Paper Review on Blacktooth

Breaking through the Defense of Bluetooth in Silence

Jugnu Gill
Harsimran Singh
Nikhil Chawla

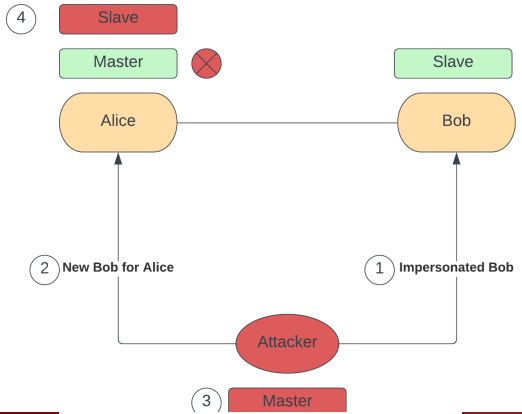
IIIT, Hyderabad

Table of Contents

INTERNATIONAL INSTITUTE OF INFORMATION TECHNOLOGY
HYDERABAD

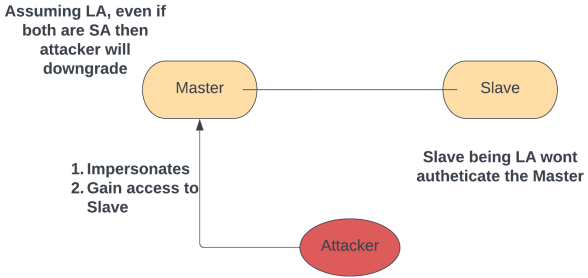
Summary : 1st Vulnerability

After impersonating Bob, Attacker will be new Bob and Attacker will gain access of the Alice by switching the master role to slave which is allowed in BR/EDR



2nd Vulnerability

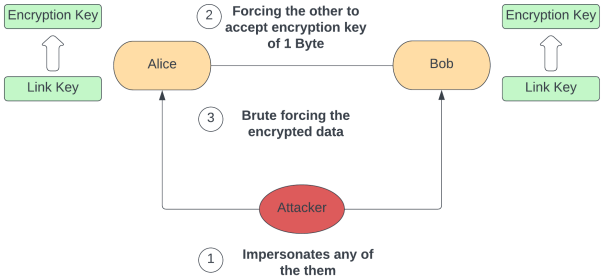
After impersonating the Master, Attacker can get full access to Slave system irrespective of the kind of the Authentication whether Legacy or Secure as in case of Secure Authentication it can be downgraded by the Attacker



INTERNATIONAL INSTITUTE OF INFORMATION TECHNOLOGY
HYDERABAD

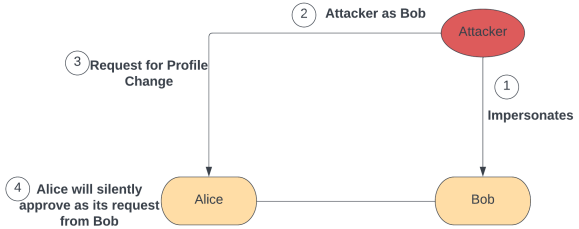
3rd Vulnerability

After impersonating any of them, it can force the other party to accept the Encryption key of 1 byte and all data from other device can now be decrypted



4th Vulnerability

If attacker has impersonated Bob, then profile switching of the Alice can enable the Attacker to get control to execute any command on Alice system.



INTERNATIONAL INSTITUTE OF INFORMATION TECHNOLOGY
HYDERABAD

5th Vulnerability

In this vulnerability, a device once connected and authenticated can escalate its privilege without any check. This can lead to changing to profile with more and more access of resources.

Broader Critiques

Lack of technical details

Paper only discusses techniques and there is a lack of details on exactly how these vulnerabilities were exploited. We can't replicate or verify the results achieved in the paper because of that.

Focus on Bluetooth Classic

The attack was only performed using BR/EDR protocol. BLE also has vulnerabilities like legacy authentication. That's why there is a need to test how much BLE devices are also exposed.

Broader Critiques

Limited Device Testing

The authors tested the attack on a limited set of devices.
Similar types of devices are repeatedly while testing which prevents us to understand the true scope of the attack.

Lack of Real World Testing

The testing was done in a lab on one device at a time.
This means that we can't gauge how many devices can an attacker track concurrently. Also, if attack will face issues because of congestion of frequency channels.

Deep Dive into Critiques

Prevent Access by Attackers

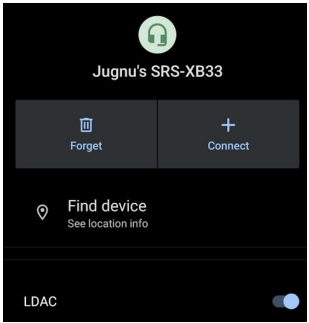
- **Turn off discoverability** - If discoverability of devices is turned off after connection is established, attacker won't be able to impersonate a device.
- **Enforcing Secure Simple Pairing (SSP)** - It ensures both devices are authenticated before data exchange begins, lack of enforcement is what the attack exploits.

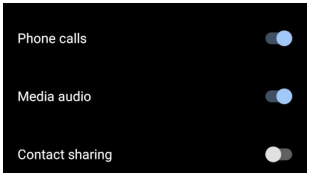
Deep Dive into Critiques

- **Auditing and Non-Repudiation Services** - They can take measures like enforcing secure authentication happens, inform users, or have the ability to track and block insecure connections.
- **Regenerating Link Key on every connection** - Attacker has to break connection of slave device and then impersonates the device, if link key is being generated on every re-connection, the attacker won't be able to impersonate. This comprises the practicality as there won't be automatic connections.

Minimize Damage from Attacks

- **Access Rights for specific Bluetooth device** - Modern devices offer features to limit the access a Bluetooth device can access. So even if the attacker changes the profile, he/she will still be limited to the resources given access by the user.





INTERNATIONAL INSTITUTE OF INFORMATION TECHNOLOGY
HYDERABAD

Deep Dive into Critiques

- **Blocking Profile Switching** - Setting allowed profiles at the time of initial pairing and limiting access to that specific profile(s) will greatly the access of attacker to cause harm.
- **Encryption By Applications** - For MITM attacks, some applications apply their own encryption before passing the data to Bluetooth protocol. In this case, attacker won't be able to decrypt message.

INTERNATIONAL INSTITUTE OF INFORMATION TECHNOLOGY
HYDERABAD

Deep Dive into Critiques

Attack Detection and Recommended Response for Victim

- **Detection due to multiple reconnects** - If device being impersonated isn't blocked off, the original slave might try to reconnect, which can lead to multiple reconnects allowing user to recognize an attack.
- **Detection due to lag in MITM attack** - In a specific case like a user is watching a video with Bluetooth earbuds, a MITM can cause video and audio to go out of sync, which can lead to user diagnosing the issue and recognize the attack.

INTERNATIONAL INSTITUTE OF INFORMATION TECHNOLOGY
HYDERABAD

Deep Dive into Critiques

- **Response by User after detecting the attack** - User should turn off Bluetooth and then immediately forget the device from Bluetooth settings, and later reset the device as there could be malware injected.
  Switching off the device can also be done to disrupt the connection.

Other Limitations

- **Piconets** - They can have upto 7 device connected to the same master, in this case attacker can disrupt a connection and impersonate it but cannot ask to connect and become master as the whole Piconet has to be disconnected before role switch happens.
- **Require to Observe a Connection** - The premise of the attack is they have to observe a connection. If user doesn't use his/her device in a vulnerable environment. Due to limited range of Bluetooth, attacker cannot perform an attack.

Deep Dive into Critiques

- **Custom Profiles** - Devices with custom profiles cannot be easily impersonated by attacker at least not without deep prior knowledge and preparation. These profiles can be implemented by anyone and used in specific application. Moreover knowledge about many of these custom profiles isn't openly available.

Improvements in the Attack

- **BlueSniping** - Bluetooth suffers from limited range. Using antenna, stand and an embedded PC. The effective can be extended to a kilometer.
  Although gaining device information still has to be done in close proximity to the target.
- **Installing Malware to target when out of Bluetooth Range** - Using the ability to switch profiles, first attacker can send malware, then switch profile like HID and install the malware. Now attacker can perform a whole new range of attacks even when out of Bluetooth range

Improvements in the Attack

- **Accessing Link Keys** - If an attacker doesn't chance upon observing a connection but can get physical access to the device temporarily. He/she can access link keys as there are many devices still not secure about this. Now the attacker can do secure authentication with victim as opportunity comes.