The Importance of End-to-End Encryption in Messaging Applications

Gede Prasidha Bhawarnawa - 13520004
Program Studi Teknik Informatika
Sekolah Teknik Elektro dan Informatika
Institut Teknologi Bandung, Jalan Ganesha 10 Bandung
E-mail : 13520004@std.stei.itb.ac.id

***Abstract*—This paper aims to discuss how communication was encrypted before the digital era until the invention of end-to-end encryption in messaging applications. The goal is to explain the implementation, the usage, and the importance of the end-to-end encryption mechanism.**

Keywords—communication security, end-to-end encryption, messaging application

I. Communication Security Before The Digital Era

Communication has rapidly improved ever since humanity evolved from the pre-literary ages. Information used to be passed on through word of mouth, which is highly ineffective as humans by nature are forgetful. This can create an information loss and the original intent within the message can also be misinterpreted as the original speaker and the message carrier can have different communication styles and dialects.

This changed dramatically once humanity learned how to use written words to convey, store, and send information. This method, at some point in time, increases the accuracy of the message sent as it has no dependency on the carrier's memory. However, a problem arises when using this method. How does the receiver make sure that the message is written by the sender and not by an impersonator?

Figure 1 Wax Seal on Envelope
(Source : Wolf & Ink, https://wolfandink.co.uk/studio-blog/2017/11/9/how-to-wax-seal-an-envelop)

In the old days, specifically the medieval times, a message can be validated by adding a seal made from molten wax. This seal acts as a method to let the receiver know of two things. The first one is the identity of the sender. Seals are unique per institution or family, and while there's still a possibility that someone can steal a seal and duplicate it, it's a rare occurrence and adds trust to the message transportation method.

The second information that the receiver knows due to the usage of message seals is that the information inside has not been tampered with. At that time, messages are written on a piece of paper or parchment, and because the seals are made by pressing a metal stamp on molten wax, some level of scarring on the paper is expected. If someone wants to modify the contents of the message, they will have to open the envelope, rip off the wax, modify the message, and re-apply the wax seal. This will be very noticeable by the receiver.

II. Digital Messaging Applications

As the world enters the digital era, old communication methods that require hard labor and long transportation time are abandoned. This is because the world is becoming more and more connected, possibly connecting more people with impossible distances thanks to using data transmission through the internet, fiber optics, and satellite technology. These advancements enable instant communication and information sharing, breaking down geographical barriers and fostering global interactions.

However, this connectivity is due to various middleware that helps transmit data from the source device or the sender to the target device or the receiver. This makes digital communications very vulnerable to man-in-the-middle attack, where a third, malicious party alters the communications between two party while the data exchanged is in transmission. Due to this vulnerability, it's hard to make sure that the original message is not modified. While virtually all applications and systems that connect one system to the other through the internet is vulnerable to this possible exploitation, one specific sector that needs to protect itself the most is instant messaging applications.

Instant messaging applications (or just messaging applications), such as Facebook Messenger, Instagram Chat,

Line, and KakaoTalk, are the main method of communication nowadays. It's easy to use system and delivery speed is one of the reasons why many people are using it instead of other digital communication methods such as email. However, there is a fear of the messaging application peeking at the private conversations of the users. To relieve this, most messaging applications implemented an end-to-end encryption.

III. End-to-End Encryption (E2EE)

End-to-End encryption or E2EE is a method of secure communication that aims to prevent third parties from accessing data while it's being transmitted from one end device to another. In this context, the end devices would be the applications installed in the users' devices. This encryption ensures that only the sender and the recipient of a message can read its content. This includes the mobile or internet service providers and the messaging application developers.

E2EE works by making sure the data is encrypted on the sender's device before being transmitted to the receiver's device. This way, even if the data gets intercepted during transmission, the interceptor can't make sense of the data because it's encrypted. However, the recipient still needs to be able to decrypt the data for the messaging application to work properly.

To make sure that both recipient and sender can communicate with each other without the risk of the data being intercepted, modified, or peeked at, E2EE implemented a combination of symmetric and asymmetric cryptography to encrypt the messages. Symmetric cryptography is a cryptography method where the encryption and decryption use the same key. Asymmetric cryptography or public-key cryptography, on the other hand, is a cryptography method where the encryption and decryption use a pair of keys: a public key and a private key. The data is first encrypted with a public key and can only be decrypted by a corresponding private key.

In E2EE implementation, before the sender and recipient start communicating, they first generate their public-private key pair. After that, they exchange their public keys to the other party. This exchange can be through QR codes (such is implemented in WhatsApp, Line, and KakaoTalk), a key server (such is implemented in Facebook Messenger and Instagram Chat), or just directly before they start communicating with each other.

After exchanging their public keys, to send a message, the sender first encrypted the message with the receiver's public key. Then it's transmitted to the receiver's application, where it can decrypt the data by using their private key. This way, the data can be transmitted safely as interceptors can't decrypt the data without the receiver's private key.

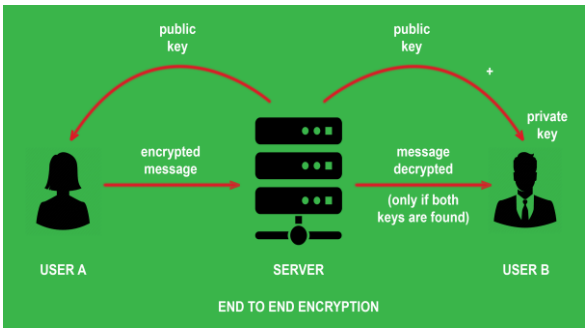

Figure 2 E2EE Schema
(Source : Wolf & Ink, https://wolfandink.co.uk/studio-blog/2017/11/9/how-to-wax-seal-an-envelop)

It's possible for the interceptor to guess the receiver's private key. The strength of this method is from the randomly generated large prime numbers that are used to generate the public-private keys. However, this method is not fool proof. It is possible for someone to brute force the private key with a dictionary of known large prime numbers.

To mitigate this, some messaging applications uses Signal Protocol, such as WhatsApp. The signal protocol uses additional modifications to the established algorithm to enhance security and safety of the messaging session, such as using a one-time use key pair or a key pair with an expiration date. That way, even though a message session can be compromised through brute force, the rest of the sessions is safe as it does not share the same key pair. Additionally, to add more layer of security, Signal Protocol also uses a unique session key that is derived from both the sender's and recipient's key pairs.

Even though E2EE has a lot of benefits, there are challenges and limitations that messaging applications must address. The first challenge is effective and secure key management. Each application and end device must be able to store their own private key and all their connections' public key in a safe and secure place. If this information gets leaked or hacked by a third party, the whole system will collapse. Therefore, some applications implemented a form of short-term storage to store this.

The second challenge is the performance overhead. Calculating large prime numbers can consume a lot of computational resources and may slow down message transmission. Some applications tend to become heavier to use to pay the price for additional security.

IV. Conclusion

End-to-end encryption (E2EE) is a critical technology for ensuring the privacy and security of digital communications. By encrypting data on the sender's device and decrypting it on the recipient's device, E2EE protects messages from being accessed by unauthorized parties, including service providers. While it offers significant advantages in terms of privacy and security, implementing E2EE involves technical challenges and complexities, particularly in key management and performance overhead.

PERNYATAAN

Dengan ini saya menyatakan bahwa makalah yang saya tulis ini adalah tulisan saya sendiri, bukan saduran, atau terjemahan dari makalah orang lain, dan bukan plagiasi.

Bandung, 24 Juni 2024

Gede Prasidha Bhawarnawa 13520004