Journal of Computer Science 3 (7): 546-548, 2007
ISSN 1549-3636
© 2007 Science Publications

Security Manager - Key to Restrict the Attacks in Bluetooth

Pushpa Suri, Sona Rani
Department of Computer Science and Applications, Kurukshetra University, India

Abstract: Bluetooth is the technology that utilizes radio frequency waves as a way to communicate wirelessly between digital devices. The Bluetooth user has the choice of point-to-point or point-to-multipoint links whereby communication can be held between two devices, or up to eight. When devices are communicating with each other they are known as piconet, and each device is designated as a master unit or slave unit, usually depending on who initiates the connection. However, both devices have the potential to be either a master or a slave. We have given the analysis of denial of service attack in the bluetooth technology. And describe the proposed solution for this attack by the use of security manager.

Key words: bluetooth, attack, pairing, security manager

INTRODUCTION

Bluetooth is an always-on, short-range radio hookup that resides on a microchip. It was initially developed by Swedish mobile phone maker Ericsson in 1994 as a way to let laptop computers make calls over a mobile phone. Since then, several thousand companies have signed on to make Bluetooth the low-power short-range wireless standard for a wide range of devices. Industry observers expect Bluetooth to be installed in billions of devices by 2007.

The concept behind Bluetooth is to provide a universal short-range wireless capability. Using the 2.4 GHz band, available globally for unlicensed low-power uses, two Bluetooth devices within 10 m of each other can share up to 720 Kbps of capacity[1]. Bluetooth is intended to support an open-ended list of applications, including data (such as schedules and telephone numbers), audio, graphics, and even video. For example, audio devices can include headsets, cordless and standard phones, home stereos, and digital MP3 player[2].

ATTACKS IN BLUETOOTH SECURITY

Types of attacks in bluetooth security:

SNARF attack: It is possible for attackers to connect to the device without alerting the user, once in the system sensitive data can be retrieved, such as the phone book, business cards, images, messages and voice messages.

BACKDOOR attack: The backdoor attack is a higher concern for Bluetooth users; it allows attackers to establishing a trust relationship through the "pairing" mechanism, but ensuring that the user can not see the target's register of paired devices. In doing this attackers have access to all the data on the device, as well as access to use the modem or internet; WAP and GPRS gateways may be accessed without the owner's knowledge or consent.

BLUEBUG attack: It allows the attacker to make premium priced phone calls, allows the use of SMS, or connection the Internet. Attackers can not only use the device for such fraudulent exercises it also allows identity theft to impersonate the user.

Bluejacking: Bluejacking allows attackers to send messages to strangers in public via Bluetooth. When the phones 'pair' the attacked can write a message to the user. Although it may seem harmless at first, there is a downside. Once connected the attacker may then have access to any data on the user Bluetooth device, which has obvious concerns.

DENIAL OF SERVICE Attack: A denial of service is "any action, or series of actions, that prevents any part of a system, or its resources, from functioning in accordance with its intended purpose".

It can be defined as an intentional attempt to prevent or degrade availability of any resources. And it results in the prevention of authorized access to resources or the delaying of time-critical operations.

It is the absence of availability. Availability is "the reliability and timely access to data and resources by authorized individuals".

Availability*:* The property of a system or a system resource being accessible and usable upon demand by an authorized entity, according to performance specifications for the system.

Availability is one of the three tenets of computer security, the other two being confidentiality and integrity as defined below:

Confidentiality*:* The property that information is not made available or disclosed to unauthorized individuals, entities, or processes.

Integrity*:* The property that data has not been changed, destroyed, or lost in an unauthorized or accidental

Corresponding Author: Sona Rani, Kukurshetra University, Kurukshetra, Haryana, India

manner. For systems, integrity is defined as the quality that a system has when it can perform its intended function in an unimpaired manner, free from deliberate or inadvertent unauthorized manipulation.

Denial of Service Attack In Bluetooth: A denial of service attack can be carried out as flooding messages in bluetooth devices. In flooding denial of service *attack* unnecessary data is sent as much as possible to a victim. As a result, network bandwidth is wasted, disk space is filled with unnecessary data or processing power is spent for unuseful purpose[3].

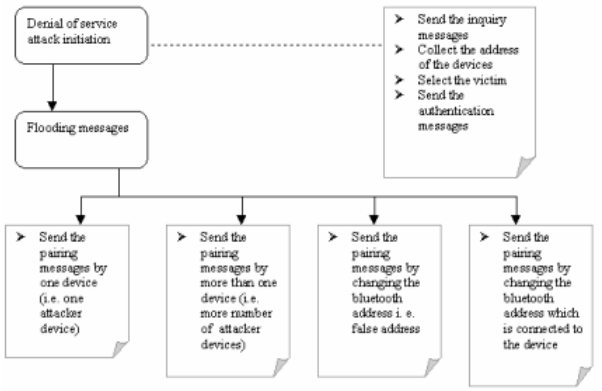

Fig. 1: Denial of Service Attack

Flooding DoS attacks can be divided into different types as shown in Fig. 1. In direct attacks spoofed packets are sent directly to the victim, here is only one attacker device, in the second type of attack more number of devices will act as the attacker that is a group of attacker devices will be there and the attacker devices will send the requests to the victim and the victim will be busy in sending the response back to the attacker devices and authorized users will not be in the position to make connections. In the third type the pairing messages is sent by changing the bluetooth address of as the address of another bluetooth device which want to make the connection with the bluetooth device (victim device). When the attacker will send the message by changing and replacing its bluetooth address with the authorized bluetooth address. The victim will send the authentication message and the attacker will send the wrong response and the victims will consider it in the failed authentication list . Next time when the authorized user with the right address (whose address is used by the attacker), send the message for pairing, the victim will ignore the request, as it is included in the failed list of devices and the denial of service will be there for the authorized user as a result.

In the fourth type of attack, if there is already paired device for the victim device, the attacker will pick up the address of the paired device and send the messages for paring. As in the bluetooth technology, there is no provision for the checking of already connected device address before considering the request for next pairing massage. The victim will remain busy in sending the response back to the attacker and the service denial will be there.

PROPOSED SOLUTION

The following are the different ways by which the denial of service attack can be avoided in bluetooth technology:

When the pairing message is sent by one device: Denial of service attack can be avoided by storing the address of bluetooth device, which failed to authenticate more than predefined number of unsuccessful attempts (Fig. 2). In this way if the victim device has a database, which will restrict the access of, failed bluetooth devices even for the request for pairing process. This can limit the denial of service attack.

When the attacker is sending the messages with the address, which is already connected, to bluetooth device: In this attack if we are implementing the security manager in the connection establishment process, then the security manager can tell that the device is already being paired (Fig. 2) and there is no need for the pairing process and if there are still pairing messages there is an attack which is going on.

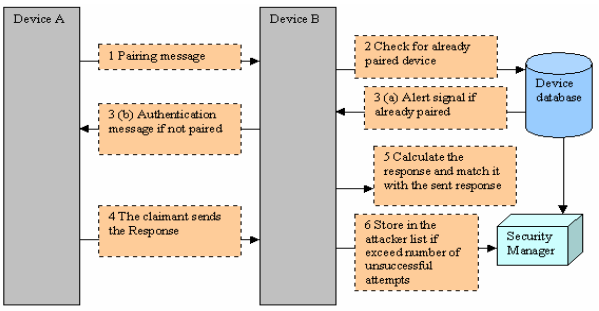

Fig. 2: Address list of already paired devices and failed authentication devices

When the pairing messages sent by more than one device: In this type of attack also if in a particular time duration, number of unsuccessful paring is more than the particular predicted number, the bluetooth device can guess that there is denial of service attack attempt is there (Fig. 3). And it can send the alert signal to the

security manager to stop the interactions with these devices.

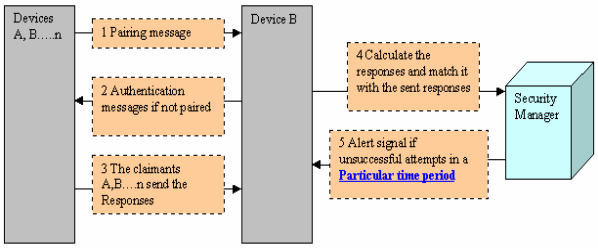

Fig. 3: Address list of failed authentication devices in 't' time period

When the attacker is changing the bluetooth address of itself with another bluetooth address: In this type of attack if the attack changes its bluetooth address with another bluetooth device and sends the wrong authentication response in reply to the message sent by the verifier (victim), the verifier will first update its failed authentication device list by adding the address of the device which is not at present in try to make the pairing but the attacker is using its address. The victim device itself sends message to the device after some time duration to authenticate the device, If it will be the right device, it will make the connection, otherwise it will fail to authenticate (Fig. 4).

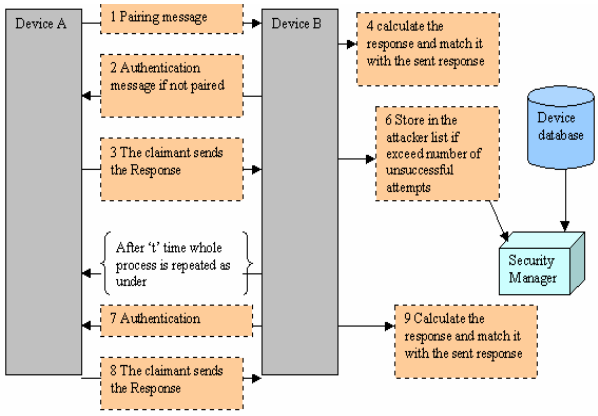

Fig.4: Repeat the authentication process after particular time period

ALGORITHM FOR THE PROPOSED METHOD

Start (pairing)
{
I f (message for pairing)
Check for the already paired devices list
If (already paired)
Alert signal to security manager
Else
Send the authentication challenge
And receive the response back
If (incorrect response is > specified number of attempts)
Add to the failed list to devices
If (incorrect response by more number of devices in particular time duration)
Alert the security manger for attack
If (response is incorrect)
After 't' time
Send the challenge to the device
Get back the response
If (response is correct)
Remove it from the list of failed devices
Else
No change

DISCUSSION

Bluetooth has several threats, which range in level of. These threats have the ability to provide criminals with sensitive information on both corporate and personal levels. The only way to avoid such threats is for manufacturers, distributors, and consumers to be provided with more information on how they are committed, current attack activity and how to combat them. The proposed method in this paper by which the security manager can avoid the denial of service attack in bluetooth.

REFERENCES

1. Bluetooth Baseband Specification, 2000 Bluetooth SIG version 1.1, www.bluetooth.com
2. Bluetooth Host Controller Interface Functional Specification, 2000. version 1.1, www.bluetooth.com
3. S. Basagni, R. Bruno, and C. Petrioli, May, 2002. Device Discovery in Bluetooth Networks: A Scatternet
4. Perspective, Proceedings of the IFIP-TC6 Networking Conference, Networking, Pisa, Italy