Czech university of life sciences

Faculty of Engineering

Reliability and safety of Bluetooth communication in case of an external attack

Bachelor's thesis

Thesis supervisor: Ing. Zdeněk Votruba, Ph.D.

Author: Vladislav Bouška

Prague 2020

Statutory Declaration

I hereby declare that this thesis is the result of my work and that it has not been submitted to this Faculty of Engineering Czech University of Life Sciences Prague or any institution for a degree. However, all references used in the development of the work have been acknowledged in the text and list of references.

In Prague.....

Acknowledgment

I would like to express my thanks to my thesis supervisor Ing. Zdeněk Votruba, Ph.D. for his guidance throughout my thesis. I would also like to express gratitude towards Ing. Jan Andraščík, Vladimír Hatrák and Daniele Antonioli, Ph.D. for their help and support.

Abstrakt: Cílem této práce je popsat jednotlivé útoky a aktuální zranitelnosti technologie Bluetooth společně s obranou a ochranou proti těmto útokům. Mimo jednotlivé útoky, je v této práci také probírána historie, vývoj a funkce technologie Bluetooth společně s principem jeho funkce. Ačkoliv je Bluetooth velice rozsáhlé téma, tato práce pokrývá nezbytné základy pro pochopení principu funkce jednotlivých prvků této technologie. Společně se základy fungování Bluetooth, je v této práci také probráno téma bezpečnostních mechanismů, jak spolu tyto bezpečností mechanismy navzájem pracují tak, aby společně tvořily relativně bezpečný a spolehlivý bezdrátový protokol sloužící k přenosu dat. Mimo to jsou v této práci také popsány vybrané způsoby napadání těchto mechanismů a chyby, které nám umožňují tyto mechanismy buďto zcela obejít a nebo je dokonce využít v náš prospěch a zcela zneužít jejich zamýšlený účel.

Klíčová slova: Bluetooth; Bezpečnost; Útok;

Abstract: Aim of this work is to describe different attacks and vulnerabilities of the Bluetooth technology together with the defense against these attacks. Besides these different attacks, this thesis also goes over the history, development, and the function of the Bluetooth technology together with the principles of its function. Although Bluetooth is a very widespread topic to cover, this thesis covers necessary basics for the understanding of how Bluetooth and its components work. Together with the basics of Bluetooth functionality, this thesis also covers Bluetooth's security mechanism and how these mechanisms work together, to create relatively secure and reliable wireless protocol for the transport of data. Besides that, this work also covers ways of attacking the above mentioned security mechanism and design errors which enables potential attackers to either go around these mechanisms, or even use them to compromise a Bluetooth link.

Keywords: Bluetooth; Security; Attack;

Table of contents

1 Introduction

Modern population cannot imagine their daily lives without smart peripheral devices such as Bluetooth enabled smart watches, wireless earphones, or even integration of our mobile devices into such use cases which would be unimaginable for the engineers who originally came up with the Bluetooth technology only a few decades ago. Computational power grew unbelievably powerful over the past few years alone. This brought large leaps forward in all fields of science and technology. But on the other hand, it also introduced most of the population to the threat of cybercrime and highlighted the importance of staying up to date with technological advances made in this field. When people get into a car, their phones automatically connect to their smart stereo system, their GPS navigation turns on, and even their handsfree system kicks in. All of this in one single device the size of a mobile phone. On one hand is the ease of use, on the other hand people carry the dream of every attacker with them every day. What is truly scary is that most of the people do not even realize that at any moment this device can be hijacked, and they can be thrown into a really unfavorable situation without their knowledge. As mentioned above, this concentration of sensitive information is a dream for any attacker. Luckily, not only the attackers but also the manufacturers of devices realize this and act upon it. Why would an attacker try to break through a heavily secured perimeter of a device, then through the security of, for example, banking application when he can easily go and do a so-called side channel attack. [1] What this thesis refers to is an OTC (One Time Code). This feature is frequently utilized in banking applications. If clients intend to send a payment, bank will first send a confirmation in a form of an SMS or by other means. With the aforementioned OTC which has to be typed into a banking website and only after this two-factor authentication will the transaction be processed. [2] What if the attacker already got access to the internet banking through other means (Session hijacking, credentials theft, physical access to the device, and remote access to the device), but the only thing keeping them from draining the balance was two factor authentication? Here Bluetooth comes into play. If there was a Bluetooth enabled watch on people's wrist, notification about the incoming SMS would be shown on their watch together with its contents. Attackers would

then only need to hijack the connection between the two devices, read out the information, and the user would be a victim of a cyberattack. This side channel attack is much more interesting than just brute forcing our way into a target device as shown by the CIA, when they needed Apple to unlock the device of a drug dealer to convict him. [3] Focus of this thesis will be the security and attacks aimed at Bluetooth connections. These attacks are not very popular, because several criteria need to be fulfilled before the attack can be carried out. Such criteria are:

1. Attacked devices must utilize MS Windows family of operation system.

   Reasoning behind this is that Linux, or other operating systems, are too uncommon to target taken into an account the other limitations of this attack (The target must use Bluetooth keyboard. This will be described more later on.). [4] Besides this factor, there is also another problem. Mainly with user privilege management. In Linux, there is the pesky SUDO command, which is required before any package can be installed. In MS Windows, there are not as frequent user authentication checks. And even if there are, another property of this attack could be used, which is wireless keylogging. Moreover, if the attack is successful, the target will most likely not even realize that they were attacked, because the only proof of said attack even going on will be a brief flash of CMD (Command line) and with that, the attack is concluded. If the target is really tech savvy, they could of course check the system logs, but who would really go to such lengths, when even legitimate software opens CMD from time to time.

2. The target must utilize Bluetooth devices which are connected to the targeted device.

   In most cases, the attack will be on a connection between the targeted device and a Bluetooth enabled UID (User Input Device). Use cases defined above talk about two possible attack modes. One being full on connection hijack and the second one being a wireless keylogger. If, for instance, hijack of a connection between a Bluetooth smart watch and a computer is performed, no real advantage would be obtained. This is the reason why the main target is an UID device.

3. Sufficient physical proximity to the target.

Amongst other limitations, proximity is one of the greatest disadvantages this type of attack suffers from. To successfully carry out this sort of attack, it is necessary to transmit the range of a Bluetooth enabled UID. This would mean anything from 10 to 30 meters depending on the device type. [5]

To wrap this introductory chapter up. This attack is very powerful if all the criteria is met. Additional factors to be kept in mind are, for instance, user privilege levels. This attack is mainly meant for HVT (High Value Targets) such as political dissidents, CEO (Chief Executive Officer) politicians and any other targets that an organization with sufficient manpower, knowhow and funding could achieve. In case of CEOs of big corporations, they will most probably not have local administrative accounts, but only domain users. This of course does not mean that the attack will not be effective. If the wireless keylogger functionality of this attack is utilized, it is possible to simply snoop credentials and utilize them at attackers will.

1.1 Basic principle and function of Bluetooth

Bluetooth utilizes ISM (Industrial, Scientific, Medical) band. The frequency range is 2.402 GHz – 2.480 GHz. This frequency range is unlicensed meaning that it is not necessary to obtain a HAM radio operator license. As mentioned above, Bluetooth devices can be connected to more than one device at once. Other slave devices to be precise can be connected to one master device at once. To put this into a perspective, imagine the following situation: A person decides to go for a run in their new smart shoes. They take their mobile phone which is connected to their smart watch/fitness tracker, they put on our wireless earphones and they connect their GPS and Bluetooth enabled running shoes to track their progress. This comes up to 3 to 1 connection. As mentioned above, Bluetooth WPAN (Wireless Personal Area Network) can connect 7 slave devices to 1 master device. This topology is defined in the Bluetooth documentation. [5] For the explanation of the Bluetooth frequency range, Wi-Fi will be used as an analogy. It is common knowledge that Wi-Fi technology has 11 channels. But what are the channels used for? Imagine,

that you are standing next to a lake. You pick up a stone and you throw the stone into the lake. Small waves form and start to spread out towards the shore of said lake. This is similar to how Wi-Fi and Bluetooth work. An antenna sends out electromagnetic waves which are then captured by a receiving antenna. But what would happen if a handful of gravel would be thrown into the lake? Multiple smaller waves would form and start to spread all over each other. This is exactly what would happen, if there were no channels and people would be in an apartment complex. Multiple Wi-Fi routers all on the exact same frequency would be interfering with one another garbling up the signals. This problem is solved by introducing channels to the equation. Wi-Fi operates on the frequency range of 2.4 GHz – 2.47 GHz. Each channel is its own frequency so that multiple devices working on the same frequency can be in close physical proximity to each other and still work. The same principle is in Bluetooth with some differences. Main differences are that Bluetooth utilizes 40 channels, of which 37 are used to actually transfer data and the 3 remaining are used for advertising. [5, 6]

1.1.1 Channel hopping

It was partially explained what channels are and what they are used for. It was explained why channels are used. Bluetooth technology uses 40 channels which are two MHz wide and are spaced by one MHz.

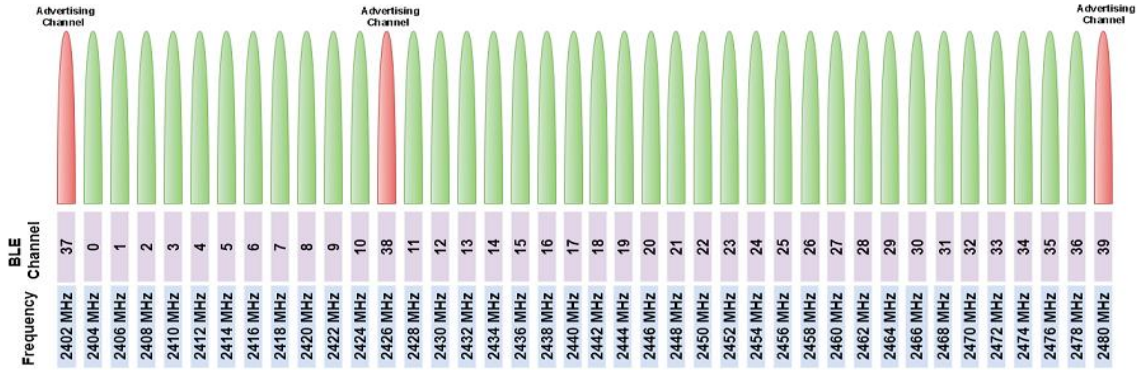

Figure 1 Bluetooth channel diagram [7]

In the picture above, it is possible to see that three of those 40 channels are used for "Advertising" and 37 are used for data transfer. This topic will be discussed in more details in following chapters. What is necessary to know is that they serve as a beacon for pairing. Multiple Advertising channels are utilized for the exact same reason as there are multiple data channels, and that reason is interference.

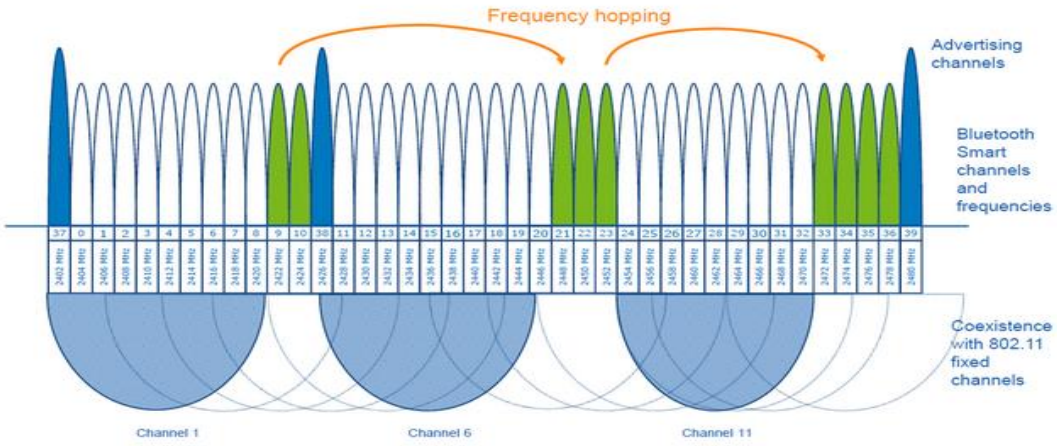

Figure 2 Channel hopping [8]

As pictured above, channel hopping is the process of cycling through different data channels. The figure above shows that Wi-Fi channels 1, 6 and 11 occupy most of the Bluetooth channels and thus only few of them are actually usable. Channel hopping is defined with the following formula: $fn+1=(fn+hop) mod 37$, where f_{n+1} is frequency or channel, which will be utilized in the next hop and *hop* is the number, which can be in the range of 5 – 16 and is set when the devices connect. [7, 8]

2 Aim of this thesis

This thesis is supposed to cover a small portion taken form the vast world of cyber security. Main problems with Bluetooth security over the years and how easy it can be for a determined cyber-criminal to get a strangle hold on IT systems or sensitive information. As discussed in previous chapters. The main idea for this thesis was to create a real-world example of hijacking a connection between a computer and a Bluetooth keyboard. This however proved much more problematic. Much more time, knowledge, and financial resources to put together the hardware necessary for a successful attack would be necessary. Of course. It would be possible to simply buy a product, that would allow carrying this attack out without any significant input. But where is the point in doing that. If any so-called script kiddie can successfully attack a real-world Bluetooth (or any other similar technology) with a simple click of a button, can it really be considered as an actual research? And even more importantly, is it really desirable to give someone who is neither skilled nor responsible enough the ability to go to the real world and wreak havoc upon the unsuspecting public?

This thesis is more of a PSA (Public Service Announcement) than an attack/defense guideline which is not exactly for the worst. Bluetooth, much like the internet was not created for the use cases for which it is used today. The internet was created for a fairly small, academic use group (or for military use). It was never intended to become this wide-spread network connecting absurd numbers of devices together. And form this wide-spread use which was not planed came security and technical complications. In the 90s computers were rare. Now nearly everyone has at least one PC and/or a mobile phone. This means not only exponential increase in the load on infrastructure but also exponentially more people, with no or extremely limited knowledge of IT as a whole. Even skilled masters of IT can fall victim to the ever-expanding world of the hacker subculture. Great example of this is the infamous NASA hack. [16] Tying this back to Bluetooth. People who have no knowledge of the technology they use and blindly trust it with their lives is a huge problem. This thesis should give a little bit of insight on how Bluetooth works and is secured.

In this thesis few potential attacks will be discussed. Some of them plausible, some of them easy and some of them basically impossible. Attack will be considered a complete success if:

A. User login credentials are obtained.
B. High level access to the target machine is obtained.
C. Keystrokes of the target Bluetooth peripheral device can be eavesdropped.

3 History and development

3.1 History

Like any other technology, Bluetooth is ever changing and improving technology. The original idea behind Bluetooth was the replacement of serial data cables. But over the years, it became much more than just mere cable replacement. Although Bluetooth is still used in industrial application, much higher percentage is used in civilian consumer market. [9]

Bluetooth is named after the king Harald Bluetooth. Even the Bluetooth symbol originates from this name. The Bluetooth symbol is created by overlaying the runes for H and B over each other. These runes are (Hagall) and (Bjarkan). [10]

Bluetooth was first implemented in the year of 1998. [11] Specifications for Bluetooth were created by the Special Interests Group also known as the abbreviation SIG. First implementation of Bluetooth was meant to replace the RS 232 serial cable link. SIGs founding members were: Ericsson, IBM, Intel, Nokia and Toshiba. The member count is up in the realms of 30 000. An interesting thing to note is that all Bluetooth protocols are backwards compatible with each other.

3.2 Development

With each iteration of the Bluetooth protocol, new features and functionality were added. This could mean improved transmission speeds, better security features or just general quality of life improvements. Development of this technology continues to accelerate developments in other technical fields such as much better computational power of devices. For comparison, the first lunar lander had an astonishing 0.003906 MB of RAM. Compared to today’s mobile phones, with over 6 GB of RAM, it is clear how strong today's tech is.

3.2.1 Bluetooth 1.x

The initial version of the Bluetooth technology. This version was plagued with problems and bugs, but it was a beginning, nonetheless. Bluetooth was initially intended to replace the RS 232 serial cable link mainly in industrial applications. What SIG did with this technology was ground-breaking at the time. Bluetooth effectively replaced IR (Infra-Red) link, which was shipped with mobile devices at that time. Bluetooth 1.x was first introduced in the year of 1999 and enabled users to share data with speeds of up to 721 kb/s (Kilobit per second). This version of Bluetooth was bundled together with higher price tier devices and still had a lot of problems with establishing a connection.

With advances done before the 2.x version mainly RSSI (Signal strength indicator), BDR (Basic Data Rate), AFH (Adaptive Frequency Hopping) and different bug fixes from previous versions, which includes fixing pairing problems and so on. Bluetooth 1.x was plagued with problems, which were mostly fixed before the 2.x version, but this version still lacks a lot of functionality that are common nowadays. [5, 12, 13, 25]

List of versions before 2.x:

- Bluetooth 1.0 – 1999
- Bluetooth 1.0b – 1999
- Bluetooth 1.1 – 2001
- Bluetooth 1.2 – 2003

3.2.2 Bluetooth 2.x

2.x version brought SSP (Secure Simple Paring), EDR (Enhanced Data Rate), which enables users to transfer data with boosted speeds. Other than new features, several bug fixes and overall quality of life improvements were made. 2.x version was much more common amongst devices and enabled users to transfer smaller sized files amongst devices. Even though the theoretical speed of the connection was brought to 2.2 Mb/s (Megabit per second) and the theoretical range

was pushed up to enable users to transfer data with up to 10 meters distance, transferring "larger" files would still take a lot of time and users would rather use USB cables or other means of transferring files amongst devices. Other improvements were mainly made in the pairing process which made Bluetooth technology much more consumer friendly and thus could enable much more appealing marketing for this technology. [5, 12, 13, 25]

List of versions before 3.x:

- Bluetooth 2.0 – 2004
- Bluetooth 2.1 - 2007

3.2.3 Bluetooth 3.x

Bluetooth 3.x introduced new feature dubbed HS (High Speed). This new feature enabled users to transfer data with speeds of up to 24 Mb/s and thus enabled users to transfer real world files over Bluetooth. This is not entirely true, because Bluetooth was not used to transfer the file itself. What was really happening is that Bluetooth was initially used to establish a connection between two devices and then Wi-Fi was used to transfer the file itself. Bluetooth was thus only used to establish a Wi-Fi link between the devices. Other new features include the introduction of the ERTM (Enhanced Retransmission Mode) and the use of alternative MAC and PHYs for transporting Bluetooth profile data. Other general improvements were made mainly in the power consumption area. The speed was also improved to one MB/s (Mega-Byte per second). [5, 12, 13, 25]

List of versions before 4.x:

- Bluetooth 3 + HS – 2009

3.2.4 Bluetooth 4.x

With the announcement of Bluetooth 4.0, Bluetooth LE (Low Energy) dubbed the Bluetooth Smart was introduced. The payload size was increased dramatically enabling us to transfer much

more data and thus the speed was improved as well. 4.2 version was designed for use with IoT (Internet of Things) and was the most used version of Bluetooth. [5, 12, 13, 25]

List of versions before 5.x:

- Bluetooth 4 – 2010
- Bluetooth 4.1 – 2013
- Bluetooth 4.2 - 2014

3.2.5 Bluetooth 5.x

Bluetooth 5.x brought general improvements to the security, range, and speed. This version is at time of writing the newest version of Bluetooth and most modern hardware is shipped with chips supporting 5.x versions. It is also worth mentioning that most Bluetooth versions from the 1.2 versions up are backwards compatible. This means ease of use to most people, but it also means vulnerabilities and technical limitations that can be classified as vulnerabilities. [5, 12, 13, 25]

List of versions:

- Bluetooth 5 – 2016
- Bluetooth 5.1 – 2019
- Bluetooth 5.2 – 2020

Table 1 Optional features [13]

Bluetooth Versions	Optional Features				
	Basic rate (BR)	Enhanced Data Rate (EDR)	High Speed (HS)	Low Energy (LE)	Slot Availability Masking (SAM)
Bluetooth 1.x	Yes	No	No	No	No
Bluetooth 2.x	Yes	Yes	No	No	No
Bluetooth 3.x	Yes	Yes	Yes	No	No
Bluetooth 4.x	Yes	Yes	Yes	Yes	No
Bluetooth 5.x	Yes	Yes	Yes	Yes	Yes

4 Physical principles of Bluetooth

4.1 Wavelength

Bluetooth uses a wavelength of 12.5 cm. This wavelength was calculated by using the following formula: $\frac{speed\ of\ light}{frequency\ [M]}$. Because Bluetooth does not use a single frequency but rather a frequency range, it works on a range of wavelengths of 12 – 12.5 cm. [14]

4.2 Interference

Bluetooth is not designed for a long range use but rather for short range PAN applications. Nonetheless, interference is a problem that must be solved for any wireless technology. Looking into mechanical interference, a 2.4 GHz signal is considered. This means that any water, be it inside of tree leaves or in the air due to rain or fog will highly affect the strength and stability of the signal. Other sources of interference are mainly other wireless devices operating in the 2.4 GHz specter. These devices, as discussed in previous chapters, are primarily other Bluetooth devices, but also Wi-Fi devices. Bluetooth solves this problem with channel hopping and adaptive channel hopping. Channel hopping is based around changing channels in a rapid succession with speed of 1600 hops a minute. Adaptive channel hopping is a more advanced variant which is generally preferable to standard channel hopping. ACH (Adaptive Channel Hopping) provides on the fly analysis of all 80 channels and negotiates use of only those channels which are in an acceptable state of interference. Added benefit of CH or ACH is that it is impractical to conduct frequency based direct jamming. 80 devices would be necessary to disrupt all channels of Bluetooth and thus this would only be practical with a significant level of equipment i.e. a car or a van filled with transmitters, power supplies and controllers. On the other hand, such an attack is more than feasible for standard European Wi-Fi networks with 11 channels or GPS, GSM networks. Legality of such “experiment” aside, this sort of attack would require limited know-how and not so significant monetary investment and could be carried out with a modified Wi-Fi

Cactus for plain 2.4 GHz Wi-Fi networks and with basically any capable transmitter for GPS or GSM networks. This however requires further research. [7, 8]

4.3 Transmitter power

Bluetooth devices are classified into 3 different power classes. Number 1 being the one with the strongest emissivity allowance and number 3 being the weakest. For comparison the 25 mW 5.8 GHz analog video transmitter used in FPV (First Person View) drone technology is capable of transmitting real time video feed back to the pilot's goggles from distances of up to several hundred meters away whilst keeping line of sight between said goggles and transmitting drone. Of course, this distance changes depending on the atmospheric and weather condition but nonetheless provides sufficient analogy for the explanation of how strong Bluetooth signal can be.

Now, that a baseline is established, real-world ranges to expect from those classes can be discussed. Class 1 devices are capable of working with 100 meters of separation between them, class 2 with 10 meters and class 3 with 1 meter. These numbers are just approximate. In the real-world other factors need to be considered. Most disruptive factors are other devices using the 2.4 GHz range (Wi-Fi, other Bluetooth devices, etc.). These devices create noise, which could be compared to audible sounds. As an analogy it is possible to imagine 2 people trying to have a conversation whilst there is a thunderstorm going on in the distance. Thunder created by the thunderstorm is overshadowing parts of the conversation and thus creating a „packet loss ". Other factors are, for instance, physical barriers i.e. wall. Bluetooth signal is capable of penetrating thinner or even brick walls but this kind of obstacle is certainly not wanted. As mentioned in previous chapters, water plays a big role as an interference factor for 2.4 GHz signals. It is possible to notice this with Wi-Fi signals. For instance, it can be seen in peoples' homes. In older family houses, it is possible to expect that in summer full Wi-Fi signal reception outside of the house will be possible. But in the winter or spring, it is possible to expect that have bad or even no reception will be available. Why is that? It is because the walls are soaked with water and thus rendering the signal useless. And lastly, there is the distance factor. Thanks

to the inverse square law, distance is a big factor when it comes to Bluetooth signal strength over distance. It is possible to assume that the mobile devices are capable of transmitting a signal at a distance of tens of meters. See Figure 3 for more accurate theoretical numbers. [15]

Power Class	Maximum Output Power (Pmax)	Nominal Output Power	Minimum Output Power[1]	Power Control
1	100 mW (20 dBm)	N/A	1 mW (0 dBm)	Pmin<+4 dBm to Pmax Optional: Pmin[2] to Pmax
2	2.5 mW (4 dBm)	1 mW (0 dBm)	0.25 mW (-6 dBm)	Optional: Pmin[2] to Pmax
3	1 mW (0 dBm)	N/A	N/A	Optional: Pmin[2] to Pmax

Figure 3 Power classifications [5]

5 Bluetooth security mechanisms

Bluetooth security can be divided into two main categories. These two categories are A – wireless link and B – physical chip security. The thesis focuses only on the first group. But it is worth to mention a little bit about what is going on with the chip itself. Focusing on the chip alone, there is an entirely new attack vector. It is not necessary to consider any encryption or any complications regarding sniffing Bluetooth. It is possible to go right to the source. Bluetooth has an interesting feature. This feature is, that raw, unencrypted data are accessible from the host device's system. This can provide an attacker with multiple opportunities to exploit this feature. It is possible again to categorize these opportunities into two main categories. First one being reconnaissance and second one being the attack itself. Considering that security through obscurity is a popular topic in security as a whole, what can be more beneficial to an attacker than look at how two devices communicate unencrypted. The second opportunity to actually attack a Bluetooth connection from the inside. Access to a device on the system level would be necessary, but this is certainly doable. There are rogue apps on the official stores from time to time, so it is not unimaginable that a rogue app could be smuggled into the store, which could then break bad and attack. [23] This scenario is however highly unlikely to result in a targeted attack just on the sheer unlikeliness of the target actually downloading the infected app. To conclude hardware-based attacks. They are interesting and can yield interesting results, but they are not the scope of this thesis.

As mentioned above, the thesis focuses solely on the wireless side of things. Bluetooth is a very interesting protocol in its resilience to sniffing. Only Bluetooth LE (Bluetooth smart) can be effectively sniffed with consumer grade hardware. Professional grade equipment is required for the sniffing of Bluetooth EDR and other versions.

5.1 Security modes

Authentication: verifying the identity of communicating devices based on their Bluetooth address. Bluetooth does not provide native user authentication.

Confidentiality: preventing information compromise caused by eavesdropping by ensuring that only authorized devices can access and view transmitted data.

Authorization: allowing the control of resources by ensuring that a device is authorized to use a service before permitting it to do so.

Message Integrity: verifying that a message sent between two Bluetooth devices has not been altered in transit.

Bluetooth connections are secured with one of four different security modes. As logic dictates. Mode one is the weakest and mode four is the strongest. Mode one is a more of a leftover from the times of Bluetooth 1.x and 2.0. It could be considered a compatibility tool. But as far as compatibility tools go, it is possible to assume that backwards compatibility spanning decades brings more to the table than just the ease of use. Taking enterprise software as an example. Many industrial and/or enterprise software solutions were written decades ago but are still in active use. These solutions are not limited to unimportant applications. It can be practically anything ranging from the program that is responsible for running the traffic lights to a backbone banking system that is responsible for handling payments. Even such critical applications as a solution for launching nuclear missiles are decades old and accept their launch keys in the form of 3.5” floppy disks. This backwards compatibility or lack of effort for modernization leaves us wide open to wide range of potential attacks. Such attacks can target the hardware itself in the case of traffic lights for example, where defeating a wafer lock is a trivial accomplishment and then changing the timing of selected traffic lights to either create traffic jams or even crashes to for example paralyze a city. And on the more destructive side of things there are nuclear missiles.

What carnage could a dedicated attacker achieve with nuclear missiles at his disposal is just up to an imagination. [5, 24]

5.1.1 Mode 1

Mode 1 connections are considered insecure. And for a good reason. As mentioned above, mode 1 links are more of a compatibility tool than a real feature. Mode 1 devices do not enable security (authentication and encryption) until instructed by another device. This leaves the connection without any protection from outside tampering and is a dream come true for any remote attacker. No exploit would be necessary because there is nothing to exploit and the connection can be used and abused at will. As mentioned above. Mode 1 devices will not use any sort of security measures until instructed to do so. If any other device sends a pairing, authentication or encryption request, mode 1 device will spring into action and enable its security mechanism per their respective Bluetooth specification version. All Bluetooth 2.0 and earlier devices are able to work in mode 1. All later Bluetooth version devices can support mode 1 for backwards compatibility reasons. However, using mode 1 is not recommended. [5, 24]

5.1.2 Mode 2

In security Mode 2, security procedures can be initiated after the link was established but before the logical channel itself was established. These procedures are a service level-enforced security mode. Security manager is described by the Bluetooth architecture and controls the access to the specific services. Policies for access control and interfaces with other protocols and users are controlled by the centralized security manager. Different security policies together with trust levels directed at access restriction can be defined for uses with different security needs to operate in parallel. Some services can be accepted without the need to accept others. This means, that it is possible to be selective with which services to allow and which to disallow. Mode 2 introduced the notion of authorization. Notion of authorization is a process which decides if a specific device is permitted or not. Bluetooth service discovery is usually done before any security checks such as authorization, encryption and so on. On the other hand, every other Bluetooth

service should require every security mechanism. Every Bluetooth version before and including 2.0 can support Mode 2. Every other Bluetooth version starting from 2.1 can support Mode 2 only with backwards compatibility purposes. [5, 24]

5.1.3 Mode 3

Mode 3 enforces link level security. This means, that security mode 3, unlike mode 2 initiates security measures even before the physical link itself was established in full. Devices operating within the Mode 3 are required to utilize encryption and authentication for each connection from and to a device. This in turn leads to a need for even simple service discovery routine having to be authorized and encrypted. After an authentication, service-level authorization is not utilized in most cases by a mode 3 device. As was the case with Mode 2, Mode 3 is also supported by up to and including Bluetooth version 2.0 devices and by newer versions in the backwards compatibility department. [5, 24]

5.1.4 Mode 4

Similarly, to Security Mode 2, Security Mode 4 (introduced in Bluetooth 2.1 + EDR) is a service-level-enforced security mode within which security procedures are initiated after physical and logical link setup. Security Mode 4 uses Secure Simple Pairing (SSP), within which ECDH key agreement is used for link key generation. Until Bluetooth 4.0, the P-192 Elliptic Curve was used for the link key generation, and therefore the device authentication and encryption algorithms were the image of the algorithms in Bluetooth 2.0 + EDR and earlier versions. Bluetooth 4.1 introduced the Secure Connections feature, which allowed the employment of the P-256 Elliptic Curve for link key generation. Bluetooth version 4.1 brought upgrades to the authentication algorithm. This upgrade utilizes HMAC-SHA-256 algorithm. The encryption algorithm was upgraded to the FIPS-approved AES-Counter with CBC-MAC (AES-CCM), which also provides message integrity. Requirements for services that are protected by the Mode 4 are classified in the following categories:

- Level 4: Authenticated link key utilizing Secure Connections is mandatory

- Level 3: Authenticated link key required
- Level 2: Unauthenticated link key required
- Level 1: No security required
- Level 0: No security required. (Only allowed for SDP)

If a link key is authenticated, it is subject to the SSP association model used. When both the local and remote device support the Secure Connections feature, the link key is generated using Secure Connections. Security Mode 4 requires encryption for all services (except Service Discovery) and is required for communication between 2.1 and later versions. Security Mode 4 devices are able to use any of the other three security modes when communicating with Bluetooth 2.0 and older versions that are unable to support Security Mode 4. [5, 24]

Table 2 Mode 4 summary [24]

Mode 4 Level	FIPS approved algorithms	Provides MITM protection	User interaction during pairing	Encryption required
4	Yes	Yes	Acceptable	Yes
3	No	Yes	Acceptable	Yes
2	No	No	Minimal	Yes
1	No	No	Minimal	Yes
0	No	No	None	No

5.2 Pairing and Link Key Generation

The most essential part of a secure communication between Bluetooth devices is a symmetric key. There is a different terminology used for BR/EDR (Link Key) and for Low Energy (Long-term Key). Short Term Key is used to exchange the Slave/Master Long Term Key in legacy low energy, but the Long-Term Key is created by both devices and is not shared for low energy secure connection. BR/EDR can use two different pairing methods. Modes three and two initialize key establishment with PIN. Whilst mode four utilizes Secure Simple Pairing. [5, 24]

6 Attack and attack vector

This chapter will discuss how is the attack meant to be carried out. The aim will not be to defeat the cryptological defense of the Bluetooth connection. This would be beyond the scope of this thesis and would most likely end up with not being able to break the encryption of the communication in real time. That being said. Bluetooth has its fair share of vulnerabilities. Vulnerabilities can be classified into 2 main categories:

- Vulnerabilities such as BIAS or KNOB enable to carry out successful MITM (Man In The Middle) attacks with key sniffing and key injection attacks.
- Lack of security. If Just Work operational mode is discussed as an example, there is four zeroes preset key. In some instances, complete lack of any encryption or message signing can be encountered, which would enable to carry out MITM attack. It is possible to say, that MITM is not even required. It is technically not even conducting a MITM attack. It is simply standing to the side eavesdropping on a conversation. MTTS (Man To The Side) would be a more fitting description.

Out of scope attacks are also worth mentioning. Windows is shipped with a “feature”. This feature is that any Windows machine inherently trusts any peripheral device that identifies itself as a UID (User Input Device). This feature is abused by tools such as Rubber Ducky. [17] Rubber Ducky and devices alike are modified USB thumb drives which allow the storage of a script which is after inserting the device into a USB port recognized as a UID device. Rubber Ducky than initializes the script stored in the memory. Example script would look like this:

```
SLEEP 3000
GUI + R
SLEEP 1000
https://www.youtube.com/watch?v=wtx0fdzRAp8
SLEEP 1000
ENTER
```

Sleep commands are used to avoid sending commands that are not actually registered by the target system. Number following a command is in milliseconds. GUI + R is a keyboard shortcut for Windows key + R key which brings up the Run prompt. The desired payload can then follow. In this case it is just a harmless YouTube vide but in real world use it could be a GIT command followed by a link to a RAT (Remote Access Tool) which would grant a persistent backdoor into the affected system. And lastly ENTER command will execute the Run prompt. This out of scope attack shows how unattended USB ports can be dangerous. In this case, it could simply avoid the problem of actually attacking a Bluetooth connection and we could simply walk to the target, plug in a USB Bluetooth dongle, and essentially gain a UID without the knowledge of the target. This could be done with a little bit of social engineering, misdirection or by the least subtle but still efficient direct interaction of simply spilling a drink on the target. Not the computer minds you, but the operator. Whilst another attacker plugs in the dongle.

6.1 KNOB

KNOB (Key Negotiation Of Bluetooth) is an attack, which targets vulnerabilities in the entropy of a key. Entropy is a randomness of a key. KNOB targets the integrity of a session key that is used to cipher and decipher communication between two devices. This attack can be implemented to multiple Bluetooth link simultaneously but for the sake of simplicity the chapter will only focus on a single link attack.

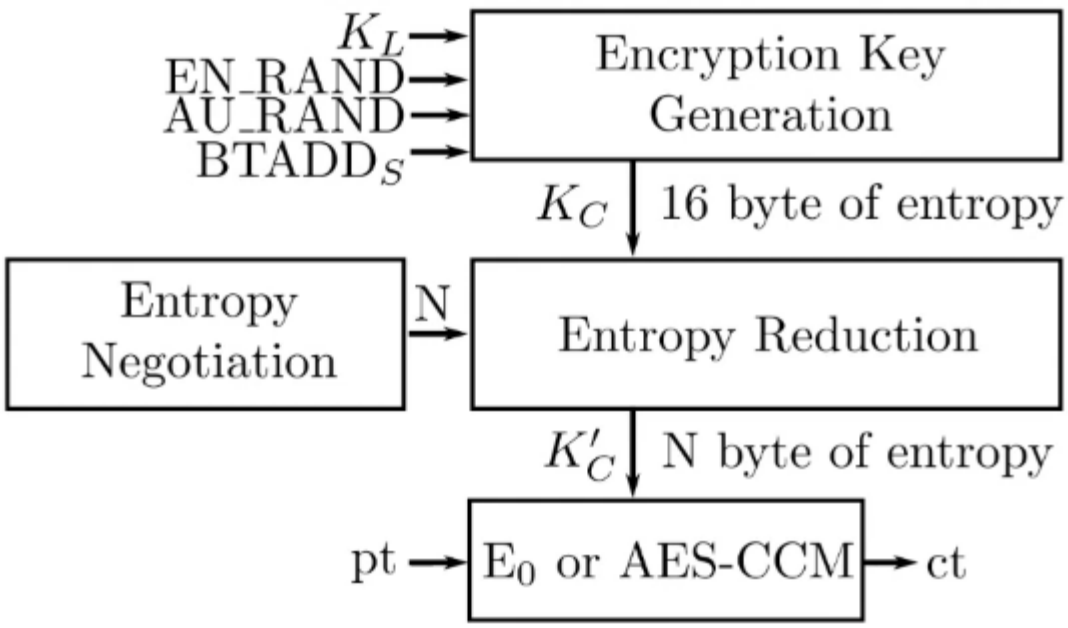

Figure 4 Entropy negotiation [18]

Pictured above (Figure 4) is the Kc (session key) negotiation process. This process takes multiple inputs and outputs the session key. Bluetooth specification compliant entropy lengths are ranging from one to 16 bytes. The goal is to change the standard 16 bytes entropy values to only 1 byte, which would enable to brute force the Kc (session key) in real time. 1 byte of entropy is equal to 2^8 = 256 different key possibilities which could be brute forced on paper by hand, let alone with a laptop. Other security concern is that entropy negotiation is not encrypted, nor integrity checked. Meaning that there is almost complete freedom regarding manipulation of entropy values. It is also worth mentioning, that it does not really matter, if the targets use the legacy E0 encryption or AES-CCM. The attack works either way with only slightly longer brute-forcing times for the AES-CCM encryption.

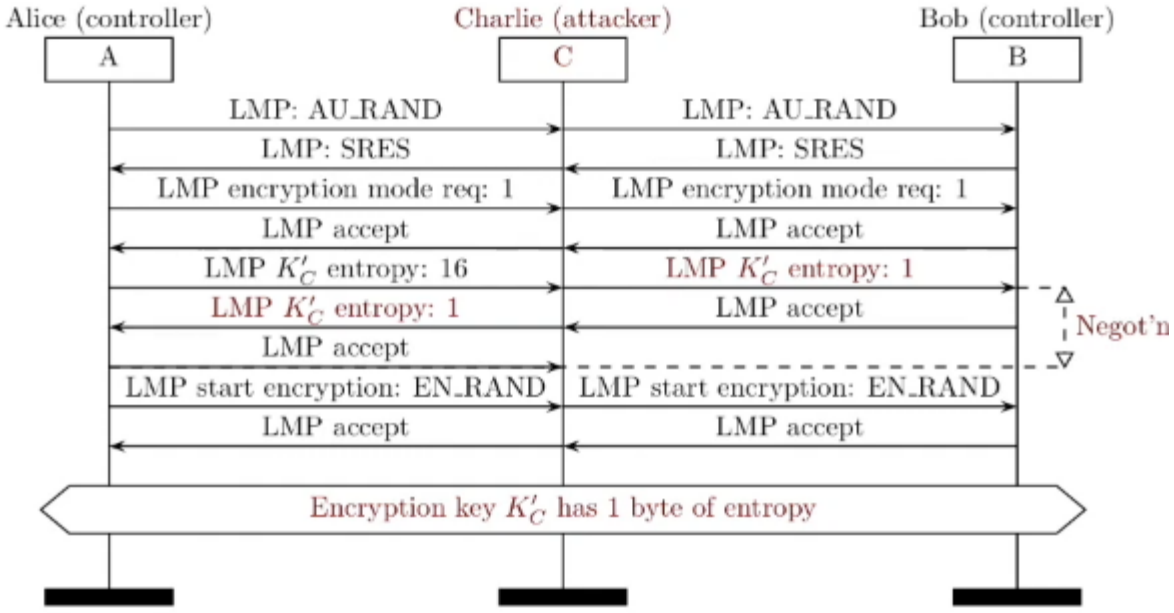

Figure 5 Entropy negotiation attack [18]

Pictured above is an entropy negotiation attack. The attack works as follows. Charlie (attacker) intercepts Alice's request for 16 bytes of entropy. Charlie changes the value from 16 bytes to 1 byte and forwards the message to Bob. Bob sends accept message to Alice which is again intercepted by Charlie and changed to change entropy to one-byte message. Lastly Alice sends accept message to Bob, which is again intercepted by Charlie and dropped. And the attack is finished. Because this process is not encrypted nor integrity protected, this entire communication is carried out in cleartext and can be easily manipulated.

Bluetooth chip	Device(s)	Vulnerable?
Bluetooth Version 4.1		
BCM4339 (CYW4339)	Nexus5, iPhone 6	✓
Snapdragon 410	Motorola G3	✓
Bluetooth Version ≤ 4.0		
Snapdragon 800	LG G2	✓
Intel Centrino 6205	ThinkPad X230	✓
Chicony Unknown	ThinkPad KT-1255	✓
Broadcom Unknown	ThinkPad 41U5008	✓
Broadcom Unknown	Anker A7721	✓
Apple W1	AirPods	*

Figure 6 Vulnerable devices [18]

The KNOB attack was discovered in May of 2018 and reported to SIG in October of 2018. It could be classified as a fairly new vulnerability.

Now, that attack functions were discussed, it is possible to discuss how to defend against it. The main problem is that the entropy negotiation is transmitted in cleartext. There should be encryption or integrity protection in place, that would essentially make this attack obsolete. Other than that, it is possible to implement TLS over Bluetooth, rendering this attack essentially obsolete. There are of course vulnerabilities and security concerns with TLS as well, but TLS as a whole is much more resilient to eavesdropping. And of course, Bluetooth was not designed to be this impenetrable protocol used for the transfer of highly sensitive or classified data. [18, 19]

6.2 BIAS

BIAS stands for Bluetooth Impersonation AttackS. As the name suggests, BIAS enables to impersonate either Master or Slave in the connection. In order to conduct a MITM (Man In The Middle) attack, it is necessary to impersonate both sides of the targeted connection (Master and

Slave simultaneously). This could be considered a slight complication, but it is nothing, that could not be overcome easily.

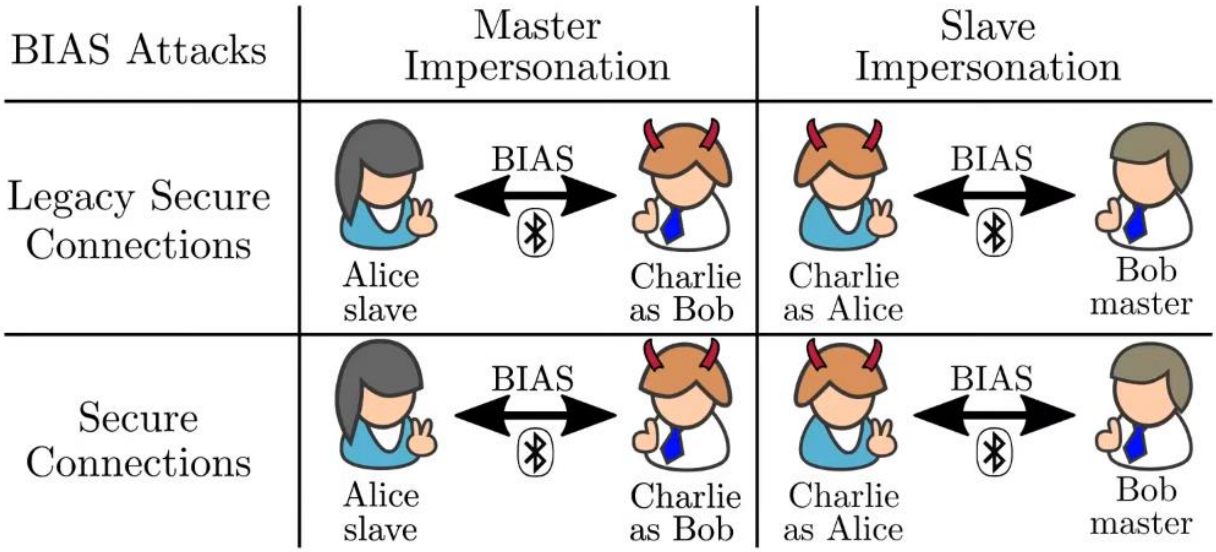

Figure 7 Attack scenarios [20]

Bluetooth uses 2 security modes. The first is LSC (Legacy Secure Connection) and the second is SC (Secure Connection). For each of these modes there are 2 sides, Master and Slave. These attacks vary slightly but ultimately, they resolve in the same thing which is a compromised Bluetooth link.

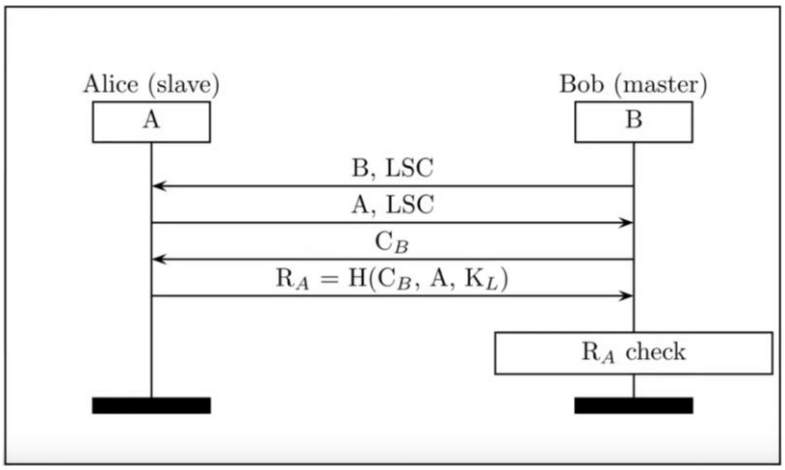

Figure 8 LSC Authentication [20]

Pictured above is the process of LSC Authentication. Bob and Alice exchange their Bluetooth addresses which are in turn used to calculate a challenge which is used for authentication. What is important about LSC, is that it is only unilateral authentication. The master in LSC communication initializes the authentication with a request, and only the slave has to authenticate to the master. This is exactly how the attack works. By exploiting this process, it is possible to impersonate both sides respectively and thus create a MITM situation and completely disrupt the integrity and security of the targeted link.

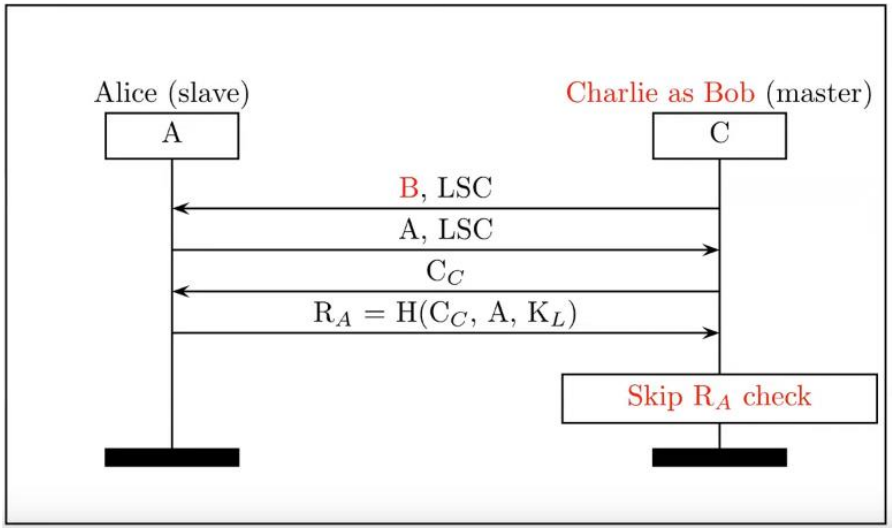

Figure 9 LSC Master impersonation [20]

Figure 9 shows how master impersonation is carried out in the LSC mode. Charlie (Attacker) poses as Bob and carries out session establishment without having to authenticate to Alice. Instead, Alice authenticates to Charlie, who is posing as Bob.

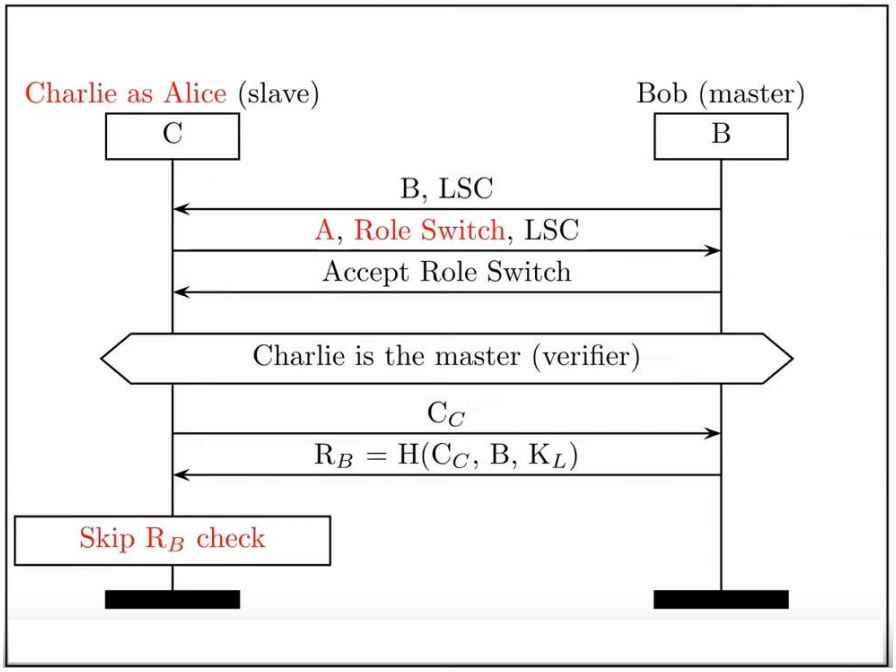

Figure 10 LSC Slave Impersonation [20]

In figure 10, it is possible to notice Charlie posing as Alice (Slave). As mentioned previously, LSC mode enables Master to authenticate its slave. Bluetooth standard enables to request a role switch and thus to become the new master of the targeted Bluetooth link. In this case, Bob sends "Alice" his Bluetooth address and a LSC connection request. "Alice" in turn sends Bob his Bluetooth address and requests a role switch. Bob is happy to switch roles because it is a standard compliant message. Now "Alice" is the new master and can authenticate Bob as a slave.

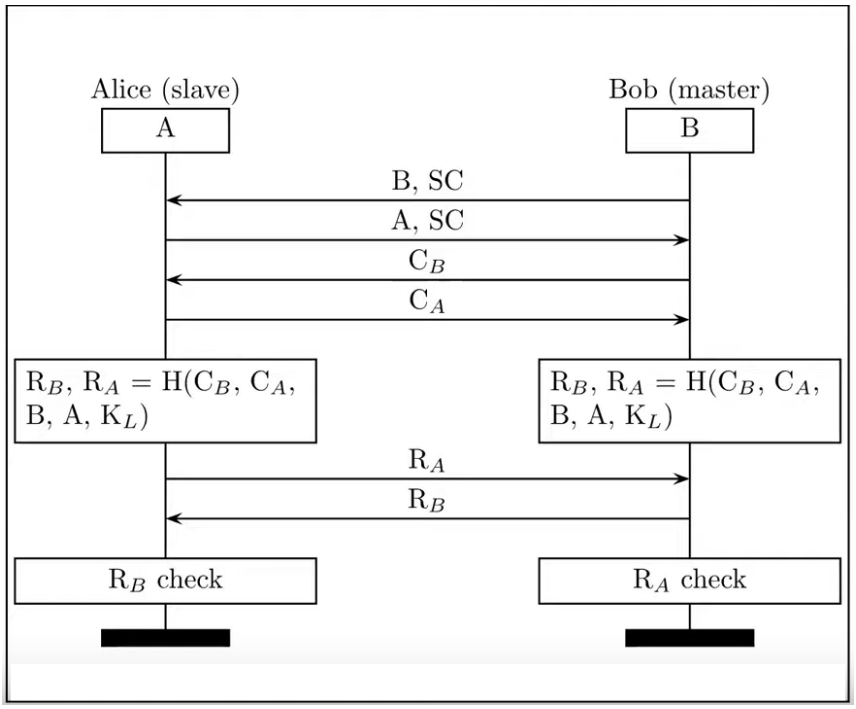

Figure 11 SC Authentication [20]

SC authentication differs compared to LSC authentication in many ways. Mainly in regard to authentication. Unlike LSC, SC supports multilateral authentication. This means, that master has to authenticate to the slave and slave has to authenticate to master. This complicates our attack a little bit. But it is definitely not a deal breaker. Figure 11 shows how SC mode works. First steps of establishing a secure connection require the two participants to share their Bluetooth addresses and an agreement on which security mode to establish a connection. In this case, the mode is SC. After this initial step, the two participants exchange security challenges Cb and Ca. Both sides (Bob and Alice) compute responses to previously mentioned security challenges Cb and Ca. Responses are named Rb and Ra. These responses are then used for authentication. For example. If Bob receives a Ra response, he will check it against his own computation. If these challenges match, secure connection can be established. If they do not match, the connection is aborted.

A considerable problem with SC, is that its process is not integrity protected. This is exactly the security problem; it will be abused in the attack later. For now, it suffices to say that BIAS is in a way similar to downgrade attacks on the TLS protocol. Where, for example, TLS 1.2 is not as easily broken, it is possible to carry out a downgrade attack to an earlier version, which are much easier to compromise.

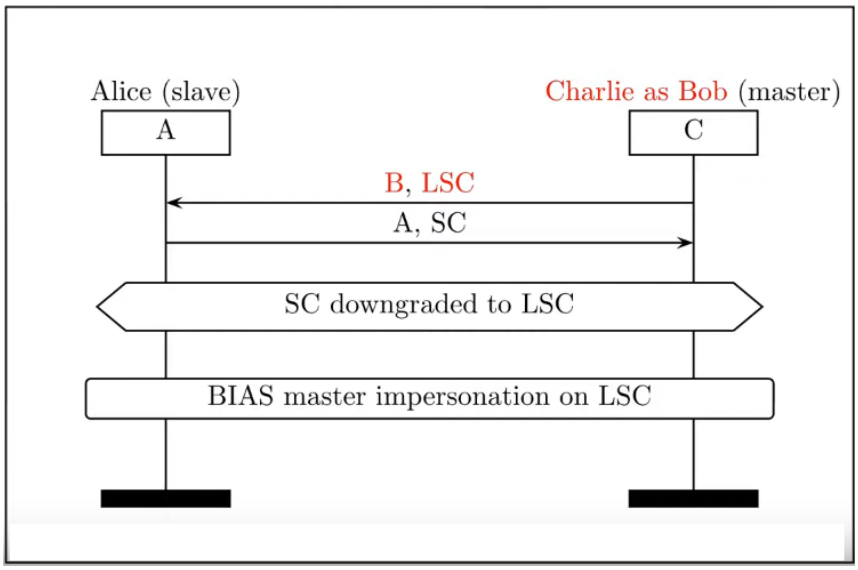

Figure 12 SC Master impersonation [20]

As mentioned above, BIAS attack on SC is not dissimilar to TLS downgrade attack. Because that is exactly what is going on here. Attacker, posing as Bob sends their Bluetooth address to Alice, together with request to downgrade from SC to LSC. This request is standard compliant and thus is accepted and carried out. From this point on, the attacker carries out LSC master impersonation attack.

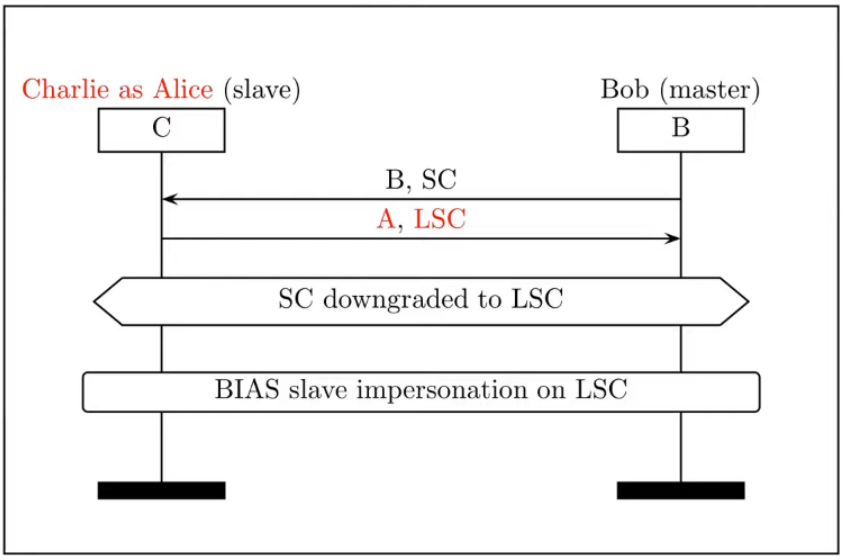

Figure 13 SC Slave impersonation [20]

SC slave impersonation is practically identical to the SC Master impersonation attack. The only difference is that the attacker sends LSC downgrade request after link Master sends his SC request and his Bluetooth address. [20, 21]

		LSC		SC	
Chip	Device(s)	MI	SI	MI	SI
Bluetooth v5.0					
Apple 339S00397	iPhone 8	●	●	●	●
CYW20819	CYW920819EVB-02	●	●	●	●
Intel 9560	ThinkPad L390	●	●	●	●
Snapdragon 630	Nokia 7	●	●	●	●
Snapdragon 636	Nokia X6	●	●	●	●
Snapdragon 835	Pixel 2	●	●	●	●
Snapdragon 845	Pixel 3, OnePlus 6	●	●	●	●
Bluetooth v4.2					
Apple 339S00056	MacBookPro 2017	●	●	●	●
Apple 339S00199	iPhone 7plus	●	●	●	●
Apple 339S00448	iPad 2018	●	●	●	●
CSR 11393	Sennheiser PXC 550	●	●	-	-
Exynos 7570	Galaxy J3 2017	●	●	-	-
Intel 7265	ThinkPad X1 3rd	●	●	-	-
Intel 8260	HP ProBook 430 G3	●	●	-	-

Figure 14 Vulnerable devices [20]

6.3 Attack vector conclusions

BIAS and KNOB are very powerful and useful attacks which can be carried out with open-source software, firmware, and hardware. Recommended hardware for this attack is Ubertooth One or newer. [22] Using TLS over Bluetooth would render this attack completely obsolete, because even with pseudo clear text access to data being transferred over compromised link would be encrypted with TLS which is much harder to compromise. Bluetooth is and will be vulnerable to any number of potential attacks. This statement can and is true for any wireless technology. Even if the protocol is completely immune to all attacks which is something that just does not happen, it is still possible to record this data transfer and store it for later use. Great example would be communication between a secret service agent and his headquarters in his home country. The enemy may not be able to break the encryption in real time, but given enough time and technological advance, it is possible to speculate what could be done with this conversation. In this use case it does not matter, if it is possible to read this data now, or in 10 years. The important thing is that it is possible to read it at all. Development of ciphers and cipher attacks is a hot topic accelerated by the spreading fear, that quantum technology brings. The world is decades, if not centuries away from a true quantum computer with enough computational power. But when the day comes, the world will change.

7 Conclusions

Bluetooth is surrounded by risks to security and stability. This thesis described some of these risks, how they function and partially how to defend against them. One of the most devastating potential risks associated with Bluetooth and its security is uninformed user which tries to use Bluetooth in a way that depends on the security mechanism that Bluetooth utilizes. Bluetooth was not designed as an impenetrable fort with layers and layers of security. This fact changed over the years, but it did not change the fact that there are still critical vulnerabilities that will allow an attacker to compromise a specification compliant Bluetooth link. As was stated in previous chapters attack this thesis described are most suited for precise even surgical targeted attacks with a specific purpose of extracting information. Be it with wireless snooping or with using a Bluetooth as a vector from which we initiate a final attack.

Risks of utilizing Bluetooth for anything other than listening to music or connecting a wireless mouse to a computer are obvious. User is presenting himself as a target for a potential attacker. Main reasons are:

- Bluetooth is a wireless protocol. Wireless technology is and will always be easier to manipulate and attack because anyone with the right equipment can listen to our channels and is subsequently able to manipulate established links.
- Security mechanisms which are in place can be partially of fully bypassed as of the latest Bluetooth version. This fact is unlikely to change in the foreseeable future and considering the ever-faster development of IT technology as a whole it is likely to be much easier for attackers to compromise Bluetooth links.

Chapter six described two Bluetooth vulnerabilities that are relatively easy to execute and have great impact on the integrity of attacked Bluetooth link. These two vulnerabilities are certainly not the only ones that are threatening the security of Bluetooth as a whole. These two vulnerabilities were chosen because they are a great example of how security mechanism can be

bypassed or even used by the attacker to achieve his goals. This thesis briefly touched up the vector of attacking the Bluetooth stack directly in the host device and thus getting unobstructed view of the inner workings of a for example Bluetooth enabled device. This knowledge can then be used by an attacker to develop an attack suited directly for the said device.

Chance of an attack succeeding is fairly high. This statement takes into account the fact that Bluetooth is a wireless protocol. This is not the only factor. The main factor is that Bluetooth is not designed to be impenetrable because it is not meant to be. It is meant to be as user friendly as possible and utilized for uses which do not require a strong resilience against attacks. Bluetooth is more than resilient against interference created by the environment or by other devices utilizing the same frequency bands.

Bibliography

[1] Side Channel Attack - an overview | ScienceDirect Topics. ScienceDirect.com | Science, health and medical journals, full text articles and books. [online]. Copyright © 2020 Elsevier B.V. or its licensors or contributors. [cit. 18.10.2020]. Available from: https://www.sciencedirect.com/topics/computer-science/side-channel-attack

[2] RB Key | Raiffeisenbank. Banka inspirovaná klienty | Raiffeisenbank [online]. Copyright © [cit. 18.10.2020]. Available from: https://www.rb.cz/en/personal/accounts/services-to-account/internet-banking/rb-key

[3] Apple case: judge rejects FBI request for access to drug dealer's iPhone | Technology | The Guardian. [online]. Copyright © 2020 Guardian News [cit. 18.10.2020]. Available from: https://www.theguardian.com/technology/2016/feb/29/apple-fbi-case-drug-dealer-iphone-jun-feng-san-bernardino

[4] StatCounter Global Stats - Browser, OS, Search Engine including Mobile Usage Share [online]. Available from: https://gs.statcounter.com/os-market-share

[5] Bluetooth Core Specification. 5.2. 2019.

[6] Introduction to Bluetooth Low Energy (BLE) | Argenox. Wireless Connectivity Solutions and Product Development | Argenox [online]. Copyright © 2020 Argenox Technologies LLC. All rights reserved. [cit. 18.10.2020]. Available from: https://www.argenox.com/library/bluetooth-low-energy/introduction-to-bluetooth-low-energy-v4-0/

[7] MathWorks - Makers of MATLAB and Simulink - MATLAB & Simulink [online]. Copyright © 1994 [cit. 18.10.2020]. Available from: https://www.mathworks.com/help/comm/ug/ble-channel-selection-algorithms.html;jsessionid=b82342b887156f4d7d2ee60b64ed

[8] Bluetooth® Low Energy Channels - Developer Help. Home - Developer Help [online]. Copyright © 2020 Microchip Technology, Inc. [cit. 18.10.2020]. Available from: https://microchipdeveloper.com/wireless:ble-link-layer-channels

[9] The State of Bluetoothin 2018 and Beyond | Bluetooth® Technology Website. Bluetooth® Technology Website [online]. Copyright © 2020 Bluetooth SIG, Inc. All rights reserved. [cit. 18.10.2020]. Available from: https://www.bluetooth.com/blog/the-state-of-bluetooth-in-2018-and-beyond/

[10] Origin of the Name | Bluetooth® Technology Website. Bluetooth® Technology Website [online]. Copyright © 2020 Bluetooth SIG, Inc. All rights reserved. [cit. 18.10.2020]. Available from: https://www.bluetooth.com/about-us/bluetooth-origin/

[11] 20 years of blue - Experience the interactive history of Bluetooth. Bluetooth® Technology Website [online]. Copyright © [cit. 18.10.2020]. Available from: https://www.bluetooth.com/wp-content/uploads/Sitecore-Media-Library/20year/default.html

[12] Bluetooth Technology: What Has Changed Over The Years | by Jaycon Systems | Jaycon Systems | Medium. Medium – Where good ideas find you. [online]. Available from: https://medium.com/jaycon-systems/bluetooth-technology-what-has-changed-over-the-years-385da7ec7154

[13] Bluetooth Versions Comparison & Profiles - RTINGS.com. Reviews and Ratings - RTINGS.com [online]. Copyright © 2020 9298 [cit. 18.10.2020]. Available from: https://www.rtings.com/headphones/learn/bluetooth-versions-comparison-profiles

[14] PAPIEWSKI, John. Bluetooth Wavelength & Frequency. Techwalla.com [online]. 2020, s. 549-562 [cit. 2020-10-18]. ISBN 978-1-7281-3497-0. ISSN 2375-1207. Available from: https://www.techwalla.com/articles/bluetooth-wavelength-frequency

[15] What is a Bluetooth class and what is a Bluetooth profile?. We make parts for IT & A/V professionals that connect, convert, extend, split & switch [online]. Copyright © 1985 [cit. 18.10.2020]. Available from: https://www.startech.com/en-us/faq/bluetooth-adapters-classes-and-profiles

[16] Gary McKinnon reveals detail on NASA data breach and ‘extraterrestrial life’ | WeLiveSecurity. WeLiveSecurity [online]. Copyright © ESET, All Rights Reserved [cit.

18.10.2020]. Available from: https://www.welivesecurity.com/2015/12/08/gary-mckinnon-reveals-detail-on-nasa-data-breach-and-extraterrestrial-life/

[17] MalDuino Elite. MalDuino Elite [online]. Available from: https://maltronics.com/collections/malduinos/products/malduino-elite

[18] ANTONIOLI, Daniele, Nils Ole TIPPENHAUER a Kasper B. RASMUSSEN. The KNOB is Broken: Exploiting Low Entropy in the Encryption Key Negotiation Of Bluetooth BR/EDR [online]. Oxford: University of Oxford, 2019 [cit. 2020-10-18]. ISBN 978-1-939133-06-9. Available from: https://www.usenix.org/system/files/sec19-antonioli.pdf

[19] KNOB Attack. KNOB Attack [online]. Available from: https://knobattack.com/

[20] ANTONIOLI, Daniele, Nils Ole TIPPENHAUER a Kasper RASMUSSEN. BIAS: Bluetooth Impersonation AttackS. In: IEEE Symposium on Security and Privacy (S&P). San Francisco: IEEE,

[21] BIAS. Daniele Antonioli [online]. Available from: https://francozappa.github.io/about-bias/

[22] Ubertooth One - Hacker Warehouse. Hacker Warehouse - Your one stop computer security shop. [online]. Copyright ©. All Rights Reserved. [cit. 18.10.2020]. Available from: https://hackerwarehouse.com/product/ubertooth-one/

[23] Android security: Six more apps containing Joker malware removed from the Google Play Store | ZDNet. Technology News, Analysis, Comments and Product Reviews for IT Professionals | ZDNet [online]. Copyright © 2020 CBS Interactive. All rights reserved. [cit. 18.10.2020]. Available from: https://www.zdnet.com/article/android-security-six-more-apps-containing-joker-malware-removed-from-the-google-play-store/

[24] PADGETTE, John, John BAHR, Mayank BATRA, Marcel HOLTMANN, Rhonda SMITHBEY, Lily CHEN and Karen SCARFONE, 2017. Guide to bluetooth security [online]. Available from: doi:10.6028/NIST.SP.800-121r2

[25] Inside bluetooth low energy. Second edition. London: Artech House, 2016. ISBN 9781630813703.

List of figures

List of tables

List of abbreviations

ACH	Adaptive Channel Hopping
AFH	Adaptive Frequency Hopping
BDR	Basic Data Rate
BR/EDR	Basic Rate / Enhanced Data Rate
CH	Channel hopping
CMD	Command line
EDR	Enhanced Data Rate
ERTM	Enhanced Retransmission Mode
FPV	First Person View
GHz	Giga Hertz
HS	High Speed
HVT	High Value Target/s
IoT	Internet of Things
IR	Infra-Red
ISM	Industrial, Scientific, Medical
kb/s	Kilobit per second
Kc	session key
LE	Low Energy
LSC	Legacy Secure Connection

MAC	Media Access Control Address
Mb/s	Mega bit per second
MHz	Mega Hertz
MITM	Man In The Middle
MS	Microsoft
mW	milliwatt
OTC	One Time Code
PAN	Personal Area Network
PHY	Physical address
PSA	Public Service Announcement
RSSI	Signal strength indicator
SC	Secure Connection
SDP	Service Discovery Protocol
SIG	Special interests group
SSP	Secure Simple Paring
TLS	Transport Layer Security
Wi-Fi	Wireless Fidelity
WPAN	Wireless Personal Area Network