E2-Chat: A Web-Based End-to-End Encrypted Messaging Service
(Technical Paper)

End-to-End Encrypted Messaging Services Are Here to Stay Even with Government Interference
(STS Paper)

A Thesis Prospectus Submitted to the

Faculty of the School of Engineering and Applied Sciences
University of Virginia • Charlottesville, Virginia

In Partial Fulfillment of the Requirements of the Degree
Bachelor of Science, School of Engineering

Rithik Yelisetty
Fall, 2020

Technical Project Team Members
Saiteja Bevara
Ashwin Pathi
Phillip Phan

On my honor as a University Student, I have neither given nor received unauthorized aid on this assignment as defined by the Honor Guidelines for Thesis-Related Assignments.

Signature Rithik Yelisetty Date 12/02/2020
Rithik Yelisetty

Approved _____ Date _____
S. Travis Elliott, Department of Engineering and Society

Signature _____ Date _____
Yixin Sun, Department of Computer Science

Introduction

Communication via internet services has become increasingly more prevalent due to the ubiquity of technology in everyone's daily lives. Communication services like WhatsApp, WeChat, and Messenger have all amassed over one billion monthly active users (Lee, 2018). These messaging services offered by Facebook, Apple, and other major technology firms have grown to their remarkable size due to users congregating on a small minority of services. In the past, consumers have often looked for the benefits of convenience and ubiquity rather than their privacy, however, in today's world, privacy is at the forefront of many users' minds. In terms of messaging, the most secure and privacy-focused communication services all tend to have one common feature: all messages sent via the platform are end-to-end encrypted (E2EE). End-to-end encrypted platforms encode messages on the sender's device so that only the intended receiver can decode the message to understand the contents. This ensures that any unintended recipients, including any middlemen like governments or the platform operators themselves, will not be able to decipher the contents of the messages. End-to-end encryption has been championed by consumers and privacy advocates as user message content cannot be collected for either advertising purposes or invasive surveillance measures. Governments, on the other hand, have strongly opposed the move as they claim that terrorists will be able to exploit the technology to advance their causes (Graham, 2016).

This paper will analyze government interference in end-to-end encrypted messaging platforms through the lens of the Social Construction of Technology (SCOT) STS framework by focusing on evaluating how humans directly impact the development and usage of technology in society. The SCOT framework is analyzed primarily through the concept of interpretative flexibility, entailing that technology and its associated social factors have to be considered

through the perspective of relevant social groups. In addition, this paper will also examine the tension between the three relevant social groups (users, governments, and platform creators), and how they each view these services. Along with the analysis of end-to-end encryption through the SCOT framework, this paper will also discuss the technical project which is focused on developing a fully web-based end-to-end encrypted messaging platform, which can be used by emerging economies where individuals have access to the internet but not a smartphone. The implemented technical project will allow the team to better understand methods that could be developed to satisfy the government's issues with E2EE platforms while ensuring that user privacy is not compromised.

Technical Project – E2-Chat: Web-based End-to-End Messaging Platform

Introduction

End-to-end encrypted systems have become some of the most popular communication methods in today's connected world, some of the most common being WhatsApp (owned by Facebook) and iMessage (owned by Apple). Both of these platforms have major issues, however, that prevent everyone from migrating to these privacy-focused services. For example, with WhatsApp, each user is required to have an Android or iOS device that has an active phone number. Each user can only have one account and cannot use the same WhatsApp account on multiple devices. To use the service via a desktop, users must use the WhatsApp web client and ensure that both the mobile phone and the laptop have internet access. Messages from the laptop are then transmitted via the phone, meaning that an unintended recipient may be able to decrypt messages during this transfer via a local Wi-Fi network. This process, along with the open-sourced methodologies of key generation and key distribution for group chats, is also used by other similar providers of E2EE messaging services like Signal (Rösler, Mainka & Schwenk,

2018). iMessage, however, differs significantly from this idea. iMessage uses built-in Apple hardware connected to their iCloud service to encrypt and decrypt messages to ensure that all devices that are logged into the same account can be linked. In addition, every message is encrypted several times, based on the number of devices linked to the sender's and recipient's iMessage account (Kumparak, 2014). This further restricts people from using E2EE services as they are required to purchase Apple hardware, and can only communicate with people that have these devices.

Project Need

The goal of this technical project is to be one of the first completely web-based end-to-end encrypted chat services. This means that the service will be accessible from any phone, laptop, or desktop device that is connected to the internet. In areas with low smartphone usage such as developing nations like India, Nigeria, and Indonesia where more than half the population does not own smartphones, but the majority have access to the internet, this service will enable users to have encrypted channels of communication (Silver, 2019). The platform can also be used by commercial clients, who prefer to use encrypted communications internally or with external customers. As with any end-to-end encrypted service, E2-Chat itself will not be able to view any of the message content but will know who the sender and intended recipients are. The service would also allow for the transfer of keys to ensure that messages can be viewed on multiple devices at the same time.

Project Implementation

This project will be developed using technologies such as React.js, GraphQL, Node.js, and web browser key generation libraries. The messaging platform being built will consist of several basic functionalities: creating one-to-one personal chats, creating group chats with up to

100 individuals, sending and receiving messages in real-time, and sending and receiving non-text-based message content like images and documents. When users initially visit the web application (regardless of platform), they'll be directed to a registration page, where they can select their custom username. When users input a unique username, a public-private RSA key pair is generated client-side. The public key will be shared, on account creation, to the server and will be used to encrypt data sent to the user. The private key will be stored in the browser cookies and will be used to decrypt messages that are sent to the user.

Once the user is "logged in", they'll be directed to a screen where they'll be able to view all of their existing messages along with the option to create a new group chat with users. When a new group is created, the creator of the group will send out a message to each of the group members indicating that they have been added to a new group. Along with this, the group creator will generate a new public/private keypair for the entire group, enabling the service to encode each message only once with the appropriate group keypair. The private key will then be sent to each user, encrypted with their personal public key. This ensures that any middleman will not be able to hijack the message to obtain the group's private key to decrypt messages. This group private key will also be stored alongside the user's private key in the browser cookies.

Once everyone has received the group's keypair, users can freely send messages in the group, each time encoding the message using the group's public key and allowing everyone else to decrypt with the group's private key. Figure 1 shows an example exchange of messages between three parties. All messages are encrypted and cannot be deciphered in transit and in the database, but can be viewed by all of the group members. This is very similar to the method used by WhatsApp. According to their whitepaper, WhatsApp uses the "client-side fan-out" method to distribute keys to every user that is within a group and then uses the "server-side fan-out" idea to

send every message from there. This improves the overall efficiency of the service as each message will only have to be encrypted one time ("WhatsApp Encryption Overview", 2017).

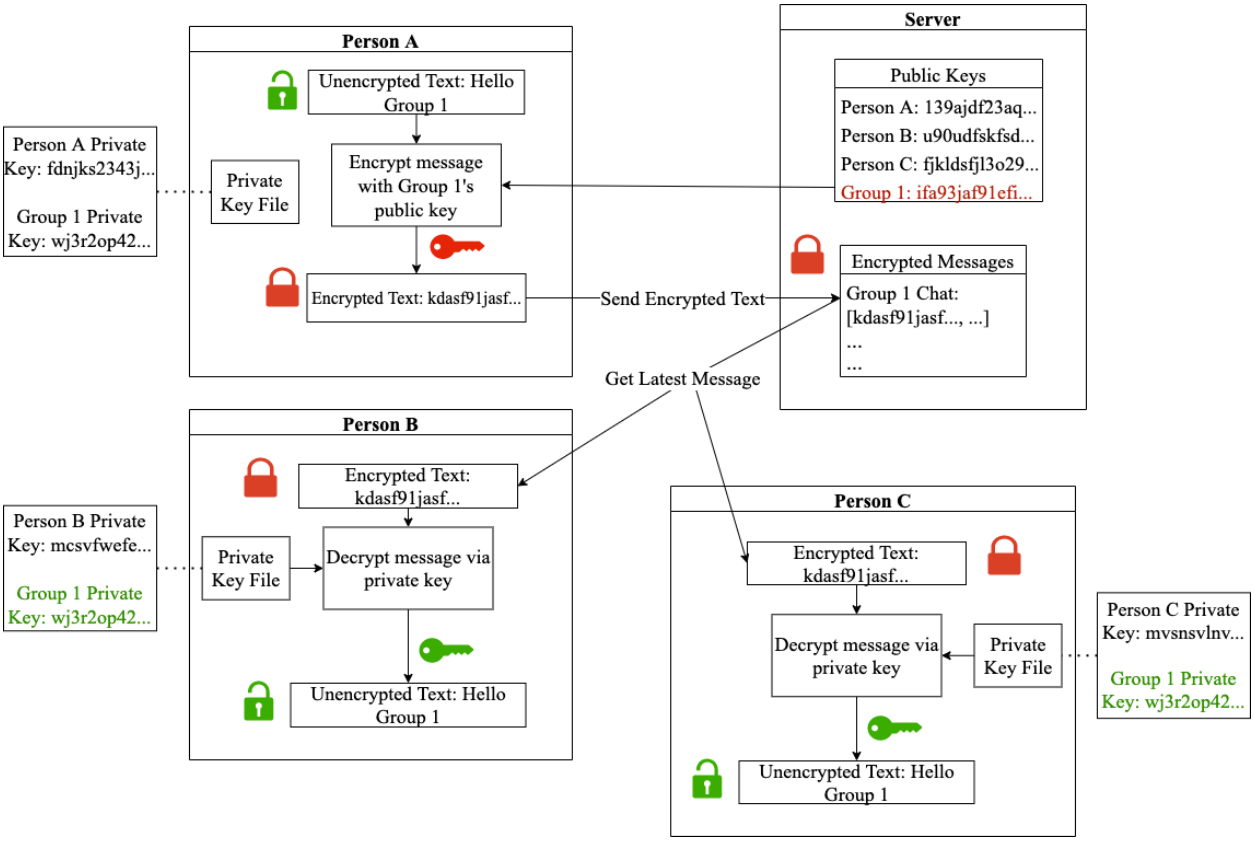

Figure 1. Example Data Flow of Encrypted Messages (Created by Bevara et al., 2020).

To send files (like images or PDF documents) via the service, files will be uploaded to the web browser and converted into a base64 string. Base64 strings will make the file seem like it is a text message and will be transmitted to the rest of the group members in the same manner as normal messages. When these messages are received by the intended recipients, the messages are decoded using the group's private key and then are decoded from base64 into the appropriate file format. This file can then be downloaded by the users to view.

To ensure that the service can be used on multiple devices, users will have the ability to export all of their public-private keypairs stored in the browser's cookies into a JSON-like

format. This file will then be encrypted and can then be downloaded locally on their machine or can be uploaded to a cloud storage option like Google Drive or Dropbox. When users go onto a new browser or a new device, they can upload this file to the service and automatically read all of the messages that they were previously able to read. If any of the public or private keys are incorrect, the user will not be able to view any of the messages as they cannot be decrypted correctly. By allowing users to move between devices, E2-Chat is positioned to be unique from existing services and ensures the same security and privacy as current end-to-end encrypted messaging providers. As evident by this model, there is no ability for the server, or anyone other than the intended receiver, to view messages that are sent in chats.

STS Thesis: Understanding the Battle of End-to-End Encrypted Chat Services

This paper will analyze current government interference into end-to-end encrypted standards and provide reasoning as to why these services should continue to exist. The paper will also provide supplemental analysis of the ongoing battle between the three relevant parties (users, technology companies, and governments) on how E2EE services should be utilized. The analysis will be completed using the Social Construction of Technology STS framework. SCOT was initially developed by Wiebe Bijker and Trevor Pinch, both of who were professors of the STS departments at their respective universities, through their article "The Social Construction of Facts and Artefacts" ("Trevor J Pinch" n.d.; "Wiebe Eco Bijker" n.d.). The SCOT framework is based entirely on how humans have the ability to shape technology – not the other way around. This is in opposition to other STS frameworks like Actor-Network Theory, where the two-way relationship between how technology and human action shape each other is evaluated. The SCOT framework revolves around three primary principles: relevant social groups, interpretive flexibility, and closure and stabilization (Rosen, 2002, p.15).

As described in the original article written by Bijker and Pinch, the concept of relevant social groups entails that there are several groups of individuals that have different perspectives on technologies. Bijker and Pinch (1984) describe that the main idea of this concept is that every member of a certain social group must have the same belief (p. 414). Everyday users value the use of end-to-end encryption as they believe that their messaging data should remain confidential and should not be accessed by any external entity. This is confirmed by a Pew Research Center survey that claimed that over 90% of adults believe that they should have control over who can view their personal data (Madden M. & Raine L., 2015). Similarly, privacy advocates have raised concerns about user messaging data being shared with advertisers to better serve targeted advertisements. Advocates have claimed that this is a blatant violation of the users' data privacy rights as they do not have the option to opt-out of sharing data. Governments want to restrict the use of end-to-end encryption as this technology prevents them from stopping crime and terrorism-related incidents (Graham, 2016). The US Government has previously tried to eliminate the risks associated with E2EE platforms by forcing companies to implement backdoors in their software. For example, the government mandated Microsoft to build a method to conduct surveillance operations on warranted individuals in their end-to-end encrypted messaging platform, Skype (Endeley, 2017). More recently, governments across the globe have tried pleading with companies, like Facebook, publicly to implement this backdoor technology, maintaining their viewpoint that they would not be able to protect their citizens against imminent attacks ("International Statement: End-To-End Encryption and Public Safety", 2020). Companies are seemingly stuck in a middle ground – offering end-to-end encryption helps improve their public perception and win privacy-related legal cases but could potentially deteriorate their relationship with governments (Wall & Musotto, n.d.). In addition, companies that choose

against implementing end-to-end encrypted messaging can benefit by collecting additional data about their users to help earn supplemental revenue through targeted advertisements.

The second concept, interpretive flexibility, entails that individuals or groups can interpret concepts differently (Rosen, 2002, p.15). Bijker and Pinch (1984) describe this concept with the example of the Hill Report theorizing that the sun oscillates through a range of frequencies. Several scientists were unable to confirm Hill's hypothesis, making it seem like his assumption had been proven wrong. The authors, however, describe how this represents interpretive flexibility, as nature itself "does not force the issue" but rather human action shapes these ideas (p.420). In the case of end-to-end encryption, the Earn It Act can be used as an example. The Earn It Act tries to prevent end-to-end encryption by forcing the providers of chat services to monitor and report child exploitation (Graham, 2020). In the view of the government, this bill has the ability to stop child sexual exploitation by forcing the companies that operate these chat services to report instances to the government. This would, in turn, give the government the ability to prosecute individuals for these crimes. In the view of users and the chat providers, this would require a full stoppage on end-to-end encrypted messaging platforms to ensure that the messages being sent are not in violation of this law. Since companies would be required to complete analysis on each message sent via their platform, they would be required to have the ability to read every message, therefore no longer maintain the status of being an end-to-end encrypted platform.

The third concept of closure and stabilization can be explained as an idea that is agreed upon by all of the relevant social groups and is eventually taken for granted (Rosen, 2002, p.15-16). In terms of end-to-end encryption, the parties involved all concede that users require a messaging platform that is more secure and private than the current non-E2EE messaging

services available. For example, Facebook has even announced that they plan to convert all of their existing messaging platforms (Messenger, Instagram, and WhatsApp) into one fully end-to-end encrypted service showing that they understand that the users want a more secure and private solution to messaging ("Hard Questions: Why Does Facebook Enable End-to-End Encryption?", 2018; Isaac, 2019). Governments have also attempted to implement measures that layout requirements regarding user data storage. In the European Union, the General Data Protection Regulation law, more commonly known as GDPR, requires companies to collect minimal amounts of user data, improve data protection security and store user data for only a specified amount of time ("What is GDPR, the EU's new data protection law?", n.d.). Laws like GDPR can be used to prosecute companies to reduce misuse of data and can improve overall user trust in both technology companies and governments.

Another idea that is agreed upon among all groups is that the amount of misinformation and illegal content sent via messaging platforms must be restricted. With standard messaging services, companies can conduct analysis through machine learning techniques on every message sent to determine if the message violates any policies set forth. Governments and users have been encouraging companies to conduct this same analysis client-side, meaning that messages are scanned before being sent to their intended recipients. If the messages violate any law, the message can either be reported to appropriate authorities or removed altogether. By doing this, users are content to see that their messages are not discernable by external authorities and can rest-easy that messages do not violate any law. Governments are satisfied that they can eliminate potentially dangerous messages from being sent and companies are willing to implement these measures to ensure that they are able to keep both governments and their users on their service.

Conclusion

The technical report will detail findings that are relevant in building out a fully web-based end-to-end encrypted messaging service and how it differs from the current standard of requiring a mobile device to send messages. The technical project will address issues like generating and transferring keys securely in order to understand possible technical issues with current implementations.

The STS research paper will examine the development of the end-to-end encrypted standard and how different social groups, particularly users, companies, and governments, have impacted these messaging platforms. The paper will also examine hindrances applied to these systems by governments across the globe to prevent mass-adoption worldwide.

The combination of this technical report and STS research paper will show how mass adoption of the end-to-end encrypted standard is possible and can improve overall user privacy in regards to their messaging data while still appeasing concerns raised by consumers, privacy advocates, technology firms, and governments.

Next Steps

To better understand the implications of end-to-end encrypted platforms for all relevant groups, I will be using existing surveys and interviews to learn about why people care so much about their privacy, specifically related to their messaging platforms. I will use policy documents and contact representatives from these messaging platforms to learn about why designing E2EE is an area of interest for them. Since this area of exploration is relatively new, there are limited academic articles written in this space. To combat this problem, I will be using news articles and cross-referencing practices to ensure that the material is accurate and trustworthy. Some of the questions that I will be targeting will include: can possible legislation be introduced to restrict

the use of E2EE platforms to only vetted individuals? Can companies create client-side filters (like those that can detect misinformation or child sex exploitation) to stop messages from being sent even without a central server reading the message content? Is there a way for governments to set up a system where they can access messages only when they have a warrant but not at any other time?

References

Bevara, S., Pathi, A., Phan, P., & Yelisetty, R. (2020). Example Data Flow of Encrypted Messages. [Figure 1]. *Prospectus* (Unpublished undergraduate thesis). School of Engineering and Applied Science, University of Virginia. Charlottesville, VA.

Endeley, R. E. (2017). End-to-End Encryption in Messaging Services and National Security—Case of WhatsApp Messenger. *Journal of Information Security*, *9*(1), 95–99. https://doi.org/10.4236/jis.2018.91008

Graham, L. (2020, July 20). *S.3398—EARN IT Act of 2020* [Webpage]. https://www.congress.gov/bill/116th-congress/senate-bill/3398/text

Graham, R. (2016, June 16). *How Terrorists Use Encryption*. Combating Terrorism Center at West Point. https://www.ctc.usma.edu/how-terrorists-use-encryption/

Hard Questions: Why Does Facebook Enable End-to-End Encryption? (2018, May 7). *About Facebook*. https://about.fb.com/news/2018/05/end-to-end-encryption/

International Statement: End-To-End Encryption and Public Safety. (2020, October 11). https://www.justice.gov/opa/pr/international-statement-end-end-encryption-and-public-safety

Isaac, M. (2019, January 25). Zuckerberg plans to integrate WhatsApp, Instagram and Facebook Messenger. *The New York Times*. https://www.nytimes.com/2019/01/25/technology/facebook-instagram-whatsapp-messenger.html

Kumparak, G. (2014, February 27). Apple Explains Exactly how Secure iMessage Really Is. *TechCrunch*. https://social.techcrunch.com/2014/02/27/apple-explains-exactly-how-secure-imessage-really-is/

Lee, C. (2018, March 8). *WeChat active accounts exceed 1 billion worldwide*. ZDNet. https://www.zdnet.com/article/wechat-active-accounts-exceed-1-billion-worldwide/

Madden, M., & Rainie, L. (2015, May 20). Americans' Attitudes About Privacy, Security and Surveillance. *Pew Research Center: Internet, Science & Tech*. https://www.pewresearch.org/internet/2015/05/20/americans-attitudes-about-privacy-security-and-surveillance/

Pinch, T. J., & Bijker, W. E. (1984). The Social Construction of Facts and Artefacts: Or How the Sociology of Science and the Sociology of Technology Might Benefit Each Other. *Social Studies of Science, 14*(3), 399–441. JSTOR.

Rosen, P. (2002). *Framing Production: Technology, Culture, and Change in the British Bicycle Industry*. MIT Press.

Rösler, P., Mainka, C., & Schwenk, J. (2018). More is Less: On the End-to-End Security of Group Chats in Signal, WhatsApp, and Threema. *2018 IEEE European Symposium on Security and Privacy (EuroS P)*, 415–429. https://doi.org/10.1109/EuroSP.2018.00036

Silver, L. (2019, February 5). Smartphone Ownership Is Growing Rapidly Around the World, but Not Always Equally. *Pew Research Center's Global Attitudes Project*. https://www.pewresearch.org/global/2019/02/05/smartphone-ownership-is-growing-rapidly-around-the-world-but-not-always-equally/

Trevor J Pinch. (n.d.). Cornell University - The Department of Science & Technology Studies. Retrieved October 12, 2020, from http://sts.cornell.edu/trevor-j-pinch

Wall, D. S., & Musotto, R. (n.d.). *Facebook's push for end-to-end encryption is good news for user privacy, as well as terrorists and paedophiles*. The Conversation. Retrieved October

12, 2020, from http://theconversation.com/facebooks-push-for-end-to-end-encryption-is-good-news-for-user-privacy-as-well-as-terrorists-and-paedophiles-128782

What is GDPR, the EU's new data protection law? (2018, November 7). GDPR.Eu. https://gdpr.eu/what-is-gdpr/

WhatsApp Encryption Overview—Technical white paper. (2017). https://www.whatsapp.com/security/WhatsApp-Security-Whitepaper.pdf.

Wiebe Eco Bijker. (n.d.). NTNU. Retrieved October 12, 2020, from https://www.ntnu.edu/employees/wiebe.bijker