Usable Security and Privacy Exam 2020

SOCIAL MEDIA SECURITY CONCERNS OF USERS

Cüneyt EREM

3277992

August 16th 2020

Rheinische Friedrich-Wilhelms-Universität Bonn
Institute of Computer Science 4

I hereby confirm that I am the sole author of this document, the survey and the R script and did not receive any outside help in creating them.

Rheinische Friedrich-Wilhelms-Universität Bonn
Institute of Computer Science 4

ABSTRACT

In this era, social media has big effects on living and almost everyone has at least one social media around the world. Billions of messages have been sending that protecting security and privacy of the users are especially important. Proving security and privacy for user messages, there are several ways. I examined whether some popular social media applications are secure and keep user's data in private. Many participants are asked questions and conducted a survey to clarify what users think about reliability of the social media applications. Two most popular social media WhatsApp and Telegram are compared for their security level and in which way people are concerned about message encryption and whether it is enough for different users with their backgrounds.

1- INTRODUCTION

The social media applications have been using for more than decades. Two most popular and well-known communication social media applications are WhatsApp and Telegram that they provide people with high usability. People can type message and send photos to each other as well as make video conferences. User only has to phone number and internet, then he/she can easily keep in touch with friends or family. So, it is particularly important to keep message content in safe because everybody share their messages that is one of their ultimate privacy. In many research topics like study on message encryption on Facebook for Jonny2 [1], message encryption has become particularly important. In this paper, encryption security and privacy for WhatsApp and Telegram and thoughts of users on security issues of these apps will be discussed. Section 2 introduces related work like what is done in Jonny2.0. Section 3 discusses initial exploration, Section 4 explains how end-to-end encryption on message systems work, Section 5 enlightens study that how participants think about application encryption and what they think. Final section 6 explains conclusion and future work.

2- RELATED WORK

Jonny papers are related to this issue that in the first paper, usability evaluation of PGP 5.0 was conducted, and they have found that PGP management has some problems in terms of usability and security. In the later paper, they have conducted user test of continuity management and found that problem was on PGP key architecture. In later study, they have solution for this problem that they have used CAAS system for encrypting Facebook messages [1].

3- INITIAL EXPLORATION

In the initial exploration, some online social media applications like WhatsApp have not proceed with end-to-end encryption for messaging for a long time. Even after the method is applied, people have argued whether encryption is applied well, and messages are protected properly or not [4]. In late 2019, WhatsApp is blamed by several people in which it was not secure enough because there were some leaks about protecting message content that it leads app unsecure and threatens people's data privacy [5, 6]. While so many social media applications put this property a few years before, WhatsApp applied this feature too late as such in 2016. Until that day, WhatsApp messages were not secure, and many message contents were not protected properly. According to X, WhatsApp has web malware, unencrypted backups,

Facebook data sharing, Hoaxes and fake news, and WhatsApp status is not private. In contrast, Telegram has always been better security requirements and infrastructure to protect data [7]. Examination study has been conducted on users about their thoughts and how they react these applications.

4- END-TO-END ENCRYPTION ON MESSAGE SYSTEM

End-to-end encryption is one of the common secure communication ways for messaging [2]. Most of time, companies keep encryption key so that they can see message content, however when end-to-end encryption is used, companies do not keep decryption key. For example, Alice uses private key to decrypt Bob's message and Bob uses Alice's public key to encrypt message and then decrypt with private key. During this exchange, third parties cannot read plaintext because they do not have private key.

WhatsApp declares that they provide secure end-to-end encryption method for protecting messages when they are sent, and message contents cannot be read even by company [3]. Each chat has its own security code and only two users can see them and verify by scanning the barcode while using app. Telegram also uses same end-to-end encryption message that no one can see private messages except users.

5- STUDY

From ethics point of view, participants have been informed about question types and data privacy. To avoid any risk of psychological harm, they were informed that they can give up filling the survey at any time and also they are said after the survey, they will be given feedback about social media application security vulnerabilities the did not know.

Password is important for protecting data privacy against other people and it is quite common to use on many different types of accounts. Users are asked which kind of password you would use. According to the results, 90 participants do not want to type password each time when they enter the application. Most common reason is that they already enter password to unlock phone. However, two step verification is an important issue. WhatsApp uses face ID to open the application each time and it is fastest way to verify user. Telegram however does not use any verification system. Therefore, instead of using long passwords, face ID must be used, and users like to use this system.

Social media administrators should care to create better configuration tools to avoid any problem while running app. Certificates should be used and https/TLS communication should be used when people want to use social media on browser. Developers must be careful because protecting user's data is top priority therefore administrators and developers need to be communicated a lot.

For the sake of usability, application must apply Nielsen principles. The applications design is easy to use that they can use app with one hand and simplicity is top priority because it has to only focus on required communication features, easy to remember that there are less but effective properties, has few errors that every update needs to fix problems immediately and each release has to be checked well and has higher satisfaction for each user. For usability testing, System Usability Scale SUS questions have been asked for one of WhatsApp and Telegram.

Evaluation can be done by many parts. Cognitive walkthrough or heuristic evaluation can be considered to find problems of usability by developers without asking users however this research is based on users' ability to see behind the walls. Therefore, evaluation with users is chosen and survey is prepared that asking questions about both WhatsApp and Telegram applications security. In questions, biased questions were avoided by diminishing 'do you like' or 'is it like' questions and objective questions were asked like 'what do you think', 'can you explain' etc. Both open and closed questions are asked as simple as possible. In some points, users are asked for attention questions, some other points, they are asked their own opinions. It requires lees time to examine and give homogenous results.

User test and challenge: WhatsApp and Telegram were tested to see whether they use usability, security and privacy are met with certain aspects by user's perspective. The survey test was conducted by tool Qualtrics that have some certain priorities. When users test the social media apps, they can ask questions they do not understand, and they filled questions and gave answers for each to see what they think exactly without interrupting of any other people or ideas. When they use the WhatsApp and Telegram, 30 of participant did not use one of these apps before so that they have lack of some knowledge and allowed to explore applications themselves. The challenging part is to avoid giving information about security vulnerabilities to the users and at the same time learn about their thoughts and concerns.

Test design: The purpose of assignment clearly stated to the participants or users that what they think about social media, WhatsApp and Telegram and its security issues. Users must answer all questions related to usability, security and privacy of the applications, future developments and their individual thoughts to improve the facilities. Different types of the applications were shown to the participants so that their security concerns were defined a bit more deeply.

Participants: The number of people were 100 and age was between 15 to 80. 30 people were novice users and others were professionally use the app every day. 70 have good collage background that are closely related to computers have a bit knowledge about security aspects.

Hypothesis: Most probably users having less experience about social media have less concerns about security.
Null Hypothesis: users having less experience and higher experience about social media have equally concern about security.
The survey has dependent variables that are usability, security issues on social media applications, time taken in daily usage, satisfaction of usability etc. and independent variables that age of users, educational background, previous knowledge about social media apps etc.

Test Monitor: The participants are asked different types of questions
-The usability of passwords and how much the are careful to use passwords are measured, then which kind of password will be useful for the app is asked
-What they know about end to end encryption and how it works were asked. Then some malwares of WhatsApp and Telegram usage is told and what their thoughts.
-Many other WhatsApp problems were asked, then some similar problems on Telegram are asked

-Then which application is more secure for data privacy and some more deep questions were asked
-SUS questions for usability concerns have been asked
-Some tricky questions especially for attention questions were asked
-some questions were designed to examine whether user have concerns about security events such as Snowden incident and also password usage background to examine whether he/she is careful, and also questions regarding companies' governments are trustful
-Most important part is for examining WhatsApp and Telegram vulnerabilities that there were some leaks and vulnerabilities for time to time, questions were designed to find out how much user trust for security and data privacy and how much he/she has security concerns regarding academic background and application usage history.
-Some questions about WhatsApp and Telegram should have been asked. To avoid fatigue bias, similar questions for both sides have been asked so that if user answer one of them, he/she can also answer with similar manner.

Results: The survey can be found on here. (Also, admin powers were given)
https://usecap.fra1.qualtrics.com/jfe/form/SV_0vwA4IHAfIvbcot
The test questions are well defined and applied to examine whether null hypothesis is true or not. According to fisher test and t test, the hypothesis that 'Most probably users having less experience about social media have less concerns about security' it is one tailed and true that null hypothesis is rejected because tables show that users using less that 6 months and having less educational background people are tent to believe that companies, governments and applications can be trusted and they are reliable secure. However, in some news and papers, it is shown that social media applications sometimes have major problems and vulnerabilities on backup services, web desktop applications, data sharing platforms etc. [5, 6]. If you have enough number of participants such as more than 100, then p value is less than 0.05 and our test becomes immensely powerful. (R script can be seen; plots have not been depicted here because of non-existing data)

6- CONCLUSIONS AND FUTURE WORK

In conclusion, social media applications have some vulnerabilities that should have been fixed some time to time. However, some users who have less knowledge about social media are not genuinely concerning with their data security and privacy as much. In contrast, they do not want to share their message or private data with others especially with their friends and family. It should be improved that security concerns have to be increased and social media end to end encryption on backup services and also web services should be empowered, and data sharing protocols should be regulated.

SOURCES

[1] S. Fahl, M. Harbach, T. Muders, M. Smith, U. Sander: Helping Johnny 2.0 to Encrypt His Facebook Conversations, 2012

[2] The ProtonMail Team: What is end-to-end encryption and how does it work?. https://protonmail.com/blog/what-is-end-to-end-encryption/, 2018

[3] W. Security: End-to-end encryption. https://faq.whatsapp.com/general/security-and-privacy/end-to-end-encryption/, 2020

[4] DataDogHQ: Is WhatsApp really end-to-end encrypted?. https://www.quora.com/Is-WhatsApp-really-end-to-end-encrypted, 2018

[5] U. Verma: WhatsApp still isn't safe: 5 things you must know before using messaging app. https://www.businesstoday.in/technology/top-story/whatsapp-5-things-you-know-using-messaging-app-facebook-malware/story/364647.html, 2019

[6] J. Frew: Is WhatsApp Safe? 5 Security Threats Users need to Know About. https://www.makeuseof.com/tag/4-security-threats-whatsapp-users-need-know/, 2018

[7] T. Team: End-to-end Encryption, Secret Chat. https://core.telegram.org/api/end-to-end, 2020

[8] T. Team: End-to-end Encryption FAQ. https://tsf.telegram.org/manuals/e2ee-simple, 2020