Volume 3, Issue 2, February 2013 ISSN: 2277 128X
International Journal of Advanced Research in Computer Science and Software Engineering
Research Paper
Available online at: www.ijarcsse.com

Security Policies for Mobile Devices in Critical Health Care Information Systems

Manasa Vemulapalli and Arun Raj Kumar .P
School of Information and Technology (SITE),
VIT University, Vellore,
Tamilnadu, India

Abstract---With developments in Information and Communication Technologies, Mobile phones play a vital role in medical fields wherein patient's health status is reported to the Doctors from time to time and during emergency. The information about the patient can be queried and retrieved from the Health Care System Database at anytime from anywhere. The critical information available in health care system consists of medical records, case history of the patient, personal information such as Social Security Number (SSN), medical insurance policy number, medical identification number, etc. The critical information is not secure against the mobile phone threats resulting in danger to patient's life. The most prominent threats affecting the health care information system through mobile devices are Wi-Fi Sniffing, sending a malicious link by Short Message Service (SMS) or a malicious attachment through Multimedia Message Service (MMS). These attacks are the threat to security goals such as confidentiality (e.g., patients data is revealed to unauthorized persons), integrity (e.g., the unauthorized access to data leads to manipulation of patients clinical data), and Availability (e.g., Denial of Service Attack). The existing Health Care Information System fails to identify the application and Operating System (OS) vulnerabilities viz., usage of improper encryption techniques to secure the data, leakage of information due to easy passwords, saving passwords on mobile devices, unauthorized access provisions, etc. Hence, efficient security policies are proposed in this paper in order to provide a secure integrated framework for Critical Health Care Information System.

Keywords: Wi-Fi-Sniffing, SSID Detection

I. Introduction

Usage of mobile phones has been increased significantly in all the areas. Recent technology developments have made the evolution of smart phones from the normal mobile phones. These smart phones have features such as GPRS, Applications, Bluetooth, 3G, and Video Conference, etc. Mobile phones inside the hospitals are strictly banned in some countries in Europe and partially allowed in some countries viz., Italy. The reasons for ban are due to radio emission from mobiles and the electromagnetic interference that affects the sensitive medical equipments. Nonetheless, the smart phones with GPRS and UMTS technologies proved to be of less harm than mobile phones with technologies like GSM. Moreover, mobile phones are beneficial to communicate with the patients residing in rural areas. Using tools such as SiteOnMobile [1], patients share their clinical information such as glucose levels, BP, etc., and doctors respond with proper medication. Today, in most of the hospitals, smart phones are used by the doctors for monitoring the patient's health status. But, the information available in smart phones and hospital data centers is compromised due to several threats and vulnerabilities. With increase in mobile phone usage, it has become the prime target for attackers. WIFI Sniffing, malware attachment through SMS (or) MMS, malicious applications download are the various ways through which the attackers sniff the entire network and cause havoc to normal transfer of critical data. In [2], Department of Homeland Security (DHS) warns the health care organizations about the threat posed by insecure network attached medical devices and proliferation of smart phones and tablet Personal Computers.

II. Motivation

Patient's health status is sent in wireless medium to the doctors. Though Wireless network offers huge benefits, it is not tedious for the attackers to break the wireless encryption security standards than the conventional wired networks. As there are threats and vulnerabilities while transferring the data through wireless medium, it may cause a severe threat to patient's life. Hence, these factors motivated us to propose efficient security policies [3] that are essential for building a secure integrated framework for the Critical Health Care Information Systems.

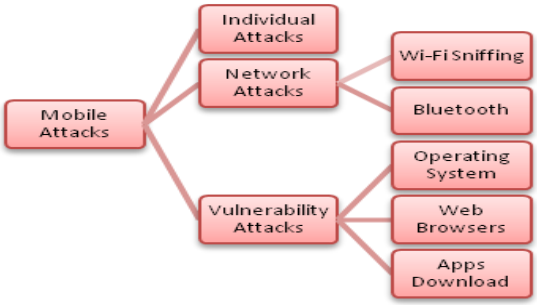
III. Methods of Attack

Different types of attacks in mobile phones are classified into individual, network, and vulnerability attack as shown in

TABLE I. ATTACKS AND VULNERABILITIES IN MOBILE PHONES

S. No	Category	Type of Attacks	Compromised security goals			Vulnerability
			C	I	A	
1.	Network Attacks	Wi-Fi Sniffing	Y	Y	N	1) Passive Data Scanning 2) SSID Detection , 3) MAC Address Collection.
		Bluetooth	Y	Y	N	1) Pairing without verification, 2) Bluetooth Signal always on.
		SMS, MMS, OR Malware	N	Y	Y	Text messages, MMS
2.	Vulnerability Attacks	Operating System	N	Y	Y	Untimely Updation of antivirus and OS
		Web Browsers	Y	Y	N	Uniform Resource Locator (URL) Navigation
		Downloaded applications	Y	Y	Y	Malicious Applications
3.	Individual Attacks	-------	Y	Y	Y	Disgruntled employee

C-
Co



nfidentiality, I-Integrity, A-Availability, Y- Yes, N- No

Fig. 1. Different types of attacks

III.A. Network Attacks

A.1. Wi-Fi-Sniffing:

Table I lists the compromised security goals for each attack and its vulnerabilities. Wi-Fi Sniffing is used by hackers or crackers to attack the Local Area Network (LAN) and take control over the whole wireless networking system. Nowadays, as the hospitals have provided wireless network and enabled the Wi-Fi access, it provides an easy way for the attackers to scan the hospital network and capture the data being transferred on the wireless network through mobiles, laptops, tablets, etc. Attacker may manipulate this information leading to loss of security goals viz.,

confidentiality, availability, and integrity. There are many open source tools available in internet for Wi-Fi Sniffing, to break the wireless encryption protocols viz., Wired Equivalent Privacy (WEP), Wi-Fi Protected Access (WPA), to identify the secret key or passphrase, and to compromise the Wi-Fi Access Point (WAP). Three main types of procedures are as follows:

1) *Scanning the Data Passively:* In this procedure, the attackers usually make their way through the radio channels of mobile devices to sniff the data. Passive scanner observes the network packets and builds the network model with a set of active hosts in the network. While observing the traffic patterns, if User Datagram protocol is encountered, it updates the existing network model with the monitored hosts sending UDP packets in the network. The attacker scans the data passively and sniffs the data being communicated over Wi-Fi. Hacker collects all the information during scanning and attempts to decrypt the secret data by different methods.

2) *SSID Detection:* SSID means Service Set Identifier. It is used to carry out different set of rules and modules of the network. Scanning of the transmitted data passively is followed by detecting the SSID in that wireless network. SSID works with different frames. Most of the attackers use multiple access points where SSID is coupled with Beacon frames. These frames have by default some value and if it is not set to zero then it would be trouble-free for the attackers to recognize the SSID for sniffing thereby leading to successful Wireless Network Sniffing.

3) *MAC Address Collection:* Detection of SSID is followed by MAC Addresses collection using the data scanned passively and different types of software for sniffing the network. This step is required for the following two purposes:
   i) To conceal the identity and access points from the attackers.
   ii) To prevent the unauthorized laptop/mobile phones accessing the Access points. The devices registered with MAC address alone access.

The following are the open source tools available for capturing the packets, sniffing, and attacking:

- Wireshark [4]
- Silica [5]
- Backtrack(Linux) [6]

The captured packets as shown in Figure 2 can be further intercepted using tools like silica hacking tool, cloud cracker tool, etc., to decode the encrypted data.

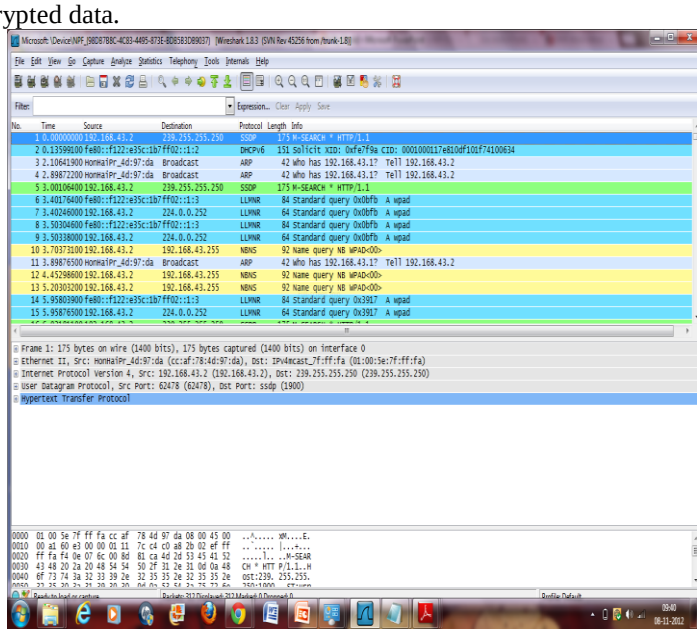


Fig. 2. Packets Captured during Mobile Communication

A.2. Bluetooth:

Bluetooth is one of the easiest ways for an attacker to access the confidential data on the mobile devices. There are two well known attacks possible on mobile phones viz., Blue Snarfing [7] and Blue Bugging [8].

1) *Blue Snarfing:* It is a method of Bluetooth attack where the attacker secretly gains access to the mobile devices. This results in attacker taking control over the mobile device and retrieving information such as addresses, passwords, etc.
2) *Blue bugging:* It is a method of taking control of the mobile device with Bluetooth. Issues authorized commands and access information without the knowledge of the mobile user. Attacker can send and receive SMS or MMS, use the internet, tap phone conversations, etc.

A.3. SMS or MMS Malware:

Malware is a malicious software or malicious file. It causes harm to the system in which it resides. Virus, Worms, and Trojan horse are all malware threats. These threats spread to the mobile phones as infection through SMS (or) MMS (or)

Email (or) Applications. Some of them infect the registry (or) libraries of operating System and some files replicate into multiple copies. After infecting the system, the damage may be in monetary terms by accessing personal finance information of patients (or) doctor (or) by manipulating the critical information regarding patients health conditions such as like glucose levels, Blood Pressure, Pulse count, etc. Also, the attacker does concealed damage at the backdoor and spread to other smart phones through Wi-Fi Networks, Bluetooth, SMS, MMS, (or) email. Usually, SMS are sent to mobiles with malicious URL. When the user navigates to that URL, malware gets installed automatically. When files such as document files, excel sheets, MMS messages, (or) spam emails with malicious files are downloaded, the mobile phones are infected losing their confidential data. Some of the malicious threats are cabir (a worm) which infects Symbian OS, Commwarrior (a standalone malicious program) which infects the Mobile phones through MMS, Phage (a virus) which affects Palm OS during synchronization with PC. Red Browser enables phishing attack by allowing the users to visit WAP sites that do not have WAP connections in reality.

III.B. Vulnerability Attacks:

Attacks on Mobile devices in critical health information is also possible because of the vulnerabilities in the mobile phones especially smart phones. In mobile phones, vulnerabilities could be in Web Browser, or Operating System, or while Downloading Applications.

1) *Web Browsers:* Attacks through web browsers are becoming the budding targets. Similar to normal web browsers [9], mobile web browsers also have plug-ins and widgets installed. Web browser acts as a source for phishing attacks, malicious website access, etc.
2) *Operating System:* The mobile phones used in hospitals are smart phones with advanced features. These phones may have different operating systems such as Android, Apple iOS, and Nokia's Symbian OS. By changing the firmware Operating System, the smart phones are prone to attacks. Jail breaking of the OS is another way that makes the Mobile phones prone to attacks. Jail breaking is the process of removing the restrictions (or) limitations of the firmware by mobile phone users (e.g. APPLE iPHONE).
3) *Downloading Applications:* Jail breaking the operating system (or) firmware allows malicious applications access through web browsers. Some applications initially tend to be genuine. Later, after gaining popularity, attackers couple malicious codes with application updates. With the help of these malicious codes, attackers easily access the critical data.

III.C. Individuals:

The attackers are always not proved to be outsiders. Attackers may also be the insiders [9] viz., organizations personnel. The access privileges to the critical information are defined for all the employees and doctors in hospitals. The authorized information viz., passwords, usernames, MAC addresses may be sold to attackers in exchange of money, or some other benefits leading to critical data leakage or loss. Further, the data may be manipulated by the attackers to cause a severe threat to patient's life or to deface the popularity of the hospitals. This cause harm for the critical health information by compromising security goals viz., integrity (unauthorized access), availability (denial of service by manipulating the clinical information and taking control over medical systems) [10], and confidentiality (the personal information of patients and their medical records can be accessed and manipulated). It's not alone the employees working inside the organization do such harm. Also, the employee fired by the management who has entire knowledge on the WIFI network and hospital data center can leak the information to the competitors or third parties for monetary benefits or for personal vengeance. This is a serious threat to the hospital database system.

IV. Security Policies for Prevention of Attacks

IV.A. Security Policy for Network Attacks:

Network attacks include Wi-Fi Sniffing, Bluetooth Attacks, SMS or MMS Malware Attacks. These attacks can be prevented if the following policies are defined in the hospital management system:

1) Strong Encryption protocol such as WPA2 must be enabled in Wi-Fi access point. Hence, Wi-Fi sniffing could be prevented.
2) Unique passwords must be used for different accounts and should be changed every one month.
3) Only MAC registered mobile phones, smart phones, or laptops must be allowed to access the hospital Wi-Fi network.
4) SSID key should be strong enough that it should not be deciphered easily by attackers.
5) Remote management passwords will be different to the different user accounts viz., Administrator, Admin, Root, etc.
6) Assigning security equivalences that give one user the same access rights as another user will be provided wherever possible.
7) Switching on the Bluetooth signal only when needed. The policy ensures the Bluetooth may not be misused by the attackers.
8) Intrusion Detection System (IDS) must be deployed between the Gateway and the Hospital Data center. This ensures the filtering of unwanted traffic (or) unauthorized access. Also, to detect the anomaly traffic (deviation from normal traffic), IDS is used.
9) Spam filters must be used in Mail server to prevent the e-mail phishing and spamming attacks.

10) Do not accept any devices for pairing without any verification. Smart phones used by doctors should be password protected.

IV.B. Security Policy for Vulnerability Attacks:

Vulnerability attacks include attacks based on web browsers and attacks based on operating systems. These attacks can be prevented if the following policies are defined in the hospital management system:

1) Operating system installed in hospital servers must be kept up to date and patched on regular basis.
2) Antivirus and Firewalls should be installed in Hospital servers and clients. The policy ensures the prevention of Root kit (a type of software which is used to hide the processes), virus, worm, etc.
3) Smart Phones must have sandbox mechanism where the malicious files can't be executed out of the sandbox. For example, Android mobile phones use sand box mechanism which helps in process isolation of malicious files from normal files.
4) Only the applications recommended by the manufacturers of OS such as APPLE, GOOGLE, and Nokia must be used. The policy prevents downloading the applications that consists of malicious codes.
5) One should not navigate to suspicious URLs. An application that seems to be attractive must not be downloaded. The policy ensures the prevent of malicious application downloading without the user's knowledge.

IV.C. Security Policy for Insider Attacks:

1) A centralized trusted personnel must be monitoring the network traffic within the Health Care Information System using Traffic Analyzer and Monitoring software.
2) If an individual is leaving the organization, then all his/her authorized access to every source of information within the system must be closed.
3) Insider attacks are caused because of the dishonest individuals of the organization. In order to prevent this attack, individuals of the organization must be trust worthy.
4) Direct root access will be limited to root console only.
5) Secure Shell (SSH), File Transfer Protocol (FTP), Telnet services will be restricted to authorized staff only.
6) LAN equipments, hubs, switches, routers, etc., must be kept in secure hub room and access to the rooms is restricted to authorized staff only.
7) Access to system console and hospital server disk/tape drives must be restricted to authorized staff only.

V. User Awareness

Users must be aware of the attacks and the rate of damage they cause to the critical information. Smart Phones must be protected by the user always which can be achieved by following security software measures such as fingerprints, or voice recognition, or through other biometrics. Mobile Phones must be locked using strong passwords preventing the unauthorized access of data. The following are the three main reasons for the users of Health care systems failing to recognize the vulnerabilities:

- Use of obsolete hash algorithms for encrypting passwords
- Storing the password on mobile devices.
- Using common key for encryption of data during communication over the Wi-Fi networks.

VI. Conclusion

Securing the critical healthcare information is achieved by preventive measures. Attacks on the mobile devices are done through the individuals of the organization by compromising the security goals such as integrity, confidentiality, and availability of the data. Manipulating the clinical information by gaining access over the network through mobile devices leads to improper treatment of the patient. If the attacker intrudes the Health care system, he can take control over the servers operating medical devices and disable the services leading to the Denial of Service attacks. Survey conducted by International Data Group(IDG) reveals that the wireless network implementation is done at the hospitals to access the electronic medical records(EMR) of the patients and to check the medication given to the patient by doctor. In order to overcome all the above problems, the Health care information system must clearly define the security policies a priori to prevent the critical infrastructure from internal and external threats. The policies mentioned in this paper are mandatory to protect the hospital's physical and Information Technology (IT) assets and to prevent the services from mobile based attacks. These policies do not ensure 100% security against zero-day attacks. Nevertheless, it requires update in the policy from time to time depending on the requirements and new technology applications.

REFERENCES

[1] SiteOnMobile a software solution that provides communication medium for rural area patients with doctors (http://www.technologyreview.in/biomedicine/27087/)
[2] "Mobile Device Threats in health care" (http://threatpost.com/en_us/blogs/dhs-warns-about-threat-mobile-devices-healthcare-051612), 16, May 2012.
[3] Security Policies Example (http://eval.symantec.com/mktginfo/enterprise/white _papers/bsecurity_and_privacy_for_healthcare_WP_

20934020.en-us.pdf)
[4] Wireshark (http://en.wikipedia.org/wiki/Wireshark, http://www.wireshark.org/)
[5] Silica tool (http://www.techweb.com/news/231600414/undefined, http://forums.cnet.com/7726-6132_102-2397372.html)
[6] Back Track (http://www.backtrack-linux.org/)
[7] Blue Snarfing (http://en.wikipedia.org/wiki/Bluesnarfing)
[8] Blue Bugging (http://en.wikipedia.org/wiki/Bluebugging)
[9] Attack Surface: Healthcare and Public Health Sector (http://info.publicintelligence.net/NCCIC-MedicalDevices.pdf)
[10] Wireless at the hospital and the threats they face (http://www.sans.org/reading_room/whitepapers/wireless/wireless-hospital-threats-face_33003)

