ASH1925028M

by Iftekhar Efat

Submission date: 13-Mar-2022 03:25AM (UTC-0400)
Submission ID: 1782958845
File name: ASH1925028M.pdf (208.22K)
Word count: 2265
Character count: 12470

Impacts of data quality, safety, and encryption

Md Rayhan Billah
ASH1925028M

March 13, 2022

Report submitted for **SE2206: Information Security** under BSc. in Software Engineering Program, Institute of Information Technology (IIT), Noakhali Science and Technology University

Project Area: **Information Security .....**
Project Supervisor: **MD. IFTEKHARUL ALAM EFAT**
Assistant Professor
Institute of Information Technology (IIT)
Noakhali Science and Technology University

Abstract

Data is an important asset used for a variety of organizational activities. Bad data quality can have a detrimental effect on the security of information systems organizations. we will identify dimensions of data quality by using semiotics as a theoretical basis. We argue that the nature and scope of data quality dimensions change as we move between different semiotic levels. An understanding of these changes is essential for ensuring information system security.

Encryption alone is not enough to protect important business data; it should be used in conjunction with other tools such as data loss prevention, mobile application management, and access management to provide adequate critical data protection. In this report, we will consider each of them .

1 Introduction

Organizations' information security has evolved into a vital business process. It is concerned not just with computer systems, but also with the environment in which data is generated and processed. IS security can be seen from a variety of perspectives. In terms of reducing the dangers posed by inconsistencies and incoherence, conduct concerning the operations of information handling organizations.

There are several encryption tools that may be used to protect data in file sharing, emails, and other endpoints (such as mobile devices or laptops.) Some businesses encrypt the whole hard drive of all their mobile devices, while others encrypt all of their emails.

Encryption has no bounds, but it does have consequences. Businesses should encrypt data until the odds of integrity/confidentiality tampering are as low as possible. However, this may have a minor impact on the target systems' performance, slowing them down in some situations. However, the benefits to business and data security frequently outweigh the disadvantages. [2]

2 Background

Most mobile communication, such as short messaging services or messaging apps, did not offer end-to-end encryption prior to 2016. iMessage was one of the most popular exceptions. It did, however, lack a user interface for key authentication, making it vulnerable to man-in-the-middle assaults. It also didn't make any security features public. Authenticated end-to-end message encryption became available to the people with WhatsApp's implementation of the Signal protocol as its default . When a new discussion is established, WhatsApp alerts users that their communications are end-to-end encrypted and offers an optional authentication process based on rapid response codes or key fingerprints.

Despite the fact that various cryptography protocols such as OpenPGP, off-the-record messaging, and Tor have been around for decades [8, 5, 2], they have all failed to gain widespread adoption due to usability issues such as key management and key authentication, as well as sometimes unreliable message delivery. End users struggle with security technologies for email encryption, according to previous

research. Usability issues are still blamed for encryption solutions' shortcomings, according to popular belief. However, we believe that even when security solutions provide high usability, perceptions and mental model concerns may continue to be an impediment. The introduction of a very usable end-to-end encryption system provides an excellent chance to investigate this topic.

Because the goal of our research was to discover factors that would aid messenger developers in developing useable and safe software, it was critical to understand how individuals imagine the process of sending and receiving mobile messages. We evaluated two options.

Text messages and WhatsApp are the two most common techniques. Rather than focusing on technical minutiae, we wanted to see if the overall result was satisfactory. Users are able to grasp high-level concepts and, more crucially, they are able to communicate effectively. the consequences of encryption. We addressed the transformation of users' mental models after the introduction of mass messenger encryption in the first section of our study, which began before the broad deployment of end-to-end encryption services. The following are some of our significant findings:

1. Users do not trust encryption
2. Users lack awareness
3. SMS is more secure than WhatsApp
4. Users do not feel targeted
5. Study participation raises awareness and attention

[1]

3 Methods

We conducted semi-structured interviews with 22 individuals from Germany to learn about their perceptions on mobile communication. We conducted our interviews before and after WhatsApp implemented end-to-end encryption to see how end users' mental models changed. In July and August 2015, 11 people took part in pre-mass messenger encryption (pre-MME) interviews. In January and February 2017, 11 new invited participants and 4 re-invited people participated in post-mass messenger encryption (post-MME) interviews.

Our research aimed to shed light on the following characteristics of users' attitudes toward encrypted messaging:

1. **Understanding of the architecture:** how users imagine mobile communication works and whether they distinguish between SMS and instant messaging.
2. **Threat model:** who users assume is able to eavesdrop and whether there are ways to prevent it.
3. **Understanding of encryption:** how do users imagine encryption and authentication and whether they understand the implications.

4. **Impact of end-to-end encryption:** change in users' understanding of mobile communication after WhatsApp's introduction of end-to-end encryption (post-MME).

3.1 Interview Guideline Design

Designing an interview guideline that covers all of the relevant subjects is a key difficulty when conducting semi-structured interviews to capture users' understandings and mental models. Previous research in this area has either used more open-ended questions with a substantial unstructured portion, or polished their interviews using pre-studies. We used focus groups to iteratively construct a guideline for individual interviews to improve this procedure. Focus groups are an authorized methodology for collecting qualitative data in psychological investigations that has a long history of use.

3.2 Focus Groups

In 2015, we ran three iterations of focus groups [27]. We employed the theoretical sampling approach for participant recruitment. Our university was the site of the first focus group. Participants who were on campus were invited by two student assistants. We recruited students with non-technical degrees from other universities and older persons with less academic backgrounds for the second and third focus groups to add additional diversity. Snacks and refreshments were provided to everyone who participated. Using a carefully established semi-structured guideline, a single, competent researcher led and supervised the focus group conversations.

3.3 Individual Interview Participants

We found participants for the individual interviews by posting ads on eBay . We also asked the 2015 participants if they would like to participate in our research again in 2017. Those that were interested were invited to our university for individual interviews. The cost of participating in the interviews was 15 euros. Appendix has a table displaying the demographics of the participants.

3.4 Ethics

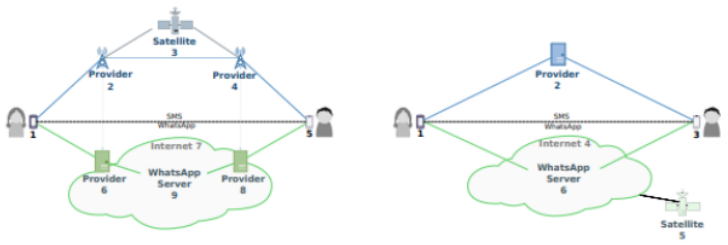
Our study did not require an IRB approval because it was conducted in Germany. Our research, on the other hand, adheres to the strict German privacy laws. We asked participants if they would be willing to be contacted again after the end of the first research. The contact information was kept separate. The information was collected anonymously, and participants were notified that they could withdraw their information at any time during or after the study.

4 Results

Several participants expressed concerns about WhatsApp's security, but they did not switch to secure messengers because all of their contacts continued to use WhatsApp. Nonetheless, the participants responded that they would use encrypted messaging apps if more of their connections and other people did. When it came to preventing eavesdropping, all of the groups mentioned encryption.

Some people feared that even encryption couldn't keep their messages safe. The second and third groups, in particular, revealed that the majority of users were unfamiliar with public-key cryptography. Passwords and symmetric encryption were the only concepts they could think of. A personal encounter or revealing a secret, according to the participants, should be part of the crucial exchange. The fact that cell numbers are linked to WhatsApp was cited by the second group as an interesting feature.

This type of control seems to be trusted by the second group. The first focus group, on the other hand, stated that this strategy is not at all reliable. By going through a simplified scenario with Alice, Bob, and Eve, the third focus group became aware of the possible threat posed by man-in-the-middle assaults. This suggests that people are capable of understanding risks without exerting effort, but they were unaware of the threat until it was pointed up to them.



(a) Before End-To-End Security (b) After End-To-End Security

Importantly, the NSA and governments were named as potential adversaries in every focus group. Obviously, most of the participants were aware of the NSA spying incident and recognized that their communications might be readily intercepted by other parties, including the US government. This finding demonstrates that news and stories have an impact on mental models.

[3]

5 Conclusion

This paper's major purpose was to capture and compare end-user mental models of message encryption. As a result, we did a two-part qualitative research project Pre- and post-MME portions, each having 11 participants. Although More than nine years ago, WhatsApp enabled end-to-end encryption. Many subjects were still alive months before our post-MME study. were unaware of it, and very minimal alterations had occurred in their mental representations. Our findings reveal that, despite the fact that The threat model was almost perfectly described by users. They don't think there's any way to achieve it technically. Defend yourself against the onslaught.

More crucially, misunderstandings regarding cryptography have resulted in a broad lack of trust in encryption. Participants said they felt insecure and assumed they couldn't defend themselves against assailants. We give recommendations for how the community might address these concerns based on our results.

Notes: All works should have a conclusion. Briefly summarise your report (once again). Discuss the most important features of what you have achieved, and the implications of your results. The conclusion should not introduce new information or ideas, however, if you feel it is appropriate, you may speculate on directions for future work.

Acknowledgements

This research is conducted in direct supervision of the Software Evaluation and Re-Engineering Research (SERER) Lab.

Notes: It is common that you will want to acknowledge the contribution of others to your work, even though these might not have been sufficient to warrant being a co-author.

Consider who might have provided valuable discussions, funding support, or moral support for the work.

BTW, you don't have to start each section on a new page. I have done that here for clarity, but it isn't usually needed.

A Appendices

This is a short appendix, just included as an example.

Notes: An appendix can be used to include material that is important, but not needed in the main body of the text, and which it might detract from the main point of the report.

A common example is code. You should not include code in the main body of a report unless it is particularly important or revealing.

However, for the convenience of your supervisors who may wish to examine the code, and for your own benefit (in having a self-contained document), you may wish to include the code in an appendix. If so, have a look at the `listings` package for LaTeX. For Matlab, there is also a `matlab-prettifier` package that may work more easily for you.

References

[1] Sergej Dechand, Alena Naiakshina, Anastasia Danilova, and Matthew Smith. In encryption we don't trust: The effect of end-to-end encryption to the masses on user perception. In *2019 IEEE European Symposium on Security and Privacy (EuroS&P)*, pages 401–415. IEEE, 2019.

[2] Nuno Laranjeiro, Seyma Nur Soydemir, and Jorge Bernardino. A survey on data quality: classifying poor data. In *2015 IEEE 21st Pacific rim international symposium on dependable computing (PRDC)*, pages 179–188. IEEE, 2015.

[3] Gurvirender Tejay, Gurpreet Dhillon, and Amita Goyal Chin. Data quality dimensions for information systems security: A theoretical exposition. In *Working Conference on Integrity and Internal Control in Information Systems*, pages 21–39. Springer, 2004.

Notes: A critical component of the work is the list of references. We have discussed their use earlier – here I simply make some notes on their presentation.

This is one of the hardest parts to get just right. BibTeX can help a great deal, but you need to put a good deal of care in to make sure that

- the references are in a consistent format;
- all information is correct; and
- the information included is in the correct style for the intended audience.

Details *really* matter in this section. It's easy to lose marks in this section.

ASH1925028M

ORIGINALITY REPORT

52%	27%	27%	12%
SIMILARITY INDEX	INTERNET SOURCES	PUBLICATIONS	STUDENT PAPERS

PRIMARY SOURCES

1	Sergej Dechand, Alena Naiakshina, Anastasia Danilova, Matthew Smith. "In Encryption We Don't Trust: The Effect of End-to-End Encryption to the Masses on User Perception", 2019 IEEE European Symposium on Security and Privacy (EuroS&P), 2019 Publication	22%
2	v1.overleaf.com Internet Source	13%
3	de.overleaf.com Internet Source	7%
4	pdfs.semanticscholar.org Internet Source	3%
5	www.itworldcanada.com Internet Source	2%
6	Submitted to American Public University System Student Paper	1%
7	Submitted to Webster University Student Paper	1%

8	www.bongos.net.au Internet Source	1%
9	www.coursehero.com Internet Source	1%
10	cps-vo.org Internet Source	<1%

Exclude quotes	On	Exclude matches	Off
Exclude bibliography	On		

ASH1925028M

PAGE 1

Proper Noun If this word is a proper noun, you need to capitalize it.

Article Error You may need to use an article before this word. Consider using the article **the**.

PAGE 2

Article Error You may need to use an article before this word. Consider using the article **the**.

Sentence Cap. Remember to capitalize the first word of each sentence.

Missing "," You may need to place a comma after this word.

Missing "," You may need to place a comma after this word.

Missing "?" Remember to use a question mark at the end of a question.

Tone This language may not be appropriate in an essay.

Article Error You may need to remove this article.

Missing "," You may need to place a comma after this word.

PAGE 3

Frag. This sentence may be a fragment or may have incorrect punctuation. Proofread the sentence to be sure that it has correct punctuation and that it has an independent clause with a complete subject and predicate.

Sentence Cap. Remember to capitalize the first word of each sentence.

S/V This subject and verb may not agree. Proofread the sentence to make sure the subject agrees with the verb.

Hyph. You may need to add a hyphen between these two words.

Article Error You may need to remove this article.

PAGE 4

Proper Noun If this word is a proper noun, you need to capitalize it.

P/V You have used the passive voice in this sentence. Depending upon what you wish to emphasize in the sentence, you may want to revise it using the active voice.

Prep. You may be using the wrong preposition.

Article Error You may need to remove this article.

Article Error You may need to remove this article.

PAGE 5

P/V You have used the passive voice in this sentence. Depending upon what you wish to emphasize in the sentence, you may want to revise it using the active voice.

PAGE 6

Confused You have used **were** in this sentence. You may need to use **we're** instead.

Sentence Cap. Remember to capitalize the first word of each sentence.

Missing "?" Remember to use a question mark at the end of a question.

P/V You have used the passive voice in this sentence. Depending upon what you wish to emphasize in the sentence, you may want to revise it using the active voice.

PAGE 7

Prep. You may be using the wrong preposition.

Article Error You may need to remove this article.

Confused You have used **A** in this sentence. You may need to use **an** instead.

Possessive You may need to use an apostrophe to show possession.

PAGE 8