**Research on Bluetooth Technology**

**Introduction**:

Bluetooth technology is a key component of wireless communications. It provides a low-energy and low-cost solution for short-range radio transmissions. Bluetooth, more specifically Bluetooth Low Energy (BLE) has become the predominant technology for connecting IoT (Internet of Things). It can be found in cell phones, headsets, speakers, printers, keyboards, automobiles, children’s toys, and medical devices, as well as many other devices. The technology can also be found in automated smart homes, to provide monitors and controls for lights, thermostats, door locks, appliances, security systems, and cameras. Bluetooth offers convenience and ease of use, but it lacks a centralized security infrastructure. As a result, it has serious security vulnerabilities, and the need for awareness of the security risks are increasing as the technology becomes more widespread. This paper presents an overview of Bluetooth technology in IoT including its security, vulnerabilities, threats, and risk mitigation solutions. [1]

**Bluetooth Security:**

There are two guides and standards for Bluetooth protocols and security, NIST 800-121-R1 and IEEE 802.15.1. NIST 800-121-R1 details the recommended Bluetooth security processes. These recommendations include the authentication and verification of the sender, confidentiality regarding information, and authorization in regard to who has control over access to the information. IEEE 802.15.1 is the standard for Bluetooth Wireless Technology. It discusses Bluetooth security in addition to the protocols surrounding Bluetooth technology. [1]

A. Bluetooth Security Modes

All Bluetooth devices operate in 1 of 4 defined access security modes: Security Mode 1 (non-secure); Security Mode 2 (service level enforced security); Security Mode 3 (link level enforced security); and Security Mode 4 (service level enforced security with encrypted key exchange). [1]

The Security Mode determines available service security levels. Security Modes 1 and 3 do not specify service security levels. Security Mode 2 can enforce any combination of the following basic security services: authentication, confidentiality, and authorization. Security Mode 4 specifies five levels of service security. In this mode, SHA-256 is used for hashing and AES CCM is used for encryption. It also uses Secure Simple Pairing (SSP) for key generation. Mode 4 is listed as the mandatory mode for Bluetooth versions 2.1 + EDR and newer versions. [1]

B. Bluetooth Trust Modes

In addition to the security modes discussed above, there are two levels of trust for Bluetooth devices, trusted and untrusted. They are described as follows:

1- Trusted—A trusted device has established a fixed relationship with another device and has unrestricted access to all services. [1]

2- Untrusted—An untrusted device only has access to a restricted set of services. Although the device has passed authentication successfully, it does not have a fixed relationship with another device. [1]

C. Discoverability in Devices

Discoverability modes of Bluetooth devices also affect the device’s security. Devices in discoverable mode are more vulnerable, as they can be recognized. The device name, class, list of services, and technical information are all exchanged in discoverable Bluetooth devices that are in range (approximately 10 m). In addition, every Bluetooth device has a unique 48-bit address used for identification, known as the BD\_ADDR. This address is similar to a MAC address, which is a manufacturer-assigned address for hardware that serves as a unique identification number. [1]

D. Bluetooth Security Services

The first time that two devices attempt a connection, a trusted relationship needs to be established through authentication. Authentication is performed by using challenge-response, based on BD\_ADDR and a link key. The link keys, once established, are kept by both devices to be used for future pairing.[1]

Bluetooth technology has certain built-in features that help secure technology. They include:

(1) Adaptive Frequency Hopping: Frequency hopping in Bluetooth uses a 2.4 GHz ISM band with 79 channels to enable hops at 1600 hops per second. During the hopping, existing frequencies are excluded. The ability to frequency hop reduces both jamming and interference. [1]

(2) E0 Cipher Suite: The cipher generally has a key length of 128 bits and uses stream ciphering. [1]

(3) Undiscoverability: This prevents devices from responding to scanning attempts. A device’s 48-bit BD\_ADDR address is also concealed.[1]

(4) Pairing: Pairing enables devices to communicate. A device’s BD\_ADDR must be known for a pairing request to be made. The BD\_ADDR is identified from a knowledge of the previous pairing or by scanning. [1]

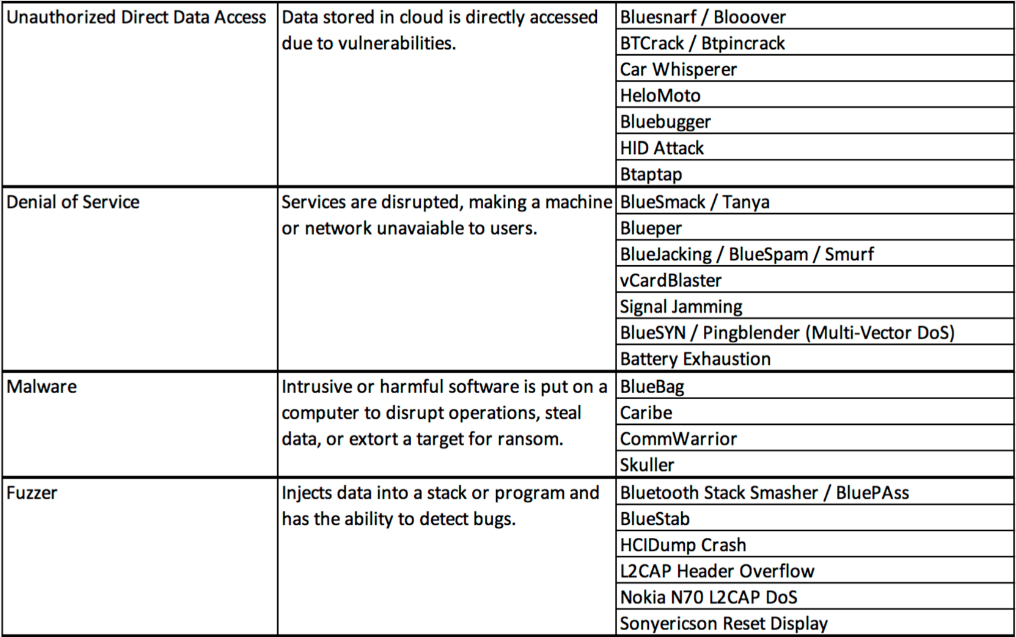
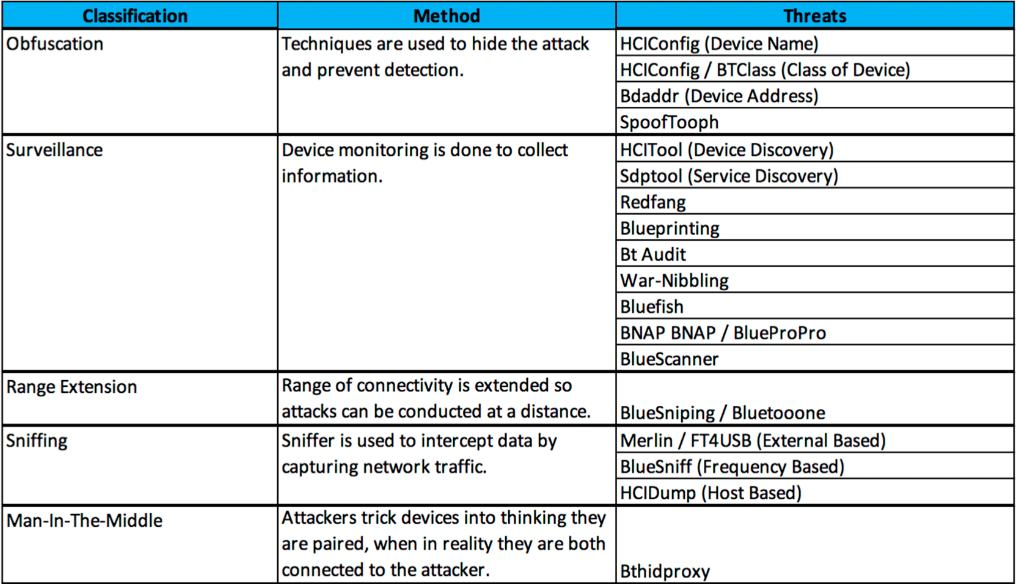
**Bluetooth Vulnerabilities and Threats:**

Vulnerabilities in Bluetooth Versions:

* Versions before Bluetooth 1.2: Link keys, which are based on static unit keys, are used for pairing and can be reused. If the key is retrieved, malicious devices can eavesdrop on the original devices, as well as spoof the original device and/or connected devices [1].
* Versions before Bluetooth 2.1 + EDR: Codes that consist of short PINs are permitted. These PINs are easy for attackers to guess due to their short length. These versions are lacking in PIN management, which is a desirable security capability at an enterprise-level. In addition, the keystreams in these early versions become vulnerable after being connected for 23.3 h. This is the time period at which the keystream repeats. This increases an adversary’s ability to decrypt messages [1].
* Versions 2.1 and 3.0: If Security Mode 4 devices are connecting to devices that do not support Security Mode 4, earlier security modes are used in the connection. For example, it is possible that Security Mode 1, which offers no security, will be used. This rollback in security modes makes versions 2.1 and 3.0 more vulnerable to attacks. In addition, SSP static keys are used in versions 2.1 and 3.0, which increases the device’s vulnerability to Man-in-the-Middle attacks.
* Versions before Bluetooth 4.0: There is an unlimited number of authentication challenge requests, which enables adversaries to obtain information on many challenge responses. This allows them to gain insight into secret link keys. In addition, the stream cipher E0 function, which is used in early versions, is considered weak [1].
* All versions of Bluetooth: Adversaries can view and potentially modify link keys if they are stored improperly. In addition, encryption key lengths may be small, which can make them vulnerable to attackers. It is possible that encryption keys can be as small as 1 byte. Regarding authentication, there is no user authentication. The Bluetooth standard only includes device authentication. It is important to note that a device can remain in a discoverable/connectable mode for an indefinite period of time [1].

**Bluetooth Taxonomy of Attacks:**

The Figure below illustrated, outlines and classifies Bluetooth-based threats [1].



**Common Bluetooth Attacks**

The pairing process is the main contributor to security issues found in Bluetooth. Attacks can be performed during different stages of the pairing process including before the pairing process has completed and after devices are paired. For example, attackers may be able to carry out Man-in-the-Middle attacks based on information they collected after pairing. Some of the more common attacks on Bluetooth are described below:

A. MAC Spoofing Attack

The attack is performed before encryption is established and during the formation of the piconet when link keys are being generated. Devices are able to authenticate each other by generating link-keys. During the attack, attackers can imitate another user. They also have the ability to terminate connections or intercept/modify data with the use of special tools. [1,3]

B. PIN Cracking Attack

The attack occurs during the device pairing and authentication process. An attacker uses a frequency sniffer tool to collect the RAND and the BD\_ADDR (Bluetooth Device Address is a unique 48-bit identifier assigned to each Bluetooth device by the manufacturer) of the targeted device. A brute-force algorithm (E22 algorithm) is then used to test all possible permutations of the PIN with the data previously collected until the correct PIN is found. [1,2]

C. Man-in-the-Middle Attacks:

such as attack occur when devices are attempting to pair. During the attack, messages are relayed unknowingly between the devices. This enables authentication without the shared secret keys. In a successful attack, the user believes the pairing was successful; however, this is not the case, as the two devices are paired to the attacker. [1,2]

D. Blueover Attack

Blueover and its successor Blueover II are auditing tools that are used to determine if a Bluetooth device is vulnerable, but they can also be used to initiate a BlueBugging attack. [1, 2]

E. Brute-Force BD\_ADDR Attack

This attack is a scanning attack on the last three bytes of the BD\_ADDR of a device [1,3]. It is important to note that the first three bytes, which are known publicly, can be set as fixed [3,5].

F. Reflection/Relay Attack

The attack occurs when the adversary impersonates a device. The attacker is not looking for any undisclosed information during the attack. It simply authenticates the connection by reflecting/relaying device information [1, 3].

G. Backdoor Attack

The attack occurs when establishing a trusted relationship during pairing. During the attack, the adversary does not appear in the register of paired devices on the target device. After a relationship is established, the attacker has access to the device's services and resources. This access is unbeknownst to the device owner. The BD\_ADDR of the target device needs to be known for a backdoor attack to be successful. It also needs to be determined that the device targeted by the attacker is vulnerable to the attack [1,3].

H. Worm Attacks

The attacks occur when a malicious software or Trojan file sends itself to available Bluetooth devices. Examples of these attacks are:

1. Cabir Worm: A malicious software that targets Bluetooth technology. Mobile phones that use the series 60 interface platforms are vulnerable to the attacks. For the attacks to be successful, the user must accept the worm. This causes the malware to install on the device. The worms are usually disguised in applications, which results in users unknowingly accepting them. Once installed, the software is the ability to use the compromised device to search for and send itself to other available devices. The Mabir worm is a form of the Cabir worm. This worm replicates by using Multimedia Messaging Service messages and Bluetooth. [1,3]
2. Skulls Worm: The Skulls Worm, a malicious SIS (Symbian Installation System) trojan file, targets Symbian mobile phones with the Series 60 platform. The worm poses as a Macromedia Flash player. The user must open and install the SIS file for the worm to become active. It then searches for additional devices to infect and the process repeats itself [1,3].
3. Lasco Worm: The Lasco worm, is a combination of a Bluetooth worm and SIS file. It targets and infects Symbian mobile phones that support the Series 60 platform. The user must open and install the Velasco.sis file. This prompts the activation of the worm. It can then begin searching for additional devices to infect and the process repeats itself [1,3].

I. Denial of Service Attacks

DDoS (Distributed Denial of Service) and ordinary DoS are two types of Denial of Service attacks. For ordinary DoS attacks, the attacker tries to crash the network or restart the system by sending packets to the targeted system. DDoS attacks can be done by a single attacker. These attacks can disable a network. They also can restrict network accessibility to a larger network. The attacks target the Physical Layer in the protocol stack or those above the Physical Layer. Some typical Denial of Service (DoS) attacks are BD\_ADDR duplication, BlueSmack, BlueChop, L2CAP guaranteed service, battery exhaustion, and Big NAK (Negative Acknowledgement), which is an attack using a continuous retransmission loop [1,6].

J. MultiBlue Attack

The attack occurs when an attacker has access to the device they wish to hack. The MultiBlue dongle, a bluetooth capable 4 GB thumb, is used to gain access to and take over the targeted device. The attacker then uses the MultiBlue application to see all discoverable devices within range and send pairing requests. The targeted device then presents a code, a pre-shared key, which needs to be entered into the MultiBlue application. This key is needed for authentication and encryption. The attacker then has control of the device [1].

**Mitigation Techniques:**

Mitigating Bluetooth vulnerabilities differ significantly from mitigating vulnerabilities in a computer system. While application software patches are used to resolve vulnerabilities in computer systems, Bluetooth devices require upgrades in device firmware. These upgrades cannot be developed by the general public and/or user community. Therefore, Bluetooth devices will continue to be vulnerable to attacks even if mitigation solutions become available [1,2].

While all attacks cannot be prevented, and security is not guaranteed, there are countermeasures that can be used to secure Bluetooth communications. Some of those mitigation techniques are described below: [1,2]

1. Enhancement of Bluetooth user awareness: it is necessary to educate Bluetooth users to ensure they have knowledge of the proper Bluetooth security practices. [1,2]

These security practices include:

* Default settings should be updated to achieve optimal standards [1].
* Ensuring devices are in and remain in a secure range. This is done by setting devices to the lowest power level [1].
* Using long and random PIN codes, which make the codes less susceptible to brute-force attacks [1].
* Changing the default PIN for devices and frequently updating this PIN (i.e., once every other month). [1,2]
* Setting devices to the undiscoverable mode by default, except as needed for pairing. Most active discovery tools require that devices be in a discoverable mode to be identified. Devices set to undiscoverable mode will not be visible to other Bluetooth devices. Devices previously configured, better known as trusted devices, will be able to connect and communicate while in this hidden mode.[1]
* Turning off a device’s Bluetooth when not needed or in use, especially while in certain public areas such as shopping malls, coffee shops, public transportation, clubs, bars, etc. This can prevent users from receiving advertisements from other Bluejackers. [1,2]
* Refraining from entering passkeys or PINs when unexpectedly prompted to do so. [1]
* Frequently updating software and drivers to have the most recent product improvements and security fixes. [1]
* It is recommended that users refrain from using non-supported or not secure Bluetooth-enabled devices or modules. This includes Bluetooth versions 1.0 and 1.2. [1]
* Pairing devices as needed. Users need to maintain that any pairing should take place in a secure non-public setting. This will help prevent attackers from intercepting pairing messages. As previously mentioned, a crucial part of Bluetooth security is pairing, so users should have knowledge regarding eavesdropping. [1,2]
* Users should use SSP instead of legacy PIN authentication for the pairing exchange process when it is possible. This will help mitigate PIN cracking attacks. [1]
* All lost or stolen Bluetooth devices should be unpaired from devices they had previously been paired with [2]. Unpairing will prevent an attacker from accessing the user’s other devices through the Bluetooth pairing. [1,2]
* Users should never accept transmissions from unknown or suspicious devices [2]. Content should only be accepted from trusted devices [1,2].
* All devices that are paired should be removed immediately after use. [1]
* Devices should be monitored and kept at close range.[1]

B. Instead of basing link keys on unit keys, they should be based on combination keys. This will prevent Man-in-the-Middle attacks. [1,2]

C. Use link encryption for all data transmissions to prevent any eavesdropping, including passive eavesdropping. Use of the HID boot mode mechanism, a connectionless human interface device, should be avoided, as it sends traffic in plaintext. [1,2]

D. Users should ensure all links are encryption-enabled when using multi-hop communication. Failure to do so could result in the entire communication chain being compromised [1, 2].

E. Require mutual authentication for network-connected devices. This will provide confirmation that the network connections are legitimate [1,2].

F. Lower the risk of broadcast interceptions by encrypting the broadcasts [1,2].

G. The maximum encryption key size should be used. In addition, a minimum key size should also be set—128 bits are recommended. The utilization of these minimum and maximum keys will protect devices from brute-force attacks [1,2].

H. To provide the highest level of security, Security Mode 3 is highly recommended. This mode of security, which is implemented at the link level, is one of the highest levels of Bluetooth security. [1, 2].

**Applications for Protecting Bluetooth Devices:**

Bluetooth firewall: The Firewall application protects devices, specifically Android devices, from all Bluetooth related attacks. Users are alerted upon any Bluetooth activity. The application also enables you to see Bluetooth capabilities on devices or specific apps [1].

Bluetooth file transfer: This application only enables authorized devices to be connected [1].

**References:**

1. @article{lonzetta2018security,

title={Security vulnerabilities in Bluetooth technology as used in IoT},

author={Lonzetta, Angela M and Cope, Peter and Campbell, Joseph and Mohd, Bassam J and Hayajneh, Thaier},

journal={Journal of Sensor and Actuator Networks},

volume={7},

number={3},

pages={28},

year={2018},

publisher={Multidisciplinary Digital Publishing Institute}

}

1. @inproceedings{cope2017investigation,

title={An investigation of Bluetooth security vulnerabilities},

author={Cope, Peter and Campbell, Joseph and Hayajneh, Thaier},

booktitle={2017 IEEE 7th Annual Computing and Communication Workshop and Conference (CCWC)},

pages={1--7},

year={2017},

organization={IEEE}

}

1. 8 @article{minar2012bluetooth,

title={Bluetooth security threats and solutions: a survey},

author={Minar, Nateq Be-Nazir Ibn and Tarique, Mohammed},

journal={International Journal of Distributed and Parallel Systems},

volume={3},

number={1},

pages={127},

year={2012},

publisher={Academy \& Industry Research Collaboration Center (AIRCC)}

}

1. 3 @book{padgette2012guide,

title={Guide to Bluetooth Security: Recommendations of the National Institute of Standards and Technology (Special Publication 800-121 Revision 1)},

author={Padgette, John and Scarfone, Karen and Chen, Lily},

year={2012},

publisher={CreateSpace Independent Publishing Platform}

}

1. 9 @article{panse2013survey,

title={A survey on security threats and vulnerability attacks on bluetooth communication},

author={Panse, Trishna and Panse, Prashant},

journal={International Journal of Computer Science and Information Technologies},

volume={4},

number={5},

pages={741--746},

year={2013}

1. 36 @inproceedings{nawir2016internet,

title={Internet of Things (IoT): Taxonomy of security attacks},

author={Nawir, Mukrimah and Amir, Amiza and Yaakob, Naimah and Lynn, Ong Bi},

booktitle={2016 3rd International Conference on Electronic Design (ICED)},

pages={321--326},

year={2016},

organization={IEEE}

}