Review of End-to-End Encryption for Social Media

Vijay Bhuse
School of Computing and Information Systems, Grand Valley State University, Allendale, MI, USA

bhusevij@gvsu.edu

Abstract: People have valid concerns about their privacy and the use of their personal information by corporations. People do not necessarily trust social media companies to protect their right to privacy. Social media companies are under pressure to provide greater levels of security and privacy to their users. The current gold standard of security protocols for messaging system is the Signal Protocol. The Signal protocol is an open-source end-to-end encryption model. It uses AES-256, HMAC-SHA256 and Curve25519 as its cryptographic primitives. This protocol is currently considered cryptographically sound and provides excellent information security. However, many social media companies are still using less secure protocols often underpinned by less secure primitives. This paper discusses in detail the various cryptographic primitives used in social media apps like WhatsApp, Twitter, Facebook, Snapchat and Instagram.

Keywords: Encryption, Cryptanalysis, Privacy, Signal Protocol, end-to-end encryption, public key cryptography.

1. Introduction

Social Media has revolutionized global communication and continues to influence it. Social media apps have become integrated into our everyday lives. Due to concerns over Cambridge Analytica's use of Facebook data and a subsequent movement to encourage users to abandon Facebook, there is a renewed focus on how social media companies collect personal information and make it available to marketers, as per Rainie (2018). An incredible amount of personal information is posted on these platforms or is sent through them via their messaging. Social media has proved to be a vital communication tool for protestors and political dissidents in various parts of the world. Primarily due to these factors, social media companies have been under increasing pressure from privacy advocates to implement stronger and stricter data security measures.

In response, several social media apps began to utilize end-to-end encryption via the Signal Protocol. While end to end encryption is a secure device to device communication model, the cryptographic primitives underpinning it are vital to its security. Karbasi (2021) states that the Signal Protocol originally utilized AES-256, HMAC-SHA256 and Curve25519, all three of which are considered cryptographically secure.

As per WhatsApp (2020), WhatsApp implemented full end-to-end encryption via the Signal Protocol in 2016. Its parent company, Facebook, implemented optional end-to-end encryption in Facebook Messenger, named Secret Conversations. Facebook has also announced that they are working to merge Facebook Messenger, Instagram Direct Message, and WhatsApp into a single message service with default end-to-end encryption. Wyrich (2020) states that Twitter has yet to deploy any end-to-end encryption for direct messages, however, the company has publicly considered the idea. As per Twitter (2021) there is scarce publicly available information on the exact protocols and primitives. Twitter currently uses secure direct messages. Snapchat is similar, the company claims that all pictures sent by users are end-to-end encrypted. Snapchat has not released any details on the protocols or primitives used. Any chats sent via Snapchat are not end-to-end encrypted and again, no technical details on how they are secured have been released as per Amnesty (2016).

This paper is organized as follows. We discuss end-to-end encryption in section 2. We discuss the cryptographic primitives used for end-to-end encryption in section 3, and end with discussion and conclusions in section 4.

2. End-to-end Encryption

First, a brief overview of what end-to-end encryption is and why it is considered cryptographically secure. As per Greenberg (2014), End-to-end encryption is a way for two processes on two different devices to send messages to each other in such a way that it is impossible for a third party, even one that is relaying the messages between the two, to view them. The basic principle behind it is the use of public key cryptography and a secure key transfer between devices. This will only allow those two processes to decrypt any messages sent between them.

The Signal Protocol is an open-source implementation of end-to-end encryption. Signal is a secure messaging application that uses end-to-end encryption to protect the privacy of its users. It has been widely recognized for the strength of its security features and has been endorsed by privacy advocates and security experts, including

Edward Snowden, who is a well-known whistleblower and privacy advocate. Signal is considered one of the most secure messaging apps available, due to its use of end-to-end encryption and other security measures such as forward secrecy. It is also open source, which means that its code can be independently audited for security vulnerabilities. As per Amnesty (2016) International, many activists, journalists, and political dissidents have recommended Signal as a safe and secure way to communicate with others, as it provides a high level of protection against government surveillance and other forms of digital spying.

The Signal Protocol uses a combination of public key cryptography and symmetric key cryptography to provide end-to-end encryption for messages and calls. The Signal Protocol uses the Elliptic Curve Diffie-Hellman (ECDH) key agreement protocol, specifically the Curve25519 curve, to establish a shared secret key between two devices. The private key is used to create a public key, which is shared with the other device. Once the shared secret key is established, the Signal Protocol uses it to generate three session keys: one for encrypting messages, one for authenticating messages, and one for encrypting calls. These session keys are used to encrypt and authenticate messages and calls using AES-256 and HMAC-SHA256, respectively. AES-256 is widely considered to be a very secure encryption algorithm and it is used by many organizations and governments worldwide. HMAC-SHA256 is a widely used method for message authentication, it creates a digest of the message and a secret key, that is sent along with the message, the recipient uses the same key to authenticate the message. Overall, the Signal Protocol is designed to provide a high level of security and privacy for its users, and it is considered one of the most secure messaging protocols available today, as per Karbasi (2021).

As per WhatsApp (2020), the Signal Protocol uses a ratchet mechanism to ensure forward secrecy, which means that if the encryption keys of one device are compromised, the attacker will not be able to decrypt past messages. During the initial key exchange, the devices use Elliptic Curve Diffie-Hellman (ECDH) key agreement to establish a shared secret key for each pair of public keys. These shared secrets are then combined to create a master secret key. Each device then derives a Root Key and a Chain Key from the master secret key. When a message is sent, the sender's device uses the current Chain Key to derive a Message Key, which is used to encrypt the message. The sender's Chain Key is then "ratcheted" forward, and a new Chain Key is derived. This ensures that the Message Key used to encrypt the current message cannot be used to derive any previous Chain Keys. Additionally, the Signal Protocol periodically creates new Root Keys and Chain Keys through a new Elliptic Curve Diffie-Hellman agreement. This ensures that even if the Root Key of a device is compromised, the attacker will not be able to derive the Chain Keys used to encrypt current and future messages. All these mechanisms ensure that the Signal Protocol provides forward secrecy, which is an important security feature that prevents past conversations from being decrypted if a device's keys are compromised later.

All the generated key pairs, apart from the Identity Key, are temporary, and are recreated frequently to limit the amount of data compromised should the keys leak. When these keys are regenerated, the key exchange process happens again, and a new master secret is created, as per Karbasi (2021).

From a typical user's perspective, one of the downsides of the Signal Protocol is that it does not support cross-device message transfer. Each device generates its own key pair and is responsible for encrypting and decrypting messages. This means that messages sent or received on one device cannot be decrypted on another device, even if the devices are owned by the same user. This means that if a user wants to use Signal on multiple devices, they will have to manually transfer their conversations and contacts to each device and would not be able to seamlessly switch between devices. This approach has been chosen to maximize the security and privacy of the users, keeping the private keys on the device and not allowing any third party to access them, thus ensuring that if one device is lost or compromised, the private keys and messages cannot be accessed. However, Signal is working on a feature called "Sealed Sender" that will allow cross-device messaging and syncing, and still maintain the same level of security and privacy.

3. Cryptographic Primitives

The cryptographic primitives that underpin end-to-end encryption are vital to its security. The Signal Protocol uses the following cryptographically secure primitives.

3.1 Curve25519

Curve25519 is the fastest elliptic curve that can be used in the Elliptic Curve Diffie-Hellman (ECDH) key exchange. The ECDH key agreement protocol allows two parties to establish a shared secret key over an insecure communication channel. It creates a shared secret from the two users using one user's private key and the other's public key. This shared secret is then used by both parties to encrypt and authenticate their messages between each other. Elliptic curve cryptography shared secret keys are significantly smaller than standard shared secret keys, while retaining comparable cryptographic strength. This difference grows rapidly as the key sizes increase. An elliptic curve key with a length of 512 bits is equal to a standard asymmetric key of 15,360 bits. The smaller key size also increases the speed of the key exchange, as per Niasar (2020). The use of Curve25519 in the Signal protocol contributes to the overall security and performance of the protocol, by providing a fast and secure key agreement mechanism that can be used to establish shared secrets between devices.

3.2 AES-256

AES (Advanced Encryption Standard) is a widely used symmetric encryption standard that refers to a set of block ciphers. The ciphers are differentiated by their key size, with AES-256 (256 bit key) being the most used. AES encryption is performed in a series of rounds, during which the data is substituted, permuted, and shifted. The number of rounds depends on the key size, with AES-256 requiring 14 rounds.

AES is widely considered to be a secure encryption standard, and it is approved for use on state secrets by the United States government. AES is also considered to be immune from brute force attacks with current technology.

The Signal Protocol uses AES-256 to encrypt messages between clients. This provides a high level of security for the messages, as AES-256 is a very secure encryption algorithm. WhatsApp and Facebook Messenger's Secret Conversations use AES-256-CBC to encrypt messages. CBC (Cipher Block Chaining) is a mode of operation for block ciphers, it makes the encryption more robust against certain types of attacks, however it doesn't include any message authentication, which is why both platforms use HMAC-SHA256 for that as per Kishore (2016). Overall, the use of AES-256 in combination with the CBC mode of operation and HMAC-SHA256, provides a high level of security for messages sent through these platforms.

3.3 HMAC-SHA256

HMAC-SHA256 is a hash algorithm used for authentication and to verify message integrity. HMAC stands for hash-based message authentication code. SHA-256 refers to the hash algorithm used in the creation of the authentication code. The security of the authentication code is dependent on the underlying hash function. SHA-256 is a specific hash algorithm in the SHA-2 standard that is considered cryptographically secure at this time, as per Kishore (2016).

When a user goes to send a message, the shared secret, created during the Elliptic Curve Diffie-Hellman Exchange, is used to derive two keys that will be hashed with the message. HMAC-SHA256 hashes the combination of the first key and the message. It then hashes the combination of the resulting hash and the second key. The result is a unique combination that can only be recreated by the exact same combination of the message, and the keys derived from the shared secret, as per WhatsApp (2020).

This primitive is the only one of the three that is currently in danger of no longer being considered cryptographically secure. The security of its predecessor, SHA-1 is questionable. SHA-2 algorithms were a refinement of SHA-1 algorithms, but the two share the same algorithmic architecture. The fear is that improvements of the techniques used to compromise SHA-1 could compromise SHA-2. Currently, this has yet to occur, and is a purely theoretical fear, as per Kishore (2016).

3.4 Other Primitives Used

Not all social media platforms utilize the Signal Protocol, but all use some sort of encryption to safeguard user data from outside attacks as well as provide authentication. Twitter developers have released many APIs designed to integrate or provide access to Twitter into various other media platforms. A common API is the button on an article or video that allows a user to easily share the content to their Twitter.

These APIs obviously must be able to securely handle user data. However, Twitter has released extraordinarily little technical data on exactly how they do this. Twitter API documentation merely says that the APIs use the TLS cipher suite to secure communications. It would be logical to assume that Twitter uses similar methods to secure the direct messages of users, but no further details are provided, as per Twitter (2021).

The TLS cipher suite comprises of some block ciphers and some stream ciphers, along with supported hash algorithms to be used for message authentication and data integrity. Not all the supported algorithms are considered cryptographically secure. It is unlikely that Twitter would use a depreciated encryption algorithm, but the lack of transparency on the matter raises concerns.

Similarly, Snapchat has made no technical details about message encryption public. The company has stated that it does use end-to-end encryption for pictures sent by users but provided no details on primitives. It does not utilize end-to-end encryption for messages. In a response to a query from Amnesty International on their security protocols, Snapchat only stated that they utilize transport encryption and encrypt user data on both their servers and the user's device. In 2016, Snapchat announced that they were working on a secure messaging system, but they informed that they cannot share any specific details, as per Amnesty (2016) International.

4. Discussion and conclusions

From a cryptographic primitive standpoint, Facebook-owned message platforms utilize some of the strongest primitives among the platforms discussed. The Signal Protocol is a highly secure encryption protocol, and WhatsApp uses it as the default encryption method for end-to-end encryption.

Twitter and Snapchat also use encryption, but they have not published the details of their encryption protocols, encryption schemes, or cryptographic primitives, making it difficult to evaluate the level of security they provide.

End-to-end encryption is the most secure way to encrypt messages between two devices. It ensures that the service carrying the message is unable to view it, providing a high level of privacy. But it can also be used by criminals to hide their activities, making it a "double-edged sword" with valid arguments on both sides.

Overall, the use of strong cryptographic primitives, such as the Signal Protocol, can help ensure the security and privacy of messages sent through messaging platforms. However, it is important for companies to be transparent about the encryption methods and algorithms they use, so users can make informed decisions about the apps they use.

References

Amnesty (2016), "For Your Eyes Only? Ranking 11 Technology Companies on Encryption and Human Rights." Amnesty International, 2016.

Greenberg, A., (2014). "Hacker Lexicon: What Is End-to-End Encryption?". *WIRED*, Archived from the original on 23 December 2015.

Karbasi, H., Amir, and Shahpasand, S. (2021) "SINGLETON: A Lightweight and Secure End-to-End Encryption Protocol for the Sensor Networks in the Internet of Things Based on Cryptographic Ratchets." *The Journal of Supercomputing: An International Journal of High-Performance Computer Design, Analysis, and Use* 77(4): 3516.

Kishore, N., and Kapoor, B., (2016) "Attacks on and Advances in Secure Hash Algorithms." *IAENG International Journal of Computer Science* 43(3): 25–34.

Niasar, M., El Khatib, R., Azarderakhsh, R., and Mozaffari-Kermani, M. (2020). "Fast, Small, and Area-Time Efficient Architectures for Key-Exchange on Curve25519." In *2020 IEEE 27th Symposium on Computer Arithmetic (ARITH)*, , 72–79.

Orlic, V., Peric, M., Banjac, Z., and Milicevic., S. (2012) "Some Aspects of Practical Implementation of AES 256 Crypto Algorithm." *2012 20th Telecommunications Forum (TELFOR), Telecommunications Forum (TELFOR), 2012 20th*: 584–87.

Twitter (2021). "Security." *Twitter - Documentation - Security*. https://developer.twitter.com/en/docs/security.

Rainie, L. (2018), "Americans' complicated feelings about social media in an era of privacy concerns", https://www.pewresearch.org/fact-tank/2018/03/27/americans-complicated-feelings-about-social-media-in-an-era-of-privacy-concerns/, Archived from the original on 27 March 2018.

Whatsapp, (2021), "WhatsApp Encryption Overview: Technical White Paper". https://cryptome.org/2016/04/whatsapp-crypto.pdf, Archived from the original on April 2016.

Wyrich, A. (2020). "Twitter's Hack Reveals Glaring Security Concerns around DMs." *The Daily Dot*. https://www.dailydot.com/debug/twitter-end-to-end-encryption-dms/.