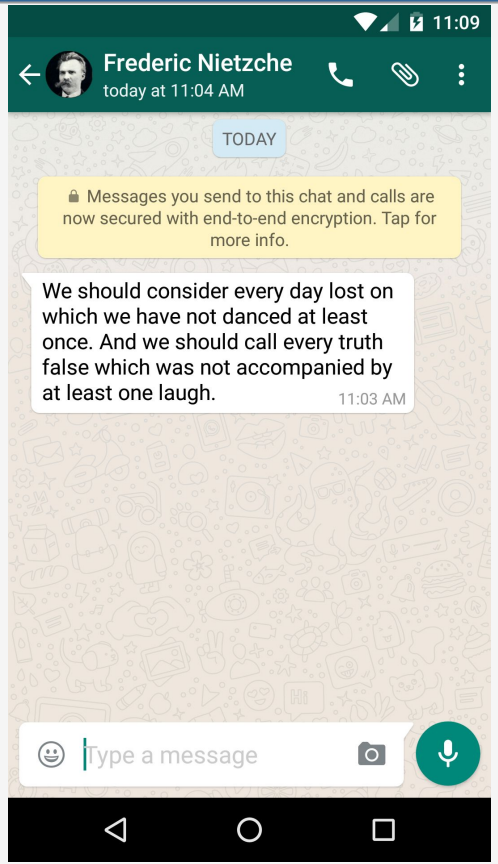
Is that you, Alice?
A Usability Study of the Authentication Ceremony of Secure Messaging Applications

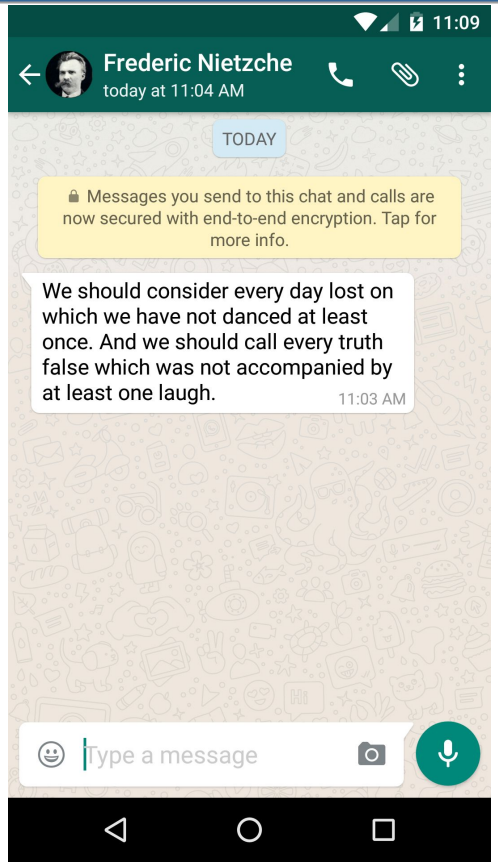
Elham Vaziripour, Justin Wu, Mark O'Neill, Ray Clinton, Jordan Whitehead, Scott Heidbrink, Kent Seamons, Daniel Zappala

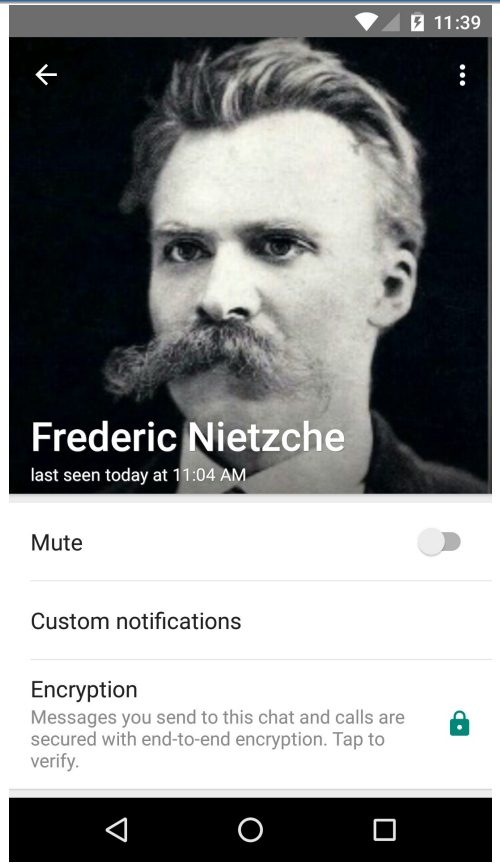
Brigham Young University

Why the Authentication Ceremony is Important

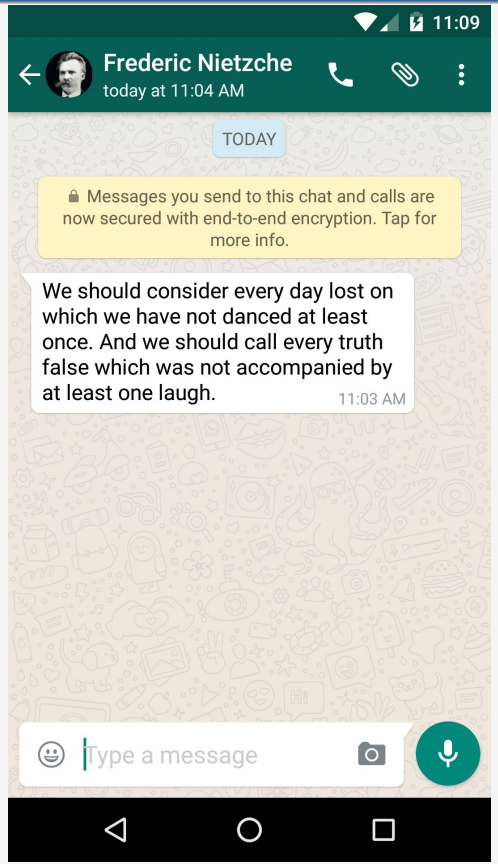


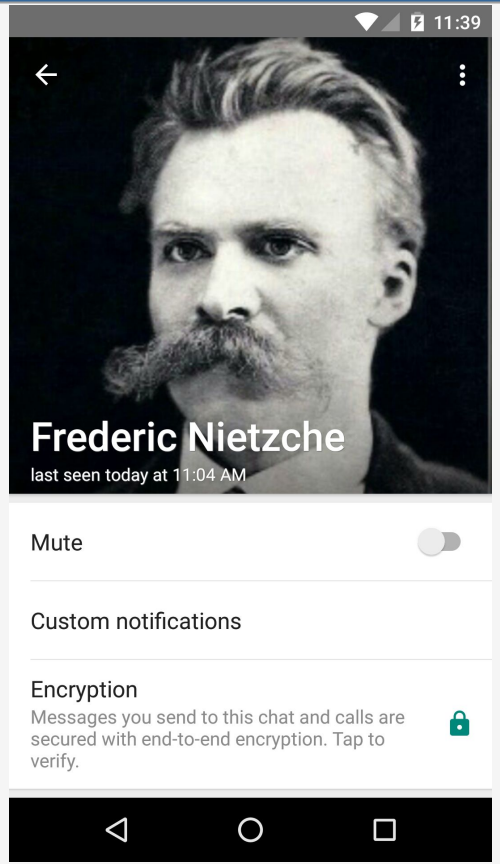
Why the Authentication Ceremony is Important

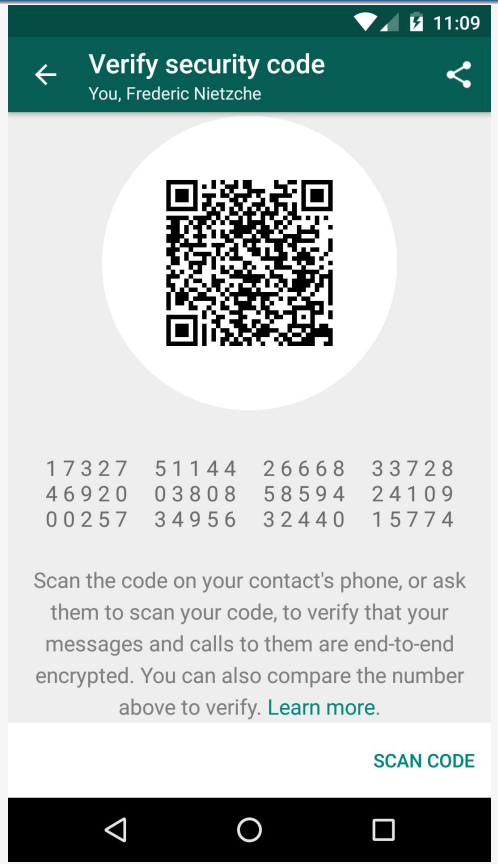




Why the Authentication Ceremony is Important





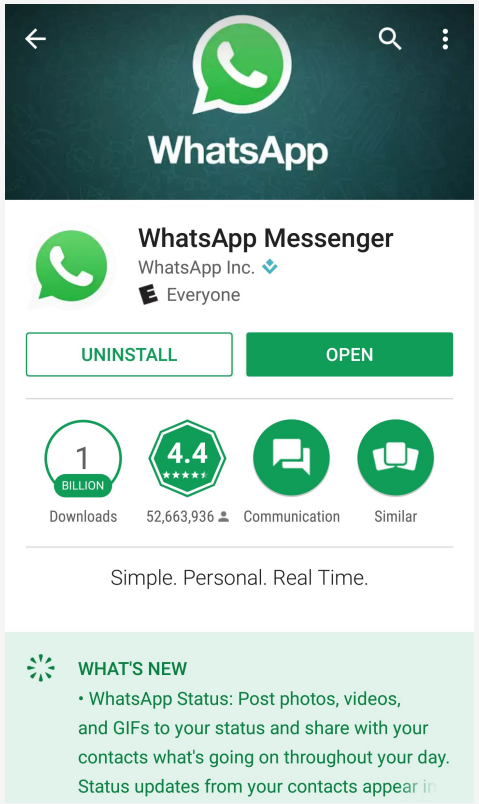


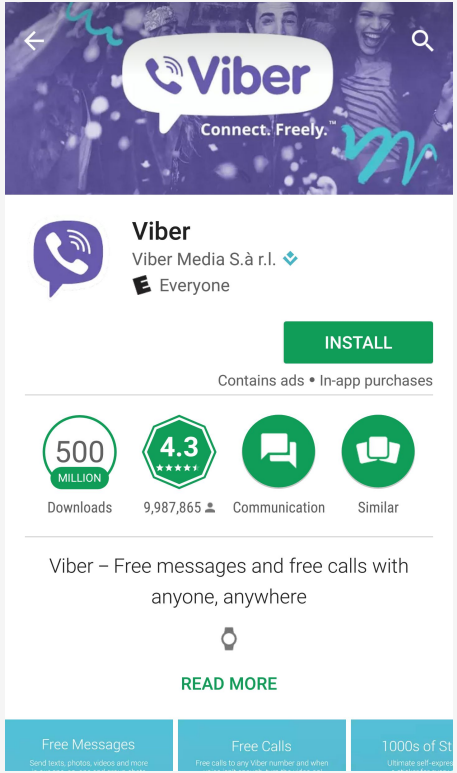
Verifying the Identity Key

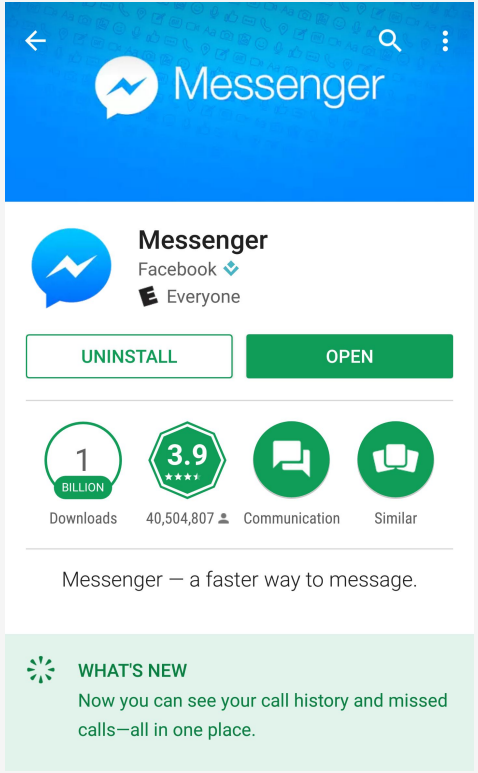
Research Questions

1. Can users find and use the authentication ceremony?
2. How much instruction will they need to find the ceremony?
3. If they can find and use the ceremony, how long does it take? Which methods to they prefer?
4. Do users trust the ceremony and the application? What factors affect trust?
5. What are their threat models?

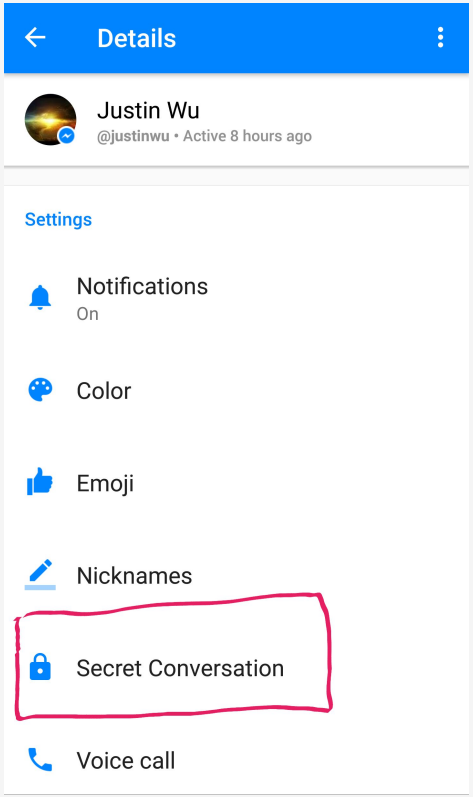
Study Three Popular Secure Messaging Applications

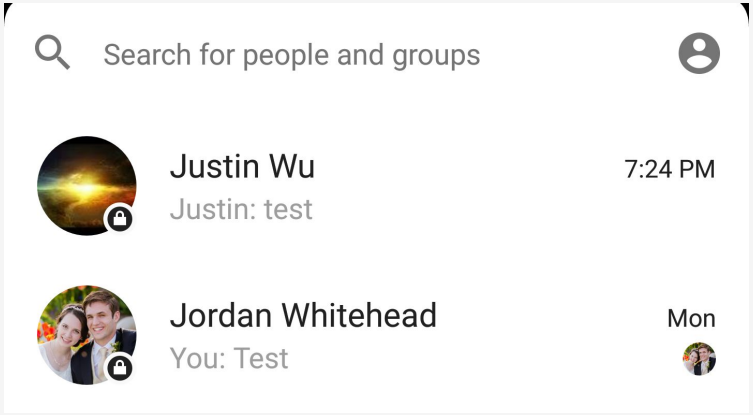


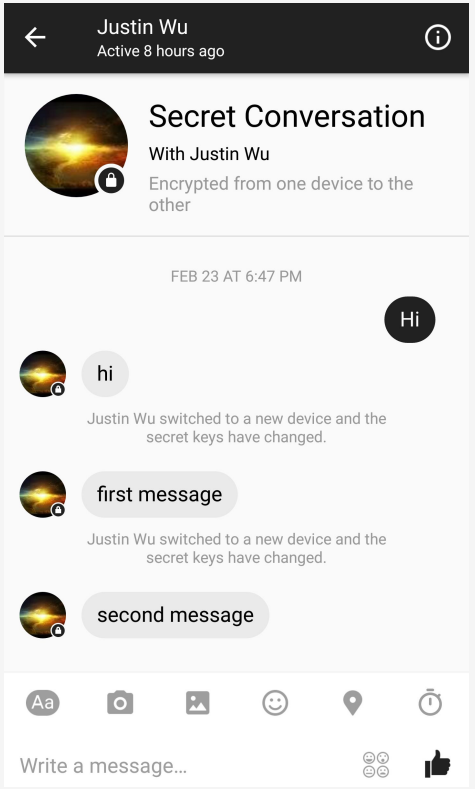




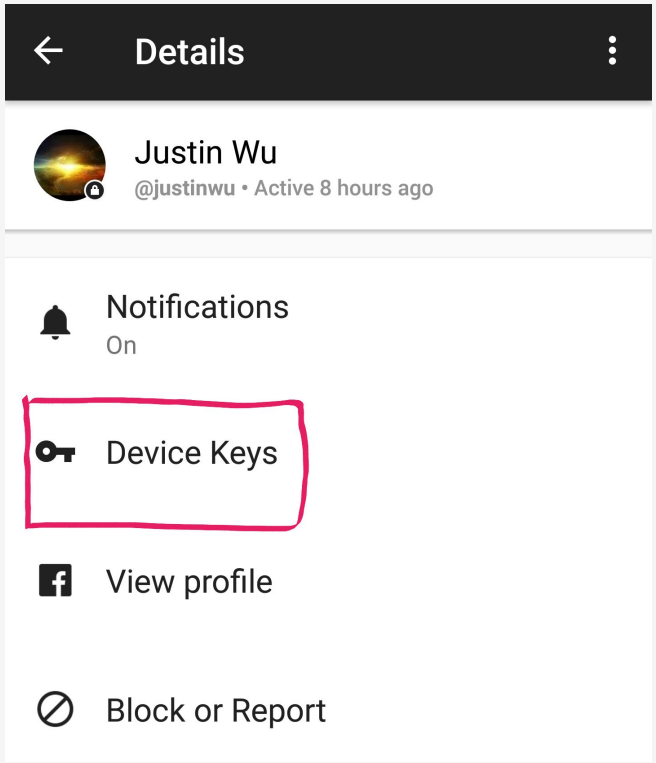
Facebook Messenger

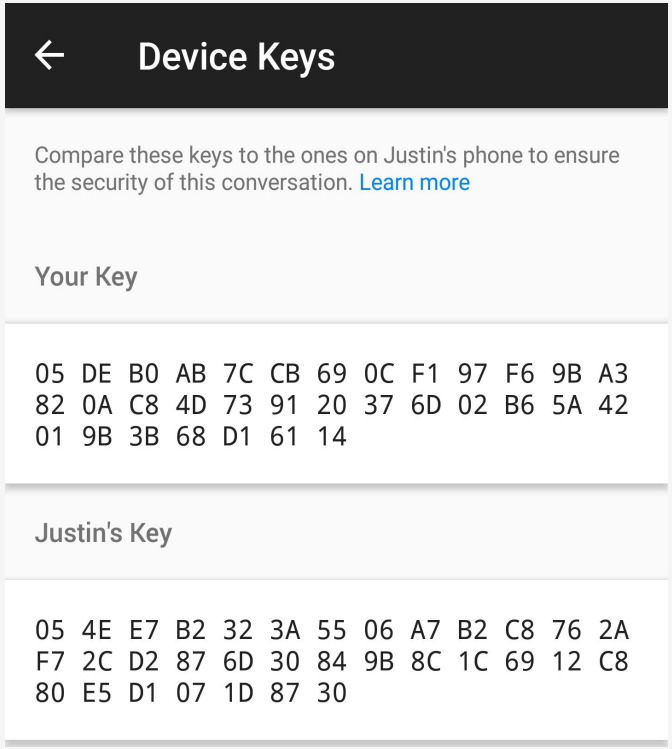




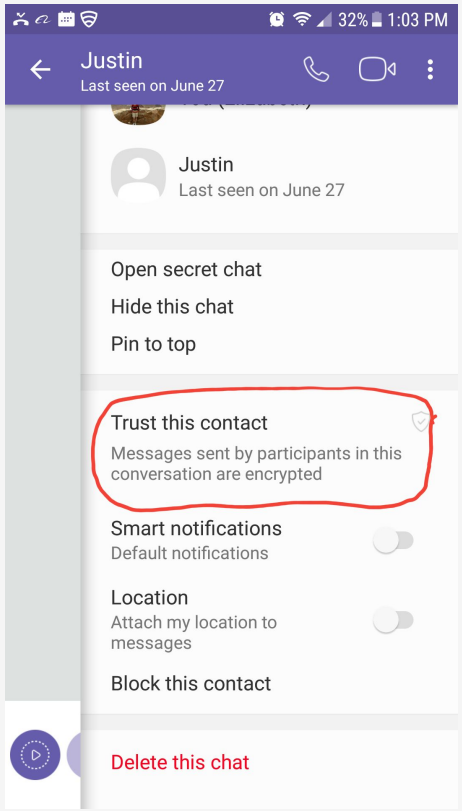


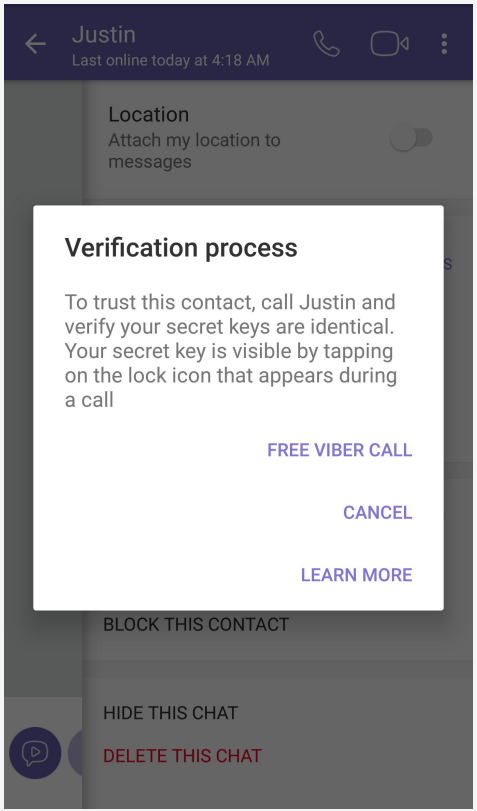
Facebook Messenger

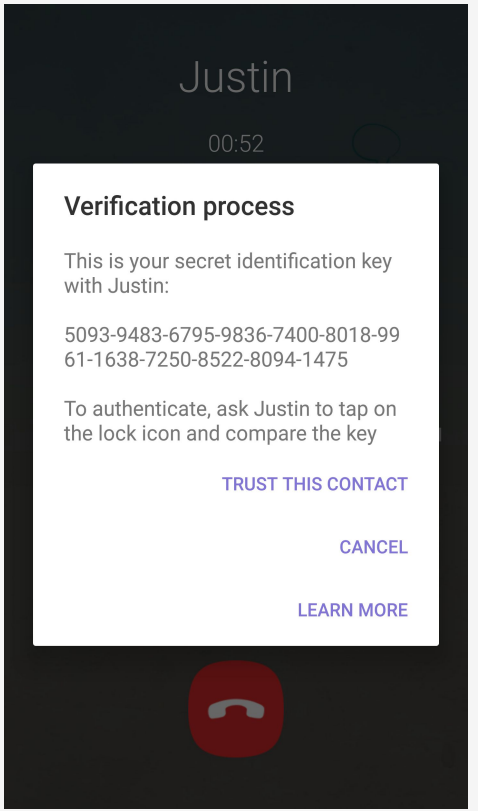




Viber


32% 1:03 PM
Justin
Last seen on June 27
Justin
Last seen on June 27
Open secret chat
Hide this chat
Pin to top
Trust this contact
Messages sent by participants in this conversation are encrypted
Smart notifications
Default notifications
Location
Attach my location to messages
Block this contact
Delete this chat


Justin
Last online today at 4:18 AM
Location
Attach my location to messages
Verification process
To trust this contact, call Justin and verify your secret keys are identical. Your secret key is visible by tapping on the lock icon that appears during a call
FREE VIBER CALL
CANCEL
LEARN MORE
BLOCK THIS CONTACT
HIDE THIS CHAT
DELETE THIS CHAT


Justin
00:52
Verification process
This is your secret identification key with Justin:
5093-9483-6795-9836-7400-8018-9961-1638-7250-8522-8094-1475
To authenticate, ask Justin to tap on the lock icon and compare the key
TRUST THIS CONTACT
CANCEL
LEARN MORE

Methodology

- 24 participants (first phase) and 48 (second phase) were recruited on campus
- Participants were recruited in pairs (with their friends)
- Each phase is within-subjects comparison of 3 applications
- Between-subjects comparison of the effect of instruction
    a. Phase 1: instruction on threats
    b. Phase 2: additional instruction on necessity of authentication ceremony

Phase 1 Instruction

1. Your task is to make sure that you are really talking to your friend and that nobody else (such as the service provider) can read your text messages.

2. Once you are sure the conversation is secure, he/she will ask you to send his/her credit card number, he left home, through the application.

Phase 1: Most do not find/use the authentication ceremony

- Only 4 of 24 participants had some success
- Security of voice vs text:
  a. Voice : Participants believed it is harder to be hacked in real-time
  b. Text : They believed it is easy to delete afterward
- Methods of authentication:

Application	Send Picture	Recognize Video	Recognize Voice	Shared Knowledge	Contact Info	Second Language	Authentication Ceremony
WhatsApp	0	0	13	10	3	2	2
Viber	0	10	4	7	2	2	4
Facebook Messenger	2	12	2	7	0	0	2

Phase 2 Additional Instruction

What Is Secure Messaging?

WhatsApp

Facebook Messenger

Viber
Connect. Freely.

When you use regular text messaging, your phone company can read your text messages.

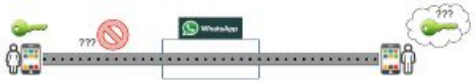
When you use secure messaging apps, you are having a private conversation with your friend.

Not even the company running the service can see your messages.

But you still need to be careful. A hacker could intercept your traffic.

To make sure your conversation is secure, these applications assign a “key” to each person.

You need to make sure the key you see is the same key your friend sees.



Secure messaging apps provide a way for you to compare these keys.

We want to see how well the application helps you do this.

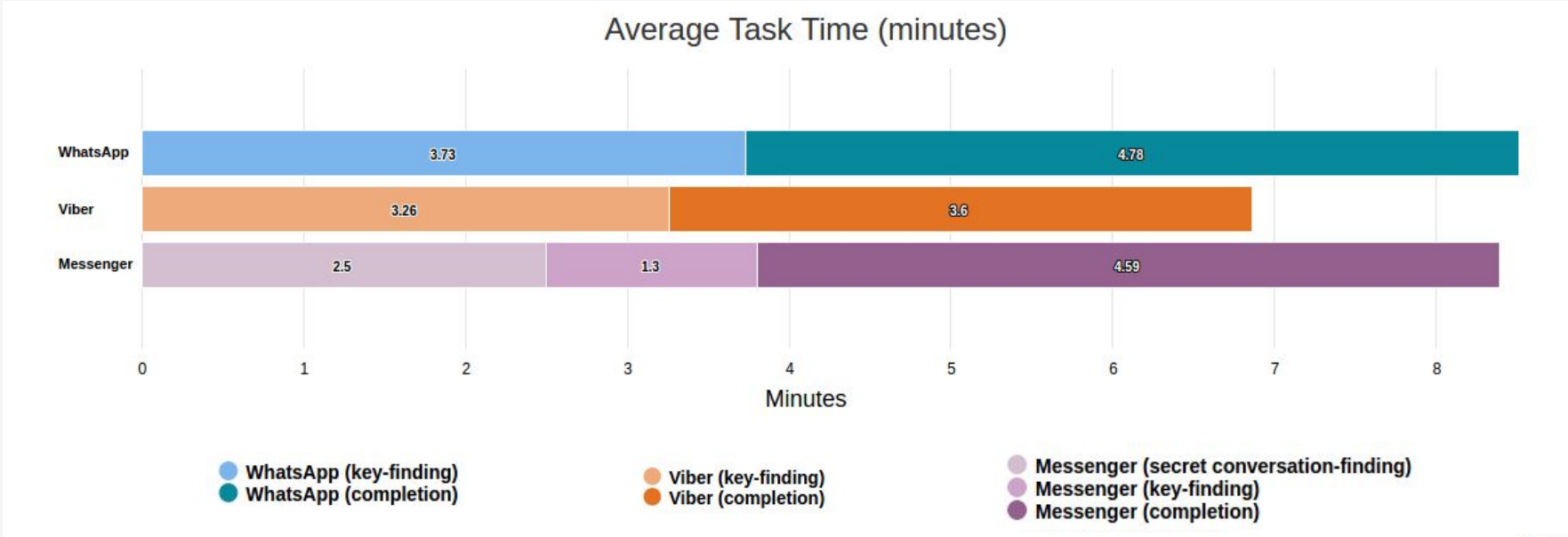
Phase 2: 78% Completed the Ceremony

Application	Success	Fail	Error
WhatsApp	19 (79%)	5 (20%)	0 (0%)
Viber	23 (96%)	1 (4%)	0 (0%)
Facebook Messenger	15 (63%)	6 (25%)	3 (13%)

- Success rate much higher with instruction
  - 78% vs 14%
- Viber significantly better success rate
  - In-app phone call and instructions to compare keys on screen

Phase 2: ... But it Takes too Long

- Mean 3.2 minutes to find, 4.5 minutes to complete the authentication
  - Finding the ceremony: No significant difference among the apps
  - Using the ceremony: Viber significantly faster than WhatsApp (3.6 vs 4.78 minutes)

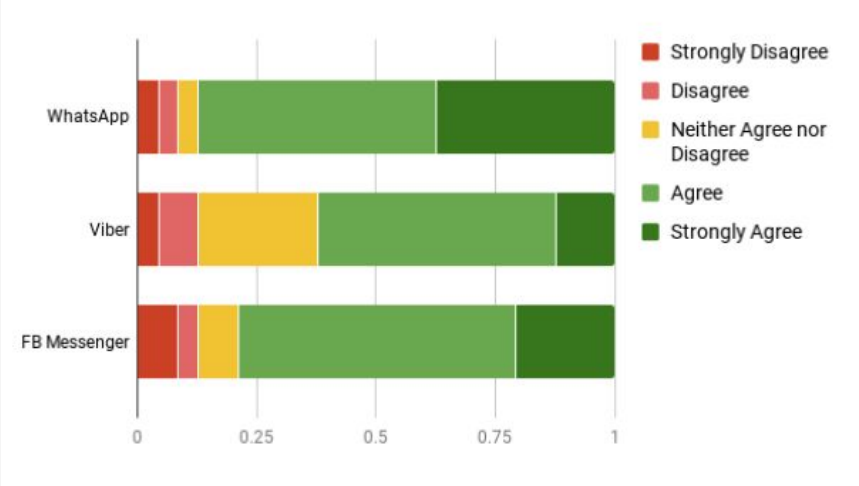


Phase 2: Successful Verification Methods

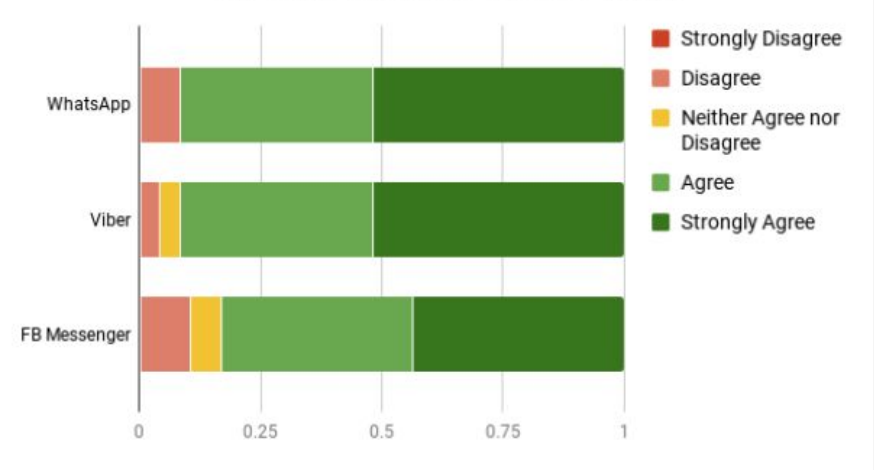
Action	WhatsApp	Viber	Messenger
Secure Methods			
Scanned QR code in person	11 (46%)	N/A	N/A
Read key in person	1 (4%)	0 (0%)	7 (29%)
Called out of band or used Viber's call method to provide key	1 (4%)	23 (96%)	1 (4%)
Less Secure Methods			
Sent key through in-app text	7 (29%)	N/A	10 (42%)
Sent key through in-app video	3 (13%)	N/A	4 (17%)
Sent key through in-app voice	1 (4%)	N/A	1 (4%)

Education Increased Trust in Viber

First Phase



Second Phase



Common Difficulties

- Participants complained about the length of the encryption key
  - *“It’s about eight years long!”* — R27A
- *Please explain why you think you have (or have not) verified the identity of your friend.*
  - 32 of 141 responses did *not* mention the ceremony
  - 28 of these mention using features of their partner as the method of verifying identity (e.g. physical appearance in video, shared private knowledge, familiar voice)

User Threat Model

- *Who do you think can read your message except you and your friend?*
  - Weak perception of active man-in-the-middle attack
  - *"just the two of us unless there were hackers" — R36A*
  - *"not WhatsApp or third parties! But probably people with skills"* — R28A

Type	Times Mentioned
Service Provider	4
Government	8
Hackers	17
Physical Accessors	18
Application Developer	19

Future Work

- Problem: Authentication ceremony does not match user's mental model about authentication
- Solutions:
  - Use social authentication — post public keys to multiple social media accounts
    i. Verifying account authenticity matches what users expect when authenticating identity
    ii. Automate the ceremony
  - Use key transparency (e.g. CONIKS) to monitor keys

Thank You!

Find study materials and data at: alice.internet.byu.edu

Contact us at : elhamvaziripour@byu.edu

Internet Research Lab

Brigham Young University