SHAPING UP SECURITY

The Dangers and Vulnerabilities of Wearables

Abstract

Whether it's an Apple Watch, Pebble smart watch or a Fitbit, Bluetooth-enabled devices abound. Despite the near ubiquity of these devices in many countries worldwide no proper efforts have been made to secure them.

Rather these devices are produced at ever increasing scales, leaving scores of unprotected devices open to information theft, hacks and use in attacks. Both Bluetooth and Low-Energy Bluetooth devices are insecure.

Can wearables be made more secure? What can individuals do to protect themselves? What role will Bluetooth devices play in future hacking attempts given their general lack of security? What consequences might result if attempts are not made to shore up the security of these devices?

Juliana Furgala

Tufts Class of '19

Table of Contents

This paper is intended to serve as PSA for both those slightly familiar with Bluetooth and for the average device user. Hopefully this paper will educate others on what exactly is happening in wearables and what we as users, developers, and creators can do to improve the future of Bluetooth.

Supporting Material – Slide deck ("Tech Talk") to promote Bluetooth awareness

Introduction

This paper offers a discussion on the core issues surrounding Bluetooth security (or the lack thereof) and how they relate to everyone as users. While hacking Bluetooth devices may not be a shiny new topic like some other exotic exploits, it is all the more important because it is a persistent and ever more relatable issue. Even back in 2012 the Bluetooth Special Interest Group (SIG) recorded a total of more than 2 billion new devices being shipped out annually[1]. Wearables alone are a multi-billion dollar industry[2]. Just looking at the increase in the number of Bluetooth member companies up to 2016[1], this annual number of products has assuredly increased. Just as we seek to manage the other forces that rule our lives so to should we acknowledge the power Bluetooth devices have over us and inform ourselves on what they are fully capable of.

To the Community

Many of the applications of security, despite their differences, have something in common – they are often unappreciated or unpublicized. As we continue to surround ourselves with new and upcoming devices we all need to be aware of what having these devices in our lives means, what information we are really trusting to these devices, and how much of our rapidly-shrinking privacy we as consumers are willing to risk for convenience. How many Bluetooth-enabled devices do you have in your house now? Five, ten?

In the rush of progress it is easy to forget how much we blindly trust these devices, how simple it is to become complacent when our problems are solved. Yet in the modern age, when it has come to public attention that individuals are taking advantage of these long-exposed security issues, it is more important than ever to maintain our own privacy and become responsible users. This paper aims to help you to improve the security of the devices in your life.

The Importance of Bluetooth (Wearable) Security

Why should we as consumers worry about the security of Bluetooth (and specifically that of wearables)? Many aspects of Bluetooth are inherently insecure and myths exist that perpetuate the idea that Bluetooth is more protected than it actually is.

Debunked Myths of Bluetooth[3]

Some of the most dangerous misconceptions are that:

a) Bluetooth is ‘limited range;’

b) The data exposed by Bluetooth devices are not sensitive;

c) Bluetooth weaknesses are only found in specific devices;

d) Devices cannot be found if they are set to undiscoverable.

Bluetooth is not actually short range. Traditional Bluetooth devices fall into three classes of varying range and power with class 1 as the most powerful with a range of up to 100 meters[3] and class

three the least powerful with a range of under 10 meters[3]. For a reference point many class 1 devices are integrated with laptops while class 2 devices are often items that work with phones[3]. Considering that 100 meters is the general maximum distance of many Bluetooth devices, that means any data being transferred over the channels is potentially being exposed to eavesdroppers up to 100 meters away. Bluetooth Low Energy does not use this system[4]; however Bluetooth Low Energy is still powerful, just more variable[4].

The information attackers can glean from Bluetooth communications can also be sensitive in nature. Attackers can gain access to Bluetooth devices and use them as a door into the connected phone, gathering and modifying contacts and calendar information, among other possibilities; this is exactly what happened in the BlueSnarfing attack[3]. Devices are only as secure as their weakest vulnerability.

Bluetooth's weaknesses are not limited to issues with specific devices. Researchers have found flaws in Bluetooth encryption itself, E0, which was created by the SIG[5]. There exists a "conditional correlation attack" that can find the encryption key used in Bluetooth communication in only 2^{38} attempts, rather than the expected 2^{128} attempts[3, 5]; this is a dramatic reduction. Once an attacker has this key they can use it to decrypt the conversation between the devices using that key and listen in. This shows that even the most "secure" Bluetooth devices may have vulnerabilities because they are Bluetooth-based.

As well, keeping Bluetooth devices "offline" does not guarantee their security. Each device has its own Bluetooth Device Address[3]. These devices can still be found by an attacker willing to brute-force the limited number of addresses a device can have[3] (think knocking on doors on a street if you do not know the house number).

Bluetooth Devices Unite!

Once a Bluetooth-enabled device is connected to, attackers can steal personal information, attempt to connect to other connected devices, and even use the device in a botnet. A botnet is a group of many devices controlled by an individual, often for nefarious purposes. Among their other capabilities, Botnets can promote spam content on the Internet and bring down websites with their sheer numbers (Distributed Denial of Service or DDOS attacks)[6]. Researchers have shown that Bluetooth devices present a threat for the way in which they can be used in botnets[6].

One way to help prevent this is to change default passwords on Bluetooth devices. Admittedly this is not foolproof as other vulnerabilities exist and in some cases the default password cannot be changed. Yet changing default passwords, no matter the device, is always a good security measure.

A Brief History of Bluetooth

In 1998 the technology now known as Bluetooth got its name[1]. This was the same year that the SIG was formed for Bluetooth[1]. At the time the group only had five member companies compared to the more than thirty thousand member companies there were as of 2016[1]. Over the course of these nearly twenty years the number of Bluetooth devices has risen dramatically[1]. However like many new technologies in the computer science field, attention is often paid to new device development with security as a secondary concern. As was mentioned in the "Debunked Myths of Bluetooth" section above, there are vulnerabilities and weaknesses in classic Bluetooth's foundation.

Bluetooth Vs. Bluetooth Low Energy

Over time classic Bluetooth evolved into a new form. Bluetooth LE (or BLE) was introduced in 2011 with the first BLE devices for sale[7]. BLE has multiple differences from its predecessor that made it more feasible to create IoT Bluetooth devices[7-8, 11]. Most significant is the lower energy use of BLE over classic Bluetooth[7-8, 11]. This is especially helpful with devices that have less powerful batteries or power supplies[7]. Low energy functionality works it by only keeping the device "on" when data needs to be transferred and keeping it disconnected otherwise[7, 8]. Classic Bluetooth, on the other hand, maintains a more constant connection and can therefore transfer more data[7]. Despite the rise of BLE, classic Bluetooth devices still exist.

Recent versions of Bluetooth LE (Bluetooth 4.2 and up) also have multiple newer security features that earlier versions of Bluetooth lacked.[8] One such feature is a new security technique in the form of "Low Energy (LE) Secure Connections"[8] which was intended to shore up the security of inter-device communications[8]; Another feature is "LE Privacy"[8] which promotes limiting the devices that can pair with a given device by using a whitelist of accepted addresses belonging to devices[8]. Yet as it will be described later these methods do not ensure the total security of these devices (in fact total security is essentially impossible).

Despite these positive changes other issues in Bluetooth such as the large range of devices have not abated. On the contrary, Bluetooth 5 quadrupled the range for devices, particularly for devices with an Internet of Things focus[8]. The general path of development of Bluetooth is a slow one with emphasis on adding items to the Internet of Things over security, although security does on occasion come into focus.

The Rise of Wearables

Wearables are part of the newest phase of Bluetooth device development. These devices have quickly caught on with research in 2014 predicting the massive increase in both the number of products and the value of the wearables market[10]. In fact, 2014 was the first year that a wearables DevCon was held (like a ComicCon for wearables developers)[10], indicating the already sizable scale of the wearables market.

Fitness gear in particular has taken a step forward with the convenience of wearables. Apple Watches can download third-party applications with a variety of capabilities. In terms of security these applications can serve as access points to information on connected devices, such as phones. Yet they also offer convenience to users who can now take phone calls on their watches and send basic texts without a phone.

Fitness companies and coaches are not yet satisfied shaking up the industry though. Gina Lee, who runs a health-care institute, feels the future of fitness is the development of the least obtrusive fitness accessories[9]. This could involve taking the next step and integrating these devices with the human body so the connection is more cohesive. With this mindset, the rise of wearables is only the beginning.

Interactions Between Wearables and You

Wearables can send a plethora of information, from fitness data in the case of Fitbits to call and messaging information for Apple Watches. This information is all vulnerable during transfer. BLE does have a method to minimize sniffing[21]. Sniffing is the process of analyzing traffic through either Wi-Fi or Bluetooth, often an attempt to gain information about others[30]. Part of BLE is using a "hop pattern" which is a device's attempt to make sniffing more difficult for a potential eavesdropper[21]. Yet these BLE devices, since they do not have a constant connection, must connect repeatedly to their chosen "base station" (or controlling device)[21]. This information can be captured by listeners who can determine what devices are involved in the communication[21]. The researchers who found this vulnerability also proposed a solution to the issue[21]. Yet as with other vulnerability fixes, users must wait for patches to resecure their devices.

Sniffing Your Wearables

Sniffing wearables is a relatively simple process. There are multiple applications, both for mobile and for desktop computers and laptops that allow an individual to sniff out the nearby devices that are sending out Bluetooth request packets. Devices with Bluetooth turned off do not send out these requests. However any other Bluetooth devices, whether set to discoverable or undiscoverable, can be found.

For laptops and desktop computers, BLEAH[22] and Blue Hydra[23-24] are both easy-to-use options. Once either tool is downloaded and run, it will search for Bluetooth devices in the area over time. Even trying one of these tools can be an experiment in the ease with which our devices can be discovered.

Another even easier way is to use RaMBLE[25-26], a Bluetooth LE sniffing app for your phone. This option, unlike the first two, offers a graphical interface with buttons and images, not just something that runs in a computer terminal.

Two of the most recent vulnerabilities discovered are known as BlueBorne[27-28] and BlueSteal[29]. BlueBorne was announced by Armis Labs after they found eight separate vulnerabilities that could reasonably be taken advantage of to completely take over victim Bluetooth devices[27-28]. These vulnerabilities worked on multiple platforms (or device systems) including Linux devices, Android devices, and Amazon and Google Home devices[27-28].

BlueSteal is a vulnerability that impacts GATT safes, which are gun safes advertised to be secure[29]. The vulnerability allowed potential attackers to unlock the safe[29]. This violates the functionality of the case, which is to keep the gun isolated and only openable by pin by the user. Fortunately this issue has been fixed by the safe company.

As these two cases illustrate, taking over devices once they are detected can be simple in many cases. That is why keeping these devices out of the spying eyes of sniffers and following the other security advice later in this paper is important.

Fixing Long-Standing Problems?

Can these long-standing problems be fixed? There are several barriers to progress that must be overcome before more complete changes can occur for Bluetooth security.

A New Approach to Building Wearables

The decision to build devices with minimal obvious security vulnerabilities is up to product and software developers. With an open market on Bluetooth devices and the ability to mass-sell items on services such as Amazon there is a push to develop items quickly before the idea can be copied. This rush means that security concerns, which slow down the development process, can go by the wayside. Therefore one of the barriers is mindset.

Consumers can modify spending habits to support more secure products and speak out publicly to promote responsible development. The idea behind responsible development is that when security is seen simply as an integral part of the development process rather than as an impediment then products will become safer to use. As well, if the SIG can be encouraged to promote a pro-security agenda some of the most egregious weaknesses may be fixed in the future, even if not in the near future.

If these issues are not already considered critical, then think about devices will be capable of in the future. In the medical field, there are individuals hoping to create implantable health devices that can use Bluetooth to message a phone and communicate statistics on the vitals of the patient[13-15]. To make this a feasible option they found a way to amplify the range of the device so the signals are not lost in the human body[15]. To check in properly these devices will likely need to emit a fairly regular signal, making turning it "off" impractical. Bluetooth is intertwined with this new technology. According to the researchers of this project the Wi-Fi needed to connect is generated from smartwatch Bluetooth transmissions and similar devices.[14,15]

To put everything in perspective, the number of Bluetooth devices far outnumbers the human population[12]. As Bluetooth devices continue to be integrated into the innermost sanctums of our lives – smart houses and even implanted devices – we need to recognize where Bluetooth is needed and where it is not.

Legacy Devices

There is also the matter of legacy devices. Legacy devices have old technology that has not been updated to the most current version or that has had newer generations of the devices released. There comes a point in a devices' life where it is no longer updated if it cannot handle the battery usage or hardware requirements of new features available in newer generation devices. When devices stop receiving updates they are frozen at their current state of security.

What if companies do not create patches? If a device is not updated with a patch then it remains vulnerable to attacks that newer devices were immunized against. One example of an updated feature is Bluetooth mesh, which was developed for use in IoT smart house devices[16]. It allows devices to hop along devices on the network to reach a controller, such as if there were multiple smart lights set up throughout

a house[16]. This feature does not require any new hardware so nearly all BLE devices can use it[16]. The only catch is that it is up to the manufacturers to release updates for specific devices to be able to use the feature. This same idea applies to security patches.

Little Chance for an Overhaul

Bluetooth development is outpacing Bluetooth security updates (which are rare as is). The matter of backwards compatibility and the societal and developmental pressure to keep integrating ensures that there is little chance for a dramatic change in security for Bluetooth. Bluetooth is also in an ongoing technological struggle with the Wi-Fi group for IoT traffic and support[16]. This pressure from the competing technology keeps Bluetooth with an eye ahead on the future, not on the past and already implemented security measures.

Given the current trajectory it does appear that Bluetooth may be on the path towards improving security but so slowly that it will be a difficult path towards adoption of more security measures. Likely many devices created to use older forms or versions of Bluetooth will not be updated to use a more secure form of Bluetooth. As well, every update that adds more capabilities to Bluetooth opens the possibility for the accidental introduction of more vulnerabilities. Yet it is a positive sign that these measures are being considered and implemented. As Bluetooth devices work further into the lives of consumers with everything from "Smart [Light] Bulbs"[17] to "Wireless Smart Beanies"[18] continuing to push for security as consumers and as developers is vital.

Defenses and Points of Action: Protecting Yourself and Your Devices

Personal Safety Practices

As it can be seen, Bluetooth devices are driven by development foremost over security. These forces force all consumers to choose what devices are truly necessary. This is the concept of acceptable risk. Devices that improve lives and make tasks more convenient often come at the price of security. Eliminating these devices entirely may in some cases be a stretch. There are some intermediate steps that can help to minimize the risk of Bluetooth devices being attacked,

The University of Michigan put a Public Service Announcement on their Safe Computing website after BlueBorne was announced, reminding individuals to "update devices regularly and to turn off Bluetooth when you are not using it."[19] Both of these steps will help to protect potentially vulnerable devices. Updating devices will ensure that they receive any security related patches. Turning off Bluetooth when it is not needed will prevent the device from automatically (re)connecting to other searching devices. It also prevents the device from sending out requests that can cause it show up on the radars of potential attackers using sniffers.

It is especially key to ensure that Bluetooth is actually turned off on unused devices, not just appearing to be. Under iOS11 and its later versions, using the shortcut buttons to try to turn off Bluetooth will only disconnect the device, not turn off Bluetooth itself[20]. A separate section for Bluetooth is available under Settings that allows users to actually turn off Bluetooth[20]. Given that Bluetooth devices

such as speakers, wireless headphones, fitness devices, etc. are generally intended to connect to phones, this is an important step.

Conclusion

As it can be seen, even the foundations of classic Bluetooth have security issues, let alone the many devices that use Bluetooth as a means of connection and communication. While there are now security-minded changes being released for Bluetooth, the rate of development of Bluetooth products combined with the presence of legacy products makes this path currently difficult. At the moment, much hope lies in the consumer. We can choose as consumers to use Bluetooth-enabled devices responsibly, to evaluate whether or not these devices are necessary, and to recognize what the accept risk is for each one of us as users. This is a very individual decision. What one user may find reasonable and palatable another may find too risky.

Ultimately it truly is up to each of us as consumers to decide what products to incorporate into their life and by doing so what products to endorse. This does not have to apply to new purchases only. By checking already owned devices with any of the above tools or sniffers it is possible to see what information is being exposed to potential eavesdroppers and attackers. Being aware of what personal information attackers could potentially gain access to is vital to protecting that information. After each consumer is armed with this knowledge then and only then can each person make an informed choice to adapt their device use to hide any truly sensitive information. Each and every one of us has this responsibility, this ability, to be apprised of ways to limit public knowledge of our lives in a world where privacy is increasingly scarce.

By choosing to buy products that emphasis security and that are built with security in mind, consumers can protect themselves. Yet this will not be sufficient to sway most companies to switch their policies or priorities since many consumers will likely still continue to buy less secure devices for price and convenience. What can we hope for the future of Bluetooth then? With a joint effort of educated users and aware developers we can aim to shift the direction of Bluetooth device development to stress security over blind speed and profit. While this effort will be far from easy what better a time than now, when security vulnerabilities are coming to light through dramatic cases of hacking?

Notes

[1] See the Bluetooth SIG website for a full chronology of Bluetooth development over the years. https://www.bluetooth.com/about-us/our-history

[3] This view is simplified. For more specific information check source 3.

[5] For presentation slides on the conditional correlation attack, see the following link. https://www.iacr.org/conferences/crypto2005/p/16.pdf

[N/A] For information on reverse engineering Fitbit read this article: https://pewpewthespells.com/blog/fitbit_re.html

[N/A] Another source for more technical specifics on the forms of attacks performed on Bluetooth devices can be found here: http://www.cs.tufts.edu/comp/116/archive/fall2015/hosullivan.pdf

[N/A] To try reverse engineering for BLE, see this link: https://learn.adafruit.com/reverse-engineering-a-bluetooth-low-energy-light-bulb/sniff-protocol

[N/A] For a more technical exploration of Fitbit security, check out this paper: https://courses.csail.mit.edu/6.857/2014/files/17-cyrbritt-webbhorn-specter-dmiao-hacking-fitbit.pdf

References and Citations

[1] "Our History," 2016, https://www.bluetooth.com/about-us/our-history

[2] N. Lomas, "Global wearables market to grow 17% in 2017…," 2017, https://techcrunch.com/2017/08/24/global-wearables-market-to-grow-17-in-2017-310m-devices-sold-30-5bn-revenue-gartner/

[3] J. Wright, "Dispelling Common Bluetooth Misconceptions," https://www.sans.edu/cyber-research/security-laboratory/article/bluetooth

[4] remixed123, "Bluetooth Low energy chip range," https://electronics.stackexchange.com/questions/87056/bluetooth-low-energy-chip-range

[5] Y. Lu, W. Meier, S. Vaudenay, "The Conditional Correlation Attack: A Practical Attack on Bluetooth Encryption," https://lasec.epfl.ch/pub/lasec/doc/LMV05.pdf

[6] K. Singh, et. all., "Evaluating Bluetooth as a Medium for Botnet Command and Control," http://researcher.watson.ibm.com/researcher/files/us-kapil/bluetoothbotnet-dimva10.pdf

[7] B. Ray, "Bluetooth Vs. Bluetooth Low Energy: What's The Difference?," https://www.link-labs.com/blog/bluetooth-vs-bluetooth-low-energy

[8] Digi-Key's North American Editors, "Bluetooth 4.1, 4.2 and 5 Compatible Bluetooth Low Energy SoCs…," https://www.digikey.com/en/articles/techzone/2017/apr/bluetooth-41-42-5-low-energy-socs-meet-iot-challenges-part-1

[9] J. Howard, "What the future holds for fitness technology," 2017, http://www.cnn.com/2017/10/18/health/fitness-technology-future-explainer/

[10] J. Wei, "How Wearables Intersect with the Cloud and the Internet of Things…," 2017, http://ieeexplore.ieee.org/abstract/document/6844949/

[11] M. Babaie, F. Kuo, H. Chen, et. all., "A Fully Integrated Bluetooth Low-Energy Transmitter…," http://ieeexplore.ieee.org/stamp/stamp.jsp?arnumber=7476842

[12] V. Iyer, V. Talla, B. Kellogg, et. all., "Inter-Technology Backscatter: Towards Internet Connectivity for Implanted Devices," http://interscatter.cs.washington.edu/files/interscatter.pdf

[13] C. Jeffrey, "Turning Bluetooth into Wi-Fi puts implanted devices online," 2016,

https://newatlas.com/interscatter-bluetooth-wireless-wearables-uw/44966/

[15] P. Dvorak, “Improved antennas let implantable devices message your phone,” 2016, http://www.medicaldesignandoutsourcing.com/improved-antennas-let-implantable-devices-message-phone/

[16] J. Kastrenakes, “Bluetooth is getting a big upgrade to make it better for smart homes,” 2017, https://www.theverge.com/circuitbreaker/2017/7/18/15988362/bluetooth-mesh-networking-standard-released-smart-home

[17] Flux Bluetooth LED Smart Bulbs…, https://www.amazon.com/Flux-Bluetooth-LED-Smart-Bulb/dp/B00GWBBZ2I

[18] Soundbot SB210 HD Stereo Bluetooth 4.1 Wireless Smart Beanie…, https://www.amazon.com/Soundbot-SB210-Bluetooth-Headphone-Speakerphone/dp/B0163N2T38/

[19] “NOTICE: Update devices or turn off Bluetooth to prevent against BlueBorne,” https://www.safecomputing.umich.edu/security-alerts/update-devices-or-turn-bluetooth-protect-against-blueborne

[20] “Use Bluetooth and Wi-Fi in Control Center with iOS 11,” 2017, https://support.apple.com/en-us/HT208086

[21] C. Walter, M. Hale, R. Gamble, “Imposing security awareness on wearables,” 2016, https://dl.acm.org/citation.cfm?id=2897038

[22] evilsocket, “bleah,” https://github.com/evilsocket/bleah

[23] S. Gallagher, “Hands-on: Blue Hydra can expose the all-too-unhidden world of Bluetooth,” 2016, https://arstechnica.com/information-technology/2016/09/hands-on-blue-hydra-can-expose-the-all-too-unhidden-world-of-bluetooth/

[24] “BlueHydra,” https://github.com/pwnieexpress/blue_hydra

[25] RaMBLE – Bluetooth LE Mapper, https://play.google.com/store/apps/details?id=com.contextis.android.BLEScanner

[26] “Bluetooth LE – Increasingly popular, but still not very private,” https://www.contextis.com/blog/bluetooth-le-increasingly-popular-still-not-very-private

[27] “BlueBorne Information from the Research Time,” https://www.armis.com/blueborne/

[28] ArmisSecurity, “BlueBorne,” https://github.com/ArmisSecurity/blueborne

[29] D. Su, A. Fletcher, “BlueSteal: Popping GATT Safes,” https://www.twosixlabs.com/bluesteal-popping-gatt-safes/

[30] M. Chow, “Networking and Attacking Networks,” https://tuftsdev.github.io/DefenseAgainstTheDarkArts/slides/week1-networks.pdf