CON Assignment 3- Bluetooth Networks– Threats and Security Measures

Rishi Shah

October 2020

1 Introduction

Bluetooth was designed as a cable replacement technology. It is a short-range radio link designed to connect portable and/or fixed electronic devices. The effective range, to date, is thirty feet or ten meters. Nowadays, each and every device has bluetooth system in it. It is employed in interconnecting cellular phones with headsets, cellular phones with PDA's, PDA's to mobile or desktop computers, and the like wirelessly.

2 Threats

• MAC Spoofing Threat- A spoofing attack is a type of cyber attack where an intruder imitates another legitimate device or user to launch an attack against the network. In other words an attacker sends a communication from a device disguised as a legitimate device.Every device that's connected to a network possesses a worldwide, unique, and physical identification number: the Media Access Control address, or MAC for short. This burned-in address (BIA) is virtually etched to the hardware by the manufacturer. Users are not able to change or rewrite the MAC address. But it is possible to mask it on the software side. This masking is what's referred to as MAC spoofing.
• PIN Cracking Attack- It is a passive attack, in which the attacker can find the PIN used during the pairing process. The attacker enumerates all possible values of the PIN. The attacker can now use this hypothesis of the initialization key, to decode messages. And after that, the attacker has full access to the device.
• Man-in-the-Middle Attack- A man in the middle (MITM) attack is a general term for when a perpetrator positions himself in a conversation between a user and an application—either to eavesdrop or to impersonate one of the parties, making it appear as if a normal exchange of information is underway.The goal of an attack is to steal personal information, such as login credentials, account details and credit card numbers. Targets are typically the users of financial ap-

plications, SaaS businesses, e-commerce sites and other websites where logging in is required.

3 Security Measures

• MAC Spoofing Threat- You have to stop using trust relationships. Trust relationships are where networks only use IP addresses to authenticate devices. Eliminating trust relationships provides an extra layer of security. You can deploy anti-virus software in our devices. Using antivirus software on your devices will make sure that they can deal with any malicious software that has been planted. You can also use VPN's as they encrypt the data so that it can not be read by external party.
• PIN Cracking Attack-The best way to stop this is to employ the use of CAPTCHA's. You can ask security questions any time a new user logins. You to design a software which can trick the attacking software. Also to stop multiple attempts in short time, you can set time delays between attempts. Whenever a new login user is there, the software should make him set a strong password.
• Man-in-the-Middle Attack- Make sure to add strong WEP/WAP encryption points on access. Having a strong encryption mechanism on wireless access points prevents unwanted users from joining your network just by being nearby. Public key pair based authentication like RSA can be used in various layers of the stack to help ensure whether the things you are communicating with are actually the things you want to be communicating with.