Journal of Theoretical and Applied Information Technology
20th March 2015. Vol.73 No.2
© 2005 - 2015 JATIT & LLS. All rights reserved·
ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

AN INVESTIGATION OF THE SECURE DATA COMMUNICATION IN MEDICAL MOBILE APPLICATIONS

ASOU AMINNEZHAD[1], MOHD TAUFIK ABDULLAH[2],POOYA KHANMOHAMADI HEZAVE[3]

[1,2] University of Putra Malaysia,[3]APU, Faculty of Computer Science and Information Technology
*Asou.aminnezhad@gmail.com, *mtaufik@fsktm.upm.edu.my, poyakhan@gmail.com

ABSTRACT

Nowadays, medical applications (apps) have become a rapidly growing and basic tool in medical education, patient care and clinical research that are vitally important to aware people with a health signal. Similar to other sorts of telecommunication and Internet applications, the medical apps are vulnerable against attackers or unauthorized interceptions. An encryption is a common way to provide the privacy of medical application users. In this paper, we examine ten popular medical applications and analyze the intercepted communication to determine the encryption of captured packets and text communications based on obtained results.

Keywords: *Medical Applications, Encryption, Data Communication, Mobile Interception*

1. INTRODUCTION

Currently, using the medical applications by individuals, medical clinics and hospitals is ubiquitous and has become a controversial topic among doctors and medical students. Numbers of doctors and students are using the medical apps as a source of reference material in a daily clinical care significantly have enhanced. Many mobile health apps are used to improve and facilitate a delivery of patient care. The doctors and students can use these apps in their daily tasks like looking up reference values, making a differential diagnosis, performing useful calculations and looking at patient's investigations [1].

Using medical applications will be major applications that bring more attention and momentum into such a research in the upcoming years. According to Research2Guidance survey [2] it assumed that approximately 500 million users will use the healthcare applications on smart phones by 2015. The survey conducted demonstrated that 30% of the doctors use the smart phone for running the medical apps. These applications have an enormous potential for improving our examination by providing a quick, comprehensive, and updated overview of current clinical guidelines.

These applications help a clinical decision-making and change the healthcare's way is delivered in the future and there are various ways to intercept the data communication. For example, interceptions can take place at client devices when communication is initiated or during the established communication session. The aim of this research is determining the data communication by using encrypted popular medical applications. We investigate these applications and analyze the captured data communications by using a histogram analysis.

The following sections in this paper will be as follows; Section 2 provides an introduction and overview of medical applications interception techniques of the ten popular android medical applications and experimental results are discussed in section 3. In addition, the findings will be discussed in section 4 and section 5 and 6 provide a discussion and conclusion. Our research will be slightly different from the base paper [1], [3], because our research on medical applications doesn't have any voice service, thus some of figures below will be different from the base paper and experiment setup. Besides that, there is not any entropy because it is commonly used for the voice and to identify whether it is encrypted or not.

2. MEDICAL APPLICATIONS

There are some medical applications that are available for different mobile devices and operation system (OS) like iOS, Android, Windows, Blackberry and etc. Most of these medical applications support a text communication. Using the medical application has been increased over the past five years. There are some main reasons for using the medical applications:

- Collect Health Data
- Provide Health messages to the client

© 2005 - 2015 JATIT & LLS. All rights reserved·
ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

- Conduct Health Surveys
- Decision support

The main objective of this project is using appropriate available technology to reduce the spending time to generate monthly reports on services by community of health officers. In this section, we manage identifying the ten popular medical applications that support packet data communication from client to server. They are Doctor Appointment, Duty Manager, Manage My Pain Lite, MediDiary Basic, MediFile, Patient Records, Track my Medical Record, Veterinary Records, BP watch and Blood Pressure.

3. OVERVIEW

Communicating with the patients that are using mobile devices like a Blackberry, iPhone, iPad and Android phones are a fast-growing trend among healthcare providers. A recent survey of almost 3,800 physicians has estimated 83% of physicians own at least one mobile device and about 25% of doctors are "super mobile" users who leverage both smart phones and tablets in their medical practices. As patients and clinicians increasingly use mobile devices to communicate with each other, the trend raises concerns about the security of protected health information ("PHI") [4]. Manage My Pain Lite and Patient Record have their own secure packet communication protocols. All the communications are encrypted with the standard 256-bit Advanced Encryption Communication (AES). Securing the medical records for transmission involved using both of symmetric and asymmetric cryptography. Medical application is able to provide end-to-end encryption and information about routing of the data packets that can be found from the flow content [5].

Medical Record needs to be secure before storing on the mobile phone to avoid any data from being compromised in the event if an SD card is removed from the phone, the information is still encrypted. Symmetric cryptography, specifically password-based encryption (PBE) was used for this purpose as it shown in Fig. 1. PBE uses a password to create a key to encrypt/decrypt the medical record. IEE and ISO announced that the exchange protocol standard (ISO/IEEE 11073- 20601) is optimized to secure manual compatibility between all sorts of PHDs and the gateway from collecting information for the devices and activating related services [6]. The security rule of HIPAA allows healthcare providers to communicate electronically with patients. The arrival time of the packet of medical application is around 10ms to 20ms. Medical record is a medical application that provides only text communication, which is packets service over the Internet. These applications are also able to connect with popular instant messaging and social network such as Facebook, Twitter and most of social networks.

Most of the examined medical applications in this paper run on Android, iOS and Windows. The authentication methods in medical application are shown below in Figure 1.

4. ENCRYPTED COMMUNICATION

It is not possible to determine whether packets transfer from client to application server are encrypted or not by analyzing the captured data. However, determining whether the captured data is encrypted is less straightforward due to a number of reasons.

Some of public algorithms such as AES, RSA and SHA-256 will remain encrypted by using access controls such as username and password and ensure that the cryptographic protection remains secure even if access controls fail [7]. General Packet Radio service (GPRS) is a packet oriented mobile data service on 2G and 3G cellular communication. It provides data rates of 56-114 kbit/seconds. It is not easy to know if the communication is encrypted or not.

In order to decode the packet data, it is important to use the fight decoder, also wireshark is capable to decrypt SSL/TLS encrypted data in packets captured in any supported format [8]. In addition, all the traffic doesn't necessarily travel through the switch to a port that the capture has been done. Wireshark is basically similar to tcpdump but it has a graphical front- end.

© 2005 - 2015 JATIT & LLS. All rights reserved·
ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

Medical Applications	Supported Mobile Platform			Version Used In Our Experiment	Authentication Method
	Android	IOS	Windows		
Doctor Appointment	✓	✓		1.0.0.8	A valid GMAIL Account
Duty Manager	✓			1.4.0	A valid E-Mail Account
MMP LITE	✓			1.9.2	A valid E-Mail Account
MediDiary basic	✓	✓		3.0	A valid Yahoo Account
MediFile	✓			1.0	A valid Hotmail Account
Patient Records	✓			9.0.0.0	Username and Password
Track My Medical Record	✓	✓		4.041	User name and Password
Veterinary records	✓			1.1	Medical Application that is install on the Mobile
BP Watch	✓			1.2.4	Medical Application that is installed on the Mobile
Blood Pressure	✓	✓	✓	2.3.1	Medical Application that is installed on the Mobile

Figure 1- Supported Platform and Authentication Methods of Medical Applications

3. EXPERIMENTS

3.0 Setup

The Android application named Shark for Root was used to capture network traffic in a pcap format. The medical applications were run on both PC and phones simultaneously. For each of the ten applications, we have provided the capture of packets for signing in the application to see if any packets will be found and is the data encrypted or not. The experiment is done many times to ensure reliability of the experiment. To ensure that there isn't any traffic, we installed an application called a No Root Firewall to allow only selected running applications. In the process of the experiment, some advertisement has popped out which interrupts the result. After many tries, the best results have been chosen.

3.1 Analysis Of Captured Packets

In order to check the encryption, we used statistical methods based on a frequency distribution of the byte values. We have used the pcap histogram tool in order to read a payload of the captured packets and plot a histogram with frequency on the Y-axis and the bytes value on the X-axis. We used this script on a kali to generate the histogram:

perl '/root/Desktop/script.pl' '/root/Desktop/(THIS IS THE NAME OF THE PCAP FILE) |gnuplot.

The dump/pcap file is captured by the Shark for Root on a bluestack PC emulator for Android devices. Afterward, a cap/dump file will be transferred to the Kali that generated the histogram. If a cluster byte value around a region 0x41 to 0x5A (representing an English uppercase alphabet set) and 0x61 to 0x7A (representing an English lowercase alphabet set) in the histogram with other regions barely covered. This indicates that the packets contain plaintexts and the captured session is not encrypted [3].

3.2 Histogram Analysis

In Figure2 we investigate these applications and analyze the captured data communications by using a histogram analysis as shown in below.

Journal of Theoretical and Applied Information Technology
20th March 2015. Vol.73 No.2
© 2005 - 2015 JATIT & LLS. All rights reserved·
ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

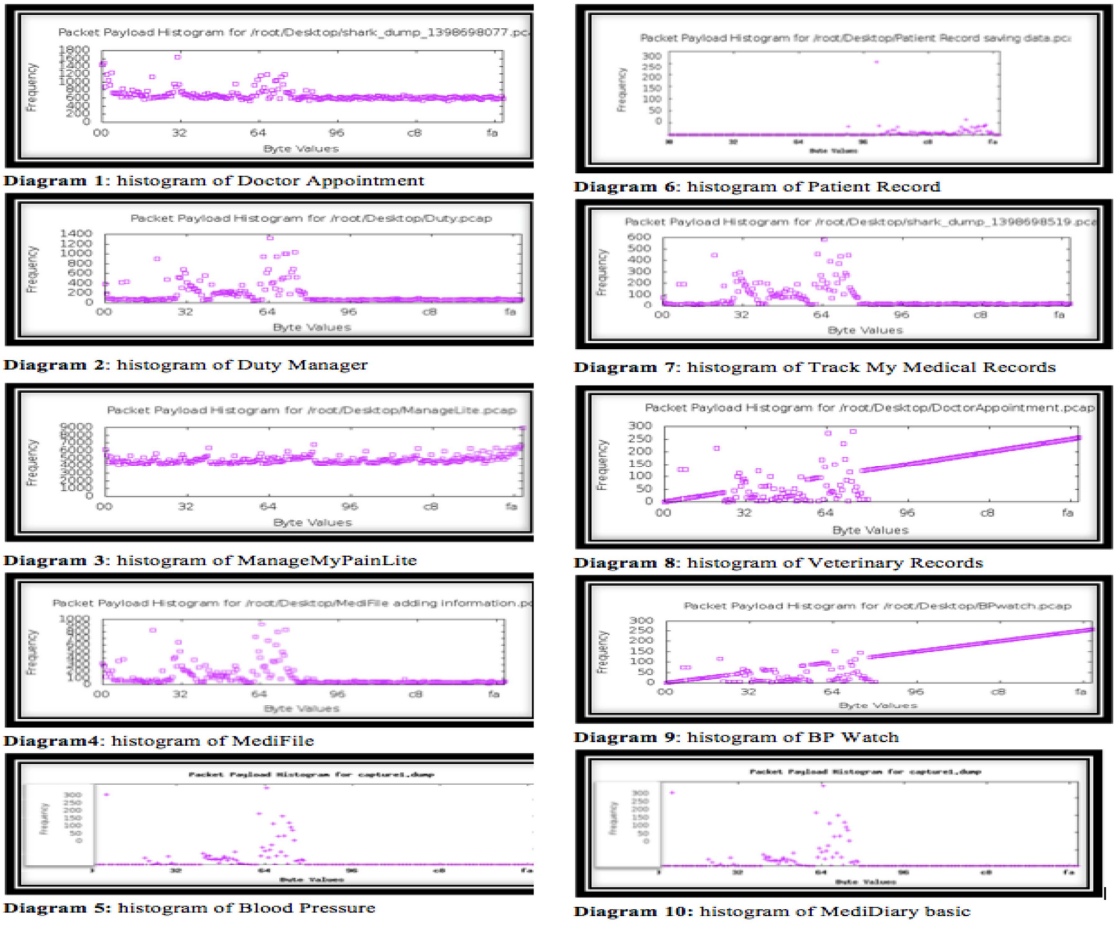

Figure2 Histogram Analyses

4. FINDINGS

We have 2 experimental tests after capturing the medical application communication sessions. In the first experiment, we analyzed the data message to find that the text is plain or non-readable and encrypted. The second experiments were performed to determine whether data communications that are used in the ten applications were encrypted or not.

4.0. Data Analysis

After using the shark for root to sniff the applications' packet in the first experiment, the pcap files were generated. We found that the medical applications provide encryption or secure communication while some applications do not provide encryption. There are some applications like Track My Medical Records and Patient Record, BP Watch, Doctor Appointment able to get the plain text from the captured packets. We can determine that some of the medical applications are used to encrypt the text communication and Transport Layer Security (TLS) and HTTPS to provide the secure communication.

4.1. Data Analysis Using Histogram

We used the shark for root application, and analyzed the found captured data with pcap histogram, which are shown in above Diagrams (Diagram 1-10). The histogram of Manage My Pain Lite was consistent in the Diagram 3. There are no clusters in any region of the histogram for proving that Track my Medical record is encrypted. Also, the Patient Record in the Diagram 6 showed a frequently distribution of bytes with no cluster. From the above observation, it can be said that Patient Record may be encrypted.

The obtained results from the Track my Medical Record were quite interesting. There is a small cluster in the region 0xF6A as shown in Diagram 7. This indicated this app is not encrypted, due to the unsecure connection and the text data that has a cluster in 0x64 regions. Besides that, the histogram of the session that is captured for Medifille showed that cluster in the region of 0x32-64 and the region. As it illustrated in the Diagram 4, there are still scattered bytes in the above histogram. There are only two medical applications that are encrypted and the rest of the medical applications show that the clusters are scrambling all over. The analysis of the other medical applications reveals cluster in certain region.

Journal of Theoretical and Applied Information Technology
20th March 2015. Vol.73 No.2
© 2005 - 2015 JATIT & LLS. All rights reserved·
ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

4.2 Network Data Analysis by SharkReader

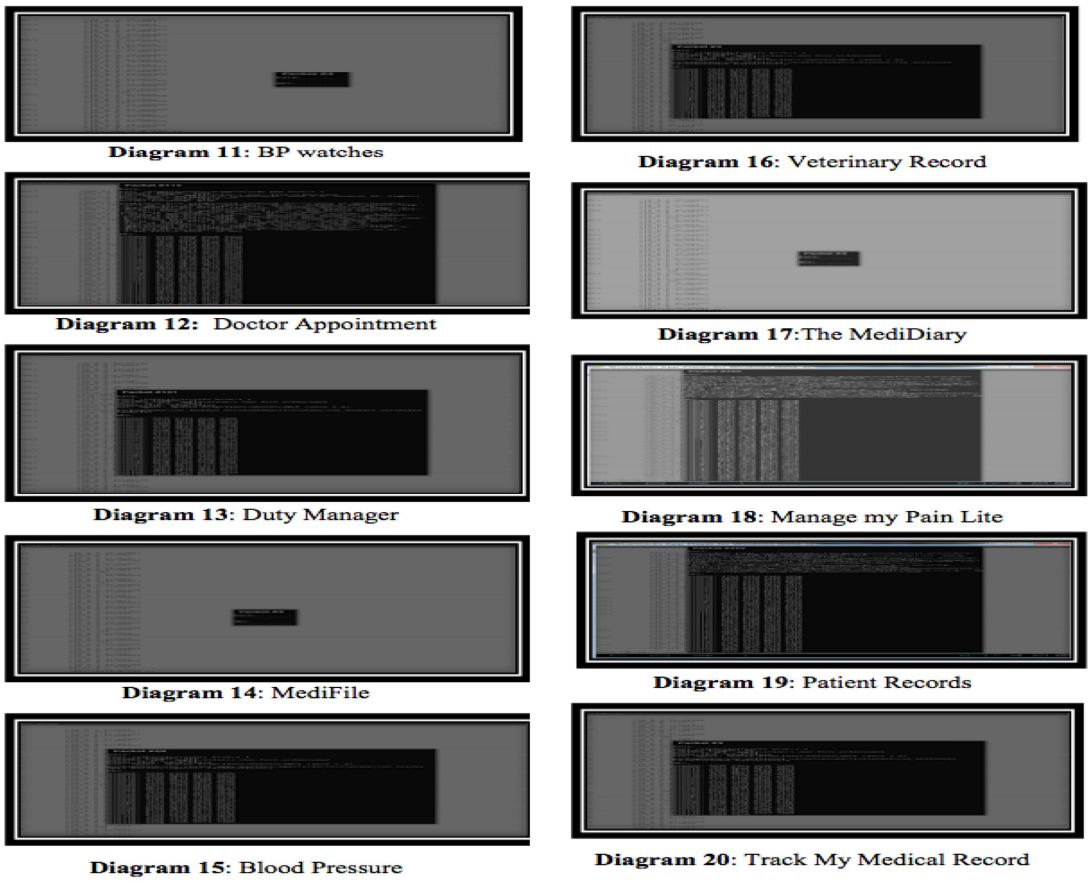

Figure3 Data Analysis by Sharkreader

4.3 Network Data Analysis by SharkReader

Description

Firstly, we used the BlueStack program for windows and Shark for Root to sniff the data to check that whether the application has packets to go through the Internet. Afterward, we installed the Shark Reader that is used to read the pcap file that was created by the Shark for Root. From the above observation, it is significant that most of the medical applications are not encrypted during the communication between client and server. The network data analysis by the Shark Reader had a steady distribution with sudden spikes as all diagrams collected in Fig. 3. The encrypted applications as mentioned above, are Manage My Pain Lite and Patient Record that the information on these applications is highly confidential and secure.

Besides that, we can figure out from the Diagram 4 and 14 that the Medifile do not have any packets to transfer from client and server. The purpose of this application is serving basic features such as a saving information while is connected to the Internet. We have tested all the 10 Mobile applications to monitor either the data is encrypted. All the proof can be seen in the Diagram 1-20.

5. DISCUSSION

Our experimental results and the description of the figures have summarized in Table 1. We found that in the Doctor Appointment, data communications is not encrypted, which shows the cluster in the histogram analysis. Also, we figured out that the data communications in Duty Manager cannot be encrypted and the data after sniffing shows it is readable. Besides, the data in the histogram analysis Diagram 2 shows the cluster during the data communication that means the Duty Manager is not encrypted.

In addition, data communication in Manage My Pain Lite application is encrypted. We analyzed the network communication by the shark reader and as

© 2005 - 2015 JATIT & LLS. All rights reserved·
ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

Diagram 18 shows that data is not readable. Besides, the clusters were not found in the histogram analysis and Diagram 3 shows the changes without huge clusters. Therefore, it shows it is encrypted and secured for the data communication. For MediDiary basic application, we analyzed the data communication by shark reader and as it shown in Diagram 17 that data has no communication and packets' transferring through the Internet. However, it has the clusters in the histogram that shown in the Diagram 10 and it suggests that data stored in MediDiary is not encrypted. For MediFile medical application based on Diagram 4, data shows that network analysis tools are not secure as data is clearly readable. We used the shark reader to sniff that shows data is not encrypted and readable as depicted in Diagram 14.

Data communication for the Patient Record is encrypted and has been shown in Diagram 19 that is not readable and caused that it would be secure. Also, Diagram 6 shows that the cluster is not available during the data communication and it means that it is encrypted and secured.

For Track My Medical Record, data had shown in the Diagram 20 that is readable when we analyzed by shark reader. Besides, the clusters available in the Diagram 7 shows that it is not encrypted and secured.

For Veterinary Records application, data communication is not encrypted. We analyzed the data communication by shark reader and as shown in Diagram 16 data is readable. Then, we analyzed the histogram shown in Diagram 8 analysis and it shows clusters during the data communication that means it is not encrypted.

For BP Watch, data communication is not encrypted. We analyzed the data communication by shark reader and as has shown in the Diagram 11, the data has no communication and packets' transferring through the Internet. BP Watch has clusters as depicted in the Diagram 9 and that means the stored data in the BP Watch is not encrypted.. For Blood Pressure application, data communication is not encrypted. We analyzed the data communication by shark reader and as displayed in the Diagram 15 data has no communication and packets' transferring through the Internet. Also, the histogram analysis based on Diagram 5 shows that this application has clusters during data communication and it is not encrypted [9]–[11].

6. CONCLUSION AND FUTURE WORK

In this research, we conduct an in-depth analysis of the ten mobile medical applications as summarized in the Table 1 by using histogram and root for shark. According to our results, only the Patient Record and Manage My Pain Lite (MMP Lite) are encrypted. The other applications use some sort of mechanism that does not encrypt the packet data during the communications. This research helps to contribute towards a better understanding of legal interception of packet interception between the client and server.

uture work in this area may focus on more sophisticated means to decode the captured unencrypted sessions. Also, currently we are working on providing more secure data transmitting for medical purpose. The re-encryption formula will help the multiuser to use and trust the cloud computing, encryption and decryption under a certain tag name that put together with the file.

© 2005 - 2015 JATIT & LLS. All rights reserved·
ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

Table 1: Summary of Findings from Experiments

Medical Apps	Encrypted Text Communication	Cluster In Histogram	Shark Reader	Network Data Analysis
Doctor Appointment	NO	YES	Non – Encrypted	Packets, Readable
Duty Manager	NO	YES	Non – Encrypted	Packets, Readable
MMP LITE	NO	NO	Non – Encrypted	Packets, Readable
MediDiary basic	NO	YES	Non – Encrypted	No packets
MediFile	NO	YES	Non – Encrypted	No packets
Patient Records	YES	NO	Encrypted	Packets, Encrypted
Track My Medical Record	YES	YES	Encrypted	Packets, Encrypted
Veterinary records	NO	YES	Non – Encrypted	Packets, Readable
BP Watch	NO	YES	Non – Encrypted	No packets
Blood Pressure	NO	YES	Non – Encrypted	Packets, Readable

REFERENCES:

[1] B. Jelle Visser and J. Griffin, "There's a Medical App for That," 2012.

[2] "The market for mHealth app services will reach $26 billion by 2017 | research2guidance." 30-Oct-2014.

[3] A. Azfar, K.-K. R. Choo, and L. Liu, "A Study of Ten Popular Android Mobile Voip Applications: Are the Communications Encrypted?," *SSRN Electron. J.*, Oct. 2013.

[4] "Healthcare Providers May Violate HIPAA by Using Mobile Devices to Communicate with Patients," 2014. .

[5] A. Simplification, "Security 101 for Covered Entities," vol. 2, pp. 1–11, 2007.

[6] "ISO/IEC/IEEE Health informatics--Personal health device communication--Part 20601: Application profile--Optimized exchange protocol." pp. 1–208, 2010.

[7] "Cryptographic Storage Cheat Sheet - OWASP." [Online]. Available: https://www.owasp.org/index.php/Cryptographic_Storage_Cheat_Sheet. [Accessed: 30-Oct-2014].

[8] "SSL/TLS: What's Under the Hood - SANS Institute," 2013.

[9] A. Aminnezhad, A. Dehghantanha, and M. T. Abdullah, "A Survey on Privacy Issues in Digital Forensics," *Int. J. Cyber-Security Digit. Forensics*, vol. 1, no. 4, pp. 311–323, 2012.

[10] H. Salehi, R. Boostani, and A. Aminnezhad, "A New Hybrid Algorithm to Solve the Task Scheduling Problem in Grid Computing," *Int. J. Comput. Appl.*, vol. 62, no. 4, pp. 37–40, 2013.

[11] A. Aminnezhad, A. Dehghantanha, M. T. Abdullah, and M. Damshenas, "Cloud Forensics Issues and Opportunities," *Int. J. Inf. Process. Manag.*, vol. 4, no. 4, 2013.