PAPER REVIEW

ON

BLACKTOOTH: BREAKING THROUGH THE DEFENCE OF BLUETOOTH IN SILENCE

Harsimran Singh, Jugnu Gill and Nikhil Chawla

IIIT, Hyderabad, India

SUMMARY

This paper discusses about 5 vulnerabilities in the Bluetooth BR/EDR specification which are exploited by the attacker to get access to a victim device. BR/EDR is the classic Bluetooth which is used in the majority of bluetooth devices at present, ranging from cars to bluetooth keyboards.
Bluetooth connection goes through a Connection Establishment, Authentication process and during this time Link Key is shared among them.
This paper has assumed that the Attacker is not present at the time of sharing this Link Key and hence Link Key is not known to the attacker. The attacker only comes into picture when connections between the devices have already been established and they are interacting via Bluetooth. One more thing which is repeatedly used in all the vulnerabilities is impersonation. Paper has mentioned by describing various technical details that the Attacker can easily impersonate any of the devices.
I guess this background is enough to get into the 4 vulnerabilities.

#Vulnerability 1

BR/EDR uses the Master/Slave architecture and anytime there can be a role switch between devices which is exploited by the attacker to gain access to the victim device.
Let us consider there are two users(Alice and Bob) which are interacting via Bluetooth. BR/EDR does not enforce master/slave to any device. Whoever has sent the connection request is the Master. Assuming Alice has sent a connection request to Bob so Alice is the master and Bob is slave.Now, Alice and Bob are interacting via bluetooth and now the Attacker comes into play . Attacker will impersonate Bob and now for Alice, Attacker is the new Bob. Now Attacker can send the request for role switch.Now Attacker is the master and ALice is slave. Attacker has full control over the Alice system as Alice is a slave.

#Vulnerability 2

This vulnerability is based upon two Authentication techniques used in Bluetooth that are Legacy Authentication and Secure Authentication.These both are different in many aspects but vulnerability takes advantage of the fact that Legacy authentication(LA)is one way i.e Master authenticates the Slave but Slave don't Authenticates the Master. However, in Secure Authentication(SA) both authenticates each other. This is extension to #1 Vulnerability that after impersonating the Bob now Therefore, the attacker without the link key can impersonate the Master and complete secure connection establishment without

authenticating the Slave. Even if both devices support Secure Connections, the attacker can downgrade SA to LA by declaring that the impersonated device does not support Secure Connections.

#Vulnerability 3

This vulnerability takes advantage of the encryption key formed from the Link key shared during the connection establishement. Both the interacting devices agree upon the length of the encryption key to be used for data transfer.

Thus, the attacker can impersonate one device and force the other one to accept 1 byte of entropy and then attempt to brute force the encryption key

#Vulnerability 4

There are various Bluetooth profiles which are used. These profiles have certain levels of access rights attached to them. However, as per the BR/EDR working profiles can be changed/added. As per current implementation of BR/EDR, these profiles can be altered without any authentication. If an attacker successfully impersonates Bob and establishes a secure connection with Alice, the attacker can use new different profiles that are inconsistent with those used by Bob previously. For instance, the attacker can impersonate Bob, which used to be a headset, and enable a Human Interface Device Profile (HID)–a profile for keyboard and mouse.

In this case, the victim gets no notification of profile change, the only way to know is to manually check the profile of the device in bluetooth settings.

#Vulnerability 5

Privilege escalation - After connection has been established and authentication has been done, at this point the host will accept any profile change request even if it may lead to privilege escalation. This is a severe vulnerability as it allows the connected device to access far more resources on the host's device that host is in the know of.

Using these vulnerabilities the paper claims to access everything possible via a bluetooth connection which includes phone, storage, calls, applications, etc. The devices which the paper tested on includes Macbook Pro 2018, iPhone 12, Samsung S10, etc.

It should also be noted that the attack failed to switch profiles on Windows and Linux systems, so access was limited to the original profile which the impersonated device was using.

VIRTUES

1. The paper presents a new attack method called ”Blacktooth” that highlights security vulnerabilities in Bluetooth technology.
2. One of the most fascinating points about this paper is that this attack does not require any malware to be installed to perform this attack.
3. The authors provide a comprehensive discussion of the potential countermeasures and mitigation techniques that can be used to defend against the Blacktooth attack.
4. Although they have not tested on all devices but still they have covered a range of smartphones devices and 1-2 laptops.
5. The paper provides a detailed analysis of the attack and presents a diverse set of evaluation metrics, including the success rate of the attack, the time required for successful exploitation, and the impact on the target device.
6. The paper includes practical demonstrations of the effectiveness of the Blacktooth attack.

CRITIQUES

The critiques of this paper can be bifurcated into two categories. The first category is 10,000 feet view which comprises critiques at a higher level of analysis, while the second category is deep dive includes critiques that examine each vulnerability in detail.
To elaborate, the first category of critiques offers a broader perspective on the paper and evaluates it from a more abstract and conceptual level. On the other hand, the second category of critiques focuses on analyzing each vulnerability individually, highlighting their flaws.

***Broader level* critiques:**

Lack of technical details: The paper does not provide a detailed explanation of the technical aspects of the attack, such as the algorithms used. While the authors do provide a high-level overview of the Blacktooth attack method, it would be useful to see more technical details provided, such as the specific commands or protocols used to exploit the Bluetooth vulnerabilities. This would allow other researchers to reproduce or extend the study more easily.

Focus on Bluetooth Classic: The paper primarily focuses on Bluetooth Classic (BR/EDR) technology and does not consider the security implications of Bluetooth Low Energy (BLE) connections, which are becoming increasingly prevalent in modern devices. While the authors do briefly mention BLE in their

discussion, it would be useful to see a more detailed evaluation of the security implications of BLE connections.
As BLE shares some vulnerabilities like Legacy Authentication but other vulnerabilities like privilege escalation can't be replicated.

Lack of practical evaluation: The authors provide a comprehensive discussion of potential countermeasures and mitigation techniques that can be used to defend against the Blacktooth attack. However, they do not provide a practical evaluation of the effectiveness of these techniques. While the authors do provide a theoretical evaluation of these techniques, it would be useful to see a practical evaluation that tests the effectiveness of these techniques against the Blacktooth attack method. This would allow other researchers and practitioners to better understand the effectiveness of these techniques in practice.

Limited device testing: The authors only test the Blacktooth attack on a limited set of Bluetooth devices, which may not be representative of the wider range of devices in use. As a result, the generalizability of the study could be limited. While the authors do test the attack on a range of devices, including smartp hones and laptops, it would be useful to see a more diverse set of devices tested, such as IoT devices, medical devices, and automotive systems. This could provide a more comprehensive understanding of the vulnerabilities of Bluetooth technology across a wider range of devices.

Deep diving into critiques **:**
These are the 4 grounds on which we are going to review the paper from the aspect of finding flaws/critiques in this paper:

1. Techniques to prevent unauthorized access by attackers to the system.

2. Strategies for minimizing the impact of a successful attack and reducing potential damage.

3. Attack Detection and Recommended Response for User.

4. Other limitations or shortcomings of the attack methodology or approach.

Techniques to prevent unauthorized access by attackers to the system

→ In the *first and second vulnerability* as we have discussed, this vulnerability is exploited with the help of Master - Slave architecture. However, one clear solution to this attack is the architecture used by BLE i.e
In BLE, the Master/Slave architecture is replaced with a "central-peripheral" architecture. The central device can initiate connections with multiple peripheral devices. Each peripheral device has a unique identifier called a "random

device address" (RDA), which is changed frequently. This RDA is used to establish a connection with a central device. The peripheral device can also be configured to ignore connection requests from unknown central devices.
However practical implementation of this method in BR/EDR is a topic of discussion so following are some of the solutions in BR/EDR itself from our understandings:

1. Since, this attack assumes that at the time of pairing the attacker won't be present and hence the link key and encryption key won't be available to the attacker.

   Now, whenever an attacker impersonates any of the interacting devices then the earlier connection between the legitimate users needs to be broken, so that the attacker can interact with the other device.

   Hence, anytime a connection is broken then users should get notified and to get connected again there should be the Authentication process again of sharing the link key. Here when it comes to sharing the link key again,this attack fails.

2. Even if we assume that the reconnection is too fast, it is difficult to detect when the connection is broken, then also this attack can be failed which will be described in next section.

3. **Discoverability Issue** - This paper has a big assumption that discoverability of smart devices is always on. However, just a simple change of turning device discoverability off after Bluetooth connection is established (this is possible that we can switch off discoverability after connection establishment) fails all of the vulnerabilities.

   Discoverability is the one which shows the public info like Bluetooth name and address available to other users.

4. There is one more technique of preventing this (*reference taken from BLE tech stack*)

   Secure Simple Pairing (SSP):

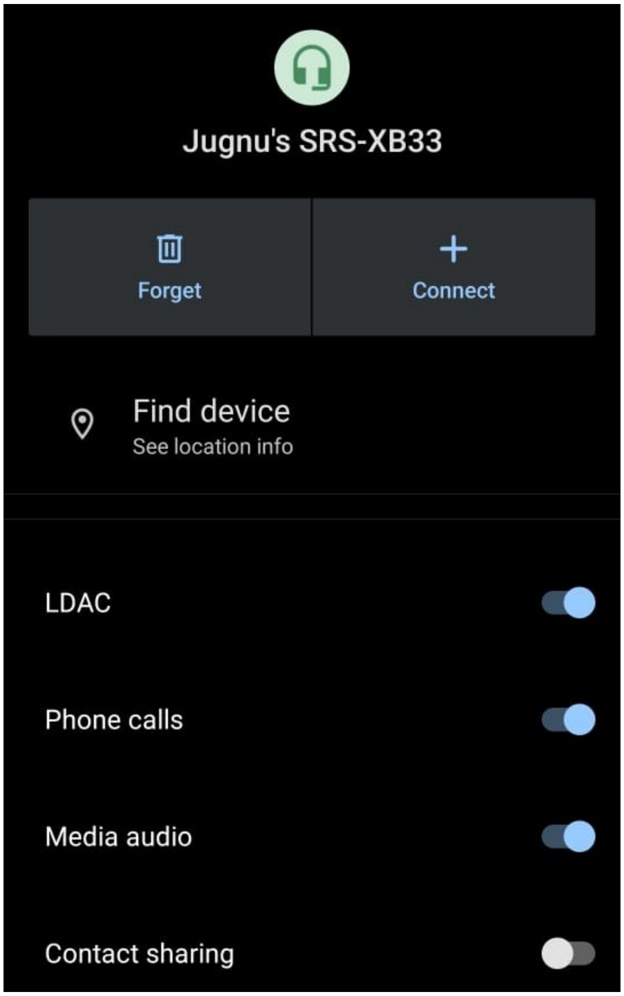
   SSP is a secure pairing method that provides better protection against attacks than the legacy pairing methods used in earlier versions of Bluetooth. SSP uses public key cryptography to generate a shared secret key that is used to encrypt data during communication. SSP also includes mutual authentication, which ensures that both devices are authenticated before data exchange begins.

5. Auditing and non-repudiation services can be implemented by different devices which should guarantee if the connection is legitimate or there is a risk like if legacy authentication happens.

Strategies for minimizing the impact of a successful attack and reducing potential damage.

1. For MITM attacks, applications can utilize their own encryption before passing the data to the bluetooth protocol. Despite breaking the encryption key, eavesdroppers will not be able to understand the data due to the encryption applied to data by application before it was passed to Bluetooth protocol.

2. Both Android and iPhone devices have already implemented a form of access control for a bluetooth device at the time of the pairing like access to contacts, phone calls, etc. If permissions are disabled at this point, even if the attacker manages to impersonate a known bluetooth device, a prompt will show up if the attacker tries to access resources which it has been explicitly denied permission to.



LDAC ☑
Phone calls ☑
Media audio ☑
Contact sharing ☐

3. Taking the example to understand cracking the *forth vulnerability*

   Suppose Alice and Bob are interacting via Bluetooth. In real life we normally don't use Bluetooth for personal data transfer. We normally use headphones or similar devices like these.

   Let's say Alice is SMARTPHONE and Bob is Bluetooth headphone, now as assumed in all attacks that Alice and Bob are already interacting and now some attacker comes. Now even if Attacker has impersonated Bob and for Alice ,Attacker is new Bob. Attackers will request for Profile Switching and need higher profiles to attack the system. But here if we have already maintained the list of profiles that Bob(with headphones) can access , then all requests for higher profiles for Bob(the attacker) will be denied automatically.

   Alternative Solution: can be whenever there is profile switching then we can enforce to exchange the link key as written in vulnerability 1,which is shared between them at the time of pairing (as they have assumed that attacker does not know anything about link key)

4. The *third vulnerability* can be prevented by setting a minimum length of encryption key to be used. If we have a minimum length of say 3-4 bytes then brute forcing this will take lots of time which becomes another limitation of this attack

Attack Detection and Recommended Response for User

1. _The user can recognize if he/she is under attack if multiple devices are showing or if the original slave device isn't being blocked, then it may try to reconnect which can lead to back and forth connection switching.

2. MITM attacks can also be recognized in specific cases like when the user is watching a video and audio through bluetooth headphones have a lag or a delay. Even a very small delay due to a MITM attack can be noticed by a user in such a case.

3. If the user suspects about being under attack, the immediate response should be to forget the device from the bluetooth menu in the settings.

4. As there is a chance that the attacker sent some sort of malware, it is recommended that the user should reset the device.

Other Limitations

1. _**Piconets** - They can be particularly problematic for Blacktooth, as a bluetooth piconet can have up to 7 connected simultaneously.

In this case, an attacker cannot just intercept a connection and do role switching as there can only be one master and the entire piconet has to be taken down to do so. Thus, blacktooth attack becomes infeasible for such scenarios.

2. **Have to observe a connection** - Simply having bluetooth on doesn't make devices vulnerable to Blacktooth, the attacker has to luck on observing a connection with some device for the attack to take place. The practical implementation shown in the paper has been performed in the Lab. However, this can be difficult if the attacker wants to target a specific device as in real world we won't be given a

3. **Custom Profiles** - Bluetooth also has the ability to implement custom profiles for bluetooth connections, in that case for Windows/Linux systems where the attacker cannot switch profiles. The attack will fail to a great extent as custom profiles are usually implemented for specific tasks like sending temperature, humidity etc from sensor to device, also MITM attacks cannot be implemented at all in such scenarios as the attacker won't have the knowledge about the profile being used.

Improvements in the attack

Assuming all the attacks as a Black box i.e considering all the ideal scenarios for the attack to happen. We can extent the scope of the attack

1. **Bluesniping** - Bluetooth has a very limited range of a few meters only. So, combining the Blacktooth attack with bluesniping attack can give it a very large range, i.e. range of the attack can increase from a few meters to a kilometer.

   Bluesniping can be performed using a specialized antenna, a stock and an embedded PC.

   Although we have to note that, eavesdropping and gathering portion of the attack still has to be performed in close proximity. Additionally, MITM attacks also can't be performed in this manner as the delay will be very noticeable.

2. **Installing malware** - In real world scenarios, an attacker will not have the opportunity to stay in prolonged contact with the target, thus the attacker can first send the malware after becoming the master and then using bluetooth profile like HCI, take control of the system and execute the previously sent malware. In this manner, attackers can cause significant damage.

3. **Accessing Link Keys** - If an attacker chance upon having physical access to the slave device. In some cases, it is possible to get link keys. In that case, the attacker can do w authentication, and can get access to the victim's primary device without raising any alarms.

References

1. https://www.ndss-symposium.org/ndss-paper/badbluetooth-breaking-android-security-mechanisms-via-malicious-bluetooth-peripherals/

2. https://csrc.nist.gov/publications/detail/sp/800-121/rev-2/final