International Journal of Information Engineering and Applications
2018; 1(2): 67-70
http://www.aascit.org/journal/information

AASCIT American Association for Science and Technology

A Study of Email Encryption on Android OS

Ghasaq Bahaa Abdulhussein

Department of Computer Network Engineering, Faulty of Art Science &Technology, University of Northampton, Northampton, UK

Email address

moonlight1950@yahoo.com

Citation

Ghasaq Bahaa Abdulhussein. A Study of Email Encryption on Android OS. *International Journal of Information Engineering and Applications.* Vol. 1, No. 2, 2018, pp. 67-70.

Received: January 27, 2018; **Accepted**: February 18, 2018; **Published**: March 23, 2018

Abstract: In the past, mobile devices are used for making/receiving calls and SMS. Smartphones become the most common and typical mobile devices in recent years. They merge the PDA (personal digital assistant) with the functionality of mobile phone. Moreover, they are provided many functionality of the computers, such as processing, communication, data storage and etc. Also, they provide many services that the computers make them available, for example web browser, video call, GPS, Wi-Fi, different social media application and etc. Recently, email is one of many relevant communication services that accessed commonly using smartphones. One of most popular operating systems in smartphones that using it, is android. In this paper, email encryption on android is present using Asymmetric key for files, emails, and texts to encrypt/ decrypt, sign email/file, and verify. Both OpenKeychain and Samsung email is used in this paper to simulate the use of PGP on android. This paper proposed the use of asymmetric in the same mobile application which is compatible with all OS platforms software.

Keywords: Mobile Security, Android, Security, Email, Encryption, Public Key

1. Introduction

Smartphone is a mobile device with advanced mobile operating system that is combined the mobile device features with the features of a personal computer. In spite of the fact that most of the users consider the smartphones similar to mini-offices, few of them essentially think through of considering it as a protected environment to store their personal information. Actually, TLS (transport layer security) and SSL (secure socket layer) protocols, that provide authentication and encryption, are not protected enough, since they are not supported by all servers. Furthermore, the FREAK vulnerability can be utilized to breakdown both Android and iPhone email encryption when TLS is used. [1]

In recent times, email is one of the most essential communication services that gain access by using mobile smartphones and in sometimes confidential data might be sent over. One of the most popular smartphones OS that make use of email, is android. Providing an application to encrypt/ decrypt and sign/verify the messages and files that send using asymmetric encryption as a client-side encryption made the email more secure and the transferred data protected while sends from the source end-user to the destination end-user.

2. Background and Literature Review

Android OS:

Google is developed a mobile operating system based on Linux kernel (java-based) called Android, which is currently running on smartphones. On the other hand, it is announced in November 2007 by the Open Handset Alliance. It is open source and releases under Apache license v2. It supports: Wi-Fi, Bluetooth, 3G and 4G communication protocols, accelerated 3D graphics, GPS, SMS messaging, and etc. [2], [3]. The developer of third party android application is using Java. However, some of the developers would like to make the source code of the application more complicated, they used C or C++ which is not improved the performance of the application. [4]

Android is attempting to re-set the goals of the traditional OS to be the most secure and usable operating system for mobile platforms, in order to provide the following objectives: [5]

1. Protect the data for both the application and the user
2. Protect system resources
3. Provide isolation for the application from the system, end-user, and other apps

In order to achieve these goals, Android supports the following features:

1. At the OS level through the Linux kernel, robust security is implemented.
2. For all the apps, mandatory application sandbox is provided.
3. Making the inter-process communication secure.
4. Signing the app.
5. Application-defined and user-granted permissions.

RSA Algorithm:

(Rivest-Shamir-Adleman) RSA algorithm is a cryptosystem for public key encryption, which is commonly used to protect sensitive data especially when they sent over the internet, which is insecure network. It is an asymmetric cryptography that uses two keys (public and private) to encrypt and decrypt. It support a technique of guaranteeing the confidentiality, data integrity, authenticity, and non-reputability in communication. There are various protocols depend on on RSA for encryption and digital signature functions, such as OpenPGP, SSH, SSL/TLS, and S/MIME [6].

Asymmetric cryptography implements a digital certificate in order to provide a layer of security and validation, which is contained an information to identifies the owner of the certificate combined with its own public key that is singed by certificate authority (CA).

The key size is directly determine the encryption strength and expanding key length brings an exponential increase in strength, while it does damage the performance and speed. RSA keys are typically 1024, 2048, 3072 or 4096 bits in long, nevertheless specialists believe that in the near future the 1024-bit keys could be broken, which is explained the moving to a minimum key length of 2048-bits, 3072 bits or 4096 bits [6], [7].

DSA and ECC algorithms:

DSA stands for digital Signature Algorithm, which has two key the public key to make the verification by any one and private key to make the creation of signature. It uses a various algorithm for signing and encrypting to RSA, which achieve same level of security so far. It is a United States Federal Government standard, and uses a SHA 256 as a signature algorithm [8], [9].

While ECC stands for Elliptic Curve Cryptography, which capable of stronger security, improved performance, and so far shorter key length. In contrast, The 256-bit ECC key compares to the same security as 3072-bits of RSA key. It is considered to be the most efficient and scalable algorithm, and it uses a SHA 256 as a signature algorithm [8].

The shorter key of ECC needs:

1. Less computer power
2. Faster
3. Secure connection

Background Research:

In 2009, Block Cipher RC2 and MD5 hash function has been performed by Indonesian researcher to provide secure email communication by building an add-on for Mozilla thunderbird however, it achieves only confidentiality features [10], [11]. In 2011, ElGamal encryption algorithm has been implemented in order to secure the email communication on android however, it achieves the confidentiality only [12], [11].

In 2012, Rabbit algorithm, which is symmetric algorithm, is used to develop an android application to encrypt/decrypt, send/receive, and read the email content on client side using java programming languages combined with email content editor. Rabbit algorithm is used 128 bit to encrypt a plaintext and 128 to decrypt a cipher text. It has 17 variables one carry, 8 inner states, and 8 counters. It supports three schemas: extraction, key setup, and next state function. Initiating value of variables is done by key setup schema, then to update the variables value, the next state function schema is used, after that to generate 128 bit pseudorandom string using the extraction schema. XOR is used between the pseudorandom string and the 128 bit of plaintext to create the cipher text. [4]

In 2012, securing email communication using hybrid cryptosystem on android devices is performed which is consisting of AES 128 bit encryption, RSA 1024 bit, and SHA 160 bit. The researchers achieve the non-repudiation, confidentiality, data integrity, and authentication [11].

In 2016, hybrid cryptosystem is suggested to be used in order to secure the emails on android platform, which is combination of hash function, public key encryption system, and symmetric encryption. Actually, all security systems use cryptographic algorithms and techniques that is unbreakable due to their entanglement. In email encryption that is proposed to design new protocol that use ping pong- 128 (symmetric cipher) and RSA cryptography (public key) with MD5 hashing function. Symmetric cipher is significantly faster than asymmetric, however it required a third party to exchange the keys. The disadvantage of RSA algorithm is the speed. Hybrid cryptosystem is considered to be the highest secure type of encryption on the assumption that the pair of public and private keys are fully protected. This cryptographic algorithms involve of providing data confidentiality by using ping pong 128 bit stream cipher, data integrity by using MD5 hash function, and authentication and non-repudiation by using combination of RSA 1024 bit with MD5 bit. [7]

In 2016, National security agency of US, lists the usage of commercial national security algorithms as shown in table 1: [13].

Table 1. *US NSA algorithms uses.*

Algorithm	Usage
RSA 3072-bit or larger	Key Establishment, Digital Signature
Diffie-Hellman (DH) 3072-bit or larger	Key Establishment
ECDH with NIST P-384	Key Establishment
ECDSA with NIST P-384	Digital Signature
SHA-384	Integrity
AES-256	Confidentiality

3. Android Email Encryption Tools

Android privacy guard (APG) is a free and open source software for the android platform. It is used for encrypting/decrypting files, email/text messages and etc. Even

though not all OpenPGP features are currently available in this app, it allows the user using a public/private key pair to encrypt/decrypt and sign files/messages. The application provides user-based, strong encryption which is compatible with GNU Privacy Guard (GPG) and the Pretty Good Privacy (PGP) software [14]. Since March 2014 this software is updated and it is no longer in a further development. Concerning December 2010 and October 2013, there was not new released version of APG [15]. However, a fork of APG called OpenKeychain has added a number of new features, which have been combined back into APG lately. It is free and open source software [16]. By depending on symmetric encryption and a strong passphrase the user can also encrypt individual files without using a public/private key pair. It has the implementation of an OpenPGP for android operating system. The license of OpenKeychain is under GPLv3+. The implementation of APG depends on the Spongy Castle APIs [17].

Features: [18], [16]

1. Donate is added in-app purchases to the developers.
2. Pre-fill email and name addresses as part of identity.
3. Connect keys to the contacts which is support offline only.
4. Import/export keys from SD card as a file.
5. Scan QR Codes to add other people's keys using the Camera.
6. NFC permission to use YubiKeys, Internet permission to retrieve keys.
7. Encrypt and sign messages, then send them via your preferred email app.
8. Decrypt messages and verify signatures.
9. Based on the keys used to sign/encrypt the received message, the response to decrypted messages with quoting and automatic filling of receiver key and signature (supported in K9).
10. Support file managers for easier file selection where necessary.
11. File encryption/decryption with asymmetric and symmetric cyphers.
12. Key management (import, create, edit, export).

In this paper, OpenKeychain has been used to simulate the using of PGP on android platform that is similar to OpenPGP implementation such as GnuPG for windows desktop. The using of the software is for the sending and receiving encrypted email messages, signed messages /email messages, and encrypt and decrypt messages/ text/files. On the other hand, Samsung Email is used as another tool to sign and send encrypted emails as well, which is the email that the OS provided to the users.

4. Tools Experiment Results

a. OpenKeychain

First of all, the user need to create/ import a pair keys (public and private) of Asymmetric encryption after install and launch the app. The key has a number of aspect as follow the expiry, the usage, and the length and type of the key. It takes time to create the key, and after that the key will be ready to share and export. When the key created on android OS, three sub keys will be created with.

On the other hand, the second person has a key as well, it need to be imported in order to exchange secure messages. As shown in figure 1 there is an orange sign which means the key is not verified with the fingerprint. Figure 2 shows the confirming the fingerprint.

Figure 1. *The fingerprint of the public key.*

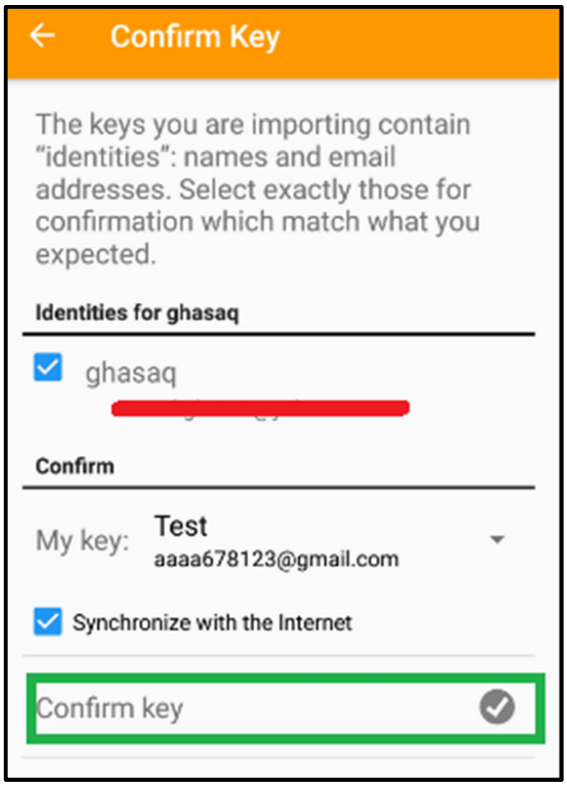

Figure 2. *The confirmation of the fingerprint.*

b. Samsung Email

The RSA key is provided with 1024 bit, and 2048 bit when the key is created. Nevertheless, this encryption technique in build-in Samsung email is support the encryption/decryption and signing/verifying on the same OS which is android and the same application which is Samsung email.

The author experimental results shows that, all apps that have been used in this paper could be performed in a single android application. Furthermore, different encryption algorithm could be implemented in order to secure the communication through the email and implementing it in all mobile platform to be compatible to communication among all end-users who have different OS on their smartphones.

5. Conclusions and Future Work

Most of the mobile application that developed to provide a secure email communication, however they have not implemented all the PGP features. OpenKeychain does implement all techniques PGP, nevertheless this mobile application is need to be implemented directly to the email without using another app. Samsung email does implement the encryption and signing into the email directly, however it is not compatible with any platform only if both users use android and same application of email.

In conclusion, this paper that provide an overview of the using secure email communication with encryption and trying to propose the use of Asymmetric encryption, which is implementation of PGP that could be similar to PGP for windows for encrypting, decrypting, signing, and verifying emails, text messages, and files that through any android email application in same application that provide email service without using different apps to do the encryption techniques and then send the email through the email app.

References

[1] J. Hwang, "IBM," 6th June 2012. [Online]. Available: https://www.ibm.com/developerworks/library/ws-ssl-security/. [Accessed 5th May 2017].

[2] M. Rouse, "TechTarget Search Enterprise Linux," Nov 2008. [Online]. Available: http://searchenterpriselinux.techtarget.com/definition/Android. [Accessed 9th May 2017].

[3] Techopedia team, "Techopedia," Copyright © 2017 Techopedia Inc.. [Online]. Available: https://www.techopedia.com/definition/4219/android-platform. [Accessed 9th May 2017].

[4] M. A. Leksono and R. Munir, "Email client application with rabbit algorithm for Android smart phone," in *2012 7th International Conference on Telecommunication Systems, Services, and Applications, TSSA 2012*, 2012.

[5] Creative Commons Attribution 3.0 License, "Source.android," Creative Commons Attribution 3.0 License, 19 April 2017. [Online]. Available: https://source.android.com/security/. [Accessed 9th May 2017].

[6] M. Rouse, "TeachTarget Search Security," Novmber 2014. [Online]. Available: http://searchsecurity.techtarget.com/definition/RSA. [Accessed 8th May 2017].

[7] S. Purevjav, T. Kim and H. Lee, "Email encryption using hybrid cryptosystem based on Android," in *International Conference on Advanced Communication Technology, ICACT*, 2016.

[8] SSL274 the web security consulatents team, "SSL274 the web security consultants," © 2017. All rights reserved. [Online]. Available: https://www.ssl247.com/kb/ssl-certificates/generalinformation/what-is-rsa-dsa-ecc. [Accessed 8th May 2017].

[9] Symantec team, "Symantec," Copyright © 2017 Symantec Corporation., 10th April 2016. [Online]. Available: https://knowledge.symantec.com/kb/index?page=content&id=SO20921&pmv=print&actp=PRINT&viewlocale=en_US. [Accessed 8th May 2017].

[10] R. Fernando, "Development Add-On On Mozilla Thunderbird For Electronic Letter Encryption," in *Institut Teknologi Bandung*, 2009.

[11] T. Mantoro and A. Zakariya, "Securing E-Mail Communication Using Hybrid Cryptosystem on Android-based Mobile Devices," *Telkomnika,* vol. 10, no. 4, pp. 807-814, Dec-2012.

[12] Y. Adinagara, I. Winarno and K. Fathoni, "Email Encryption Using ElGamal Method on Mobile Devices," in *Institut Teknologi Sepuluh Nopember*, 2011.

[13] National Security Agency United Stated of America, "Cryptome.org," US National Security Agency, Jan 2016. [Online]. Available: https://cryptome.org/2016/01/CNSA-Suite-and-Quantum-Computing-FAQ.pdf. [Accessed 8th May 2017].

[14] APK4Fun.com, "APK4Fun.com © 2014-2017," 24th March 2014. [Online]. Available: https://www.apk4fun.com/apps/org.thialfihar.android.apg/. [Accessed 15th April 2017].

[15] Creative Commons Attribution-Share Alike 3.0 Unported License., "Security-in-a-Box," 10th Aug 2016. [Online]. Available: https://securityinabox.org/en/guide/apg/android/. [Accessed 15th April 2017].

[16] OpenKeychain developers, "OpenKeychain.org," [Online]. Available: https://www.openkeychain.org/about/. [Accessed 18th April 2017].

[17] D. Schürmann, "GitHub," © 2017 GitHub, Inc.. [Online]. Available: https://github.com/open-keychain/open-keychain. [Accessed 15th April 2017].

[18] Google play developers, "Google play," ©2017 Google, [Online]. Available: https://play.google.com/store/apps/details?id=org.sufficientlysecure.keychain. [Accessed 18th April 2017].