Just Make it Invisible to the User? A Case Study of Invisible Flash Drive Encryption

Jens Christian Opdenbusch, Konstantin Fischer, Jan Magnus Nold, M. Angela Sasse
Ruhr University Bochum

Abstract

USB Flash drives are used in high-security contexts when networks are strongly separated. We conduct a task observation and interview study (n=14) to investigate problems users might face when a company deploys flash drive encryption software that is almost completely invisible to the user. We find a strong disparity between participants' knowledge of the flash drive encryption during the interviews and the observation of them interacting with it.

1 Introduction

USB Flash drives are, to this day, used in companies to transfer data between devices and machines. This is especially relevant in high-security environments with strongly separated networks.

In this study, we investigate possible pitfalls of enterprise flash drive encryption software in a high-security corporate environment that users have to interact with when copying files to others that do not use the same software. With the software enabled, files are invisibly (i.e., not visible to the user and without interaction of the user) encrypted when written to a removable flash drive, and invisibly decrypted when read from a flash drive, using a key shared across all authorized company laptops. This protects company data on lost or stolen USB flash drives.

Within the usable security research community, it is generally accepted that security should not get in the user's way and be automated where possible (e.g. [1, 4, 6]), however, studies such as Ruoti et al. [9] have shown, that too much invisibility can lead to users not noticing that e.g. encryption is even happening – which we also observed.

Research Goal Our objective was to identify any challenges end-users may face when utilizing invisible flash drive encryption software, and gauge their understanding of the limitations associated with such a system. This led to the following two research questions:

RQ1: Which problems do end-users encounter when (unknowingly) using the flash drive encryption?

RQ2: Do the employees know about the limitations imposed by the automatic flash drive encryption?

Approach We observed n = 14 participants carrying out a covert task. During this observation, we asked questions on why the participants were doing what they were doing – similar to the concept of contextual inquiry [3]. After the task observation, we conducted semi-structured interviews.

Findings I) We find a strong disparity between latent and situation-dependent knowledge of the system within our participants. While almost everyone failed the covert task, everyone knew during the semi-structured interviews how they would have succeeded in theory.

II) The invisibility of the investigated system's design is competing with Nielsen's first heuristic for usability [8]: "The design should always keep users informed about what is going on, through appropriate feedback within a reasonable amount of time."

2 Methodology

To inform our user study design, we first conducted a cognitive walkthrough [5] of different tasks a user might face, using a demo version of the software provided by the manufacturer. We identified use cases, where the almost entirely invisible encryption tool *does* require user interaction and user awareness. This guided our study design, consisting of I) a covert task observation including a debriefing, and II) a semi-structured interview.

Recruitment After two rounds of piloting, we worked with the company's information security specialist to recruit employees who had used the interface encryption software. Employees were asked whether they wanted to participate in

a voluntary information-security-related study. Only if they were interested and willing to participate did they receive an invite. This recruitment yielded 14 participants, distributed over two locations of the company.

Task Observation We aimed to collect qualitative data about the usage of flash drive encryption and whether the participants were aware of it in an everyday setting. To measure awareness, we could not directly ask the participants to engage with the encryption software. Thus, we used a covert approach by artificially constructing a problem and asking the participant for help: Participants were asked to fill out a demographics questionnaire on a clearly labeled company laptop and then share the questionnaire with the researcher via a USB flash drive. To achieve this, the participants had to remember the existence of the encryption software and interact with it to disable the automatic encryption before copying the data. Otherwise, the researcher would not be able to read the transferred data. While the participant tried to copy the questionnaire, the researcher let the participant explain what they were doing. This resulted in the participant taking the role of a teacher while the researcher took the role of an apprentice wanting to learn how the system works, as intended by Beyer and Holtzblatt in their definition of *contextual inquiry* [3].

Interviews After the covert task observation, we debriefed our participants, explaining the true purpose of the study. The covert task debriefing was followed by a semi-structured interview to learn about previous experiences with the encryption software. The interview guide targeted usage patterns and any difficult encounters the participant had with the encryption software.

Analysis R1 coded all interviews using the constant comparative method [2] using MAXQDA [7].

Ethics We followed the Menlo Report of security research [10] and found the re-identification of the participants as a significant risk that we needed to address. The research plan was disclosed to the company's works council to ensure that neither the researchers, nor the company could re-identify the participants and no harm would be caused to the participants during the study. Additionally, two works council members volunteered for the second round of piloting and thus experienced the study first-hand before everyone agreed to continue with recruiting. All participants received a consent form that informed them about their rights. Prior to the task observation, they were asked for their agreement to indicate the start of the study. All participants gave their agreement. While recording the interviews, some participants said that *they would like to state something off the record*. We removed those statements from the analysis.

3 Key Results

3 out of 14 participants mentioned that the copying of the data would result in encrypted data on the flash drive before copying the data. The other 11 participants knew after the data transfer happened and the researcher was unable to open the files that they must have been encrypted by the software installed. To transfer the data, a special USB token is necessary to disable the flash drive encryption before copying the data. 8 participants knew about these tokens but did not own one themselves. Only team leaders and administrators had tokens to disable the encryption software temporarily. The process of getting authorization to disable the software and someone coming by and temporarily disabling the encryption software was brought up as very time-consuming, while one participant reported that they are in need of such token "almost daily".

Knowing that they need the token is already saving employees a lot of time compared to copying the data without remembering the encryption software. Every participant forgot to disable the encryption at least once in their work life, while 11 participants had the data intended for someone else. For three participants, this was also how they learned about the existence of such software on their company laptops. Scenarios in which our participants forgot about the encryption software ranged from internal data transfers on systems that were not using the encryption to data intended for a customer that could not be shared due to the encryption.

During the interviews, participants described when and why they needed to disable the flash drive encryption. The only visible clue the encryption software offers is a small indicator on the file icon of an encrypted file that is only visible if the view option of (large) file icons within Windows Explorer is set (see Figure 1), and the encryption software is installed. Participants reported overlooking this indicator in practice. When the encryption software is not installed, the file has a different file extension. This extension was mentioned by one participant who is always checking on a second computer (that does not have the encryption software installed) whether they can open files copied onto flash drives.

4 Discussion

Invisibility removes user interaction, which is desirable when no interaction is needed. However, invisibility can be harmful when awareness of restrictions imposed by a security tool is necessary, especially if they have to be remembered before carrying out the primary task a user tries to achieve. This system behaviour competes with the visibility of the current status of files, similar to the first heuristic of Nielsen [8] that states that such status should always be made visible. This was especially apparent after conducting the interviews: Our participants were able to explain the necessary restrictions the flash drive encryption imposes when asked directly, which they did not remember when completing the covert task.

Acknowledgments

We thank the manufacturer of the encryption software for providing us the software which allowed us to conduct our cognitive walkthrough. We also thank the company and the employees who collaborated with us. Additionally we thank Ayana Welskopf for assisting in the Poster-creation. This work has been funded by the Deutsche Forschungsgemeinschaft (DFG, German Research Foundation) under Germany's Excellence Strategy - EXC 2092 CASA - 390781972.

Appendix

File Icons The encryption-indicating icon shown on top of the PDF file icon in Figure 1 has been changed to avoid identification of the encryption software, as the manufacturer wants to remain anonymous.

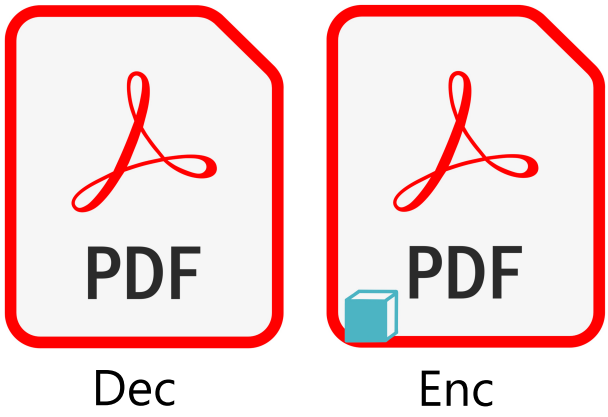

Figure 1: A visualization of the easy-to-miss icon the encryption is placing on the file icon of an encrypted file (right) in comparison to a non-encrypted file (left). This additional, encryption indicating icon is only visible on devices that have the investigated encryption software installed.

References

[1] Erinn Atwater, Cecylia Bocovich, Urs Hengartner, Ed Lank, and Ian Goldberg. Leading johnny to water: Designing for usability and trust. In *Eleventh Symposium On Usable Privacy and Security (SOUPS 2015)*, pages 69–88, 2015.

[2] Barney G Glaser. The constant comparative method of qualitative analysis. *Social problems*, 12(4):436–445, 1965.

[3] KAREN Holtzblatt and H Beyer. Contextual design: Defining customer-centered systems. *San Francisco, CA: Morgan Keufmann*, 1998.

[4] Osama Ahmed Khashan and Abdullah Mohd Zin. An efficient adaptive of transparent spatial digital image encryption. *Procedia technology*, 11:288–297, 2013.

[5] Clayton Lewis and Cathleen Wharton. Cognitive walkthroughs. In *Handbook of human-computer interaction*, pages 717–732. Elsevier, 1997.

[6] Enrico Magli, Marco Grangetto, and Gabriella Olmo. Transparent encryption techniques for h. 264/avc and h. 264/svc compressed video. *Signal Processing*, 91(5):1103–1114, 2011.

[7] MAXQDA - Distribution by VERBI GmbH. MAXQDA. https://maxqda.com, accessed July 10, 2024.

[8] Jakob Nielsen. 10 Heuristics, 1994. http://www.nngroup.com/articles/ten-usability-heuristics/, accessed July 10, 2024.

[9] Scott Ruoti, Nathan Kim, Ben Burgon, Timothy Van Der Horst, and Kent Seamons. Confused johnny: when automatic encryption leads to confusion and mistakes. In *Proceedings of the Ninth Symposium on Usable Privacy and Security*, pages 1–12, 2013.

[10] U.S. Department of Homeland Security. The Menlo Report: Ethical Principles Guiding Information and Communication Technology Research, August 2012.