CS808: Computer Security Fundamentals

3.7: Article: End-To-End Encryption

When two parties wish to communicate securely, e.g. using a messaging system, they can do this in two general approaches. The server they use to appropriately distribute the communications (e.g. an application server) can have a symmetric key for Alice and Bob. This is represented in Figure 1.

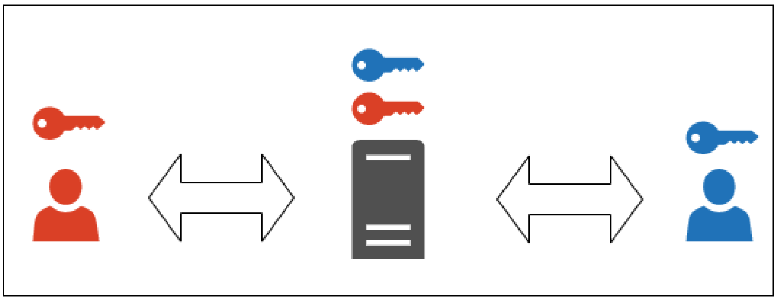

Fig 1

Note Figure 1 and Figure 2 are a somewhat simplified version, there are likely multiple intermediaries, but the principle remains the same. When Alice sends an encrypted message, this can be decrypted and re-encrypted with Bob's key. In this approach the communication is secured over insecure channels, but the server is able to decrypt the communication. This is problematic for a number of reasons. Clearly individuals may wish to retain privacy in their communications, even from the service they are using. Additionally, should the server be compromised all communications will also be compromised.

Neither of these are ideal. Instead, we can deploy end to end encryption. This can be achieved using different mechanisms, but it is fundamentally structured as follows. The server does not hold the decryption key for either Alice or Bob, so encrypted communication goes through the server without the ability to decrypt it. One way of achieving end to end (E2EE) encryption is through symmetric keys with a key sharing algorithm such as Diffie-Hellman. This is represented in Figure 2. Public key cryptography can also be used to achieve this.

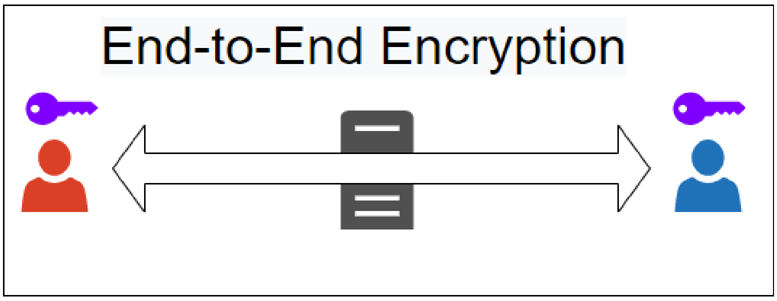

Fig 2

E2EE is used in popular messaging apps such as Signal and WhatsApp. They make use of mechanisms we have seen elsewhere, albeit variations on them. In particular, it makes use of Elliptic Curve and Triple Diffie Hellman and public key cryptography as well as symmetric cryptography. If you are interested, you can find further details in the Signal documentation.

E2EE has been controversial, particularly around governments wishing to have access to all communication should they believe there to be an issue of national security. If you are interesting in reading about this controversy you may like to read this article.

Last modified: Thursday, 29 September 2022, 5:48 PM

◀ 3.6: Video: Digital Signatures (10:47)

Jump to...

3.9 Cryptography Questions ▶

You are logged in as **Neil Hutton** (**Log out**)

CS808