A Survey into Bluetooth: BIAS and KNOB Attacks

Garrett Strange
November 22, 2020

ABSTRACT

An exploration into Bluetooth, impersonation, and negotiation attacks based upon a man in the middle attack approach and decoding encryption algorithms discussed in class. The research conducted follows Daniele Antonioli, Nils Ole Tippenhauer, and Kasper Rasmussen since they are the ones to research and execute these attacks originally. These attacks are relevant today since they happened within the last 2 years and have since been addressed by the Bluetooth Special Interest Group. This paper will explore the use of Bluetooth, how these attacks work, and the devices affected as well as the procedures taken to defend from these attacks in the future.

Key Words- BIAS, KNOB, impersonation attack, long-term key, Bluetooth, man in the middle, legacy, secure connection, SIG

Description- An exploration into Bluetooth impersonation and negotiation attacks to compromise modern Bluetooth devices.

TABLE OF CONTENTS

1. INTRODUCTION

Modern Bluetooth has revolutionized how we as consumers and producers use technology at a day to day basis. With an emphasis on Bluetooth devices and wireless personal access points in general this raises the question, how stable is this platform that we use and take for granted? When pairing devices how do we know it is the same device we paired with last time and not an imposter disguising themselves as the device on the other end? For all we know there is an attacker waiting on the other end waiting for us to hit the pair button and stealing potentially valuable information without the user being aware. This survey will go into exactly that, an attack coined BIAS or spelled out Bluetooth Impersonation Attacks as well as a look into KNOB(Key Negotiations Of Bluetooth) attacks since both work hand in hand to break standard Bluetooth protocol across the majority of modern Bluetooth capable devices [Antonioli et al1].

2. BLUETOOTH OVERVIEW

This section will be a brief overview of Bluetooth and its specifications to allow a better understanding of what exactly is happening in these attacks. When researching these attacks there were a lot of acronyms and nomenclature that will be explained in their respective sections.

2.1) *What is Bluetooth*

Bluetooth is a personal access network (PAN) technology that allows pairing of devices within their own closed network [wikipedia5]. A Bluetooth network is considered an “octet” which is eight devices in a network that will automatically communicate with each other if Bluetooth pairing is prompted. This can be seen when using a mobile device to connect to wireless headphones, and then the same device can be used to pair to a car radio system just by being in proximity.

To pair Bluetooth devices a predetermined protocol is followed which allows the devices to pair with each other and this protocol changes if the devices have been connected before which the BIAS and KNOB attack will exploit in a later section. The first pairing will always be the most secure since it normally requires a PIN code of some sort, like a bank account, which ensures that both devices are safely connected. This first connection is known as establishing a long-term key, which becomes relevant later since this key is what the KNOB attack breaks [Antonioli et al1].

2.2) Bluetooth Protocol

The Bluetooth protocol consists of an authentication process in which each device will test the other device to ensure both devices are who they indicate they are. This involves the long-term key described above and the Bluetooth address of each device. Below is an example of how two devices interact with each other on authentication.

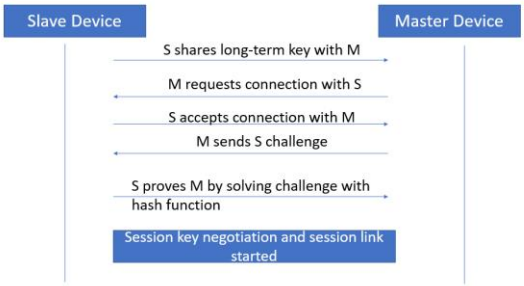

Fig 1.) An example of how two Bluetooth devices share the long-term key with each other as well as prove and authenticate the device. This is known as legacy secure connection [Antonioli et al1]. S/M are abbreviations for slave and master devices.

As seen above in Fig 1 this process requires the slave device to prove to the master device that it knows the hashing algorithm used to authenticate the devices. Notice however, that the master does not have to prove to the slave device that it is indeed the master. This is the first flaw shown in Bluetooth since the attacker can just give the slave device a challenge within the usual threshold Bluetooth operates in, essentially allowing the attacker to act as the master and impersonate the real master device.

There is another, better implementation of the Bluetooth which involves the slave and master devices swapping roles to make sure the authentication process does not have any loopholes. This requires both the slave and

master to prove to each other they know the hash function since it requires knowing the long-term key and unlike the legacy secure connection one side of the connection cannot be faked easily. The next section will explain how the encryption process works, as well as a general encryption algorithm is used and why.

2.3) Bluetooth Encryption

To ensure Bluetooth is secure, a hashing algorithm is used between key pairs when devices make their long-term key. Newer Bluetooth uses this process called Secure Simple Pairing (SSP) [Antonioli et al2]. This is better than the legacy pairing explained later but requires an encryption algorithm built into the Bluetooth device.

Since Bluetooth is inherently low energy, meaning it only uses as much power as needed to keep the connection, and is rather small, it requires a small but efficient encryption algorithm for device pairing. This is accomplished by using an algorithm called elliptic-curve cryptography which is only 16 bytes long but is difficult enough to crack that it is good enough for use in the long-term key encryption process [wikipedia6].

This elliptic-curve encryption is powerful since Bluetooth chips do not have the space to store normal security systems like RSA (Rivest-Shamir-Adleman), which use upwards of 3000 bytes since their algorithm is based on large prime numbers [wikipedia6]. This works by building the elliptic curve's architecture into the Bluetooth chip, so all chips have similar instructions in how to form the long-term key as well as how to solve it while keeping the space used relatively low. These specifications are changed based on the Bluetooth Special Interest Group which monitors and releases mandatory updates to Bluetooth for them to be of industry standard [wikipedia5].

2.4) Bluetooth SIG

To wrap up on the background of Bluetooth it is important to address the Bluetooth Special Interest Group (SIG) since they are the organization behind how Bluetooth functions and how it is distributed at an industrial level. It is important to note however, that Bluetooth SIG does not sell Bluetooth products but is rather a research group that helps guide the standard for devices and chips. For a Bluetooth chip to be qualified as true Bluetooth it must pass specifications created by the group [wikipedia5].

This becomes important since these attacks were never released to the public or acted upon for a malicious purpose but rather educational to show exploits that could be abused if not fixed in the future.

To wrap up, Bluetooth has been developed to be used on a daily basis so knowing how it functions at an architectural level is important to discuss the attacks on this architecture and the groups behind making Bluetooth functional at an industrial level.

3. BIAS OVERVIEW

Bluetooth Impersonation Attacks, abbreviated as BIAS, involves exploiting the Bluetooth authentication process without involving the long-term key pair created at device connection creation. This man in the middle attack involves impersonating as a device trying to pair with an already existing device in a Bluetooth without knowing the long-term key that was established at the first key pair between devices. This section will discuss the different approaches this attack uses to gain access into a Bluetooth network in both legacy and more modern secured connection authentications.

3.1) Legacy Secure Method

Using the same procedure as described in Fig 1 it may be obvious now how the legacy secure connection has a glaring vulnerability an attacker can exploit. The master device never needs to prove to the slave device that the master is actually the master and not an impersonator. Since the BIAS attack can just disguise itself as the master, the slave will never know it is connecting to another device since the authentication process will be executed without errors each time.

This assumption may seem simple, but this is exactly why these Bluetooth connections are

considered legacy since they are not in use for modern Bluetooth connections. What does become interesting however is that this method still works if we flip the impersonator to act as the slave as well. The figure below will show an example of this.

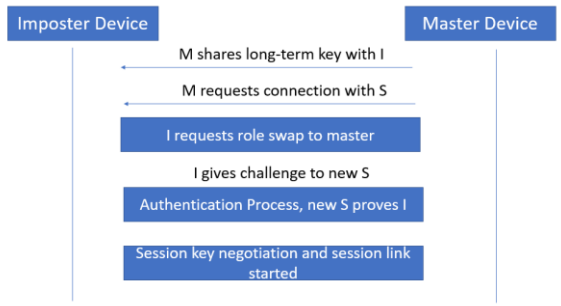

Fig 2.) This model shows how even as the slave device, the imposter can ask for a role swap and the master will accept and become the new slave, completely negating needing the long-term key and allowing authentication without the key again similar to Fig 1 [Antonioli et al1]. I is abbreviated for the imposter device and M/S is for master and slave respectively.

To explain this a bit more this attack can abuse the fact that legacy secure connections can swap roles without proving who they are beforehand. This creates a compromised system whether the impersonator is the slave or the master since the attacker can just ask for a swap and authenticate like there was nothing wrong to begin with while also making the new slave prove it is actually the other device with the attacker never having to prove anything.

3.2) Modern Secure Connection

To counter this legacy breach, Bluetooth also allows a secure connection only mode [Loveless], which only allows connections and information to come and go through an encryption algorithm as described above in the elliptic curve section. This requires more power however and in situations where Bluetooth is not given this extra duty cycle it bogs the device connection down. This makes secure connection more situation since this method is not always available even if it is a better strategy than running the legacy connection protocol.

As mentioned in the paragraph before, secure connection deals with adding a layer of encryption to the Bluetooth connection and transmission between devices. Secure connection also requires extra steps in the authentication process including the role switching of master and slave, which helps increase the security threshold on devices, but requires more power than some Bluetooth devices can handle or are allowed to handle.

This BIAS attack however does not stop at legacy connection and, because of an unseen flaw in the architecture of Bluetooth, can easily break into the secure connection protocol with ease.

3.3) Downgrade Attack Method

The first way BIAS breaks secure connection protocol is by feigning ignorance to secure connection. Since secure connection is a fairly new concept in Bluetooth devices have a legacy protocol built in to fall back on if the device says it does not understand secure connection. Below is a diagram describing the process.

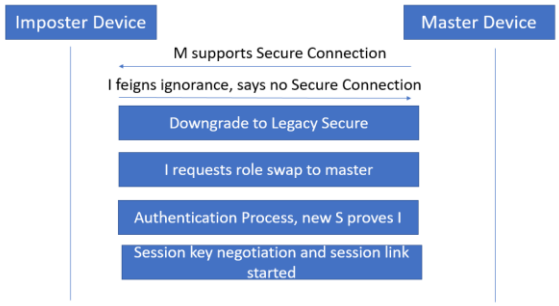

Fig 3.) Downgrade method to get back to legacy secure connection, the same process as Fig 2 except the imposter acts like it does not know what secure connection is and bypasses this by downgrading the connection to legacy [Antonioli et al1].

As seen in Fig 3 this method goes around the more secure connection and negotiates to the other device that legacy connection is enough to create a session link. Notice again how no long-term key was needed and again the old master device actually proves to the imposter that it is the device that the attacker is trying to get into without the attacker revealing no information at all.

So far a BIAS attack works on every level of Bluetooth and does not seem to have a weakness, but Antonioli et al expands and goes further to explain how it can reflect these attacks even if the device being attacked does not allow for the downgrade method to get to legacy connection.

3.4) Reflection Attack

If the device does not allow downgrading to legacy connection, Antonioli et al suggests using a reflection attack which adds a few extra role swaps as the impersonator to essentially bounce back and forth between master and slave to pass the authentication process again without the long-term key [Antonioli et al1]. Below is an example of the role swapping taking place.

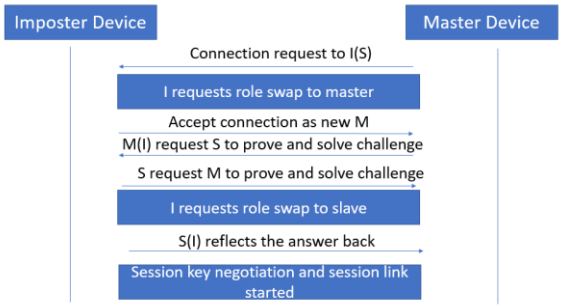

Fig 4.) Example of BIAS reflection using role swaps. Since the imposter knows the answer to the challenge since it was the same one who sent it, the other device assumes the imposter knows the long-term key without the key ever being distributed [Antonioli et al1]. Roles are put in parenthesis to help keep track of imposter's slave and master roles.

As seen in figure 4 this strategy of reflecting the answer back to the master device seems too easy and the Bluetooth manual referenced in Antonioli et al's paper has a section on reflection attacks and how they should not work but they never reference the authentication process BIAS attacks target [Antonioli et al1]. It was thought, at the time of this attack being presented, that using the unique Bluetooth addresses for each device would stop this attack, but in reality the reflection can happen before the authentication can happen since the attacker can just override and ask for a role swap before the authentication can complete.

The Bluetooth standard also mentions reflection attacks by using a FIFO (first in first out) preemption, but while this does hinder the attack a priority queue can be used to override the FIFO process for authentication [Antonioli et al1].

Overall BIAS proves that the Bluetooth standard must address the authentication process for security breaches, and, by the time of writing this report, a statement and solution has been incorporated into the standard to include the BIAS attacks in its implementation for Bluetooth [wikipedia5] Going off this attack however Antonioli et al moved on to another aspect of Bluetooth security breaches that emerged only a year later in 2019 with another loophole called a KNOB attack.

4. KNOB OVERVIEW

Along side the BIAS breach emerged another method for breaking the Bluetooth authentication process. This time the process involved breaking the encrypted session key between devices while negotiating the key down to only 256 options [Antonioli et al2]. This attack took place during the session key negotiation section of the Bluetooth pairing as seen in any of the figures explained above. This is known as KNOB or Key Negotiation of Bluetooth. The reason this was included at the end here was because KNOB attacks can not impersonate the device like BIAS can but working together, they are very efficient at breaking Bluetooth protocol. Below this key negotiation will be broken down further.

4.1) Key Negotiation

Like BIAS does above, this key negotiation happens every time two devices connect to each other, so the attacker does not have to be there for the first pairing. Since Bluetooth session keys only have up to 16 bytes of entropy [Antonioli et al2], this process can be negotiated down to only 1 byte during the negotiation process. Below is a diagram describing the process.

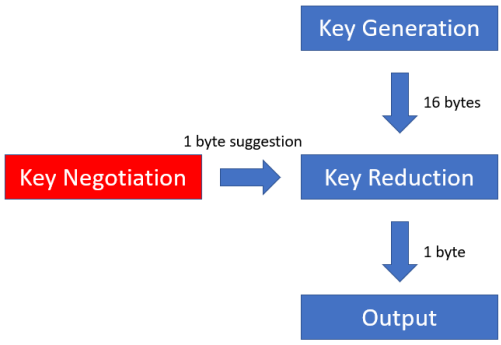

Fig 5.) Showing the example of inserting a lower key through negotiation during the session link procedure seen in other figures [Antonioli et al2].

Since most devices allow negotiation of the key to an extent this is not surprising that a malicious user could break into the system to brute force the key. The only problem is that this key negotiation requires a man in the middle attack similar to BIAS, so this is why when both are used together it turns into a devastating combo. To combat this negotiation legacy devices have made a higher minimum of entropy that can be used when encrypting the session key [Antonioli et al2].

4.2) Legacy Bluetooth

As stated above legacy Bluetooth has created a countermeasure to this key negotiation by only allowing the key to be negotiated down to 7 bytes of entropy. This increase of entropy makes the process of brute forcing the encryption key magnitudes higher and since the encryption happens every time the devices pair the attacker has to either be quick enough or knowledgeable enough about the device architecture to break in. As of this paper being written however the policy has been addressed by the Bluetooth SIG and a statement has been released on KNOB attacks making the encryption require more bytes of entropy on all devices not just legacy [wikipedia5].

At first these KNOB attacks seemed a bit of a stretch since they assume a lot about the Bluetooth architecture but Antonioli et al shows that plenty of modern Bluetooth devices from tech companies like Google, Apple etc are all vulnerable to this attack when combined with the BIAS addressed earlier. This will be addressed more in the summary section below.

5. SUMMARY

To conclude, Bluetooth is a pervasive technology with uses in daily life from cars to phones to IoT devices connecting to large networks of devices. Since the standard of Bluetooth is always changing it is not surprising there are still loopholes being found even today. Just browsing the Wikipedia for Bluetooth and multiple breaches can be seen throughout the years as well as the Bluetooth standard being updated. This paper was an exploration into the two newest breaches, BIAS and KNOB attacks and how when these attacks are put together can completely break down Bluetooth protocol and breach most any modern device [Antonioli et al1].

Since KNOB attacks need the impersonator in BIAS to switch roles and negotiate the key as described in the BIAS and KNOB overviews it felt right to include both to show their capabilities together. This also shows a lesson in cybersecurity of how even though Bluetooth is a network device, the weakness was still in the hardware first then the software second which is how most security breaches are executed historically. Being curious about this I found a paper dating from 2009 which approaches the topic of Bluetooth impersonation so even 11 years later this same attack still emerges and is a problem for Bluetooth [Mendoza3].

This will always be a problem with this kind of technology since it will never be realistic to completely scrap old devices from the network on the drop of a pin so legacy features will almost always be relevant to any piece of technology. Pairing that with the simplicity of connecting devices with Bluetooth to the user and it is obvious that more attacks similar to the ones described above will continue to emerge in the future and then patched out continuing the cycle.

6. REFERENCES

[1] Antonioli, D., Tippenhauer, N. O., & Rasmussen, K. (2020). BIAS: Bluetooth Impersonation AttackS. *2020 IEEE Symposium on Security and Privacy (SP), Security and Privacy (SP), 2020 IEEE Symposium On*, 549–562. https://doi-org.proxy.ulib.uits.iu.edu/10.1109/SP40000.2020.00093

[2] Antonioli, D., Tippenhauer, N. O., & Rasmussen, K. (2019). *Low entropy key negotiation attacks on Bluetooth and Bluetooth low energy.* https://eprint.iacr.org/2019/933.pdf.

[3] Loveless, M. (2018). Understanding Bluetooth Security. Retrieved 21 November 2020, from https://duo.com/decipher/understanding-bluetooth-security

[4] Mendoza, P. A. (2009). *An Enhanced Method For The Existing Bluetooth Pairing Protocol To Avoid Impersonation Attacks*.

[5] https://en.wikipedia.org/wiki/Bluetooth

[6]https://en.wikipedia.org/wiki/Elliptic-curve_cryptography

APPENDIX

BIAS — Bluetooth Impersonation AttackS

KNOB — Key Negotiation of Bluetooth

SIG — Special Interest Group

SSP – Simple Secure Pairing