EAI Endorsed Transactions
on Scalable Information Systems
Research Article EAI.EU

Enhancing Security of Android Operating System Based Phones using Quantum Key Distribution

Nageen Saleem[1], Areeba Rahman[1], Muhammad Rizwan[1], Shahid Naseem[2], Fahad Ahmad[1,*]

[1]Department of Computer Sciences, Kinnaird College for Women, Lahore, Pakistan
[2]Department of Information Sciences, University of Education, Lahore, Pakistan

Abstract

The Android-based devices are gaining popularity now a day. With the widespread use of smartphones both in private and work-related areas, securing these devices has become of paramount importance. These devices are prone to various security issues of malicious attacks and performance problems. Owners use their smartphones to perform tasks ranging from everyday communication with friends and family to the management of banking accounts and accessing sensitive work-related data. These factors, combined with limitations in administrative device control through owners and security-critical applications, make Android-based smartphones a very attractive target for attackers and malware authors of any kind and motivation. Applications keep and manage diverse intrinsic data as well as sensitive private information such as address books. Smartphones enable swift and easy data exchange via 3G, 4G, and Wi-Fi. Thus, personal information stored on smartphones is prone to leakage. Up until recently, the Android Operating System's security model has succeeded in preventing any significant attacks by malware. This can be attributed to a lack of attack vectors which could be used for self-spreading infections and low sophistication of malicious applications. The research provides a distinctive solution to the security threats being found in the Android operating system. This paper presents a data security and quality enhancement method based on amalgamating quantum attributes into the Android operating system that could effectively solve the issue raised. The paper provides a proposed architecture of Quantum Key distribution being embedded within the Android OS to improve efficiency. However, QKD is a new technology. The research unleashes the possible ways in which quantum could be effectively embedded in smartphones to resolve certain data security problems. Quantum key distribution implements the Android to guard and use in the case of a run-time kernel compromise. That is, even with a fully compromised kernel, an attacker cannot read key material stored in Quantum key.

Keywords: Quantum Key Distribution (QKD), BB84 Protocol, Third-party applications, Encryption.

Received on 10 October 2019, accepted on 12 June 2020, published on 15 June 2020

doi: 10.4108/_____

*Corresponding author. Email: Fahad.ahmad@kinnaird.edu.pk

1. Introduction

The most prevalent mobile platform is Android mobile OS in the world. The Android operating systems have been subjugated the smartphone world with a share of 86.8% [1]. Android systems provide a very user-friendly interface and due to its vulnerable and open-source characteristics, it has attracted many software developers. As a result, a large number of user-friendly applications have been developed until now that not only made our life easier but also provide a platform for learning [2].The applications are developed for some specific purpose that targets a single domain. But there are many apps worldwide that are used in different research areas. Nowadays, smartphones are sensor-based and they have a built-in feature of sensing that provides ease and it is also a gateway towards research in many different realms [3]. A typical Android architecture is presented in Fig.1 [4].

Hardware and sensors. Android is based on Linux kernel and it follows Linux Discretionary Access Control (DAC) [5]. The unique ID and sandbox assigned to each