6-1-2016

Security and Privacy Analysis of Medical Wearables

Brian M. Chalif
Dartmouth College

Brian Chalif
Thesis Proposal
Dartmouth Computer Science Technical Report TR2016-805
Advisor: Charles Palmer

Security and Privacy Analysis of Medical Wearables

Abstract

The release of Google glass and the Apple and Samsung smart watches in the past two years pushed wearables to the forefront of technology. The realm of medical wearables will specifically see a huge growth as wearables become more common place. There are documented cases of security and privacy breaches in the five main potential breaching areas: wearable device itself, Bluetooth communication, smartphone or personal computer app, Wi-Fi data exchange, cloud storage. Privacy policies for individual wearables are not always in the best interest of the individual and government regulations on wearables security does not always fully vet wearables. Interviews with industry professionals, both clinical and research, concluded that doctors are not very knowledgeable about wearables and are not very worried about security, the public does not understand security of these devices, and the security concerns should not stop the progress that is being made in this field.

Introduction

Wearables are here. Wearables are the future. The release of Google glass and the Apple and Samsung smart watches in the past two years pushed wearables to the forefront of technology. Wearables extend beyond glasses and watches to include medical devices, sports analysis, clothes, bio-infused, military, big data collection, and much more. With these new technologies come new security and privacy issues.

As was shown with the invention of portable phones, security measures and protocol change as technology becomes more advanced. At first no one cared. Then phones were able to take pictures and use the Internet, both presenting security issues, which translated to policy changes with in secure environments. In the coming years, as wearables become more prevalent on a day-to-day basis, there will be changes to security protocol in the private sector, in companies such as IBM, Google, and even airline companies, and also in the public sector in all classified government business. These security issues are more clear, however the opposite end is much less clear: the security and privacy of the user. With the onset of

wearables, users will have tons of personal data that could be intercepted, changed, or deleted.

This will become especially important for medical wearables. There needs to be clear security standards, in order to ensure that medical wearables are secure. Users do not want these devices to be large and clunky, but also want them to be secure, presenting difficulty in design. These devices can be responsible for not only the day-to-day, but also the minute-to-minute or second-to-second health of the user so it is crucial that they are secure. The future of wearables will be heavily in the medical realm, as devices are being used now to early diagnose chronic conditions such as congestive heart failure, as well as measure chronic diseases like diabetes. According to IDC report, consumers will buy nearly 112 million wearable devices in 2015. A 78.4% increase from 2014 sales. Most gadgets will be health related [1].

This paper will briefly discuss the history of wearables and medical wearables. Then I will discuss possible security and privacy breaches in five different areas: wearable device itself, Bluetooth communication, smartphone or personal computer app, Wi-Fi data exchange, cloud storage. There will be a survey of privacy policies in wearables followed by an explanation of the current FDA policy and other regulations and laws**.** The final section is an analysis of interviews with leading doctors and research in medical wearables.

History of Wearables

The start of wearables is up for debate, as it is unclear what technically classifies as a wearable. I will start at the one of the earliest dates with the invention of the eyeglasses in the late 13th or early 14th century [2]. The world's first watch, the Pomander, dates to 1505. In the 17th century Qing Dynasty, a fully functional abacus on a ring was invented that could be used while being worn [3]. (Image 1) The next significant wearable was the invention of the watch in 1868 by Swiss watch manufacturer Patek Philippe [4].

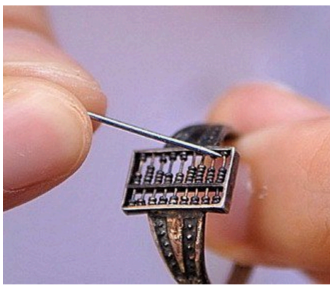

Image 1

Image 2

Image 3

In 1907, German inventor Julius Neubronner attached a camera to a pigeon, which was the earliest form of a wearable that could actually gather data. (Image 3) The first true wearable computer (as we would classify them today) was invented in 1961. Edward Thorpe and Claude Shannon invented a mechanism to time the roulette ball and better predict where it would land. (Image 2). Then it would use radio waves to communicate to the gambler. This was a huge step in wearables, as it was the first time a computer was used.

In 1975, Pulsar created the first wristwatch calculator. It was made of gold, only 100 were made, and cost $3950. It was a huge success and was later recreated in a stainless steal version for a lower price of $550. In 1979, Sony introduced the Walkman, which was the first portable music listening device.

In the 1980's, the mass production of microchips made smaller and lighter computers more easily accessible, opening the door for wearable electronics. Steve Mann (who is often cited as the father of wearable electronics) worked on the EyeTap project in the 1980s. This device allowed the user to see out of one eye while the other eye recorded all information that was coming in. He worked on this project for many years and it became much less bulky over time. This was essentially an early iteration of Google Glass. In 1989, the Reflection Technology Private Eye [5] was released. It was a head mounted display, which used a vibrating mirror to create a visual for the user. Although, never released to the public, it was used in research to build augmented reality to repair equipment.

In 1994, Steve Mann made the first wireless webcam. He recorded content and started uploading the videos to the web, being the first person to do this. In the mid-90s wearables really took a stride and became a clear part of the future of technology. This was evident in Defense Advanced Research Project Agency (DARPA) hosting of "Wearables in 2005" workshop in July 1996. This was a conference to discuss research and see where the field was headed. In 1999 Studio 5050 in NY invented the mBracelet. This was a wireless payment system and the first wrist wearables.

In 2000, the first Bluetooth headset was shipped. In 2004, the first GoPro was released, introducing the first wearables that could record video. The Fitbit was released in 2009, which was the first modern fitness wearable. In 2012, a smartwatch company Pebble, ran a Kickstarter that raised $10.2 million (the most successful Kickstarter to that point). Although not going mainstream, this paved the way for android and apple watches in the future. In 2013, Google Glass was released, which was the first time the user was able to integrate reality and a visual from a computer. In 2014, Tommy Hilfiger released a jacket with embedded solar panels allowing people to charge their phones on the go. This is significant because it is the first mainstream clothing wearable [6].

The future of wearables is in augmented and virtual reality (AR and VR). The Oculus Rift, which has not yet been publicly available, but only available for developers, will bring virtual reality to the public. However, there are endless companies working on AR and VR, from the visual like Oculus Rift to including touch in haptics with the Tesla full body suit. Wearables are increasingly popular in young people. According to a 2014 Forbes article, 71% of 16-24 year olds want wearable tech [7].

Medical Wearables

The beginning of medical wearables can start at the same beginning as normal wearables, with invention of the eyeglasses over 700 years ago. Contacts were first invented in 1887 by A.E. Fick, a Swiss physician [8].

In 1932, Albert Hyman invented the first artificial pacemaker, but it was not until 1958 when the first pacemaker was implemented [9]. Between 1993 and 2009, 2.9 million U.S. patients received permanent pacemakers [10]. Hearing aids started in the 1940s, but it was not until the 1980s that the first mainstream hearing aids were made [11] [12].

However, the more commonly considered medical wearable is a device that can monitor a patient's daily life and return data to help diagnose or monitor health issues. This was envisioned more than 50 years ago, however it was not until the last decade that these technologies have really been implemented [13]. These devices are good for people with chronic conditions that need to be measured for weeks or months at home or in an outdoor environment [14].

In 2003, the Vitatron C-Series was the world's first fully digital pacemaker. This device, unlike previous pacemakers, allowed doctors to download information in seconds. In 2006 brought the first true commercial product came to the market, with Nike and Apple introducing a small wearable to put in a shoe that gathers information on steps, calories burned, intensity of activity, and sleeping habits. This was later encompassed by Fitbit in 2009 [15].

Google Glass is wearable that has been used in some medical situations. One such example is in 2013, Phillips Healthcare displayed patient vitals in Google Glass, so the doctor did not need to turn away from the patient. Google Glass is also used to record surgery for Point of View instruction at a later point. The following devices were all invented in the last few years.

Proteus Digital Health developed an ingestible editable. This is a huge step for wearables, as they had never been ingestible before. The sensor is in pill form and would be taken with other medications. Then the device transmits information, time taken, along with reaction to the medication, such as heart rate, how much rest/activity the body gets to a patch on the patient, which is then transmitted to a app on a phone or tablet. This is the first time a doctor can have quantifiable data on

how patients are reacting to medication [16]. There is also PillCam, which is exactly what it sounds like: a camera pill. It has tiny cameras that enable studies of the health of the stomach and intestinal tract [17].

Quell is strapped to the body to help with chronic pain. When strapped to body, it senses oncoming chronic pain and acts to simulate nerves and black pain signals to the brain [18]. Quell Relief is a Knee brace that has an electrode that adds relief in addition to the normal brace. Valedo Back Therapy is a sensor that is attached to the back while doing exercises. The user completes games, like a video game, and data is collected and analyzed and changes what exercises they need to do to fix back pain [19].

The Zoll LifeVest is a wearable defibrillator. It monitors the patient's heart and warns the patient if they should seek medical attention right away. If the patient goes unconscious, the device delivers an electrical shock to attempt to restore a normal heart beat [20].

Thync is a stick-on that sends waveforms to neural pathways to shift from energetic and calm. There are also embeddable and invisibles, which are either inserted into your body or are a patch that are not visible. One example of this is the skin-like devices that monitor vitals [21].

There are many devices that allow for tracking of vitals, such as heart rate, breathing, blood pressure, temperature, and sleeping habits. This list of companies/devices in this category could go on for a long time, but to name one notable new technology is a new project by Northwestern University and University of Illanois at Urbanna-Champaign [22]. This device is significant because it is only five square centimeters wide, looks like actual skin, and uses a new crystal technology to measure temperature. In the future, they will use the same technology to measure other vitals as well.

Smart Stop by Chrono Therapeutics is a device that helps people quit smoking. It collects data and when the person is craving a cigarette or nicotine, it delivers a medication to the person to curtail the craving [23]. iTBra by Cyracadia is a smart bra that tracks the skin and alerts the possibility of breast cancer [24]. Fitguard is a device that detects the severity in head injuries [25]. There are devices to measure UV exposure, help with center of gravity, provide prosthetic limbs, measure skin temperature (disposable strips), monitor foot ulcers, and track mental health.

In medicine, an increase of patient data from wearables is and will continue to completely change the patient-doctor interaction and save millions of lives. The Institute of Medicine has made a "National Statement of Purpose" in which they identified six key aims for improving healthcare. These all come back to an increase in data to actually improve the situation [26].

Security

Wearables are open to security breaches at many different places, due to the complexity of the device. There is the device itself, the transfer of data to a phone or web app and then the transfer of data to the cloud or device server. I will split the security of wearbales into six sub-sections, as was done in Cyr et all [27]. The five that have potential for security breaches are the device itself (a), Bluetooth communication (b), smartphone or personal computer app (c), app connection to cloud through Wi-Fi (d), cloud storage with wearable API and web service (e). (Figure 1) These five sections outline the main possible areas for security breaches in wearables. The last section will look at policy of individual wearables and see how they may not protect the user's privacy. Each of these sections will briefly discuss general security flaws that could occur, with some specific examples from current wearables.

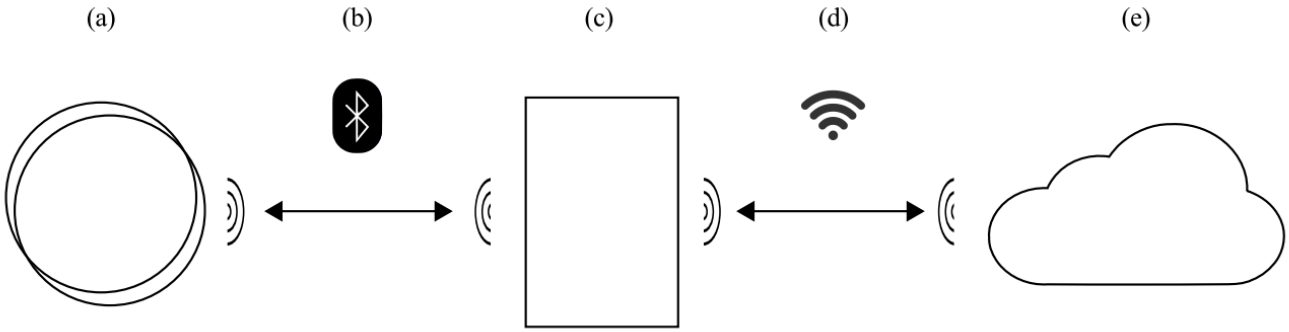

Figure 1. (a), Bluetooth communication (b), smartphone or personal computer app (c), app connection to cloud through Wi-Fi (d), cloud storage with wearable API and web service (e) [27]

i. Device

Medical devices can (and usually do) have long product life cycles. They last longer than operating systems that they run on. MRI machines still run on Windows 95 and pacemakers run on Windows XP [28]. This is problematic, because the software and hardware of these devices need to be able to defend against security issues for many years into the future, let alone the current potential threats.

A study at Princeton showed that a popular commercially available glucose monitoring and insulin delivery system could be hacked. These can be attacked both in a passive and active way. The active way allowed them to impersonate the user and control the medical device and alter the intended therapy. They were able to do this mostly through interception of wireless data, however they were able to send data to the device itself unchecked [29].

A 2008 study led by Kevin Fu highlighted some of the potential security risks with a FDA approved implantable cardioverter defibrillator (ICD), which has been implanted in hundreds of thousand of patients. They were able to reverse-engineer a 2003-model ICD and launch software attacks form a short distance. They were able to extract data (vital signs and medical history), eavesdrop on the communication between the device and the programmer, reprogram the setting that detect abnormal heart rhythms, and keep device in "awake" mode, in order to deplete battery. In the same study they were able to deactivate the device and prevent it from delivering the life-saving shock to save the user. They also were able make the device deliver multiple shocks, which would induce a heart failure [30].

The Stuxnet worm is a worm that crawls through windows machines looking for vulnerabilities [31]. Hanna et al. used this worm to load firmware on to a Cardiac Science G3 Plus Automated External Defibrillator (AED). This is not only dangerous for that one person, but the worm could self-replicate and spread to other AEDs [31].

ii. Bluetooth Analysis

During the Bluetooth connection from the device itself to the web or phone app, there are many areas for security breaches. This can come in many forms. A third part can eavesdrop and see what is being sent. Even if the user can not see what is specifically being sent, because it is being encrypted and secure, the fact that they can see anything being emitted at a constant rate, leaves room for issues, such as possibly changing or altering the data. A malicious attacker could also use a denial of service, where they block the device from sending any new information [32].

Fitbit uses standard BTLE, instead of standard Bluetooth 4.0 protocol. A study from MIT was able to sniff the traffic of Fitbit. This study showed that using Ubertooth suite, all traffic to and from the Fitbit Flex device could be captured. This allowed the capturing of all Bluetooth traffic from initial device pairing to all future data synchs. The Fitbit responded to all Bluetooth broadcasts within range. This allowed the study to obtain the private address of all BTLE devices nearby (mostly being Fitbits). The issue with this is that a third party could track activities of specific users. They could "construct a profile on each user's surroundings and activity patterns. [27]" In addition, they explored a pre-existing vulnerability, in which the key exchange can be captured, exposing the encryption key.

The Princeton study on the glucose monitoring and insulin delivery system also was able to intercept the wireless communication between the device and the app. They were able to obtain the frequency of the device because it is publically available online. They obtained this data and after alterations and analysis they were able to see the data that was being sent in in an 80 bit parsed format. They then were able to detect what information was being sent and what it meant [29].

The 2008 Kevin Fu study on ICD was also able to intercept the data being sent out of the ICD.

iii. Phone or Web App Analysis

The Fitbit android app was picked apart by the same MIT study to search for possible security issues. After decompiling the app, there is a feature called "live data mode", which is a metric when the application displays live metrics. This information was unencrypted. This live data, when encrypted, is nearly identical to the un-encrypted data, meaning that it does not use randomized encryption [27]. They were even able to go in and change this data. This did not translate to the server, however it did change the data that was visible on the device itself.

iv. Network Connection

Similar to Bluetooth, there are a lot of similar threats with Network connection. Data can be intercepted and spied on, changed or deleted. Using Charles Proxy, MIT was able to track network traffic. During the pairing process of the Fitbit and the phone, the app did post in the android log a warning message that the app was running insecure content. This is positive that it realized this, however negative because the app did not do anything to stop. It would have connected and therefor been a possible attack vector [27].

CodeBlue, a medical sensor research project based out of the Harvard Sensor Network Lab. This has multiple sensors over the patient's body to monitor various vitals. This device is susceptible to greyhole attacks [33] [34]. This essentially means that a packet that is being sent over the network can be dropped or discarded at a standard rate of a certain number of packets every certain amount of time. This type of attack is hard to monitor, but would result in data being viewed by a third party that should not have access to the data. CodeBlue is also susceptible to Sybil attack. Simply, this attack is when a third party takes on the identify of the source of the data and therefore intercepts the data as it is being sent.

v. Cloud Storage

For the purposes of this paper, I chose not to write about cloud storage, as it is really less about the wearable devices themselves, but rather more about security in cloud storage. More can be read about in regards to cloud storage computing in the following citations: [35-40]. There are a ton of concerns with cloud storage, and all this data in the cloud is something needs to be taken care of.

vi. Company Policy

When using a wearable, users sign a privacy policy or terms and conditions. These are often long, wordy, and not read by the user. I will discuss four wearables: Fitbit, Jawbone, and BASIS [41].

Fitbit users have no right to the privacy of their data because to use the device, users agree to Fitbit's terms and conditions, which give Fitbit the power to "use and commercially exploit any text, photographs or other data and information you submit to the Fitbit services". In addition, users "waive any rights of publicity and privacy" to data that is submitted to the device [42]. This results in the Fitbit user having little to no right of their own health data. In addition, Fitbit, records the user's GPS location, unless opted out.

Jawbone uploads the user's profile to a publically searchable directory. This includes user information, along with a picture. The device also collects a lot of other data from the user, including full name, photo, gender, height, weight, date of birth, GPS location, contacts, and calendar information [43]. The user has the right to delete this data, however it is unclear if this data is then deleted from the Jawbone server.

In BASIS's terms and conditions, they state, "all biometric data shall remain the sole and exclusive property of BASIS Science, Inc." [44] BASIS includes time-stamped heart rate, skin temperature, ambient temperature, galvanic skin response, and accelerometer measurement all as biometric data. They have the right to do anything they want with this data, include use it for commercial purposes, such as selling it for marketing or sales use. BASIS also contradicts itself in the terms and conditions and the privacy policy: "we keep all your information confidential and encrypted" [45], contradicting the privacy policy, "we do not encrypt data in our database" [46].

These three wearables lead to a few important conclusions. Users do not know how much power the wearable company has over their data. In the three wearables discussed in this section, none allow for the user to completely remove their data. The other, BASIS, has exclusive right to the user's data. Two of the wearables have the right to use the data for other purposes, such as sell the data. Only Jawbone lets user retain control of and have the rights to their own data. BASIS lets staff have access to and view user data.

The significance of this is that after all of the previous five sections, even in an appealingly secure system, the user does not often have control over their actual data. They may have no control or partial control, but in none of the three discussed here, does the user have close to complete control of their own medical data.

Laws and Regulations

I will only discuss United States policy, as it varies widely by country. The two main healthcare policy are the American Health Insurance Portability and Accountability Act of 1996 (HIPAA) [47] and the Health Information Technology for Economic and Clinical Health Act (HITECH) [48].

HIPAA requires comprehensive data security. This includes security and confidentiality (patient health information is secure), providing protection against any infringement of security, confidentially, and integrity, protect against unauthorized access/usage of patient information [49, 50]. HITECH addresses the increase in information technology in healthcare, specifically in storing, capturing, transmitting, sharing, and using patient health data. It states that the people who manage patient health information should notify the patient if there is a breach in their data.

The other big regulation on medicine, specifically for wearables, is the FDA's Center for Devices and Radiological Health. The CDRH's broad mandate is to "protect the public health in the fields of medical devices." However, in 1997, this became harder to accomplish due to the passing of the Medical Device Modernization Act, which had an objective of streamlining the device approval process. The big problem with the passing of the MDMA is that the FDA has differed most of the regulation onto the businesses and companies building and selling the devices themselves. The companies set up their own safety testing and protocol [30].

On the FDA's website, section 21 of the Quality Standards regulation even states, "it is the responsibility of each manufacturer to establish requirements for each type or family of devices that will result in devices that are safe and effective, and to establish methods and procedures to design, produce, distribute, etc. devices that meet the quality system requirements." This is concerning because it is giving almost all the power in regulation and safety to the companies developing the products. As for-profit companies, these companies want to make money, therefore it is not in their best interest to spend large amounts of resources on security, besides the minimum needed.

There is regulation for certain devices. For instance the 1976 amendment to the Food, Drug, and Cosmetics Act required different amounts of FDA inspection, depending on the classification of the device. A device that could fail and have no effect on the patient required no inspection, but devices that are integral to the patient's life would need stringent inspection by the FDA. However, this does not account for the security of data at all for the non-life threatening. In the life threating devices, this does not account for someone spying on data [51]. Also, these regulations did not account for the rapid increase in technology.

Recently, the CDRH is addressing medical wearables again because of the new resurgence of wearables. In January 2015, they released a draft to guidance for general wellness, low risk devices. The big take away here is that the CDRH will not be examining low risk devices [52]. This leaves big areas for data vulnerabilities because it is entirely up to the company to regulate their own security.

There are significant jumps that some wearables need to get through, if they are life-sustaining wearables or wearables that claim to address a specific medical

condition. However, even within this circumstance (and of course in the less regulated low-risk wearables), there is a lot of room for vulnerability and data breaching.

Interviews

To accompany the security analysis and policy/regulation analysis of wearables, I conducted interviews with doctors and professors across the country in order to obtain more information from experts. I interviewed three doctors at three different hospitals and six different professors from 5 different universities. These interviews led to the key contribution of the paper: broad tenets for medical wearable security. [53-60]

Doctors are not very knowledgeable about wearables

In two of the doctor interviews, they said the security was out of their expertise, which is true. However, this could lead to being naïve about the possible security threats. For instance, Dr. Michael Zile, Professor of medicine at the medical University of South Caroline, said, "[There is] pretty substantial companies behind these devices, so they are protected." Dr. David Standaert, Professor at University of Alabama at Birmingham, stated that "[No wearables] have reached clinical practice yet." Although most medical wearables have not reached clinical practice, this is not true in many areas of practice. In cardiac medicine, wearables are used. Dr. Philp Binkley, Professor of cardiovascular medicine at Ohio State University, uses two devices in his practice.

Furthermore, Doctors are not very worried about security. While interviewing the three doctors, the general consensus before I prompted them with potential security concerns was that security for these devices are not a huge problem. Even after prompted, one of the doctors still did not think security of devices was a large problem. "I don't think there is much potential for device tampering," Dr. Binkley said after I asked about security concerns with wearbales. Overall, Doctors do not all seem to all be on the same page for the role of wearables in medicine and their security.

Wearables are a huge part of the future of medicine

While talking to both the doctors and the researchers, the general consensus was that wearables will be a huge part of the future of medicine. Dr. Zile, said that "[Wearables] will become normal practice. It will become more routine." Dr. Binkley said, "We are going to see the trend of more and more devices. Devices that will be more complex that measures many different physiologic signals. We will be trying to monitor patients before they come so sick that they need to come into the hospital."

This is not a huge surprise to those in the field, however this is not what the general public thinks. People do not understand how this will massively change

healthcare from an office space to an at home diagnosis, with data being collected at all times and earlier in order to detect diseases earlier. This will make medicine more patient focused instead of doctor focused, said Dr. Standaert.

Security not holding back innovation and the benefits of the device

Two interviews mentioned the same idea of the huge benefit verse the potential risk. Dr. Zile mentioned that for each patient they would need to weigh the benefits and risks of getting wearables. The benefit being the service the wearable provides and the risk being the potential security issues. For most, this risk is not a huge deal because most people do not believe they will be a target of hacking. In addition, the benefit of a device like a pace maker outweighs the risk because without the device the patient would die.

Furthermore, those interviewed said that patients, researchers and policy makers should not look at security as a blocker of the progress that is being made in medical wearables, otherwise the progress will be slowed greatly. Niraj Jha, Professor of Electrical Engineering at Princeton University, said, "A lot of these devices are very beneficial to the patient, so just because there are security concerns, does not mean the medical field should not be using them." Anand Raghunathan, Professor of electrical and computer engineering at Purdue University, made the comparison to Dick Cheney, when he had the security threat with his pacemaker, while he was president. He said the average person is not going to be concerned about security. But for "high-value" people, like Dick Cheney, the security is a much bigger concern. In the end, Raghunathan observed that the bad news sells more than the good, but that the benefits of these devices heavily outweigh the security risks.

Doctors should not be concerns about security

Two researchers and one doctor each said that the security of the device should not be the doctor's job. The doctor's job is the medicine. They should be diagnosing a patient, not worrying if the data they collect is true or not. Dr. Zile said that the companies are substantial and the devices are secure. Jha said, "It is not a doctor's job to worry about security. Electrical engineers should build devices that are secure."

Companies are not as concerned as they should be

Raghunathan said "I think manufacturers are concerned about security. But not nearly as concerned as they should be." He said that many companies are using basic security that is built into things like Bluetooth and Wi-Fi, however this does not meant he device is safe. He said manufacturers need to start thinking about security more holistically, in order to cover the large context of possible hacks. Greif Paul, Professor of electrical engineering at University of Strathcylde Glasgow, made the point that the security is not only in the device itself, but in the companies

holding the data. Companies have access to this data, but he posed the question of what happens in the event that the company is acquired or sold and how this could effect how the data is being used? The issue is the consumer rarely knows how it effects them. The big issue is these companies are not competing on security: there is no competitive advantage for bettersecurity in medical devices. Rather, it is the opposite – if a company invests in security they will likely get less profit.

The public does not understand security

Repeatedly in many interviews, it was stated that the public does not understand the potential security concerns. Some said that the problem was that the security issues are blown up in the media, while others said that the public does not know much about the potential security issues. Raghunathan said, "The problem is society at large does not understand the concerns enough." Raghunathan, Jha ,and Kevin Fu, Professor of computer science and electrical engineering at Michigan University, had the same statement about wearables' security in media: "concerns are blown out of proportion by the media." Jha also mentioned the Cheney example and how it sensationalized issues with wearables, when in reality that is not the main concern in wearable security. David Kotz, Professor of computer science at Dartmouth College, mentioned sometimes an article is written based on one study and then many other similar articles are published, all based on the same study. The specific article he was referencing was a study that asserted that by looking at someone's heart rate, which is collected on an Apple Watch or Fitbit, for instance, it can be determined if the wearer is pregnant. This article was sensationalized, however it is unclear whether or not this actually can even be done accurately. This is just another example of how the public does not understand the true security concerns of wearables.

Fu said that the issue is the problem the media hypes up is not actually the problem in security. The media hypes up the idea that a device could be hacked or a security failure because of a breach. However, the bigger security concern in wearables, according to Fu, is the availability. Many of the devices that face the biggest problems are the one's that are 10 years old and were made before stricter FDA regulations. These devices were made when security was not as much in mind and the hardware is not much older. These devices are subject to normal bugs that come in through hospital systems that normal, up-to-date software and hardware can handle, but these older systems can not. These devices will not be hacked and controlled, but rather they will just stop working or not be accessible by the doctors that need to access them.

Conclusion

Medical wearables are here to stay. They are already part of daily medical practice and this will only continue to grow in the future. They will grow to detect issues earlier and while patients are at home, in order to prevent illness at earlier stages. There are many examples of security breaches in all aspects of a wearable:

Bluetooth communication, smartphone or personal computer app, app connection to cloud through Wi-Fi, cloud storage with wearable API and web service. This could lead to anything from authorization and authentication, availability, and confidentially issues. This could lead to a wide range of security issues, including data modification, impersonation, eavesdropping, replaying, or simply deleting. Even if this is all secure, there are potential issues with privacy policies of individual companies, in that the data is not secure or really owned by the individual.

After interviewing many industry professionals, both clinical and research, some key conclusions were made. Doctors are not very knowledgeable about wearables and are not very worried about security. However, many think this is not the doctor's job. This is rather the job of the device makers – the engineers. However, the issue is that the companies are not as concerned with security as they should be, according to some researchers.

The other two large conclusions from the interviews are one, the public does not understand security of these devices. Often security issues are blown out of proportion because of the media. And two, the security concerns should not stop the progress that is being made in this field. The security concerns do not outweigh the millions of lives that could be helped with the continued development of a medical wearable technology.

References

[1] Sarkar, Shuvro S. "Is Wearable Technology the Future of Healthcare?" *Is Wearable Technology the Future of Healthcare?* RapidValue Solutions, n.d. Web. 22 May 2016. <http://www.rapidvaluesolutions.com/wearable-technology-the-future-of-healthcare/>.

[2] Medici, Laurenti De' "The History Of Wearable Technology – Past, Present And Future." *The History Of Wearable Technology*. WT Vox, n.d. Web. 22 May 2016. <https://wtvox.com/featured-news/history-of-wearable-technology-2/>.

[3] Winchester, Henry. "A Brief History of Wearable Tech." *Wareable*. Wearable, n.d. Web. 22 May 2016. <http://www.wareable.com/wearable-tech/a-brief-history-of-wearables>.

[4] Philippe, Patek. "First WristwatchShare." *First WristwatchShare*. Guinness World Records, n.d. Web. 22 May 2016. <http%3A%2F%2Fwww.guinnessworldrecords.com%2Fworld-records%2Ffirst-wristwatch%2F>.

[5] Hopping, Clare. "The 5 Rubbish Wearables That Actually Make Google Glass Look Cool." *TechRadar*. TechRadar, n.d. Web. 22 May 2016. <http://www.techradar.com/us/news/portable-devices/the-5-rubbish-wearables-that-actually-make-google-glass-look-cool-1247061>.

[6] Desjardins, Jeff. "Infographic: The History of Wearable Technology."*Visual Capitalist*. Staysourced, 20 May 2015. Web. 22 May 2016. <http://www.visualcapitalist.com/the-history-of-wearable-technology/>.

[7] Victor Lipman. Forbes."71% Of 16-To-24-Year-Olds Want 'Wearable Tech.' Why Don't I Even Want To Wear A Watch?". September 22, 2014.

[8] "When Were Contact Lenses Invented?" *Infoplease*. Infoplease, n.d. Web. 22 May 2016. <http://www.infoplease.com/askeds/contact-lens-history.html>.

[9] Mohee, Kevin. "SSCTS." *History: Pacemakers*. SSCTS, n.d. Web. 22 May 2016. <http://www.sscts.org/pages/historypacemakers.aspx>.

[10] Greenspon, Arnold J., Jasmine Patel, Edmund Lau, Daniel Frisch, Reginald Ho, Behzad Pavri, Jorge Ochoa, and Steven Kurtz. "Trends In Permanent Pacemaker Implantation In The United States 1993-2009: Increasing Complexity Of Patients

And Procedures."*Journal of the American College of Cardiology* 59.13 (2012): n. pag. Web.

[11] Knoblauch, Max. "The History of Wearable Tech, From the Casino to the Consumer." *Mashable*. N.p., 13 May 2014. Web. 22 May 2016. <http://mashable.com/2014/05/13/wearable-technology-history/#7gE1y29rCZqg>.

[12] Abrams, Harvey B. "Digital Hearing Aids." *Ear and Hearing* 30.3 (2009): 385-86. Web.

[13] Bonato, P. "Advances in Wearable Technology and Its Medical Applications." *2010 Annual International Conference of the IEEE Engineering in Medicine and Biology* (2010): n. pag. Web.

[14] Bonato, P. "Wearable Sensors/systems and Their Impact on Biomedical Engineering." *IEEE Eng. Med. Biol. Mag. IEEE Engineering in Medicine and Biology Magazine* 22.3 (2003): 18-20. Web.

[15] "History of Wearable Health Trackers." *Sharecare*. N.p., n.d. Web. 22 May 2016. <https://www.sharecare.com/health/health-apps-and-wearables/slideshow/wearable-health-trackers-timeline#slide-5>.

[16] "Proteus Digital Health." *Proteus Digital Health*. N.p., n.d. Web. 22 May 2016. <http://www.proteus.com/>.

[17] Jervis, Shivvy. "The Future Will Eat Itself: Digesting the next Generation of Wearable Tech." *The Guardian*. Guardian News and Media, 13 Jan. 2016. Web. 22 May 2016. <http://www.theguardian.com/media-network/2016/jan/13/future-eat-digesting-next-generation-wearable-tech>.

[18] "Back to the Future History of Wearable Technology." Iamdigitalnews, n.d. Web. <http://www.iamdigitalnews.com/2015/07/29/back-to-the-future-history-of-wearable-technology/>.

[19] "Medical Device for Back Therapy at Home - Valedo® - Valedo®."*Valedo*. N.p., n.d. Web. 22 May 2016. <https://www.valedotherapy.com/>.

[20] "No Bystander Intervention Required." *ZOLL Medical Corporation*. N.p., n.d. Web. 22 May 2016. <http://lifevest.zoll.com/>.

[21] Fellman, Megan. "News." *'Skin-Like' Device Monitors Cardiovascular and Skin Health: Northwestern University*. N.p., n.d. Web. 22 May 2016. <http://www.northwestern.edu/newscenter/stories/2014/09/skin-like-device-monitors-cardiovascular-and-skin-health.html>.

[22] Kosir, Spela. "Wearables in Healthcare." *Wearable Technologies*. N.p., 15 Apr. 2015. Web. 22 May 2016. <https://www.wearable-technologies.com/2015/04/wearables-in-healthcare/>.

[23] "Our Solution." *RSS*. N.p., n.d. Web. 22 May 2016. <http://www.chronothera.com/>.

[24] "Early Detection Is KEY." *Cyrcadia Health*. N.p., n.d. Web. 22 May 2016. <http://cyrcadiahealth.com/>.

[25] "FITGuard by Force Impact Technologies." *FITGuard by Force Impact Technologies Comments*. N.p., n.d. Web. 22 May 2016. <https://www.fitguard.me/>.

[26] Crossing the Quality Chasm: A New Health System for the 21st Century, Committee on Quality of Healthcare in America, Institute of Medicine, Washington, D.C., 2001.

[27] Cyr, Britt, Webb Horn, Daniela Miao, and Michael Specter. "Security Analysis of Wearable Fitness Devices (Fitbit)." (n.d.): n. pag. Massachusetts Institute of Technology. Web. 22 May 2016. <https://courses.csail.mit.edu/6.857/2014/files/17-cyrbritt-webbhorn-specter-dmiao-hacking-fitbit.pdf>.

[28] "Will the Demise of XP Shut Down Your Business...or Heart? -." *Privacy Professor*. IBM for Midsize Business, 25 Mar. 2014. Web. 22 May 2016. <http://privacyguidance.com/blog/will-the-demise-of-xp-shut-down-your-business-or-heart/>.

[29] Li, Chunxiao, Anand Raghunathan, and Niraj K. Jha. "Hijacking an Insulin Pump: Security Attacks and Defenses for a Diabetes Therapy System." *2011 IEEE 13th International Conference on E-Health Networking, Applications and Services* (2011): n. pag. Web.

[30] Sandler, Karen, Lysandra Ohrstrom, Laura Moy, and Robert McVay. "Killed by Code: Software Transparency in Implantable Medical Devices." (2014): n. pag. 21 July 2010. Web.

[31] Clark, Shane S., and Kevin Fu. "Recent Results in Computer Security for Medical Devices." *Lecture Notes of the Institute for Computer Sciences, Social Informatics and Telecommunications Engineering Wireless Mobile Communication and Healthcare* (2012): 111-18. Web.

[32] Jennings, Richi. "A Review of Bluetooth Attacks and How to Secure Mobile Workforce Devices." *A Review of Bluetooth Attacks and How to Secure Mobile Workforce Devices*. N.p., n.d. Web. 22 May 2016. <http://www.webroot.com/us/en/business/resources/articles/corporate-security/a-review-of-bluetooth-attacks-and-how-to-secure-mobile-workforce-devices>.

[33] Kumar, Pardeep, and Hoon-Jae Lee. "Security Issues in Healthcare Applications Using Wireless Medical Sensor Networks: A Survey."*Sensors* 12.12 (2011): 55-91. Web.

[34] Kambourakis, Georgios, Eleni Klaoudatou, and Stefanos Gritzalis. "Securing Medical Sensor Environments: The CodeBlue Framework Case." *The Second International Conference on Availability, Reliability and Security (ARES'07)* (2007): n. pag. Web.

[35] Subashini, S., and V. Kavitha. "A Survey on Security Issues in Service Delivery Models of Cloud Computing." *Journal of Network and Computer Applications* 34.1 (2011): 1-11. Web.

[36] Ren, Kui, Cong Wang, and Qian Wang. "Security Challenges for the Public Cloud." *IEEE Internet Computing IEEE Internet Comput.* 16.1 (2012): 69-73. Web.

[37] Sengupta, Shubhashis, Vikrant Kaulgud, and Vibhu Saujanya Sharma. "Cloud Computing Security--Trends and Research Directions."*2011 IEEE World Congress on Services* (2011): n. pag. Web.

[38] Pearson, Siani, and Azzedine Benameur. "Privacy, Security and Trust Issues Arising from Cloud Computing." *2010 IEEE Second International Conference on Cloud Computing Technology and Science* (2010): n. pag. Web.

[39] Hashizume, Keiko, David G. Rosado, Eduardo Fernández-Medina, and Eduardo B. Fernandez. "An Analysis of Security Issues for Cloud Computing." *J Internet Serv Appl Journal of Internet Services and Applications* 4.1 (2013): 5. Web.

[40] Modi, Chirag, Dhiren Patel, Bhavesh Borisaniya, Avi Patel, and Muttukrishnan Rajarajan. "A Survey on Security Issues and Solutions at Different Layers of Cloud Computing." *J Supercomput The Journal of Supercomputing* 63.2 (2012): 561-92. Web.

[41] Paul, Greig, and James Irvine. "Privacy Implications of Wearable Health Devices." *Proceedings of the 7th International Conference on Security of Information and Networks - SIN '14* (2014): n. pag. Web.

[42] "Terms of Service." *Fitbit Website Terms and Conditions*. N.p., n.d. Web. 22 May 2016. <http://www.fitbit.com/uk/terms>.

[43] "Jawbone® | Privacy." *Jawbone Privacy*. N.p., n.d. Web. 22 May 2016. <https://jawbone.com/legal/privacy>.

[44] "Basis Privacy Policy | Basis." *Basis*. N.p., n.d. Web. 22 May 2016. <http://www.mybasis.com/legal/privacy/.>.

[45] "Basis Terms of Service." *Basis*. N.p., n.d. Web. 22 May 2016. <http://www.mybasis.com/legal/tos/>.

[46] "Basis Privacy Policy | Basis." *Basis Privacy Policy*. N.p., n.d. Web. 22 May 2016. <http://www.mybasis.com/legal/privacy/.>.

[47] HIPAA. Office for Civil Rights, United State Department of Health and Human Services. Medical Privacy. National Standards of Protect the Privacy of Personal-Health-Information. August 21, 1996

[48] HITECH. Health Information Technology for Economic and Clinical Health Act February 17, 2009

[49] "Strong User Authentication and Hipaa Cost Effective Compliance with Federal Security Mandates - Search Results - TechRepublic."*TechRepublic*. N.p., n.d. Web. 22 May 2016. <http://www.techrepublic.com/whitepapers/strong-user-authentication-and-hipaa-cost-effective-compliance-with-federal-security-mandates/2345053>.

[50] Kumar, Pardeep, and Hoon-Jae Lee. "Security Issues in Healthcare Applications Using Wireless Medical Sensor Networks: A Survey."*Sensors* 12.12 (2011): 55-91. Web.

[51] "U.S. Food and Drug Administration." *Overview of FDA Modernization Act of 1997, Medical Device Provisions*. U.S. Food and Drug Administration, n.d. Web. 22 May 2016. <http://www.fda.gov/MedicalDevices/DeviceRegulationandGuidance/GuidanceDocuments/ucm094526.htm>.

[52] "Draft Guidance for Sponsors, Industry, Researchers, Investigators, and Food and Drug Administration Staff: Certifications to Accompany Drug, Biological Product, and Device Applications/Submissions."*Biotechnology Law Report* 27.4 (2008): 336-37. *General Wellness: Policy for Low Risk Devices*. U.S. Department of Health and Human Services, Food and Drug Administration. Web. 23 May 2016. <http://www.fda.gov/downloads/medicaldevices/deviceregulationandguidance/guidancedocuments/ucm429674.pdf>.

[53] Philip Binkley. (February, 2016). Telephone Interview.

[54] David Standaert. (February, 2016). Telephone Interview.

[55] Michael Zile. (February, 2016). Telephone Interview.

[56] Niraj Jha. (February, 2016). Telephone Interview.

[57] Anand Raghunathan. (February, 2016). Telephone Interview.

[58] David Kotz. (February, 2016). Telephone Interview.

[59] Kevin Fu. (February, 2016). Telephone Interview.

[60] Greig Paul. (February, 2016). Email Interview.