Available online at www.sciencedirect.com

ScienceDirect

Procedia Computer Science 124 (2017) 721–727

Procedia Computer Science

www.elsevier.com/locate/procedia

4th Information Systems International Conference 2017, ISICO 2017, 6-8 November 2017, Bali, Indonesia

The Existence Of Cryptography: A Study On Instant Messaging

Vania Beatrice Liwandouw*, Alz Danny Wowor

Informatics Engineering Department, Faculty of Information Technology, Universitas Kristen Satya Wacana
Jl. Diponegoro 52-60, Salatiga, Central Java, Indonesia, 50711

Abstract

The use of smartphone for communication through the Instant Messaging (IM) application has become a dependency and trend model in society. Thus, choosing the right cryptography application to secure data in communicating becomes important. This study analyzes several cryptography applications running on android and iOS platforms, to provide recommendations for users regarding cryptography application that have passed the testing and are able to secure messages so that privacy and confidential communications can be achieved without having to prefer one IM only. The results of this study provided that the best recommended cryptography application that can be used on IM is Encrypt, followed by AES-Crypto, EnDe-Crypto, and Kryptokaz.

Keywords: Cryptography; instant messaging; smartphone

1. Introduction

The concept of efficiency and optimization work that is accommodated in a single device, indirectly alter people's behavior toward smartphones from needs becoming dependency. According wearesocial.com data, more than 50% of the world's population uses the internet, and over than 90% of the world's internet users access using smartphones [1]. Correspondingly, internet and smartphone combination presents a wealth of options for communicating such as social media, instant messaging, video calls, etc. The top 5 highest user rankings showed in Figure 1 is dominated by instant messaging (IM). By all means IM not only the human needs in communication, but also has become a trend as a model of modern society. This is an indication of the desire to communicate efficiently, more privacy and confidentiality.

Recently, people fully believe in a reputable IM that claims their application is secure without knowing clearly what cryptography algorithm is being used. Dissatisfaction between knowledge and existing technology, raises problems in communicating. First, the concept of functionality; Of which over 2.5 billion people have a tendency to use multiple applications in a device [3]. Second, concept of trust; Almost every IM applications proclaims end-to-end

* Corresponding author. Tel.: +0-000-000-0000 ; fax: +0-000-000-0000.
E-mail address: vania.liwandouw@gmail.com

10.1016/j.procs.2017.12.210

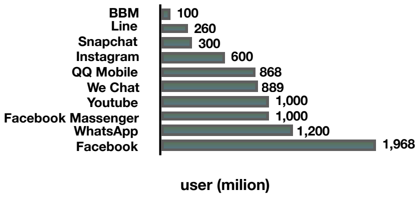

Fig. 1: Social Media User Data (April 2017) [2]

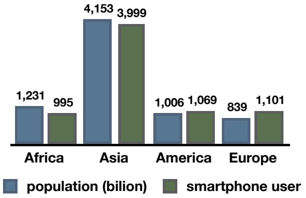

Fig. 2: Smartphone User Data (January 2017) [1]

encryption as a security scheme, and ensures every user can communicate securely. Moreover user ratings on certain applications are instantly increasing, whereas according to [4], [5], [6], [7], [8], [9] and [10] said security features on IM are less secure, since they vulnerable to assault. Third; Any developer who tries to prioritize security features in communicating as reported [11] and [12], in reality not chosen as an option in communicating.

Thus, a rational solution that can be given as an incision on all three issues is the need for cryptography application that apply a verified algorithm, then the ciphertext can be shared using a variety of IM applications. Therefore, this study analyzes several cryptography applications running on multiple platforms to provide recommendations for user regarding cryptography application that have passed the testing and are able to secure messages. So that, privacy and confidential communications can be achieved without having to prefer one IM only.

2. Research construction

2.1. Research sample

Cryptography applications on smartphones that can share ciphertext on IM apps are numerous. Kryptokaz, Encrypt, EnDe-Crypto, and AES-Crypto was selected as samples in this study since they run on android and iOS platform. Besides it also use AES algorithm that has been defined as a standard information security by NIST.

2.2. Research process

The tests are performed for each cryptography application using plaintext variations that can represent the possibility of plaintext used by user. The first test is to examine how each algorithm can generate a random ciphertext with graphical visualization. Another random test is to observe the distribution of data, assuming any data that is evenly distributed at each interval will be complementary information for declaring ciphertext randomness.

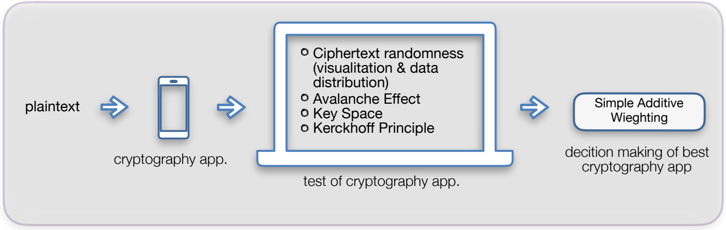
plaintext
cryptography app.
Ciphertext randomness (visualitation & data distribution)
Avalanche Effect
Key Space
Kerchkoff Principle
test of cryptography app.
Simple Additive Wieghting
decition making of best cryptography app

Fig. 3: An Overview of Research Process

The avalanche effect values is the second test and becomes a significant indicator to examine how great the algorithm is able to make changes to the ciphertext, although only 1 bit difference occurs in plaintext. Furthermore, next test is key space to acknowledge the complexity of space and time that required for brute force attack cryptanalysis. Henceforth, the compliance of each algorithm to the Kerckhoff principle relating to confidentiality only on keys when the algorithm publicly known.