

Breaking Down iMessage's End-to-End Encryption, and How It Got Hacked in iOS 9.3

Xiaoyu Shi

Mentor: Ming Chow

Part I: Abstract

iMessage, as an instant messaging service developed by Apple Inc., is the default messaging application on both iOS and OS X devices. Due to the fact that it is costless and that it is convenient for sending attachments, most users of Apple devices have been using iMessage instead of Short Message Service, or “text messages”. Earlier this year, Eddie Cue, Apple’s senior VP of Internet Software and Services, has disclosed that as many as 200,000 iMessages could be exchanged per second [1]. Besides that, although iMessage is not open source, Apple has published documents asserting that its end-to-end encryption has made iMessage one of the safest means of communication [2]. However, recent concerns of iMessage security have been raised following the discovery of an iMessage security flaw that allows third parties to decrypt attachments to iMessages, like images and videos, if the raw encrypted data has been intercepted. This paper will focus on Apple’s security specifications and its promises to the users, how the end-to-end encryption of iMessage is conducted, and dive into the topic concerning how this vulnerability of iMessage was found.

[1] Apple says people send as many as 200,000 iMessages per second
<http://www.businessinsider.com/eddy-cue-200k-imessages-per-second-2016-2>

[2] https://www.apple.com/business/docs/iOS_Security_Guide.pdf

Part II: Background

1. Statistics and status quo of Apple devices and iMessage
 - a. Brief introduction of Apple Inc., focusing on the increase of Apple devices unit sales, the market share of iOS. <https://www.statista.com/topics/847/apple/>

Apple Inc., founded by Steve Jobs, has always been marked as a company of technical innovation, minimalistic designs and creative advertisements. Apple's revenue has greatly boosted after 2010, with the introduction of iPhone 4 and a great many prominent devices. The market of Apple peaked in 2015, with 223.7 billion dollars in revenue and 59.5 billion dollars in net income.

The market share of iOS devices on smartphones has been oscillating around 15%, which has surpassed Symbian since 2011 to be the second smartphone operating system after Android.

2. What is iMessage? Its introduction and development
 - a. Analyze iMessage as the primary messaging service on Apple devices, and its wide use among users. <http://www.businessinsider.com/eddy-cue-200k-imeessages-per-second-2016-2>

iMessage is the default messaging application on iOS and OS X devices, which means that it can be conveniently used on all major products of Apple, including iPhones, iPod Touches, iPads, iWatches, and iMacs. iMessage supports texts, documents, media, locations, contact information, and group messages. It can operate on Wi-Fi, mobile phone Internet access, or other forms of Internet access; meanwhile, a message sent to a specific user can appear on any of the user's devices. Being a convenient and low-cost methodology of sending and receiving messages, most Apple users rely heavily on iMessage services. As early as 2014, Tim Cook announced that Apple has been handling 40 billion iMessage notifications per day. The number, although impressive enough back then, has even further augmented in recent years. In February 2016, Eddy Cue, Apple's senior vice president of Internet Software and Services, revealed in an interview that "200,000 messages a second are sent on messages (iMessage)" at peak rates, which might count up to 63 quadrillion messages per year.

- b. Introduce iMessage's development history since its deployment in iOS5.

iMessage was introduced in 2011 by Scott Forstall at the Apple Worldwide Developer Conference (WWDC 2011), and was put in use in iOS 5 later in the same year. In 2012, Apple also announced that iMessage will replace the old chatting application, iChat, as part of OS X Mountain Lion, which marked the availability of iMessage on all Apple devices. iMessage was also added to iWatch once it is issued.

With the development of operating systems from iOS 5 to 10, there are a few major changes happening in iMessage. In iOS 8, iMessage added voice messaging to its features, while greatly updated media communications. In iOS 10, users are able to configure text “bubbles,” add screen effects such as light glows and drawing, and send sticker packs.

Part III: iMessage Security

1. Apple’s security promises to its users
 - a. https://www.apple.com/business/docs/iOS_Security_Guide.pdf

In the official iOS security guide issued by Apple, Apple guarantees that all contents of messages are protected by end-to-end encryption, so that no one but the sender and receiver can access them. Apple has also revealed that there will be no log entry for sending and receiving of data; and due to its encryption methodology, Apple itself do not have the ability to decipher user messages.

There are also mentions of the storage of encryption keychains, the use of Apple Push Notification service (APNs), and that users should set up strong passwords for their Apple ID, which are used to log in to iMessage.

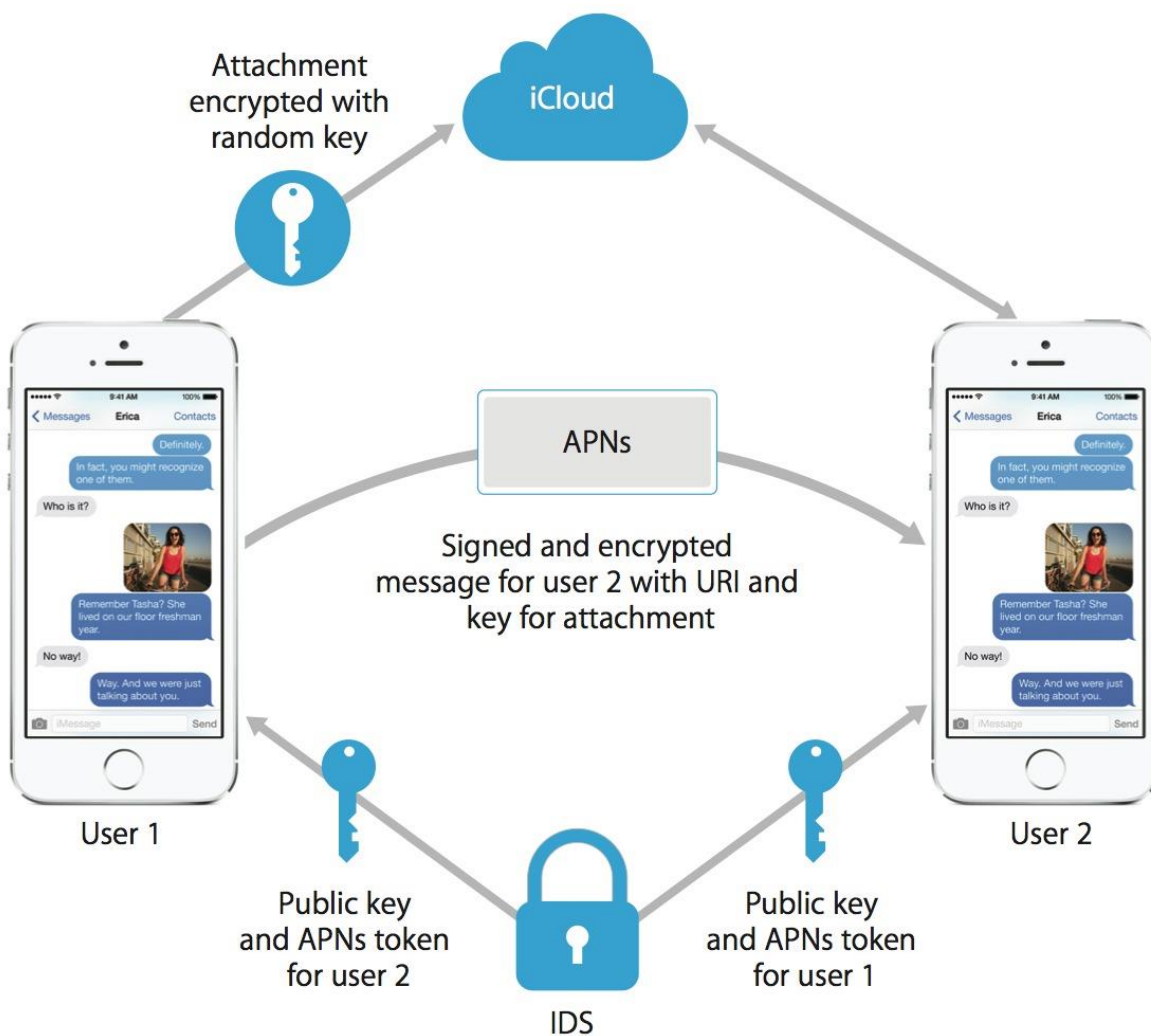
2. iMessage’s end-to-end encryption, and how it really works
 - a. what actually happens if you enable iMessage, <https://techcrunch.com/2014/02/27/apple-explains-exactly-how-secure-imessage-really-is/>

As explained by the official iOS security guide, iMessage uses an end-to-end encryption. iMessage utilizes a service called Apple’s directory service (IDS), which saves the public keys and APNs addresses for all of the devices associated with iMessage users. If a user opens up iMessage, its public key is sent to the IDS so that someone else can find the user’s devices. However, there is also a private key generated with the public key that is encrypted and kept on the device, and will not be sent to servers.

For each receiving device, the sending device retrieves the receiver’s public key, then generates a random 128-bit key and encrypts the message with it using Advanced Encryption Standard (AES) issued by the US government. The message is then encrypted using the public key of the receiving device. The combination of the encrypted message is then hashed with SHA-1, and the hash is signed with Elliptic Curve Digital Signature Algorithm using the sending device’s private signing key. Then the entire information consisting of the encrypted message text, the encrypted message key, and the sender’s digital signature, is sent to the server, and then the receiver may decipher with the corresponding private key via APNs. The message is fully encrypted before it leaves the sender, and is not decrypted before arriving at the receiver’s device.

Thus, the name “end-to-end” encryption is used to address this encryption methodology.

However, as Apple also mentioned in the security guide, some data, such as the timestamp and APN routing data, are not encrypted. Also, things are different with large attachments, such as tenacious messages and pictures. Apple transfers photos and other media on its iCloud servers while encrypted and hashed. In those case, the sender generates a new, random key and a Uniform Resource Identifier (URI) which catalogs the address on iCloud. Apple sends the key and URI to the receiver and then the receiver renders attachment information and make that readable.



The encryption module of iMessage, provided by the official iOS security guide

- b. What if someone else has the public/private key?

As a matter of fact, the public keys are on the server, and are comparatively easy to access. However, messages are only able to decrypt with the receiver’s private key, which is stored on the device and never sent out. Having only

If an attacker has the private key, theoretically all messages could be deciphered. However, the private key, being an RSA 1280-bit key for encryption and an ECDSA(Elliptic Curve Digital Signature Algorithm) 256-bit key on the NIST P-256 curve for signing, is possible but hard to brute force. If an attacker want to access information with this way, he or she would prefer to get the private key in a way other than brute forcing, which can be seen in the analysis of the attack on iMessage.

3. Security Concerns with iMessage

- a. Recent suspicions, Apple's relations with NSA and/or other government agencies.
[http://www.apple.com/privacy/government-information-requests/;](http://www.apple.com/privacy/government-information-requests/)
<http://fortune.com/2015/10/20/tim-cook-against-backdoor/>

Apple has announced its policy concerning government requests to be carefully reviewing the "valid legal basis" behind requests of information, and is strongly against back doors in devices for information exploitation. A recent case involves the FBI, as Apple has announced its reluctance to help the government agency in hacking the iPhone of Syed Rizwan Farook, one of the attackers involved in the assault in San Bernardino this past December. As a result, FBI has found a third party for this case of data decryption.

Apple has even won praise from Snowden on the stance on customer privacy, as it alleges to never sell customer data.

- b. Vulnerability specific to iMessage,
[https://www.washingtonpost.com/world/national-security/johns-hopkins-researchers-discovered-encryption-flaw-in-apples-imessage/2016/03/20/a323f9a0-eca7-11e5-a6f3-21ccd5f74e_story.html;](https://www.washingtonpost.com/world/national-security/johns-hopkins-researchers-discovered-encryption-flaw-in-apples-imessage/2016/03/20/a323f9a0-eca7-11e5-a6f3-21ccd5f74e_story.html)
<https://isi.jhu.edu/~mgreen/imessage.pdf>

Despite iMessage's large number of user basis, the encryption protocols used by iMessage have never been subjected to rigorous cryptanalysis. Although the official security guide provides simplistic details for security on Apple devices in general, the detailed encryption protocols are not revealed, even for academic purposes. As Johns Hopkins Professor Matthew Green (et al) mentioned after the cryptanalysis of iMessage, that "surprisingly, there has been very little analysis of the system, in large part due to the fact that Apple has declined to publish the details of iMessage's encryption protocol."

- c. Attack Module: forged TLS certificate; attacks on attachments and long messages

First of all, one of the vulnerabilities spotted in iMessage is that iMessage does not properly authenticate the message payload. In a more thoroughly designed protocol, this section of the ciphertext would be authenticated using

a MAC, which is a more accurate way of identifying the sender, However, Apple relies on an ECDSA signature, which is generated in signing the encrypted information, to guarantee the authenticity of the sender. However, the signature can be forged according to researchers.

As mentioned in analyzing iMessage's end-to-end encryption, long text messages and attachments are sent to iCloud and their URIs are encrypted and sent to the receiver. The researchers have found the encryption of attachments stored in Apple's iCloud server to be vulnerable.

In the first stage of the attack, they developed a software mimicking Apple's Server in order to intercept the attachment data. As a result, they received a URI to the attachment (which is a photo) and discovered that when an iMessage contains an attachment, the message contains the 256-bit AES signature key to be encoded as 64 ASCII hexadecimal characters and is contained within a field named "decryption-key"

Although the researchers could not see the key's digits, they brute forced the 64 digits and send it back to the target phone. The attachment respond with revelation of structure in to each correct position of digits, and researchers repeats this process for each of the 64 hexadecimal symbols of the encryption key.

4. Other security concerns about iMessage

a. Social Engineering

Although iMessage has been trying to maintain iMessage security, there are still chances that it can step further in avoiding social engineering. Apple now encrypts the user data before sending it to the server, and decrypts the data after it has been received. However, there will be no anti-social engineering analysis in forged URIs and malicious content – users are only able to get to know more about the website validity once they click on the information and open them in Safari, Apple's default web browser.

However, there might be a trade-off between information integrity and privacy and analysis of malicious content. Nevertheless, it is not an issue that Apple is able to do nothing about. There could be simple anti-social engineering alerts as easy as notification before entering the URIs attached in iMessages.

b. Apple's customer support and user education, what has been done and what still needs to be done

Apple has mentioned the importance of setting strong passwords for Apple IDs and iCloud accounts. It also requires the combination of upper and lower case letters, special characters, and numbers in its passwords. However, Apple could provide more education in how to guard the website and how to minimize

information exploitation potential once a device is lost, and more information against social engineering.

Part IV: Conclusion

Apple has been renowned for its focus on security and the protection of user information. It not only provides advanced encryption methodology on its devices, but has also rejected governmental agencies trying to exploit user information via back doors and other forms of collaboration. However, Apple has been unenthusiastic in providing information of its encryption protocols for studies in academia, thus its encryptions, such as end-to-end encryption used by iMessage, has not been fully analyzed and tested. In the recent analysis conducted by researchers in Johns Hopkins University on iMessage of iOS 9.3, a major security flaw is found that allows attackers access information via attachments sent in the iMessage.

Although Apple has fixed the security flaw in iOS 10, there are also a lot of issues that the company is supposed to implement. For example, Apple should provide more education on social engineering and how to minimize information exploitation possibilities, and it could also further collaborate with academic researchers in development of encryption and security analysis.