International Journal of Engineering Applied Sciences and Technology, 2018
Vol. 3, Issue 5, ISSN No. 2455-2143, Pages 71-74
Published Online September 2018 in IJEAST (http://www.ijeast.com)

Security System for Bluetooth Networks BLUEWEB SECURITY SYSTEM

Nayyar Ahmed Khan
Department of CS and IT
Shaqra University, Shaqra,
Riyadh KSA

Mohammad Ahmad Mohammad Nasim
Department of Computer Science
Shaqra University, Sajir,
Riyadh

Mobarak Abaker Adam Hassan
Department of Computer Science
Shaqra University, Sajir,
Riyadh

Abstract— **We aim to give a perspective regarding network security of blue web when the data transfer is under process. This will be done by designing an anti-virus network which can elicit the virus and will sort it out from the useful data. Corruption is a fatal thing which can bring anything to inertia; it has not even spared the revolutionary technological boon to the mankind shortly named as internet. One latest victim is Bluetooth technology. As we know that Bluetooth provides a way to connect and exchange information between devices such as mobile phones, laptops, personal computers, printers, GPS receivers, digital cameras, and video game consoles over a secure, globally unlicensed short-range radio frequency. While transmission, the hard disk, of any of the two devices can be accessed and hence corrupted by the other as there is no security check for the various viruses.**

Keywords— **Bluetooth, Security, Protocol, Architecture, System, Program Code, Scatter net.**

I. WHAT IS BLUETOOTH?

Bluetooth wireless technology is a short-range communications system intended to replace the cables connecting portable and/or fixed electronic devices. The key features of Bluetooth wireless technology are robustness, low power, and low cost. Many features of the core specification are optional, allowing product differentiation. The Bluetooth core system consists of an RF transceiver, baseband, and protocol stack. The system offers services that enable the connection of devices and the exchange of a variety of data classes between these devices. Bluetooth technology is actually derived from a combination of wireless technologies. The Bluetooth wireless technology operates on an open frequency within the 2.4 gigahertz band, which is the same as Wi-Fi, cordless phones and various other wireless devices. Bluetooth technology has been around for years, however for many people it is just another “tech” term.

II. HOW IT WORKS?

Bluetooth is a connection-oriented service. In order to connect two Bluetooth devices, one of them, normally the device initiating the connection, elevates to. The master, leaving the second device as a slave.

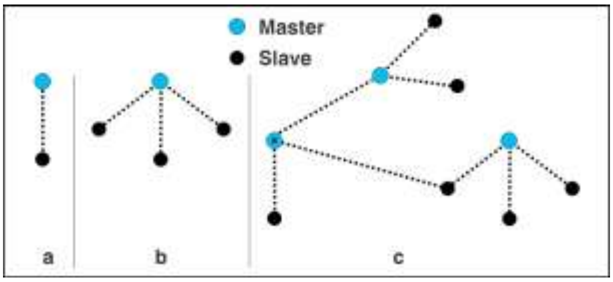


Figure: Pico net of two (a) or more (b) devices, scatter net (c)[1]

In Bluetooth, connections with up to seven devices, which form a piconet, are possible, where communication is led by the master device. Finally, a device is able to participate simultaneously in several pioneers (in only one of them acting as the master). The resulting topology is called scatternet (c). A master may reserve SCO (synchronous connection oriented) connections to up to three slaves in his piconet, using certain time slots. Those connections, granting symmetric data rates to both communication partners are used for voice transmission primarily. Unused timeslots may now be used for exchange of point-to-multipoint packets between the master and all slaves in the piconet via ACL (asynchronous connectionless) packets. These connections grant higher data rates in only one direction.

III. RANGE OF FORCES

Bluetooth is designed for low power use. The standard range for Bluetooth devices is 10m (Around 33 feet). The 10m range is perfect for what Bluetooth was developed to do. Newer high-powered Bluetooth allows a range of up to and sometimes over 100m [2]

Power Class	Max. Power Consumption	Max. Operating Range
1	100 mW (20dBm)	100 m
2	2,5 mW (4 dBm)	20 m
3	1 mW (0 dBm)	10 m

Table 1. Power and Operating Range

In most cases the effective range of class 2 devices is extended if they connect to a class 1 transceiver, compared to pure class 2 network. This is accomplished by the higher sensitivity and transmission power of Class 1 devices.

IV. APPLICATIONS

- Wireless control of and communication between a mobile phone and a hands-free headset. This was one of the earliest applications to become popular.
- Wireless networking between PCs in a confined space and where little bandwidth is required.
- Wireless communications with PC input and output devices, the most common being the mouse, keyboard and printer.
- Replacement of traditional wired serial communications in test equipment, GPS receivers, medical equipment, bar code scanners, and traffic control devices.
- For controls where infrared was traditionally used.
- Sending small advertisements from Bluetooth enabled advertising hoardings to other, discoverable, Bluetooth devices.
- Dial-up internet access on personal computer or PDA using a data-capable mobile phone as a modem.

V. VULNERABLE ISSUES IN TRANSMISSION

Today, all communication technologies are facing the issue of privacy and identity theft. Bluetooth technology is no exception. The information and data we share through these communication technologies is both private and, in many cases, critically important to us. Everyone knows that email services, company networks, and home networks all require security measures. What Bluetooth users need to realize, is: Bluetooth requires similar security measures. Recently, Bluetooth technology has been popping up in the news. Unfortunately, most of the news involves confusion and misinformation regarding the security of Bluetooth. Recent reports have surfaced describing ways for hackers to crack Bluetooth devices security codes.

5.1 Bluetooth viruses

Some Bluetooth networks are vulnerable to inadvertently spreading mobile phone viruses. The viruses detect vulnerable devices and infect them in the effort to propagate. The mobile phone viruses can corrupt data on a device as well as damage the actual device.[3]

5.2 Trojan

In the context of computing and software, a Trojan horse, or simply Trojan, is a piece of software which appears to perform a certain action but in fact performs another such as a computer virus. Contrary to popular belief, this action, usually encoded in a hidden payload, may or may not be actually malicious. Simply put, a Trojan horse is not a computer virus. It is instead a categorical attribute which can encompass many different forms of codes. Therefore, a computer worm or virus may be a Trojan horse. A simple example of a Trojan horse would be a program named "waterfalls.scr" where its author claims it is a free waterfall screensaver. When run, it instead unloads hidden programs, commands, scripts, or any number of commands with or without the user's knowledge or consent.

5.3 Malicious entities

Malicious entities may steal the identity of legitimate users and masquerade as them on internal or external corporate networks. Malicious entities may be able to violate the privacy of legitimate users and be able to track their movements. Malicious entities may deploy unauthorized equipment (e.g., client devices and access points) to surreptitiously gain access to sensitive information. Malicious entities may gain unauthorized access to an agency's computer network through wireless connections, bypassing any firewall protections. Viruses or other malicious code may corrupt data on a wireless device and subsequently be introduced to a wired network connection.[5]

VI. EXISTING SCENE

6.1 Request/Response Scenario

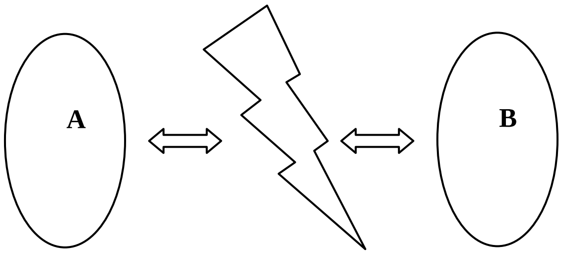
A ⟶ Request ⟶ Firewall ⟶ B

Device A sends a request to device B, via Firewall architecture.

B ⟶ Response ⟶ Firewall ⟶ A

Device B accepts the request and sends a response, via Firewall architecture to device A.[6]

6.2 Connection Establishment



VII. PROPOSED MODEL

For a secure communication via Bluetooth, the following security targets are defined as:

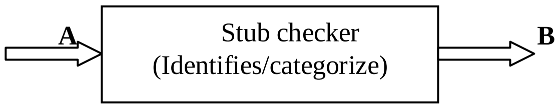
- Confidentiality
- (device) Authentication
- (device) Authorization
- Integrity[4]

As we have come to know about the various flaws in the Bluetooth communication. Some of the prominent attacks on this technology are SNARF, BLUEBUG, BACKDOOR, Bluejacking. These flaws in Bluetooth security lead to disclosure of personal data. Thus, we aim to propose a model having a STUB CHECKER in the device itself that identifies and categorizes all malicious codes through an algorithm during the transmission.

7.1 Proposed Algorithm

```
Logiccheck (stub)
{
    stub;
    validation ( )
        {
        routine inspection;
        }
}
```

Whenever any file is sent from device A to device B,it is made to traverse through this Logic Checker,if it identifies any stub it sends it to the validation function where in the routine inspection if it finds anything suspicious or threatening code it stops the transmission then and there.



(Black Box)

Data transfer through the stub checker

VIII. ALGORITHM PROPOSED IN CONTEXT

Algorithm Proposed for the Issue: This algorithm needs to be implemented as a bi-product whenever the complete Bluetooth driver will be set as in case of a PDA or Personal Computer Machine

```
Boolean logicCheck (file[ ])
{
    databaseSignature dbs;
    while(!true)
        {
        logicCmp(file[ ]!=dbs)
            {
            Return false;
}
        logicAdd()
            {
            If(logicCheck(file)!=dbs)
                {
                Dbs.addSigntr();
    updateDbs();
}
            }
}
Return false;
}
```

Algorithm Applicable:

1. logicCheck():Function to compare the stubs in the Bluetooth file array.
2. databaseSignature: An array of predefined virus stubs that can be updated at any instance.
3. logicCmp(); To compare the database Signature with the receiving file.
4. LogicAdd (): Function to add the virus signature to the existing database Signature file if a new infection of any malicious code is retrieved.
5. Dbs.addSigntr(): Function to add the details of virus definition.
6. updateDbs(): Function to remove the vulnerability and append the stub to the existing virus databaseSignature.

IX. CONCLUSION

The above paper proposes a model to secure the Bluetooth network connections. This modal makes use of the various security stub based checking for the Bluetooth in the form of short ranged forces. These forces uses the logical function to provide additional security in the networks established by the Bluetooth web. Overall the modal is very effective and eligible to be applied to the Bluetooth networks where the transmission of the files is done with the help of the secure mechanisms.

X. REFERENCES

[1]. P. Bhagwat and R. Seigal. A routing vector method (RVM) for routing in Bluetooth scatternets. In *IEEE International Workshop on Mobile Multimedia Communications (MoMuC'99)*, San Diego, CA, November 1999.

[2] A. Das, A. Ghose, A. Razdan, H. Saran, and R. Shorey. Enhancing performance of asynchronous data traffic over the Bluetooth wireless ad-hoc network. In *Proceedings of INFOCOM'2001*, Anchorage, AK, April 2001.

[3] N. Johansson, U. Korner, and L. Tassiulas. A distributed scheduling algorithm for a Bluetooth scatternet. In Proceedings of ITC'2001, Salvador, Brazil, december 2001.

[4] B. Miller and C. Bisdikian. Bluetooth Revealed: The Insider's Guide to an Open Specification for Global Wireless Communications. Prentice-Hall, 2000.

[5] T. Salonidis, P. Bhagwat, L. Tassiulas, and R. Lamaire. Distributed topology construction of Bluetooth personal area networks. In Proceedings of INFOCOM'2001, 2001.

[6] B. Hajek and G. Sasaki. Link scheduling in polynomial time. IEEE Transactions on Information Theory, 34(5), 1988.