Analyzing Medical Communication Apps

Nikhil Chopra, Kanika Gupta

September 29, 2016

1 Related Work

A past survey on patients have shown that approximately 38% of patients have wanted to check their blood pressure, monitor their heart beat, track weight, nutrition, glucose levels and other health factors on a mobile device [1]. Due to this dependency of patients on mobile phones and improvements in the field of telecommunications, software applications and data transmission, mHeath applications have become very popular [2, 3].

As per the past studies, mHealth apps use several sensors to determine an individual's health status and assist with health related decision making [4]. These apps can wirelessly connect with remote servers for the purpose of storing health data in a cloud [5, 6], monitoring the health condition and vital signs in an emergency, and archiving health data in personal computer [2, 7]. Due to these potential threats and risks, major types of possible attacks include Resource depletion attack, Replay attack and External Device Miss-Bonding (DMB) attack [2]. Resource depletion attacks can exhaust resources of an mHealth device, such as, battery, bandwidth, storage and so on [2]. Replay attacks attempt to spoof the sensor readings to induce the users or other mHealth devices to make wrong decisions [2]. A DMB attack targets the mobile gateway running the Android Operating System and exploit app-to-device authentication mechanisms [2].

Previous works have shown that sensitive data of a patient broadly comprises of: (1) Instant Messages between a medical advisor and patient [8]; (2) Personal Health Information (PHI) [9, 10, 11] of a patient [5]. The main risks posed to data protection by mHealth apps are the consumers' lack of knowledge about the app, insufficient security measures to safeguard the consumers' sensitive data, information shared with third party and lack of user authentication prior to log-in to the app such as username and password [12, 13, 9].

Significant work has been done in the past to develop robust security measures such as role-based access control mechanisms, authentication with a unique ID linked to a Public Key Infrastructure (PKI), which should be implemented in mHealth apps [9, 14, 15]. Studies have shown that Virtual Private Networks (VPNs) should be used for exchanging critical information for telemedicine applications [16, 17]. Jabber Protocol has proven to be more secure than VPN with some trade-offs and thus should be effectively used in mHealth apps [17].

Even if the data security standards have been defined but there is no standardised methodology to make sure that these standards are met and enforced [18, 14]. According to a recent study on mHealth apps, the results showed that only 1% of the apps authenticated the users prior to login and 50% of the apps stored patients data in a cloud [12]. Nearly 65% of the apps shared patients information with the advertisers and 5% of the apps permitted users to delete their personal information completely [12]. MEDJACK and MEDJACK.2 reports are the best examples of infections in major healthcare institutions [7].

Though there has been considerable effort towards finding the vulnerabilities in the mHealth apps, the focus has always been on the application level issues that can lead to security vulnerabilities [19]. In this paper, we attempt to study the security mechanisms by reverse engineering the widely used mHealth apps with focus on encryption methods and secure communication channels to uncover vulnerabilities in them.

References

[1] S. Narisi, "Mobile health apps create privacy risk," http://www.healthcarebusinesstech.com/mobile-health-apps-privacy.

[2] L. Ohno-Machado, X. Wang, A. Iranmehr, and X. Jiang, "Privacy, security, and machine learning for mobile health applications."

[3] T. G. Rani R. Shetty, "Design and development of mobile phone based healthcare system for emergency situation," 2014.

[4] L. R. Y. Cifuentes, L. Beltran, "Analysis of security vulnerabilities for mobile heath applications," 2015.

[5] L. L. Rui Zhang, "Security models and requirements for healthcare application clouds."

[6] H. Lin, J. Shao, C. Zhang, and Y. Fan, "Cam: Cloud-assisted privacy preserving mobile health monitoring," 2013.

[7] T. research Labs, "Anatomy of attack."

[8] E. Bones, P. Hasvold, E. Henriksen, and T. Strandences, "Risk analysis of information security in a mobile instant messaging and presence system for healthcare," 2006.

[9] B. Martnez-Prez, I. de la Torre-Dez, and M. Lpez-Coronado, "Privacy and security in mobile health apps: A review and recommendations," 2014.

[10] B. C. Zapata, A. H. Niirola, J. L. Fernndez-Alemn, and A. Toval, "Assessing the privacy policies in mobile personal health records."

[11] P. V. Gorpa, M. Comuzzib, A. Jahnend, U. Kaymak, and B. Middleton, "An open platform for personal health record apps with platform-level privacy protection."

[12] R. Adhikari, D. Richards, and K. Scott, "Security and privacy issues related to the use of mobile health apps," 2014.

[13] F. Mancini, K. A. Mughal, and S. G. andJ. Klungsoyr, "Adding security to mobile data collection," 2011.

[14] P. SINC, "Developers neglect privacy, security in health app," 2015.

[15] F. Zubaydi, A. Saleh, F. Aloul, and A. Sagahyroon, "Security of mobile health (mhealth) systems," 2015.

[16] BrianE.Dixon, JulieM.Hook, and JulieJ.McGowan, "Using telehealth to improve quality and safety," 2008.

[17] I. Sachpazidis, R. Ohl, G. Kontaxakis, and G. Sakas, "Telehealth networks: Instant messaging and point-to-point communication over the internet," 2006.

[18] D. D. Luxton, R. A. Kayl, and M. C. Mishkind, "mhealth data security: The need for hipaa-compliant standardization."

[19] R. F. Olanrewaju, N. B. Ali, O. Khalifa, and A. AbdManaf, "Ict in telemedicine: Conquering privacy and security issues in health care services."