat. No. 8153.0). Retrieved from: http://www.abs.gov.au

Carlsen, J. (2014). 2014 Encryption Software Product Comparisons. Retrieved from: http://encryption-software-review.toptenreviews.com/

Cole, E. (2013). Chapter 6 - Prevention is Ideal but Detection is a Must. *Advanced Persistent Threat.* Boston, Syngress, 123-144.

Furnell, S. M., Jusoh, A., & Katsabas, D. (2006). The challenges of understanding and using security: A survey of end-users. *Computers & Security*, *25*(1), 27-35.

Furnell, S. (2010). Usability versus complexity–striking the balance in end-user security. *Network Security, 2010*(12), 13-17.

Horizon Blue Cross Blue Shield of New Jersey Notifies Members, Offers Protection Following Office Theft. (2013). Horizon Blue. Retrieved from: http://www.horizonblue.com/about-us/news-overview/company-news/horizon-bcbsnj-notifies-members

Ibrahim, T., Furnell, S.M., Papadaki, M., & Clarke, N. L. (2010). Assessing the Usability of End-User Security Software. *Trust, Privacy and Security in Digital Business*. Springer Berlin Heidelberg. *6264*, 177-189.

Johnston, J., Eloff, J. H., & Labuschagne, L. (2003). Security and human computer interfaces. *Computers & Security*, *22*(8), 675-684.

Mani, D., Choo, K.-K. R., & Mubarak, S. (2014). Information Security in the South Australian Real Estate Industry: A Study of 40 Real Estate Organisations. *Information Management & Computer Security*, *22*(1), 24-41.

NBNCo. (2014). *Rollout FAQs.* Retrieved from: http://www.nbnco.com.au/when-do-i-get-it/about-the-rollout/faq.html

Nielsen, J. (1994). Heuristic evaluation. In J. Nielsen, & R. L., Mack (Eds.), *Usability Inspection Methods*. New York, NY: John Wiley & Sons

Gujrati, S., & Vasserman, E. Y. (2013). The usability of Truecrypt, or how I learned to stop whining and fix an interface. Paper presented at the Third ACM conference on data and application security and privacy Hyatt Regency, San Antonio, Texas.

Senft, D. J. (2013). Mobile devices: Technology aid—security risk. *Geriatric Nursing*, *34*(2), 149-150.

Shiaelesa, S., Chryssanthoub, A., & Katosa, V. (2013). On-scene triage open source forensic tool chests: Are they effective? Digital Investigation, 10(2), 99-115.

StatCounter GlobalStats.(2013). *Top 7 Operating systems in Australia* on Feb 2013. Retrieved from: http://gs.statcounter.com/#os-AU-monthly-201302-201302-bar

Szewczyk, P. (2012). An Australian Perspective on the challenges For computer and network Security for novice end-users. *Journal of Digital Forensics, Security & Law*, *7*(4). 17-30

Symantec Corporation. (2014). *Internet Security Threat Report 2014*. *19*. Retrieved from: http://www.symantec.com/content/en/us/enterprise/other_resources/b-istr_main_report_v19_21291018.en-us.pdf

Trochim, W. M. K. (2001). *Research methods knowledge base* (2nd ed). Cincinnati, OH: Atomic Dog Publishing.

Turner, M. (2011). European national news. *Computer Law & Security Review*, *27*(1), 92-97.

Wall, D. S. (2013). Enemies within: Redefining the insider threat in organizational security policy. *Security Journal*, *26*(2), 107-124.

Wharton, C., Rieman, J., Lewis, C., & Poison, P. (1994). The cognitive walkthrough method: A practitioner's guide. In Nielsen, J., and Mack, RL (Ed.), *Usability Inspection Methods* (pp. 105–140). New York, NY: John Wiley & Sons

Whitten, A., & Tygar, J. D. (1999). Why Johnny can’t encrypt: A usability evaluation of PGP 5.0. *In Proceedings of the 8th USENIX Security Symposium,* McGraw-Hill*, 99*. Retrieved from: www.cs.berkeley.edu/~tygar/papers/Why_Johnny_Cant_Encrypt/OReilly.pdf