南京郵電大學
Nanjing University of Posts and Telecommunications

Security threats in Bluetooth technology

汇报人：1023041123孙苏云

目 录

1. 背景

1.1蓝牙

蓝牙是一种广泛用于连接设备交换数据的无线技术。使用超高频无线电波。两个蓝牙设备之间的有效工作范围为10到100米。

由于蓝牙使用未经许可的ISM频段，它不需要任何监管机构，并且消耗非常有限的功率。此外，蓝牙是一种自动化技术，不需要额外的设置来启动通信。不同厂家、不同型号的设备可以通过蓝牙轻松通信，没有任何兼容性错误。

1.2 蓝牙核心架构

蓝牙架构的核心组件包括蓝牙控制器、主机控制器接口(HCI)传输层以及蓝牙主机。

蓝牙控制器：包括链路管理层（负责启动两个蓝牙设备之间的链路）、基带层（负责使用无线电频率在蓝牙设备之间建立链路）、无线电层（负责发送和接收蓝牙数据包）。

主机控制器接口HCI：蓝牙主机通过HCI层发送和接收命令与蓝牙控制器进行通信。

蓝牙主机：负责与另一个外围设备的蓝牙主机连接和交换数据。

2. 蓝牙安全威胁

蓝牙安全威胁大致分为两类：攻击和恶意软件。

2.1 攻击

定义：“试图获得对系统服务、资源或信息的未经授权的访问，或试图破坏系统完整性。”或“任何试图收集、破坏、拒绝、降级或破坏信息系统资源或信息本身的恶意活动”。

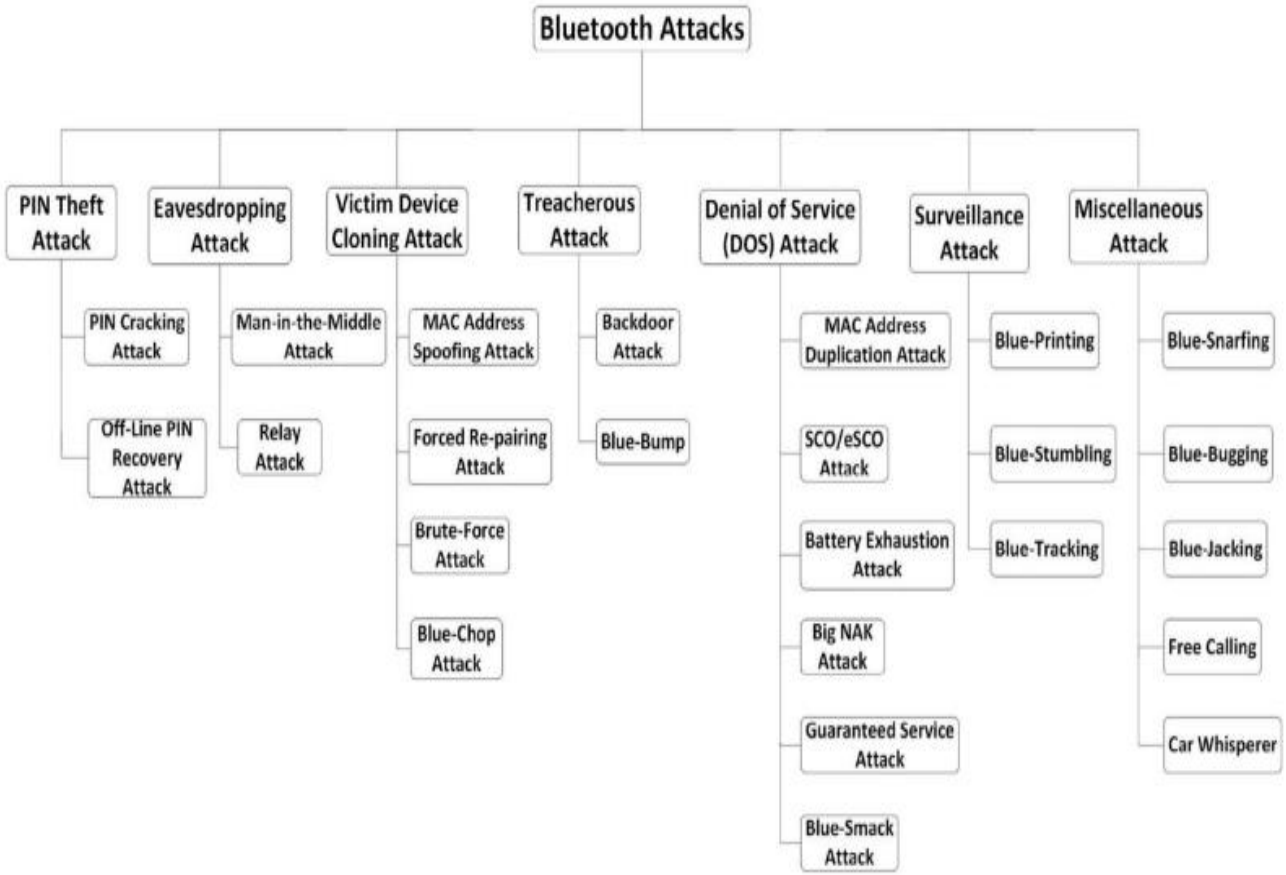
分类：主动攻击（直接攻破设备的安全系统，获得对受害设备的控制权）和被动攻击（操纵受害者或应用不同的方案来获得对受害者设备的控制）。本文将其具体分类为PIN窃取攻击、窃听攻击、受害者设备克隆攻击、背叛攻击、DoS攻击、监视、杂项攻击。

2.2 恶意软件

定义：“一种插入系统的程序，通常是隐蔽的，目的是破坏受害者数据、应用程序或操作系统的机密性、完整性或可用性，或者以其他方式骚扰或扰乱受害者。”

分类：特洛伊木马和蠕虫

3. 蓝牙攻击



蓝牙攻击分类图。遵循类似渗透方法或对受害者留下相同影响的攻击被分组在一个标题下。

Table 1 – Severity of bluetooth attacks.

High severity	Medium severity	Low severity
PIN Cracking Attack	Man-in-the-Middle Attack	Blue-Chop
Off-Line PIN Recovery	Relay Attack	DoS Attacks
Backdoor Attack	MAC Address Spoofing Attack	Blue-Printing
Blue-Snarfing	Forced Re-pairing Attack	Blue-Stumbling
Blue-Snarfing	Brute-Force Attack	Blue-Tracking
Blue-Bugging	Blue-Bump	Blue-Jacking
Free Calling		
Car Whisperer		

攻击的严重程度列表。根据对受害者设备造成的影响进行分类。高危攻击包括PIN码破解攻击、离线PIN码恢复 、后门攻击等；中危攻击有中间人攻击、中继攻击等；低危攻击有DoS攻击等。

3. 蓝牙攻击

3.1 PIN盗窃攻击

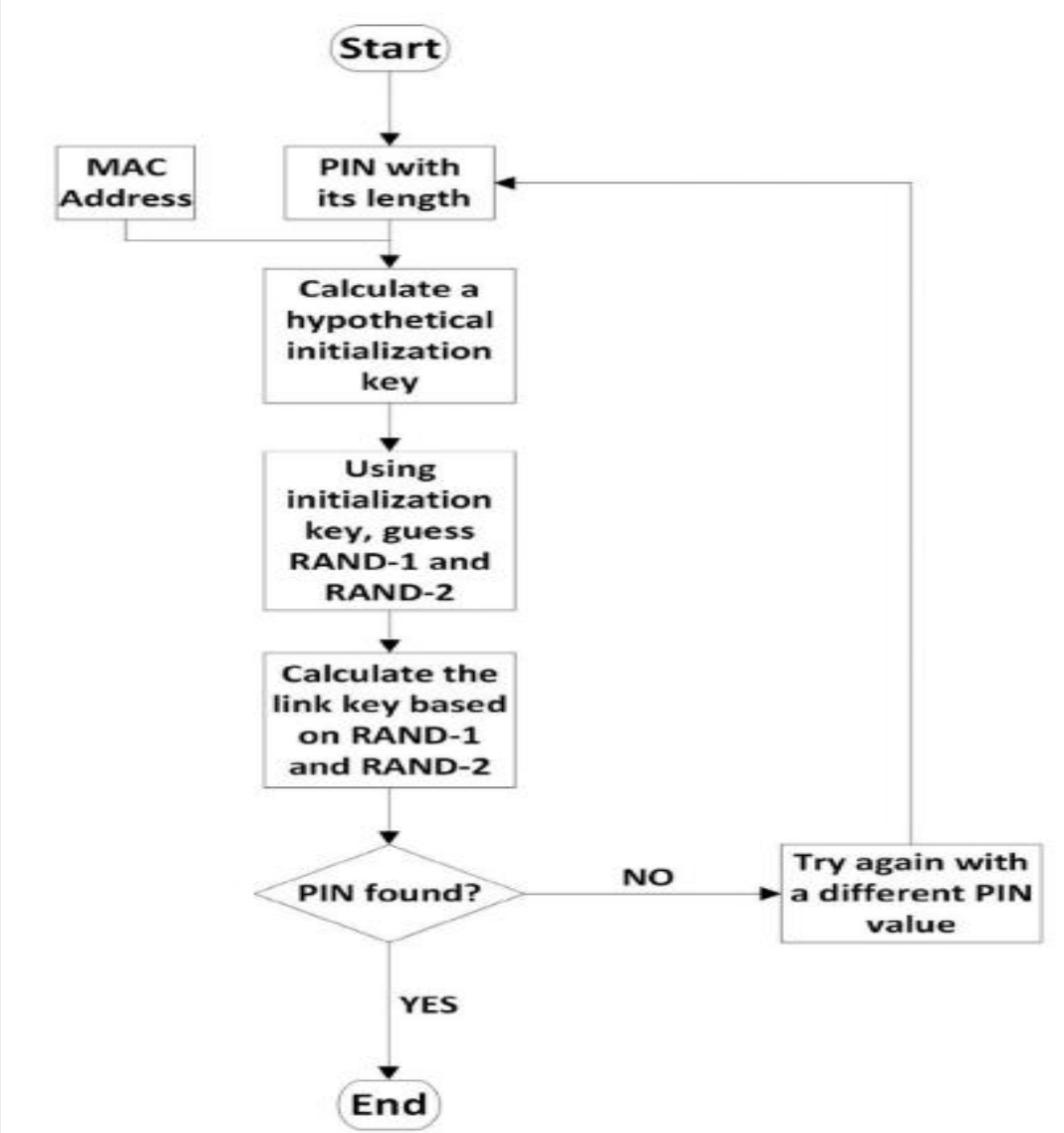
这类攻击通过窃取PIN码，随后与受害者设备建立连接，意图进行恶意活动。包括PIN破解攻击、离线恢复攻击。

3.1.1 PIN码：用于对蓝牙设备进行安全认证的密码。PIN码用于配对时验证设备之间的身份，并确保连接的安全性。

3.1.2 PIN破解攻击：一种通过暴力破解或其他方法试图直接猜测和破解设备或系统上使用的PIN码的攻击。

3.1.3 离线PIN恢复攻击：一种通过获取和分析存储在设备或系统中的加密PIN数据或哈希值，尝试在设备外部进行PIN恢复的攻击。

它通过使用解密算法计算PIN码，根据带长度的PIN码和MAC地址生成初始化密钥，再根据它生成两个随机值RAND-1和RAND-2。设备使用这两个随机值来创建链接密钥，以便建立连接。



3.2 窃听攻击

这类攻击攻击者利用两台受害设备之间的通信窃取信息。

3.2.1 中间人MITM攻击：通过使用假接入点访问和修改蓝牙设备之间传输的数据的方法。

流程：两个蓝牙设备正在配对，设备通过蓝牙进行通信和数据传输，攻击者通过假接入点入侵从而获取和修改数据。

3.2.2 中继攻击：攻击者在通信双方不知情的情况下，通过拦截和重放消息来进行未经授权的操作。

攻击者将两个虚拟设备连接到两个受害设备上。受害者相互通信时，受害者其实是向攻击者的设备传递信息，攻击者设备窃听通信并继续不定时地向受害设备提供反馈，因此攻击不会被检测到。

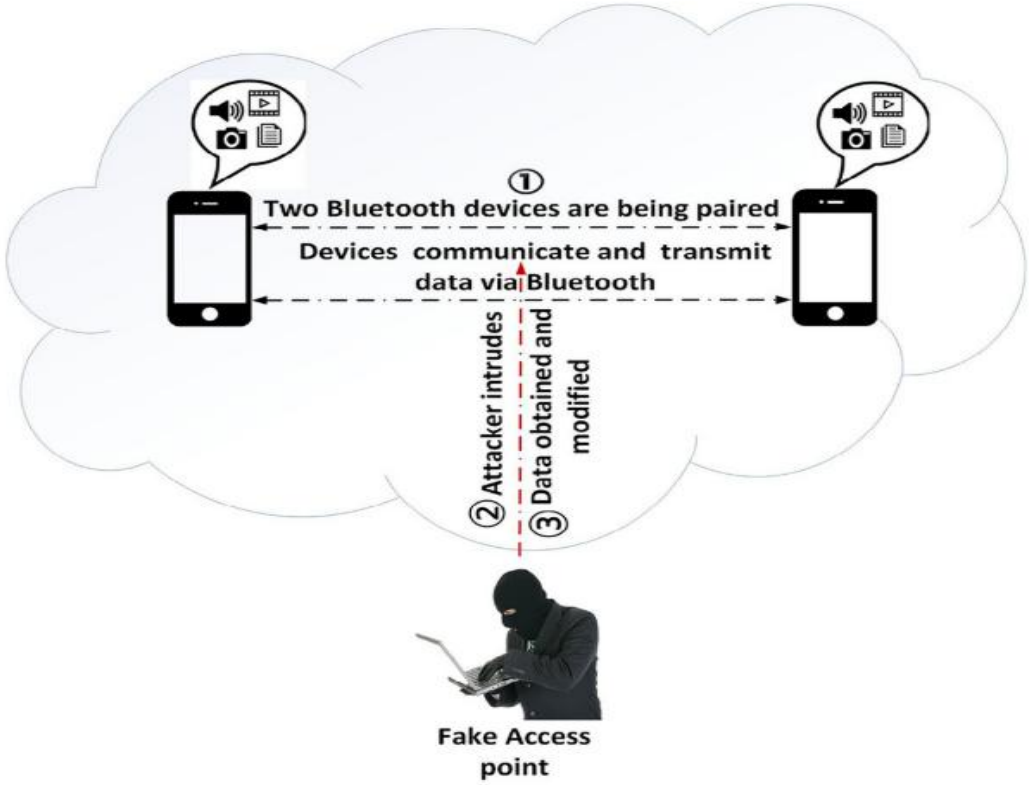


Fig. 4 – Man-in-the-middle attack.

3.3 DoS攻击

DoS攻击即拒绝服务攻击。DoS攻击通过窃取或改变受害者设备的信息，DoS攻击只是为了对受害者造成干扰，它通过使资源对受害者不可用而使受害者设备暂时瘫痪。它会给网络造成不必要的流量，阻塞网络。这类攻击包括MAC地址复制攻击、SCO/eSCO攻击、电池耗尽攻击、Big NAK 攻击、保证服务攻击、blue-smack攻击。

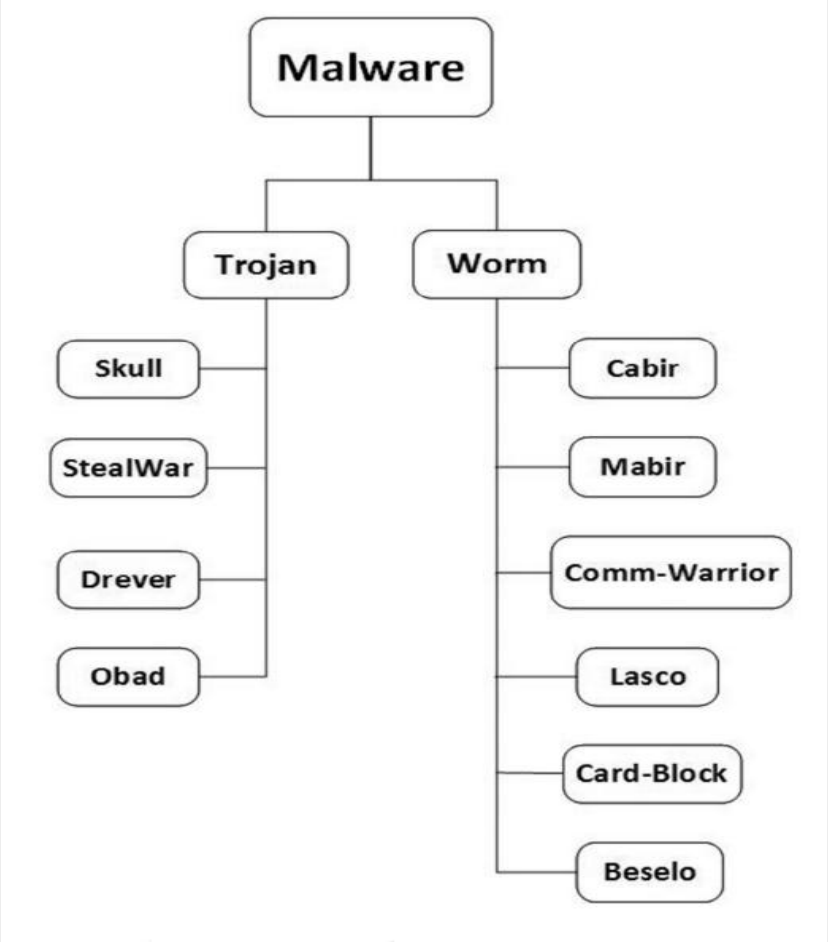
六种不同类型的DoS攻击对比研究如下表所示

表 2 - DoS 攻击之间的类比。

攻击协议	干扰piconet	麻痹装置	克隆受害设备
MAC地址重复攻击			✓
SCO/eSCO攻击	✓		
电池耗尽攻击		✓	
大NAK攻击	✓	✓	
保证服务攻击	✓	✓	
Blue-Smack攻击	✓		

4. 蓝牙恶意软件

蓝牙恶意软件主要有两种类型:特洛伊木马和蠕虫。具体蓝牙恶意软件分类图如下所示。



4.1 特洛伊木马

它是一种欺骗用户进入系统并运行恶意活动的恶意软件，不能自我传播。它可能会窃取敏感信息，并可能给攻击者提供访问权限。

首先攻击者向受害者发送木马，然后攻击者获取受害者设备的访问权限，从而窃取敏感信息。

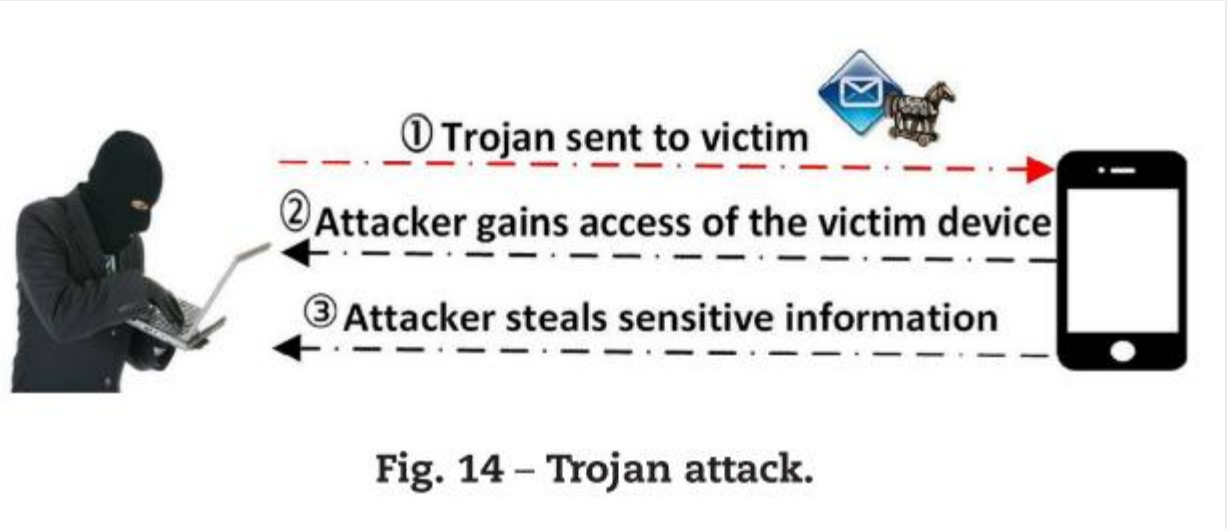


Fig. 14 – Trojan attack.

4.2 蠕虫

蠕虫是一种通过自我复制在其他设备之间传播的恶意软件。下图显示了蠕虫从受感染的设备传播到所有其他附近设备的示意图。首先攻击者将蠕虫感染到设备中，然后被感染设备会将蠕虫传播到附近的设备中

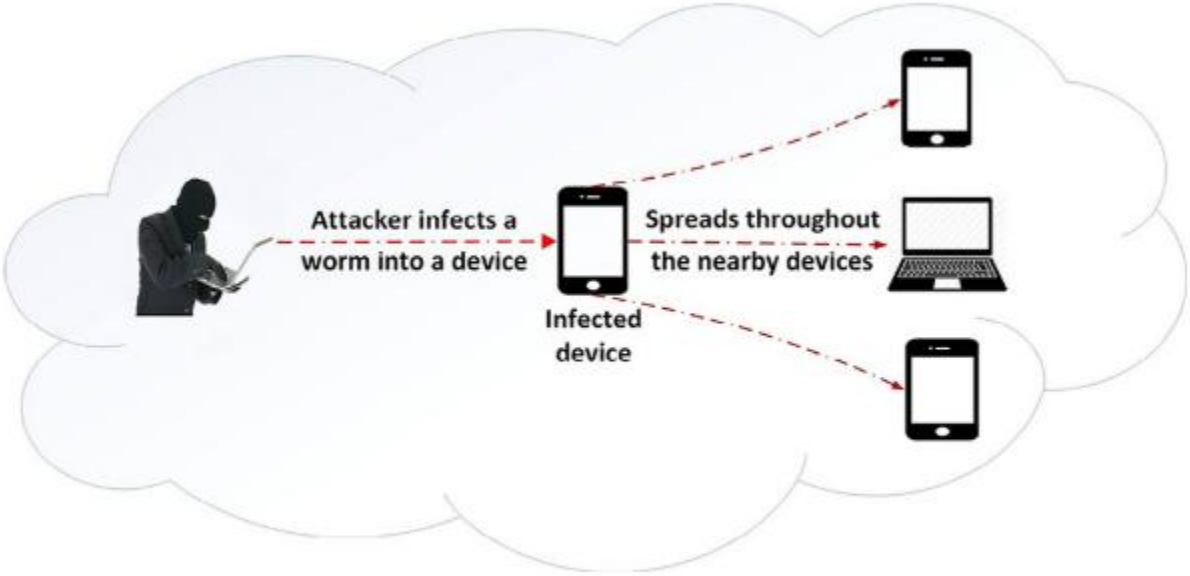


Fig. 15 – Worm propagation.

5. 解决方案

5.1 制造商角度

Philip and Das(2011)提出了一种对抗MITM攻击的安全架构。这里的身份验证是使用密钥和混沌图像加密来完成的，这使得配对机制具有鲁棒性。
Albazrqaoe等人(2016)提出了一种名为BlueEar的蓝牙数据包嗅探器，可以将数据包捕获率提高到90%。
singele和Preneel(2006)提出了高级配对协议，增强了配对机制。

5.2 用户

（1）基本预防：包括关闭蓝牙、保持设备不被发现模式、安装杀毒软件、防火墙和反垃圾邮件软件来保护设备、从可信来源下载软件等。
（2）配置默认设置：包括更改设备的默认名称、禁用未使用的服务。
（3）配对指南：包括使用强PIN码、每隔一段时间更换PIN码、短距离配对、避免与未知设备配对等。
（4）观察设备行为：通过观察设备行为，用户可以很容易地防止窃听攻击(中间人攻击和中继攻击)、恶意软件和DDoS攻击。包括注意异常活动、监控电池寿命、监控数据使用情况等。

南京郵電大學
Nanjing University of Posts and Telecommunications

感谢您的观看！