Security of Mobile Communications in the Medical Setting

Hannah Clark

14 December 2015

Cell phones, particularly smartphones, are omnipresent in our way of life and offer significant advantages in speed, ease, and variety of formats of communication over earlier technologies. This could help provide great improvements in the ability to care for patients in large medical practices and facilities by allowing staff to be contacted or notified of important updates in a patient's status or care more effectively and efficiently than possible with devices such as pagers.

However, any new technology opens up new ways for information to be leaked or left vulnerable. In the medical field especially, the security of information such as patient medical records, is paramount. Improvements in care through better communications could actually be very detrimental if the information contained in them were to be accessed by an unauthorized entity, both for the patient and for the practice or facility.

I will analyze the technologies used as well as technologies likely to be considered, both on lower and higher levels of technology, for medical communications in larger practices and facilities for the level of security they provide. This will include the communications technologies and corresponding protocols which allow for real time updates and are used in smartphones, particularly with iOS; more basic cell phones; and devices such as pagers. With this information, it will be possible to see whether security concerns are low enough that better communication and the benefits it comes with can be used.

1 Introduction

In most settings, pagers are a technology long past their prime. However, they are still widely used for communications in hospitals and other large

medical facilities. Since cell phones, and more recently, smartphones have become ubiquitous in other professions and areas of life, we must wonder why the medical world clings to the older technology.

Pagers, the precursor to cell phones, rely on radio to receive messages, and typically cannot send a response. Two way pagers exist, but we will not consider those for the purposes of this paper. There are a number of options for type of message: tone only, voice, numeric, and alphanumeric. While a pager is capable of holding multiple messages, there are significant limitations on both the number of messages stored and the total amount of data stored.[1] There are a variety of protocols for message transmission, with FLEX being the most popular protocol when pagers reached their peak usage.[2] FLEX is a time based protocol, where devices are assigned a frame of the transmission cycle in which to receive their messages that is used to determine whether a message is actually meant for a given device.[3] An alternative method of device identification is demonstrated by the POCSAG protocol, which includes a device code in the preamble transmitted before the message to identify the intended recipient.[4]

Despite the limitations of one way messaging and message storage capacity, there are benefits to choosing pagers for communications in the medical setting. Cell phones often have poor reception in hospitals, but pagers work quite well. In addition, in emergencies when cell service may not be available or the networks over loaded, pagers generally still function well. On the other hand, the limitations could be quite costly, both in lost productivity for medical personnel and in longer discharge times for patients.[5]

Cell phones, allowing two way communication, could potentially reduce those losses and have been widely adopted in place of pagers precisely due to improved communication. Cell phones also rely on radio, communicating with a transceiver via radio signals. Both voice calls and text messages, or SMS, are transmitted to these transceivers through relatively low power signals before being routed to the appropriate transceiver or phone network for the destination phone through switching stations.[6] The two-way real-time nature of cell phone communication can reduce delays of needing to find a phone to respond to a page. In addition, cell phones can receive more data in a coherent form than a pager can, allowing more detailed communications for doctors to decide how to respond to requests. However, we cannot ignore the previously mentioned drawbacks of poor performance in hospitals or during emergencies.

Smartphones, or cell phones with more advanced capabilities, pose an even wider variety of real-time communication methods with their capacity for internet access. Aside from traditional voice calls and SMS, smartphones

can send data over the internet for either text or voice message, as well as receive notifications through push notification services. For the purposes of this paper, we will consider options available for iPhones specifically, including basic secure communication with a server to implement secure text messaging, secure implementation of VoIP, and the Apple Push Notification service, or APNs.

Text messaging can be implemented either using standard HTTP or HTTPS protocols with the standard networking libraries in the iOS SDK or using the Websocket protocol through those libraries or third party libraries. The HTTP or HTTPS protocols allow for a program to receive near real-time updates through polling. Websockets allow for real-time updates without polling to reduce unnecessary network traffic and have the same security or authentication available to HTTP protocols.[7] An additional option for sending text messages is push notifications. These use a service that will pass notifications from a provider to a specified device. Rather than the device polling a server directly, a server with a valid certificate for APNs sends notifications to the APNs server, where it is stored and passed to the correct device when the device connects to the service.[8]

VoIP allows for voice calls using internet rather than, or in addition to, traditional phone networks. The process of making a call relies on a request-response framework similar to HTTP, with stages such as dialing, ringing, answering, etc. defined as requests and responses,[9] and the actual conversation is transmitted by converting voice recording to and from digital signals that can be separated into small packets that travel over the internet.

Due to the reliance on internet, all of these options, despite their benefit of providing real-time options for communication, cannot be solely relied upon in case of emergency. In some emergencies, it is highly likely that internet connections may be down, making these techniques useless. Because each technology has benefits and drawbacks, this paper will not attempt to proscribe a single technology that should be used, but rather determine how to securely use each device that could be chosen with regards to patient information and determine which the most viable options through that information. These will be determined by the ability to sufficiently safeguard personal information that could be reasonably be expected to be transmitted over networks used for each technology and information that could be stored or accessed through access to the device.

2 To The Community

Receiving critical medical care in a timely manner can be a life or death matter. To be able to accomplish this, doctors need to be able to receive all relevant information as quickly and efficiently as possible to make the best possible decisions. Pagers can clearly be a hindrance here. They can notify a doctor who is needed somewhere, but they cannot supply as much additional information right away so a doctor may prepare enroute and therefore somewhat waste the doctor's time. To get additional information, the doctor would need to find a phone to contact whoever paged them, and the wait to get the information over phone before the doctor could continue on their way to the patient. The wasted time has been estimated to be 45 minutes of lost time for staff due to communication using pagers, resulting in discharge times of 101 minutes later, although these numbers may be higher than the actual times due to bias in the study.[10]

More modern mobile communications devices, such as cell phones or smartphones, can overcome those hindrances. Both allow real time two way communication, preventing the need to stop and find a phone to ask for more information. In addition, the information that is conveyed up front can be a much larger quantity because even if individual messages still have size limitations, the number of messages that can be received and stored is larger and the organization of stored messages makes it easy to determine which go together. By the reasoning of improved quality of communication, cell phones or smartphones should replace pagers. However, improved communication has important ramifications for privacy and information security.

The improved scale of information that real time notifications can include with cell phones and smartphones means that if the device or the security of the communication channels is compromised, more information can be released. This increases the likelihood of the message containing details about the patient and their health or treatment being included, given that they can be important to convey the type or urgency of a notification to the doctor. This is of concern to both patients and medical staff. If a breach occurs, where patients' personally identifiable information (PII) or personal health information (PHI) is released, then the facility could be be forced to pay large settlements fines or to implement corrective measures possibly at great expense as a consequence, as Lahey hospital has been ordered to do.[11] The patient must also be concerned if some of the information could be used against them, either in relation to their continued health or their finances, such as identity theft. To truly be able to benefit from improved technologies, the security risks must be understood and mitigated to prevent

causing harm while attempting to reap the benefits of the technology.

3 Action Item: Securely Using Pagers

3.1 Transmissions

For POCSAG pagers, it is very easy for an attacker to listen in on messages sent over the system. Because messages are sent to all pagers, although only read by a pager with a matching device code, it is possible to pose as any device on the network and read the messages by simply using a modified device, not necessarily a pager, that can access the network by receiving the radio signals and that uses a decoder that accepts all device codes. It is also possible to build a or program device that will intercept and read FLEX messages. There exist several sources online that give the specification of the FLEX or POCSAG protocols, allowing anyone with sufficient technical knowledge to build or program a device that could listen in on such a pager network. However, the typical use case for pagers is generally to alert staff to make a call or report somewhere. Neither of those types of messages includes PHI or PII, so while it still is not particularly desirable to let someone listen in on the paging network, it does not compromise patient data if paging messages are read by others in transmission as long as those are the only types of transmissions.

3.2 Device Security

Access to a device will give all of the information that the device contains. However, because the main use case of a pager is alerting a doctor to either make a phone call or to go somewhere, with minimal space for detail, the messages once again typically will not compromise PHI or PII of patients. Therefore, access to a device is of minimal concern, at least in terms of information that could be accessed. In addition, if a device is lost or stolen, it is very easy to stop messages being sent to it by notifying those with the ability to send a message to not do so. Overall, while the information sent to pagers is easily accessed, pagers are easy to securely use because it the use case generally does not involve including PHI or PII in messages. As long as the messages sent do not include such data, which they are unlikely to anyway, then pagers can be securely used, at least in relation to patient data.

4 Action Item: Securely Using Cell Phones

4.1 Transmissions

There are several possible ways to access the transmissions of a cell phone, for either voice or SMS communications. The actual methods to do this vary based on the type of network used by the cell phone carrier, generally GSM or CDMA. CDMA phone transmissions could until recently be intercepted by using a device called a femtocell, a device meant to boost a carrier's signal, although companies running such networks claim to have fixed the problem.[12] For GSM there is the alternative of an IMSI-catcher, which can intercept transmissions by tricking devices into believing it is a cell tower and which is not detectable by most phones.[13] The only way to avoid an IMSI-catcher is to use a device that can typically detect when a phone is connected to the IMSI-catcher instead of the true transmission tower, such as the very expensive CryptoPhone.[14] Even this is not foolproof, as there are IMSI-catchers that are claimed to be undetectable, although these are intended for government use.[15] With these technologies available, it is not possible to be certain that transmitted information is secure, therefore, to use them securely, no PHI or PII should be transmitted.

4.2 Device Security

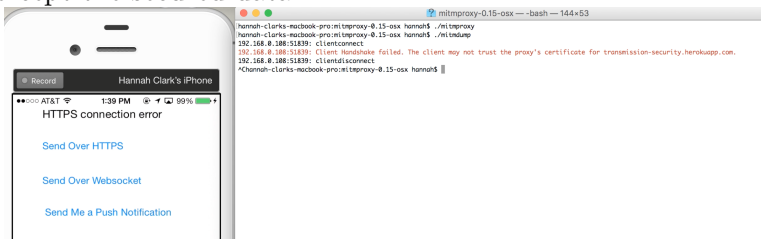
If a device can be physically accessed by an attacker, then the attacker likely has full access. The earlier devices that we are mainly considering in this section could not be passcode protected, allowing anyone to see what is stored on it. To prevent PHI or PII from being compromised, no such information must be transmitted to or stored on the device.

5 Action Item: Securely Using Smartphones

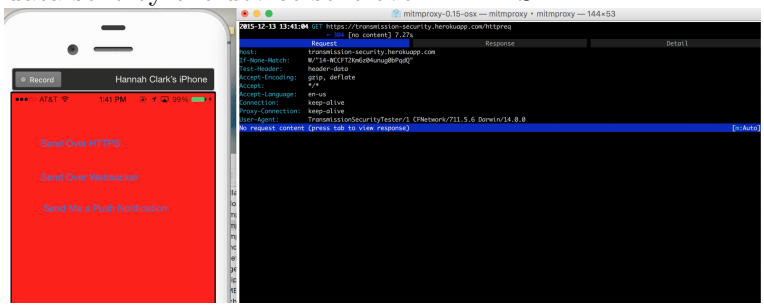
5.1 Communication over HTTP(S) and Websocket

For the communications over internet, we will assume a wifi network is being used instead of a cell phone data network to avoid the security risks from such networks. In addition, we will not directly consider how secure the wifi network, but rather how to secure the data transmissions from the smartphone. If data is sent over the internet using HTTP or a Websocket that does not use any encryption, anyone launching a man in the middle attack or sniffing network packets will be able to read it. However, it is possible to send data over the network in an encrypted form, using HTTPS

or ensuring that the Websocket connection uses TLS. The packets will be encrypted, so while they still may be intercepted with packet sniffing, they cannot be read without the correct private key to decrypt them. Man in the middle attacks, or the use of a proxy to intercept requests, may still be a problem. To test this, we used an iOS application that sends data using HTTPS and encrypted Websocket as the target and mitmproxy and mitmdump to perform the attack for HTTPS. After setting the machine on which mitmproxy was running as the http proxy in the device settings, we began to see HTTP and HTTPS network traffic from the device. When done without loading any certificates onto the device, we are not able to intercept the secured data.

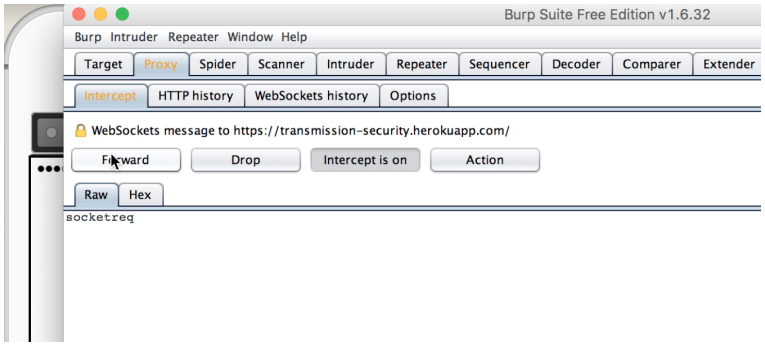


However, when a certificate was installed on the device, we were able to see data sent by the device sent over HTTPS.



Because directly setting a proxy only works for HTTP and HTTPS due to the limits on using proxies in iOS, we needed to alter the experiment for Websocket. To do this, we used DNS spoofing through Metasploit's fakedns to make the device believe that server was a different machine, which allowed that machine to receive traffic sent. This required changing the DNS settings in the phone's network connection, as well as being aware of the port the device was attempting to connect to, which could be determined by packet sniffing. To receive information that was being sent to the machine, we set up the Burp Suite proxy to listen on that port. The proxy then received all the information sent over the Websocket connection.[1]

[1]For more details on the technique used, visit https://blog.netspi.com/intercepting-



To be able to transmit PHI and PII safely, attackers must be prevented from being able to load files onto the device, as well as somehow force the device to use a proxy. The best way to prevent this is through policy on what the device can be used for. If there is no email or other applications that could receive such files installed and if the user does not access anything on the internet which would allow such files to be saved on the device, then the device should be safe from such an attack. DNS spoofing must be prevented on the network level as well, so there should be policy such that if followed, it is not feasible for attackers to access the network. To securely use HTTPS or Websocket communication, encryption must be used and there must be a sufficient policy that will prevent the users of the device from unintentionally allowing attackers to bypass the encryption on the transmissions.

5.2 VoIP

The VoIP also provides for using TLS to secure the transmission of information.[16] Therefore, information that is sent over the network using a VoIP service that correctly implements a TLS connection should be as secure as communication over HTTPS, as long as the same precautions are taken.

5.3 Push Notifications

Apple Push Notifications service enforces connection over TLS, so the transmissions between server and APNs and between APNs and the device are as secure as long as proper precautions are taken against man in the middle attacks. There is the secondary consideration of a device receiving push notifications meant for another device. APNs uses a token generation system where a token is created using the device token created from the device's certificate the first time a device connects to APNs. The token is used

native-ios-application-traffic/

in subsequent connections and must match the connecting device.[17] Thus, a device would have to be identical to another to receive notifications for that other device. In addition, the device token must be provided when the provider of the notification sends the notification to APNs,[18] which makes sure that the message will be delivered to the correct device when it checks. The requirements for securing push notifications are therefore the same as for the other transmission methods using internet.

5.4 Device Security

It is possible for patients' PHI or PII to be stored on a smartphone. Therefore, the security of the device itself is an important factor of the security of this communication option. The first level of security is preventing anyone who gains access to the physical device from being able to immediately access information stored on it. This can be done through a passcode. While it can be guessed, this slows down the attacker from having immediate access to the data. On recent versions of iOS, the passcode capabilities include passcodes of well into the double digits or possibly higher in length and which may be composed of alphanumeric and special characters. This allows for very strong passcode, based on brute force abilities for those lengths and character sets. To extend the time needed for brute force or other guessing attacks, there is a time delay between passcode entry after a threshold of incorrect entries.[19] To avoid access without passcode entry, the user files, where data for apps is stored, are encrypted.[20] After a device has been identified as lost or stolen, data can still be protected by using the ability to remotely wipe user information from the phone.[21] With a passcode and the other precautions in place and correctly utilized, a breach due to a lost or stolen device has minimal likelihood of occurring. The other consideration is the ability to install software on the device which could access the information. However, this is easily countered by not installing additional apps, or only installing apps on a known safe list. Overall, the security of the device itself is sufficient that breach due to access to a device is not likely, as long as the passcode itself is kept secure.

6 Conclusion

On examining each technology, we can see that there are different risks associated with each. The messages sent from pagers can be seen by attackers with comparatively little trouble. Cell phone communications can also be

intercepted, although the devices needed to do so can be more costly. Because of this, the only way to protect PHI or PII when using those devices is to not include it in any communications sent using such devices. Since the same restrictions are placed on cell phones as pagers, they only minimally expand the communication abilities of doctors. In addition, because cell phones are not as reliable as pagers for emergency communication, pagers may actually be the better choice between the two.

Smartphones, however, and their internet capabilities, allow for a dramatic improvement in communication. Data transmitted, as long as it is over wifi so it cannot be intercepted in a manner similar to cell phone transmissions, has sufficient protections to allow it to contain PHI or PII, as long as certain policy is in place. Because loading a certificate for a proxy for a man in the middle attack onto the phone will allow the data transmitted to be intercepted, there must be policy about the use of the device that will prevent unknown files from being loaded onto the device, such as through email. Sufficient policy, as well as being sure to use TLS encrypted connections, will allow for communications to include PHI or PII, so smartphones can be used to save doctors time by allowing these communications. This policy must ensure that users do not load any additional files aside from those of approved applications or approved websites so that attackers cannot place the needed files on a device to be able to intercept the data in an unencrypted form. Beyond that, the policy must cover network security and general device security ,such as sufficient passcodes, ability to and when to use remote wipe features, and guidelines about who may access a device and what networks they may connect to. If all precautions are taken, the possibility of a breach is quite low. Smartphones using communications over the internet can safely replace the pager for medical communications in most circumstances, given proper precautions, although there are additional concerns beyond security before a decision to substitute the phones for pagers can be made.

Notes

[1]Michalas, Yianni, and Leandros Tassiulas. "Paging System Design Issues and Overview of Common Imaging Protocols," 2-3. July 15, 1998. `http://www.ee.umd.edu/~leandros/papers/pagsys.pdf`

[2]Gonzales, David Ruimy. "FLEX Protocol Delivers De Facto Messaging Standard for Handhelds." EE Times, July 25, 2000. Accessed November 10, 2015. `http://www.eetimes.com/document.asp?doc_id=1275957`.

[3]Michalas. "Paging System Design Issues and Overview of Common Imaging Protocols," 11.

[4]Michalas. "Paging System Design Issues and Overview of Common Imaging Protocols," 7.

[5]Kopytoff, Verne. "Where Pagers Haven't Gone Extinct Yet." Fortune, July 16, 2013. Accessed November 9, 2015. http://fortune.com/2013/07/16/where-pagers-havent-gone-extinct-yet/.

[6]Miller, Michael, *Wireless Networking Absolute Beginner's Guide*, 56. Indianapolis, IN: Que Publishing, 2013. http://www.quepublishing.com/articles/article.aspx?p=2021961.

[7]"About HTML5 WebSockets." WebSocket.org. 2013. Accessed November 2, 2015. http://www.websocket.org/aboutwebsocket.html.

[8]"Local and Remote Notification Programming Guide." IOS Developer Library. Last modified October 21, 2015. https://developer.apple.com/library/ios/documentation/NetworkingInternet/Conceptual/RemoteNotificationsPG/Introduction.html\#//apple_ref/doc/uid/TP40008194-CH1-SW1.

[9]Rosenberg, J., Schulzrinne, H., Camarillo, G., Johnston, A., Peterson, J., Sparks, R., Handley, M., and E. Schooler, "SIP: Session Initiation Protocol", RFC 3261, DOI 10.17487/RFC3261, 13. June 2002. http://www.rfc-editor.org/info/rfc3261.

[10]Kopytoff. "Where Pagers Haven't Gone Extinct Yet."

[11]"HIPAA Settlement Reinforces Lessons for Users of Medical Devices." U.S. Department of Health and Human Services. Last Modified November 25, 2015. http://www.hhs.gov/about/news/2015/11/25/hipaa-settlement-reinforces-lessons-users-medical-devices.html.

[12]Rashid, Fahmida. "Black Hat: Intercepting Calls and Cloning Phones With Femtocells." PCMag, August 1, 2013. http://securitywatch.pcmag.com/hacking/314370-black-hat-intercepting-calls-and-cloning-phones-with-femtocells.

[13]Storm, Darlene. "Are your calls being intercepted? 17 fake cell towers discovered in one month." Computerworld, September 2, 2014. http://www.computerworld.com/article/2600348/mobile-security/are-your-calls-being-intercepted-17-fake-cell-towers-discovered-in-one-month.html.

[14]Storm. "Are your calls being intercepted? 17 fake cell towers discovered in one month."

[15]Storm. "Are your calls being intercepted? 17 fake cell towers discovered in one month."

[16]Rosenberg. "SIP: Session Initiation Protocol," 141.

[17]"Local and Remote Notification Programming Guide."

[18]"Local and Remote Notification Programming Guide."

[19]Apple. "iOS Security: iOS 9.1 or later," 12. Last Modified September 2015. https://www.apple.com/business/docs/iOS_Security_Guide.pdf.

[20]Apple. "iOS Security: iOS 9.1 or later," 4.

[21]Apple. "iOS Security: iOS 9.1 or later," 10.