A LITERATURE SURVEY ON IPHONE OPERATING SYSTEM (iOS)

Nayana V[1], Dr.R.Reka[2]
[1]BE CSE, [2]Professor & Head/CSE,
Annai Mathammal Sheela Engineering College, Erumapatty, Namakkal, Tamilnadu

ABSTRACT

iOS is Apple's mobile operating system developed originally for the iPhone, and later deployed on the iPod Touch and iPad as well. It is derived from Mac OS X, with which it shares the Darwin foundation, and is therefore a Unix-like operating system, by nature. In iOS, there are four abstraction layers: the Core OS layer, the Core Services layer, the Media layer, and the Cocoa Touch layer. The operating system uses roughly 500megabytes of the device's storage. Version 4, announced in April 2010, introduced multi-tasking as well as several business-oriented features, including encryption for email and attachments. At the WWDC 2010 keynote on June 7, 2010, Apple announced that iPhone OS had been renamed iOS. Apple licenses the trademark for "iOS" from Cisco Systems (who own IOS), the same company with which Apple had earlier settled a dispute over the "iPhone" trademark.

1. INTRODUCTION

iOS (formerly **iPhone OS**) is a mobile operating system created and developed by Apple Inc. exclusively for its hardware. It is the operating system that presently powers many of the company's mobile devices, including the iPhone, iPad, and iPod Touch. It is the second most popular mobile operating system globally after Android.

Originally unveiled in 2007 for the iPhone, iOS has been extended to support other Apple devices such as the iPod Touch (September 2007) and the iPad. As of January 2017, Apple's App Store contains more than 2.2 million iOS applications, 1 million of which are native for iPads. These mobile apps have collectively been downloaded more than 130 billion times.

The iOS user interface is based upon direct manipulation, using multi-touch gestures. Interface control elements consist of sliders, switches, and buttons. Interaction with the OS includes gestures such as swipe, tap, pinch, and reverse pinch, all of which have specific definitions within the context of the iOS operating system and its multi-touch interface. Internal accelerometers are used by some applications to respond to shaking the device (one common result is the undo command) or rotating it in three dimensions (one common result is switching between portrait and landscape mode). Apple has been significantly praised for incorporating thorough accessibility functions into iOS, enabling users with vision and hearing disabilities to properly use its products.

Major versions of iOS are released annually. The current version, iOS 11, was released on September 19, 2017. It is available for all iOS devices with 64-bit processors; the iPhone 5S and later iPhone models, the iPad (2017), the iPad Air and later iPad Air models, all iPad Pro

models, the iPad Mini 2 and later iPad Mini models, and the sixth-generation iPod Touch.

2. LITERATURE SURVEY

ChristianJ.D'Orazio [1] et.al. said that, Mobile devices and apps such as cloud apps are a potential attack vector in an Advanced Persistent Threat (APT) incident, due to their capability to store sensitive data (e.g. backup of private and personal data in digital repositories) and access sensitive resources (e.g. compromising the device to access an organizational network). These devices and apps are, thus, a rich source of digital evidence. It is vital to be able to identify artifacts of forensic interest transmitted to/from and stored on the devices. However, security mechanisms in mobile platforms and apps can complicate the forensic acquisition of data. In this paper, we present techniques to circumvent security mechanisms and facilitate collection of artifacts from cloud apps. We then demonstrate the utility of the circumvention techniques using 18 popular iOS cloud apps as case studies. Based on the findings, we present the first iOS cloud app security taxonomy that could be used in the investigation of an APT incident.

David Zimbra [2] et.al. discusses that Micro blogging Word Of Mouth (MWOM) using Twitter has been found to impact the success of experiential products such as movies. However, the influence of the type of device or platform used for tweeting (iOS or Android) on the relationship between well-established tweet metrics - valence, volume, and time period of tweeting - and movie performance is not yet known. Furthermore, it is not known if users of these platforms differ in the aspects of movies they discuss and how that may influence tweet metrics. In this study, we investigated these gaps by analyzing more than four million tweets for 29 movies from both iOS and Android users and conducted a robustness check on another 8 movies. Results from mixed model estimations show that valence of tweets on Android before a movie's release and volume of tweets on iOS after the release significantly influence the revenues of a movie. Results also show that mentions of director and script are more important in the case of Android users whereas mentions of production and music are more important in the case of iOS users. Finally, results show that it may be more productive for movie studios and advertisers to reach the more prolific Twitter users on Android but relatively newer Twitter users on iOS. These findings have significant implications for movie studios as well as mobile advertisers to target their promotions to these platform users accordingly.

Christian J.D'Orazio [3] et.al. described that SSL/TLS validations such as certificate and public key pinning can reinforce the security of encrypted communications between Internet-of-Things devices and remote servers, and ensure the privacy of users. However, such implementations complicate forensic analysis and detection of information disclosure; say, when a mobile app breaches user's privacy by sending sensitive information to third parties. Therefore, it is crucial to develop the capacity to vet mobile apps augmenting the security of SSL/TLS traffic. In this paper, we propose a technique to bypass the system's default certificate validation as well as built-in SSL/TLS validations performed in iOS apps. We then demonstrate its utility by analysing 40 popular iOS social networking, electronic payment, banking, and cloud computing apps.

Luis Gómez-Miralles [4] et.al. tells that Smartphones and mobile devices nowadays accompany each of us in our pockets, holding vast amounts of personal data. The iPhone and iPad are between the most important players in this new market, especially in enterprise environments due to the supposed higher level of security of the iOS platform. Recent research has exposed a number of iOS services that are used by forensic tools to extract information from the devices, and are also prone to being abused by malicious parties. iOS platform tool to prevent this abuse by disabling unnecessary services, and analyze its antiforensic consequences, the privacy implications, and the possible countermeasures (anti-antiforen).

Christian J.D'Orazio [5] et.al…states that with the increased convergence of technologies whereby a user can access, store and transmit data across different devices in real-time, risks will arise from factors such as lack of appropriate security measures in place and users not having requisite levels of security awareness and not fully understanding how security measures can be used to their advantage. In this paper, we adapt our previously published adversary model for Digital Rights Management (DRM) apps and demonstrate how it can be used to detect vulnerable iOS devices and to analyze (non-DRM) apps for vulnerabilities that can potentially be exploited. Using our adversary model, we investigate several (jailbroken and non-jailbroken) iOS devices, Australian Government Medicare Expert Plus (MEP) app, Commonwealth Bank of Australia app, Western Union app, PayPal app, PocketCloud Remote Desktop app and Simple Transfer Pro app, and reveal previously unknown vulnerabilities. We then demonstrate how the identified vulnerabilities can be exploited to expose the user's sensitive data and personally identifiable information stored on or transmitted from the device. We conclude with several recommendations to enhance the security and privacy of user data stored on or transmitted from these devices.

B.A.NaglaaEmanKamal [6] et.al. explains that in patients with ILD, a static expiratory pressure–volume curve of the lung is generally shifted downward and rightward and spirometer results reveal reduced vital capacity (Thompson et al., 1989). However, reduced vital capacity may occur even in patients with obstructive lung diseases and in other situations, such as chest wall restriction, lung resection, inspiratory muscle weakness, or poor cooperation with spirometer. In addition, spirometer is sometimes difficult to perform with elderly, cognitively impaired patients, or severe respiratory distress. iOS is a simple, noninvasive method requiring only passive patient cooperation that allows for the evaluation of lung function through the measurement of both airway resistance and airway reactance. The aim of this study is to assess the role of IOS in the evaluation of the cases of interstitial lung diseases.

Mohammad Dehghanimohammadabadia [7] et.al. explains that a unique Iterative Optimization-based Simulation (iOS) framework is presented, which includes a threefold integration of simulation, optimization and database managers. With this iOS model, optimization occurs frequently at the operational level in order to optimize system variables during the simulation run. In other words, a trigger event momentarily pauses the simulation and signals the optimization manager to optimize the status of the system. Meanwhile, a snapshot of the system, which includes the system status parameters, is transferred to a database. The optimization manager uses this data as an input to the analytical modeling and solves the problem optimally by considering the pre-defined objectives, constraints and updated state of the system. The framework automatically re-formulates the mathematical model using updated parameters, and then, the optimization manager finds a solution in a reasonable amount of time. The database manager is then updated based on the current optimal solution and simulation continues from this point in time. This cycle is repeated for each trigger event in the system and lasts until simulation reaches its timespan. Deploying this promising iOS model enables practitioners to take advantage of long-term simulation runs of their system, while it has been optimized multiple times according to the occurrence of any predefined incidents. The performance of the proposed IOS framework is evaluated using a manufacturing case study, and its results are compared with Simulation-Based Optimization (SBO).

Kenneth M.OvensGordonMorison [8] et.al. proposes that Instant messaging applications continue to grow in popularity as a means of communicating and sharing multimedia files. The information contained within these

applications can prove invaluable to law enforcement in the investigation of crimes.

Kik messenger is a recently introduced instant messaging application that has become very popular in a short period of time, especially among young users. The novelty of Kik means that there has been little forensic examination conducted on this application.

This study addresses this issue by investigating Kik messenger on Apple iOS devices. The goal was to locate and document artifacts created or modified by Kik messenger on devices installed with the latest version of iOS, as well as in iTunes backup files. Once achieved, the secondary goal was to analyze the artifacts to decode and interpret their meaning and by doing so, be able to answer the typical questions faced by forensic investigators.

ChristianD' Orazio [9] et.al… declares that due to the increasing use of mobile devices and apps to view copyright protected content (e.g. movies) on the go, Digital Rights Management (DRM) protections have primarily been used to protect the digital intellectual property and control their distribution and usage on mobile devices. Unsurprisingly, attackers have sought to circumvent or bypass DRM control in order to obtain unauthorized access to copyrighted content. Given the ongoing and rapidly changing nature of mobile device technologies, it is essential for DRM protection designer to have an in-depth understanding of an attacker's capabilities and the potential attack vectors (e.g. vulnerabilities that can be exploited to bypass DRM protection). In this paper, we propose an adversary model that formalizes the real world capabilities of a DRM attacker targeting Apple iOS devices. We then demonstrate its utility using four Video-on-Demand (VoD) apps, one live TV app, and a security DRM protection module. To avoid similar structural mistakes in future designs, we outline two recommendations

CONCLUSION

iOS (formerly iPhone os) is a mobile operating system created and developed by Apple Inc. iOS is designed to be simple and easy to use, it does not include several features found in a traditional operating system. Apple's iOS provides more basic user interface than Mac OS X, each new version adds more features.

REFERENCES

(1)Christian J.D'Orazioa, Kim-Kwang RaymondChoo Circumventing iOS security mechanisms for APT forensic investigations: security taxonomy for cloud apps in Feb-2018.

(2)David Zimbra, Rupinder P.Jindal Movie aspects, tweet metrics, and movie revenues: The influence of iOS vs. Android in Oct- 2017.

(3) Christian J.D'Orazio, A technique to circumvent SSL/TLS validations on iOS devices in Sep-2017.

(4) Luis Gómez-Miralles Hardening iOS Devices against Remote Forensic Investigation in 2018.

(5)Christian J.D'Orazio, LuRongxing Choo,Kim-Kwang, Raymond A Markov adversary model to detect vulnerable iOS devices and vulnerabilities in iOS apps in Jan-2017.

(6) B.A.Naglaa, EmanKamal Role of IOS in evaluation of patients with interstitial lung diseases in Oct- 2016.

(7) Mohammad Dehghanimohammadabadi, Thomas K.KeyserbS. Hossein Cheraghib A novel Iterative Optimization-based Simulation (IOS) framework: An effective tool to optimize system's performance in Sep- 2017.

(8) Kenneth M, Ovens, Gordon Morison Forensic analysis of Kik messenger on iOS devices in June- 2016.

(9) ChristianD'Orazio, Kim-Kwang Raymond Choo An adversary model to evaluate DRM protection of video contents on iOS devices in Feb-2016.