User Understanding and Perspectives on End-to-End Encrypted Instant Messaging Apps

Charlotte S. Rikardsen*, Britta Hale†, Stig F. Mjølsnes†

† NTNU, Dep. of Information Security and Communication Technology, Trondheim

* charlotte.rikardsen@gmail.com

† {britta.hale,sfm}@ntnu.no

Abstract

Instant messaging applications are increasingly claiming to offer end-to-end encryption. Yet actual, user perspectives on the necessity, appropriateness, and desirability of such "secure apps" are poorly understood. This work considers two user surveys on university students, and focusing on both user perspectives and claimed level of security understanding for three secure instant messaging apps – Signal Private Messenger, the Secret Conversation feature of Facebook Messenger, and Crypho. The first survey maps the students' knowledge of secure instant messaging and common usage of these apps, while the second survey takes a closer look at the awareness and practices among those students who have used at least one of the target applications.

Keywords: End-to-end encryption, secure instant messaging, Signal, Secret Conversation for Facebook Messenger, Crypho, Signal protocol, Crypho protocol.

1 Introduction

Mass surveillance of digital communications has become a major privacy concern in our society. End-to-end (E2E) encryption in mobile instant messaging apps provides confidentiality between users, protecting communication against eavesdropping as well as the mass surveillance capabilities of telecom operators and even nation-state actors. Ideally, users should not have to trust any network entity or third party. However, it is not clear that users are aware of the security guarantees of the apps they use, or even if they deem such guarantees to be important. This gap in mapping the user population is especially critical with regards to young generations, who are both technologically aware and will use messaging applications for a far greater proportion of their lifetimes than preceding generations.

To address this issue, we conduct two user surveys, based on a university student populace, about secure instant messaging and applications offering the service. The first survey is intended to map the target group's knowledge on secure instant messaging, while the second survey contains more in-depth questions on the three secure instant messaging applications (Signal Private Messenger, the Secret Conversation feature of Facebook Messenger, and Crypho). From a user's

This paper was presented at the NISK-2017 conference; see http://www.nik.no/.

point of view, the second survey aims to answer the research questions of which application is best and most trustworthy. Both surveys consist of questions with multiple choice options. Our target group is students at Norwegian University of Science and Technology (NTNU) Gløshaugen, which serves as the population basis of these surveys. Samples are drawn from this population, with a sample size of 96 in the first survey and 42 in the second survey. While these sample sizes are relatively small, they are sufficient for the statistical analyses we consider in this paper. Ultimately our results indicate certain trends in user understanding and app usage which are important to the development of security apps – these results are unbiased (for academic purposes only). Furthermore, this work paves the way for future user studies on a larger scale.

Survey 1 goals: are designed to discover the population's awareness on secure instant messaging.
Goal 1.1: Analyse the use of secure messaging apps vs. the desire for privacy.
Goal 1.2: Analyse the use of secure messaging apps vs. the understanding of End-to-End (E2E) encryption.
Goal 1.3: Analyse understanding of message privacy.
Goal 1.4: Analyse if secure applications are uniformly used for to communicate with different groups (friends, family, etc.)
Goal 1.5: Compare the popularity among applications.

Survey 2 goals: have more in-depth questions about three secure instant messaging applications Signal Private Messenger, the Secret Conversation feature of Facebook Messenger, and Crypho. The survey assumes that the population has used at least one of the applications. For simplicity, we refer to the Secret Conversation feature of Facebook Messanger as "Facebook Messanger", but note that the security properties are stronger under this feature.
Goal 2.1: Compare popularity of applications. Is Crypho more popular, being based in Norway? Compare users' preferences in secure instant messaging applications.
Goal 2.2: Analyse users' trust in secure instant messaging applications.
Goal 2.3: Analyse users' app preference with respect to communication with different groups (friends, family, etc.)
Goal 2.4: Analyse the use and trust of the secure messaging apps vs. the understanding of E2E encryption.

In the analyses of the surveys, statistical tests were used to form conclusions about all NTNU students at Gløshaugen – students studying for degrees in technology, science, engineering, etc. The first survey assessed students' knowledge on secure instant messaging, E2E encryption, and mapped their use of secure applications. An interesting result from the first survey is that students care more about others not being able to read all of their messages, than keeping their messages private (Analysis 1.f [Cha]). Although the students do not like others to read all of their messages, few of them actually use a secure instant messaging application several times a day (Analysis 1.d). Approximately half of all NTNU students at Gløshaugen are familiar with the terms "E2E encryption" and "secure instant messaging" (Analyses 1.a and 1.e, respectively).

The analyses of the second survey emphasise that Signal and the Secret Conversation feature of Facebook Messenger were used equally for personal communication with friends (Analysis 2.b). However, Signal was used more

for personal communication with family than the Secret Conversation feature of Facebook Messenger (Analysis 2.h). Where there is insufficient data to draw inferences about the population, we summarize the responses for the sample group. This applies to the use of Crypho and user perspectives on which application is most trustworthy.

For full details on survey questions, responses, and analyses see [Cha].

Outline In the following sections we compare the relevant apps (§2), and address the survey methods and data collection(§3). Using the survey results, we address the analysis goals (§4).

2 Comparison of the Apps

We consider three secure instant messaging apps: Signal Private Messenger (Signal), the Secret Conversation feature of Facebook Messenger, and Crypho [Cha]. These applications claim to offer E2E encryption. They differ on how the private messages are encrypted. Signal and Facebook Messenger encrypt messages using the *Signal protocol* [CGCD$^+$16]. Crypho uses the *Crypho protocol* for E2E encryption of messages [Cry].

"Signal" is the name of both an instant messaging application called *Signal Private Messenger*, and an E2E encryption protocol called *Signal protocol*. Open Whisper Systems invented both the application and the protocol. The Signal application is a successor of the encrypted voice calling application Redphone, and the instant messaging application TextSecure. Redphone and TextSecure were merged into one application and renamed Signal in November 2015 [Opeb, FMB$^+$16]. Signal offers the services text messaging between two users, group chat between several users, voice/video call between two users, and the uploading of attachments for text messaging and group chat.

The Signal protocol has two phases to send alternately encrypted and authenticated messages back and forth [Opea]. The first phase is an initial phase where the first message is the key agreement to find a shared session key between two parties, called the *Extended Triple Diffie-Hellman (X3DH)* key agreement protocol. The second phase is for subsequent messages, and called the *Double Ratchet algorithm*. In this phase, the established session key from the first message is reused. Thus, the session key will update for every message exchange to achieve *forward secrecy*, as performed by the *ratcheting* technique [CGCD$^+$16]. Extensive operations happen in the key agreement for the first message, and it is more efficient to reuse the established session key for later messages. This is why they call the Signal protocol a "two phase" stateful protocol.

The Signal protocol combines the X3DH key agreement protocol followed by the Double Ratchet algorithm. Curve25519 is used for the Triple Diffie–Hellman (3-DH) key agreement handshake with pre-key pairs in the X3DH protocol [CGCD$^+$16, FMB$^+$16]. Messages are encrypted with AES in Cipher Block Chaining (CBC) mode and authenticated using Hash Message Authentication Code–Secure Hash Algorithm 256-bit (HMAC-SHA256). Edwards-curve Digital Signature Algorithms based on Twisted Edwards curves (XEdDSA) is used as digital signature scheme to sign the public pre-key.

Many people have signed up for a Facebook account. Thus, the application that Facebook delivers with message functionality is widely used. Facebook Messenger is

a standalone application that a user can install on her device, as long as she has a Facebook account. As for Signal, Facebook Messenger also uses the Signal protocol for E2E encryption.

Facebook Messenger does not provide E2E encryption by default. Users must initiate E2E encryption by enabling the feature *Secret Conversation* with the intended recipient. The recipient also has to initiate a Secret Conversation back to the initiator. Hence the recipient will not receive the message from the initiator unless the recipient initiates a Secret Conversation back with the initiator. This only applies to the first message exchanged; for subsequent messages the recipient receives the initiator's messages encrypted. If a user changes her device, she again needs to initiate a Secret Conversation with the same recipient. This is consistent for Signal too, since private keys are generated and derived on the device [Fac]. The private keys never leave the device. The Secret Conversation feature of Facebook Messenger are limited to text messaging and the uploading of attachments between two users.

Crypho is an application designed by a Norwegian privately held company building technical solutions for secure and private communication, intended for organizations. More than 70 countries use Crypho, with user groups including financial institutions, journalists, lawyers, governments, software companies, and human rights activists[1]. Transport Layer Security (TLS) is used as a standard encryption on the transport layer for device-server communication, and Crypho uses additional security primitives as well to encrypt messages E2E on the application layer.

The Crypho protocol's goal is to E2E encrypt messages, file shares, group chats, and voice/video calls for a person or an organisation. The Crypho protocol uses encryption algorithms like AES with 256-bit keys in Counter with Cipher Block Chaining-Message Authentication Code (CCM) mode, ElGamal Elliptic Curve Cryptography (ECC), and scrypt to encrypt messages [Cry]. Elliptic Curve Digital Signature Algorithm (ECDSA) is used as the digital signature scheme. A user's private keys are stored *encrypted* on the server. To obtain the encrypted private keys, a user uses a passphrase. The passphrase is never communicated to the server or stored on the user's device. This gives a user the advantage of obtaining her encrypted private keys from the server, decrypt her private keys with the passphrase, and accessing her message history on multiple devices.

Further details on the apps and protocols can be found at [Cha].

3 Survey Method and Data Collection

Both surveys are distributed and shared with students at the Department of Information Security and Communication Technology (IIK) and the Department of Computer Science (IDI) by email. Recruitment also consisted of talking to students in the canteens, at students' offices, in the hallway, association offices, data laboratories, etc.

For the second survey, an additional email distribution was made using the "shared message channel" at NTNU [NTN]. NTNU sent the surveys to 500 students at the Faculty of Information Technology and Electrical Engineering (IE). The

[1] See, e.g. *Enterprise Mobile Chat and File-Sharing with End-to-End Encryption.* Available at https://appadvice.com.

ITEMIZE Hacker Club at IIK was also contacted to review and test the applications, resulting in nine sample points. Survey responses were collected in the period from February 12th to March 30th, 2017.

At NTNU Gløshaugen there are 13164 students [Nor]. Overall, 96 participants (64 males, 32 females) took part in the first online survey using Google Forms[2]. It consisted of 15 questions and lasted about 5 minutes to complete. The participants were a random sample of technical NTNU students at Gløshaugen. There were no requirements for participating in the first survey. One participant was 35-44, 22 participants were 25-34, and the remaining 73 participants were 18-24 years old. Participants are mostly from Norway (87), and the remaining participants are from other countries (9).

Furthermore, the second survey has 42 responses (33 males, 9 females) from students at Gløshaugen. It consisted of 27 questions and lasted about 10 minutes to complete. The participant space for the two surveys may overlap or be disjoint. In the second survey, the population is the same as for the first survey. The second survey is also collected online with Google Forms. This is a combination of a random sample of 33 respondents of the population and 9 ITEMIZE-respondents who tested the applications. All 42 respondents are considered as a random sample of technical NTNU students at Gløshaugen. As a requirement for participation in the second survey, respondents must have used at least one of the three applications.

In the second survey, 27 participants were 18-24 years old, and the remaining 15 participants were 25-34 years old. Participants are mostly from Norway (38), and the remaining participants are from other countries (4).

Survey 1 questions:

1. How often do you use text messaging (on your phone or tablet)?
2. How important is it for you to keep your text messages private?
3. How important is it for you that others can not read all of your text messages?
4. Have you heard about “secure instant messaging”?
5. Do you know what "end-to-end encryption" means?
6. Which of these applications have you heard about?
7. Which of these applications have you ever used?
8. What have you used the application(s) for?
9. How often do you use text messaging with a secure application?

Survey 2 questions:

1. Have you heard about the Secret Conversation feature of Facebook Messenger?
2. Which of these applications are you currently using and how often?
7. I trust the end-to-end security of the application.
9. Signal Private Messenger: What have you used the application for?
10. Signal Private Messenger: What do you like about it?
13. If you use Facebook Messenger, do you usually start a Secret Conversation with the intended recipient?
14. Facebook Messenger + Secret Conversation: What have you used the application for?
15. Facebook Messenger + Secret Conversation: What do you like about it?
17. Crypho: What have you used the application for?
18. Crypho: What do you like about it?

[2]https://www.google.com/forms

20. Which application do you like best?

We omit questions from the second survey for which the number of responses did not provide meaningful data, for example question number 3, etc. The survey questions are designed to use simple language, instead of more well-defined security terminology. In particular, Survey 1 Question 2 and Question 3 will bear strong similarities for an informed reader, but are designed to detect a potential lack of user understanding in the meaning of "message privacy" (confidentiality).

As explained in Appendix A there are conditions that must be satisfied in order to make statistical inferences about the population; these conditions include minimal sample sizes. To analyse the statistical results of both surveys, 1-proportion z-test, 2-proportion z-test, 1-proportion confidence interval, and 2-proportion confidence interval are used. An overview of all statistical test results from both surveys is given in Tables 1 and 2.

Table 1: Overview of analyses from the first survey

Analysis	**Related question(s)**	**Test**	**Result**
1.a)	5	1-prop. z-test	H_1: $p > 0.50$
1.b)	3	1-prop. conf. interval	$0.39 < p < 0.59$
1.c)	1	1-prop. z-test	H_1: $p > 0.60$
1.d)	9	1-prop. z-test	H_1: $p < 0.25$
1.e)	4	1-prop. conf. interval	$0.37 < p < 0.57$
1.f)	2, 3	2-prop. z-test	H_1: $p_1 - p_2 > 0$
1.g)	6	1-prop. z-test	H_1: $p > 0.50$
1.h)	7	1-prop. z-test	Inconclusive[1]. H_0: $p = 0.50$
1.i)	8	2-prop. z-test	H_1: $p_1 - p_2 > 0$

[1]This is not a result. There was insufficient evidence to change the initial assumption H_0.

Table 2: Overview of analyses from the second survey

Analysis	**Related question(s)**	**Test**	**Result**
2.a)	7	1-prop. conf. interval	$0.37 < p < 0.68$
2.b)	9, 14	2-prop. z-test	Inconclusive. H_0: $p_1 - p_2 = 0$
2.c)	9, 14, 17	2-prop. z-test	H_1: $p_1 - p_2 > 0$
2.d)	7	2-prop. z-test	H_1: $p_1 - p_2 > 0$
2.e)	20	2-prop. z-test	Inconclusive. H_0: $p_1 - p_2 = 0$
2.f)	20	2-prop. conf. interval	$-0.03 < p_1 - p_2 < 0.37$
2.g)	1	1-prop. conf. interval	$0.37 < p < 0.68$
2.h)	9, 14	2-prop. z-test	H_1: $p_1 - p_2 > 0$
2.i)	10, 15, 18	2-prop. z-test	H_1: $p_1 - p_2 > 0$[2]
2.j)	15, 18	2-prop. z-test	H_1: $p_1 - p_2 > 0$

[2] H_1 only applies to the comparison of Signal and Crypho. Since the comparison of Signal and Facebook Messenger must continue to assume H_0.

4 Results

Full statistical analyses for quantitatively analysing the survey results can be found at [Cha]. Here we apply the survey analyses to the stated goals in §1. We use a significance level of $\alpha = 0.05$ throughout.

Goal 1.1

Goal 1.1 is linked to Analyses 1.b, 1.c, and 1.d. More than 60% of all NTNU Gløshaugen students use text messaging several times a day (p-value=0.0392), and less than 25% of all NTNU Gløshaugen students use text messaging with a secure application several times a day (p-value=0.0047). Between 39% and 59% of all NTNU students at Gløshaugen think it is important for them that others cannot read all of their text messages (95% confidence level). The percentage of how many students that use a secure messaging application is lower than the percentage that does not like others to read all of their messages. Thus, there is a discrepancy between use of secure messaging and the perceived importance of it.

Goal 1.2

Goal 1.2 is collected in Analyses 1.a, 1.d and 1.e. There is sufficient evidence to believe that more than 50% of all NTNU students at Gløshaugen know what E2E encryption means (p-value=0.0021). While less than 25% of all NTNU students at Gløshaugen use secure instant messaging several times a day (p-value=0.0047, Figure 1). Between 37% and 57% of all NTNU students have heard about secure instant messaging (95% confidence level). As a result, more students are familiar

with the terms “E2E encryption” and “secure instant messaging”, than the students who actually use secure instant messaging several times a day.

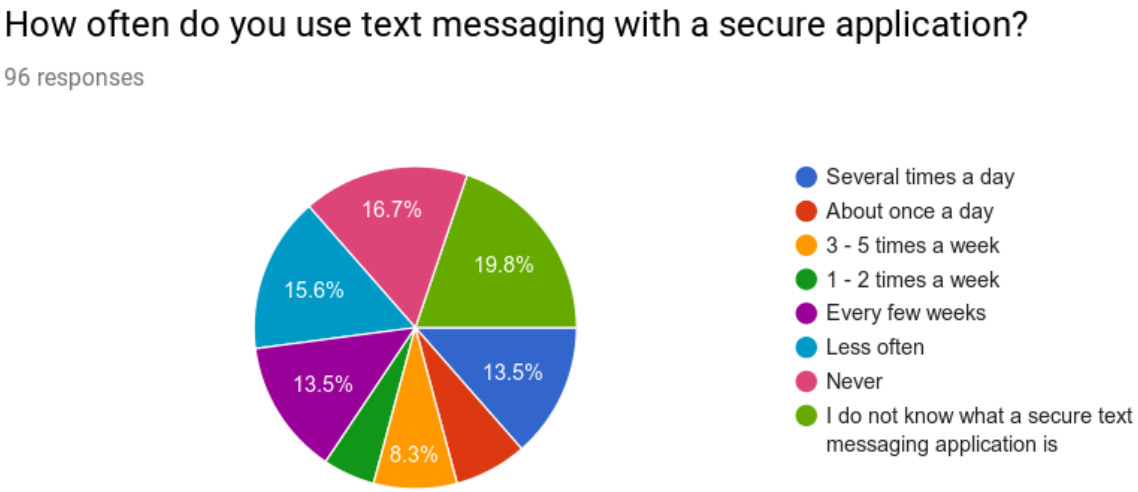

Figure 1: The response distribution from Question 9 from the first survey.

Goal 1.3

Questions 2 and 3 are reasonably similar but formulated differently. A uniform response distribution was expected from Questions 2 to 3, but the result is divergent. Students were not consistent in their answers; many of them changed their answer from Questions 2 to 3 observed in the raw data sample. Therefore, the Analysis 1.f is conducted to compare the observations, and our reasoning is that students are more concerned that others cannot read all of their messages, than keeping their messages private (p-value=0.0495).

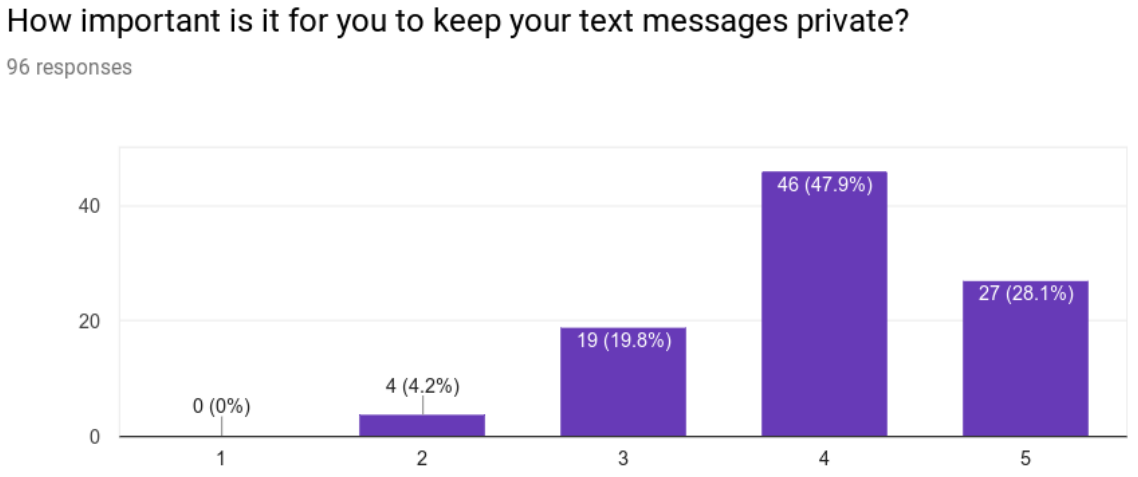

Figure 2: The response distribution on Question 2 from the first survey, where number “1” means “Not important at all”, and “5” means “Extremely important”.

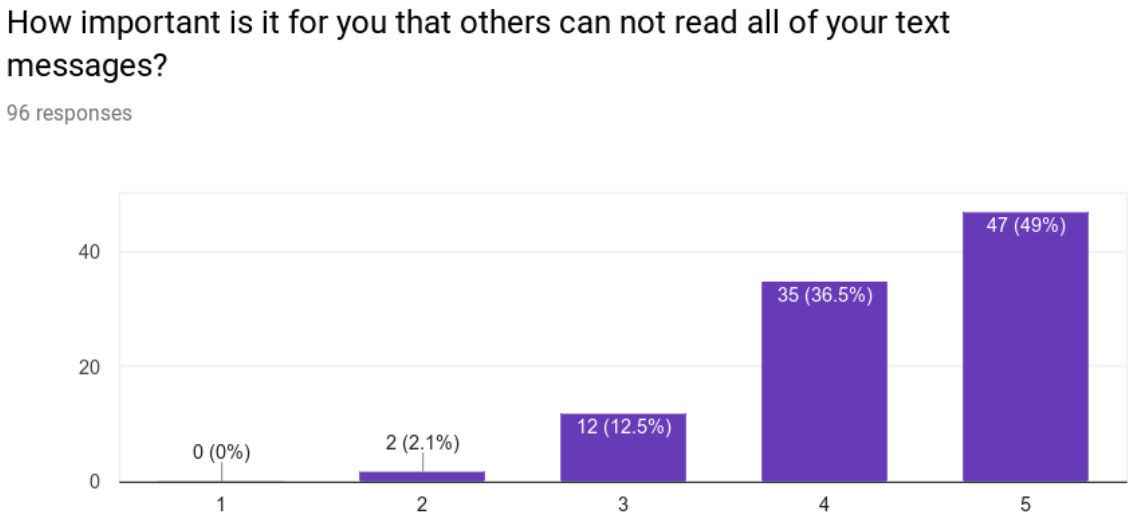

Figure 3: The response distribution on Question 3 from the first survey. Compared to Figure 2 we see the noticeable difference in the response distribution for the alternatives "4" and "5".

Goal 1.4

From the raw data, more students use a secure application with friends than with family. Therefore Analysis 1.i compares if students are communicating more with friends than family with a secure application. From the 2-proportion test in Analysis 1.i, we can assume that more students use a secure application to communicate with their friends than family (p-value=0.0005).

Goal 1.5

In Analysis 1.g over 50% of all NTNU students at Gløshaugen have heard about Hangouts (p-value=0.0021), iMessage (p-value=0), Viber (p-value=0.0122) and WhatsApp (p-value=0). From the sample of students, the three applications considered in the second survey, Signal Private Messenger, Facebook Messenger with Secret Conversation, and Crypho were not among the popular applications.

Goal 2.1

There were insufficient responses to make statistical inferences about the whole population, because the number of responses does not fulfil the conditions required. We can see a trend in survey responses in for example Question 2, none of the sampled students answered that they are using Crypho several times a day (Figure 4).

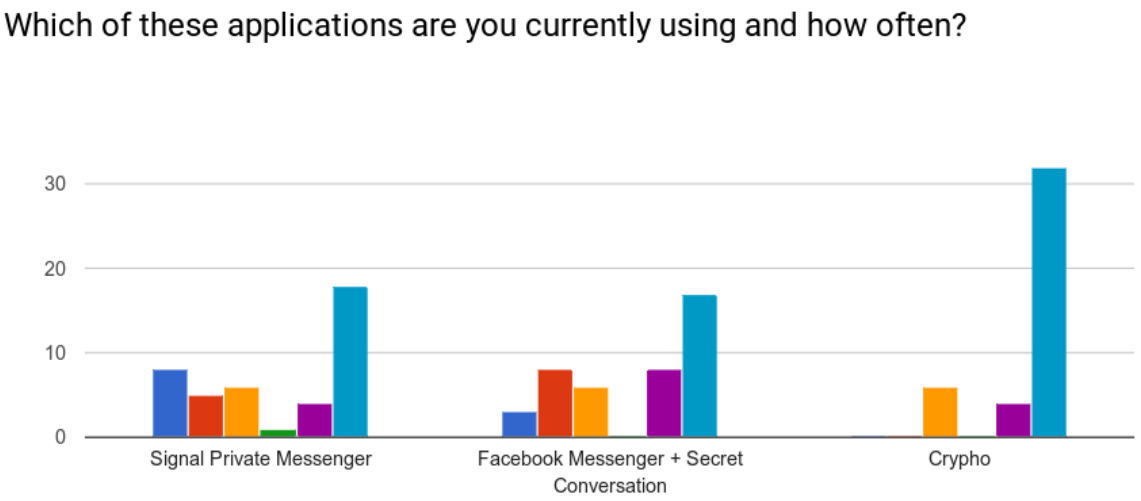

Figure 4: The response distribution on Question 2 from the second survey. App use scales from left to right, where dark blue implies regular app use and purple implies little app use. Light blue corresponds to never using the app.

No tests are conducted for students' use of Crypho, because the response proportion for the population's use of Crypho did not fulfil the statistical test conditions.

One test is possible to perform on Crypho data, which compares if the proportion of students that have never used Crypho is greater than the proportion that have never used Signal or Facebook Messenger. We can assume that the proportion of students that have never used Crypho is greater than the proportion that have never used Signal (p-value=0.0005) or Facebook Messenger (p-value=0.0009), as tested in Analysis 2.c.

We conclude that students like Signal and Facebook Messenger equally (95% confidence level), based on Analysis 2.f. Since 0 is in the interval, it is possible that $p_1 - p_2 = 0$, and there is no difference between the rating of Signal and Facebook Messenger. There were 3 students in the sampled responses that rated Crypho as best, which is an insufficient number of responses to make inferences about the whole population.

The comparison of which application that is the easiest to use (Analyses 2.i and 2.j), shows that all NTNU students at Gløshaugen think Signal (p-value=0) and Facebook Messenger (p-value=0) are easier to use than Crypho.

Goal 2.2

The analysis of students' trust in the E2E encryption of Signal is conducted in Analysis 2.a. Between 37% and 68% of all NTNU students at Gløshaugen trust Signal (95% confidence level). The sample size was insufficient to make statistical inferences about the whole populations' trust of Facebook Messenger's and Crypho's E2E encryption.

In the sample, 22 students trust Signal, and only 9 students trust Facebook Messenger. The raw data shows diverging trends since both Signal and Facebook Messenger use the Signal protocol for E2E encryption. A possible theory is that the sample students do not have knowledge about the E2E encryption protocol behind Signal and Facebook Messenger.

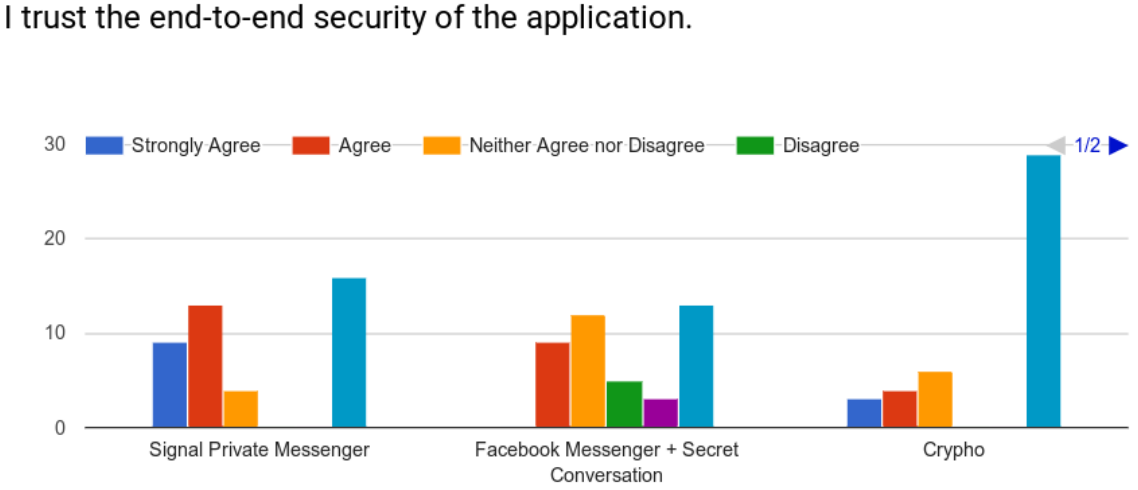

Figure 5: The response distribution on Question 7 from the second survey. App trust scales from left to right, where dark blue implies strongly agree in app trust and purple implies strongly disagree in app trust. Light blue corresponds to never using the app.

Goal 2.3

Analysis 2.h tests if more students use Signal than Facebook Messenger to communicate with their family. There is a sufficient evidence to conclude that all NTNU students at Gløshaugen use Signal more than they use Facebook Messenger to communicate with their family (p-value=0.0281).

Goal 2.4

The piece-wise comparison in Analysis 2.d shows that the proportion of NTNU Gløshaugen students claiming knowledge of E2E encryption is higher than the proportion claiming trust in the E2E encryption of Signal (p-value of 0.0057), Facebook Messenger (p-value=0), and Crypho (p-value=0).

Analysis 2.g covers Question 1, with the result that the proportion of all NTNU students at Gløshaugen that have heard about and used Facebook Messenger with Secret Conversation is between 37% and 68% (95% confidence level). From Question 13, only 3 students in the sample answered that they regularly start a Secret Conversation with the intended recipient when they use Facebook Messenger. Although there were insufficient responses to make inferences about the whole population, we can see a trend in the survey responses that if the sampled students use Facebook Messenger, they are seldom starting a Secret Conversation with the intended recipient.

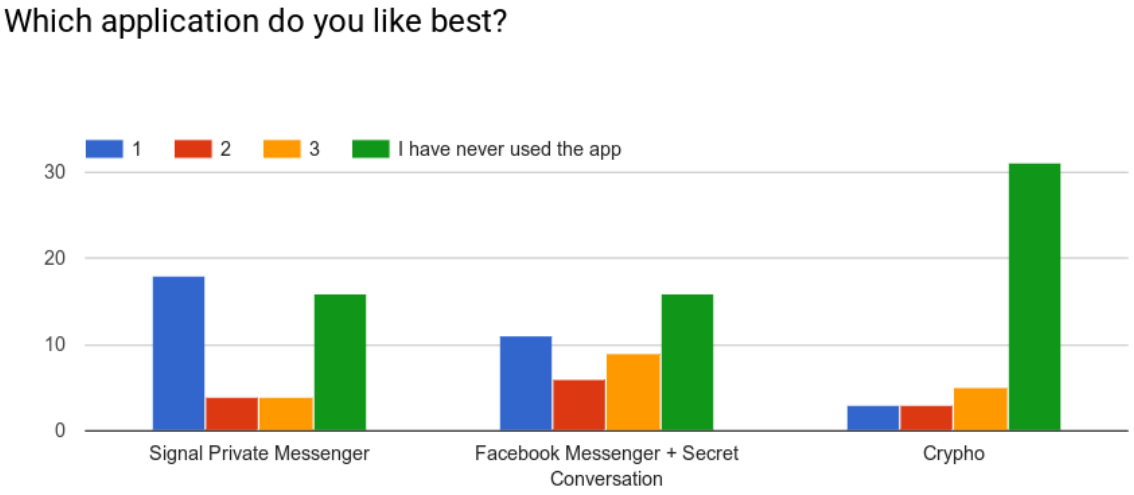

Figure 6: The response distribution on Question 20 from the second survey, where "1" implies first choice, "2" implies second choice, and "3" implies third choice.

5 Conclusion

Ultimately, these results provide an insight into user preferences for secure applications and awareness of E2E encryption. We note that most students appear aware of these terms, and user preference tends toward Signal and Facebook Messenger with Secret Conversations over Crypho, despite the latter being a Norwegian company and hence a "local" company for the surveyed population. Finally, we note that although confidentiality is considered important by many students, far fewer act on that tenet by using secure messaging. App usability, in the context of ISO 9241-11 [usa] extends the analysis questions we address in this work, including efficiency and overall user experience. We leave this for future work.

References

[CGCD+16] Katriel Cohn-Gordon, Cas Cremers, Benjamin Dowling, Luke Garratt, and Douglas Stebila. A Formal Security Analysis of the Signal Messaging Protocol. Technical report, PDF). Cryptology ePrint Archive. International Association for Cryptologic Research (IACR), 2016.

[Cha] Charlotte Rikardsen. Secure Instant Messaging End-to-End Analysis of Security Protocols. NTNU Master's Thesis, June 2017, Not published. Accessed August 22, 2017.

[Cry] Crypho AS. Crypho Security Whitepaper. Available at https://www.crypho.com. Accessed August 5, 2017.

[Fac] Facebook. Messenger Secret Conversations - Technical Whitepaper. Available at https://fbnewsroomus.files.wordpress.com. Accessed August 16, 2017.

[FMB+16] Tilman Frosch, Christian Mainka, Christoph Bader, Florian Bergsma, Jörg Schwenk, and Thorsten Holz. How secure is textsecure? In

IEEE European Symposium on Security and Privacy, EuroS&P 2016, Saarbrücken, Germany, March 21-24, 2016, pages 457–472, 2016.

[Nor] Norsk Senter for Forskningsdata. Database for Statisktikk om Høgre Utdanning - Registerte studenter fordelt på campus. Available at http://dbh.nsd.uib.no/statistikk. Accessed August 19, 2017.

[NTN] NTNU Wiki. Shared message channels. Available at https://innsida.ntnu.no. Accessed August 3, 2017.

[Opea] Open Whisper Systems Blog. Advanced cryptographic ratcheting. Available at https://whispersystems.org/blog/advanced-ratcheting/. Accessed July 6, 2016.

[Opeb] Open Whisper Systems Blog. Free, Worldwide, Encrypted Phone Calls for iPhone. Available at https://whispersystems.org/blog/signal/. Accessed July 2, 2016.

[Ste] Steve L. McMullin. Assumptions/Conditions for Hypothesis Tests and Confidence Intervals. Available at http://www.b-g.k12.ky.us. Accessed July 19, 2017.

[usa] ISO 9241-11:1998. Ergonomic requirements for office work with visual display terminals (VDTs) – Part 11: Guidance on usability. https://www.iso.org. Retrieved 23 Oct. 2017.

A Appendix: Assumptions and Conditions

To analyse the statistical results of both surveys, different tests are performed. Consequently, it is necessary to check if a test can be applied by assuring that certain conditions are fulfilled.

Satisfy Randomness

In order to perform the statistical analysis, both surveys must satisfy a randomness condition. Randomness is defined to be an equal chance of selecting any student of the population. Emails were sent to all students at IIK and IDI, and every student that received the email was equally likely to answer the surveys. Surveys were shared by email for the second time, and NTNU sent emails to 500 randomly selected students at IE. The sample is not representative of all students at Gløshaugen that may affect the results. The sample is considered as sufficiently representative, since NTNU students at Gløshaugen are mainly technical students.

For those students recruited in person on the entire Gløshaugen campus area, each of them was equally likely to answer the surveys. The recruitment is representative of the population, since students were recruited in canteens, students' offices, hallways, association offices, data laboratories etc. from different buildings at Gløshaugen. Willing students received a piece of paper with link to the surveys. Thus, the recruitment is assumed to be a random sample from all students at Gløshaugen.

The ITEMIZE group is a non-random subgroup that could affect the analysis results. However, in the interest of making inferences on the population, they are treated as random with the rest of the sample. They are also technical students at Gløshaugen, and likely to have used the applications like other respondents.

For both surveys this conclusion of randomness will apply to all the tests from here on.

1-Proportion Z-Test

Following conditions are needed for 1-proportion z-test [Ste]:

- The sample of the population must be randomly selected.
- The sample must be less than 10% of the population.
- And the sample size must be large enough:

$$n \cdot p \text{ and } n \cdot (1-p) \geq 10 \text{ for a significance test.}$$

- Calculation of the z-test statistic value:

$$z = \frac{\hat{p} - p}{\sqrt{\frac{p(1-p)}{n}}}$$

2-Proportion Z-Test

Following conditions are needed for 2-proportion z-test [Ste]:

- The two samples must be independent and randomly selected.
- The sample size must be large enough:

$$n_1 \cdot \hat{p_c} \text{ and } n_1 \cdot (1-\hat{p_c}) \geq 5 \text{ and}$$
$$n_2 \cdot \hat{p_c} \text{ and } n_2 \cdot (1-\hat{p_c}) \geq 5 \text{ for a significance test.}$$

- Calculation of the z-test statistic value:

$$z = \frac{\hat{p_1} - \hat{p_2}}{\sqrt{\frac{\hat{p_c}(1-\hat{p_c})}{n_1} + \frac{\hat{p_c}(1-\hat{p_c})}{n_2}}} \quad \text{where } \hat{p_c} = \frac{x_1 + x_2}{n_1 + n_2}$$

1-Proportion Confidence Interval

Conditions to calculate confidence interval [Ste]:

- The sample of the population must be randomly selected.
- The sample must be less than 10% of the population.
- And the sample size must be large enough:

$$n \cdot \hat{p} \text{ and } n(1-\hat{p}) \geq 10 \text{ for a confidence interval.}$$

- Calculation of the confidence interval estimation:

$$\hat{p} \pm z^* \sqrt{\frac{\hat{p}(1-\hat{p})}{n}}$$

2-Proportion Confidence Interval

Following conditions are needed for 2-proportion z-test [Ste]:

- The two samples must be independent and randomly selected.
- The sample size must be large enough:

$$n_1 \cdot \hat{p_1} \text{ and } n_1 \cdot (1-\hat{p_1}) \geq 5 \text{ and}$$
$$n_2 \cdot \hat{p_2} \text{ and } n_2 \cdot (1-\hat{p_2}) \geq 5 \text{ for a confidence interval.}$$

- Calculation of the z-test statistic value:

$$\hat{p_1} - \hat{p_2} \pm z^* \sqrt{\frac{\hat{p_1}(1-\hat{p_1})}{n_1} + \frac{\hat{p_2}(1-\hat{p_2})}{n_2}}$$