iJRASET
International Journal For Research in Applied Science and Engineering Technology

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 8 **Issue:** V **Month of publication:** May 2020

DOI: http://doi.org/10.22214/ijraset.2020.5380

www.ijraset.com

Call: 08813907089 | E-mail ID: ijraset@gmail.com

International Journal for Research in Applied Science & Engineering Technology (IJRASET)
ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.429
Volume 8 Issue V May 2020- Available at www.ijraset.com

A Comparative Study on Home Router Security

Akshat Kumar
Department of Computer Science & Engineering, Galgotias University, Greater Noida, 201310
School of Computer Science And Engineering, Galgotias University

***Abstract:** As we know Routers are vulnerable to attack by the way they are configured. Like having credentials already defined over the internet can allow cyber criminals to compromise our security by the brute force attack. Another major concern is when an attacker use entry point to infiltrate our network. A normal home router contains services such as Dynamic Host Configuration Protocol(DHCP),Domain Name System(DNS),Trivial File Transfer Protocol(TFTP),Telnet and so on but they do not run any protection software such as anti-virus. The more and more use of non-Internet features such as network storage or voice over IP into the routers raises many security concerns. In this research paper, we investigate the issue regarding these cases and importance of these devices to be secured. We conclude by suggesting ways to protect routers from botnets without users interaction, which is possible with the use of ISP, this way while respecting the privacy of the user we can identify what further work needs to be done to the Routers.*

I. INTRODUCTION

A. Motive Behind It

Routing devices are a very common devices present in almost every local environment. It is usually provided by Internet Services Provide(ISP) to the customers and is mostly already configured so the user can start the connection as soon as he buys it.The user can connect home environment to the router after configuring the credentials of the router. Mostly no extra configurations are added to the router because either user doesn't want to or he does not have the knowledge to do so or in some cases they are to tired and think it as an extra work to do for no benefit at all . Because of this reason, by default the security which is provided by router is very poor as a wireless router are not configured with encryption by default .

A router is always provides with a firewall in order to prevent any unsolicited connection to your computer when it is connected over the Internet . A good and trusted router provides a full protection using the firewall but a bad router have various issues as well as some loop holes present in their firewall.

A normal router contains four Ethernet ports which are used for wired connections. Because of the increase in wireless devices the use of the Ethernet port has been decreased. Now some of consumer routers are provided with only one Ethernet port. On the other hands some of the high end router still have four or more Ethernet ports. In order to connect with two different ISPs high end router are provided with multiple ports. For example, one can be connected to the DSL modem and other can be connected to a cable modem. This type of example is applicable for the location having high need of Internet Access. By this the devices are connected to one or another modem even if any of the modem fails.

These routers are not only used for the small scale like home network but combining together its provides a large network which is used by large scale industries or corporate environment. Mostly these routers are used by small industries and large firms because they do not want to or can't or even have to send a large amount of money simply on the infrastructure. Like these company not all companies are IT Firms(Information technology) so they do not see the importance of securing these devices . This is no different than a user at home because the router have already have default configuration which seems to work just fine.

This papers research is based on the analysis of web interfaces security against different kinds of web based attacks and our special focus would be on the UI redressing attacks as well as cross site scripting. Our main motive is to change important default settings in the router so that we can give a perfect control to the user. After the attacker gains access to the router inside house their is a different kind of senerio we face.

The first is that attacker can disguise himself as the middle person and can change the default setting like DNS or IP gateway according to his or her need like he can gain full access to the home network along with all its traffic. Second is that he can make router to reboot itself anytime so you cannot access the internet when needed. Third and the most important of all is that he could built bots using your router.

B. Importance of This Topic

In this research paper we tend to discuss different kinds of attacks that were made on the home environment device that is router. Before that we have to know about the attacks that were used to attack the router which also includes the different methods which already exist inside the router. In this paper we will also discuss the attacks with their result on an actual router. Along with the attack on router and their method we will also discuss different types of module that exists, how they work together effectively and also discuss about how each specific module work.

In this we will also discuss vulnerabilities of the system and how each attack can be specifically made to each module of the router and also discuss the solution for the attack on each module.At first we tried to understand the vulnerability of a single module and then we tried the combination of different module and noted the result of how much vulnerable to the attack they are.After the study we tried to become attacker and attacked our own system to check is security as well as to prove that botnet can be created easily on an embedded device. Our believe is that these types of attacks represent grave danger and has not been taken seriously by the community of network security.

C. Wide Spread Of the Problem

The spread of the botnet has become a major concern in the resent upcoming year as the are used for various attacks mostly which are DDOS(Distributed Denial Of Service) and sending of bulk of email spam for the purpose of advertisement. Because of this vendors of the system are trying to find the flaws and are frequently updating their security patches to protect the computers by antivirus and anti spam. Digital connection technology or DCL is a which is widely use for the home computer because of its security and the reason behind it is the network addressing translation device or NDT since the network is an IP or which is inside a private range network. The main advantage of this design is that router acts as an additional firewall also which protect our device from the outside network. Another common configuration of home routers is that the bridged setup, during which the router relays traffic from the ISP to the pc with none process of the packets, effectively connecting the pc on to the net with the pc being appointed a public scientific discipline address by the ISP (either statically or dynamically). The IP address which is publicialy assigned is mostly stable as the power of the router is turned on -- so we can consider that this address will be used for a long time by this device. But we should remember that because of DSL being being a power off seldom it is more in danger for attack from other parties.

We knoe that NAT is the most common configuration of the home router because its is considered a safe approach, but this router is usually at the edge of our home network that is why it is safe for us to assume that it can be discovered by and can be accessed from someone outside the network . That is the reason why this router has become the target practice for the attackers. One more reason for its vurnubility is that the router is alos at the edge of the LAN form the user side. This device is usually left powered on even if all the devices connected to it are turned off. The attacker wants to control the device which is usually active and is online all the time this type of routers are the most suitable for them that is why they are very much attracted to these devices . Another reason is that these type of devices are widely deployed are are often miss configured which is suitable for them .

Ang Cui, et al., from university of Colombia have shown the how easy it is to exploited these type of devices by targeting the big IP addresses from around the big countries such as Japan, India, Netherlands. Australia etc .This research is still going on but it can be said that results of vulnerable devices can still be found. The first paper was printed in Gregorian calendar month 2009 and the result its shows is the global scanning they are performing.

Table of Vulnerable devices in percentage

Large Area of devices Found	Corrupted Devices (in persent)
Japan	75
Canada	60
India	57
Korea (Republic of)	57.1
Hungary	54.5
Australia	50
Netherlands	48.6

D. Botnet

The collection of devices which are connected through the internet either a computer or a server or a mobile devices and which are controlled by a similar type of malware or a virus is commonly known as a Botnet. Most the users of the system is not aware that is system is corrupted. These devices are controlled by the cyber criminals so as to keep their malicious deeds hidden from the user and to perform their operations from the background. A bot can be defined as a machine which is compromised and is infected with a harmful code which is set by the attacker. A system can be infected by both ways, in one the attacker him self sends the infected code or its the other way in which the system is infected automatically by a self propagating bot.

Most common of such approach is that as soon as the targeted system is compromised it waits for the commands from masterbot which is through an IRC channel.

The task of botmaster is to manage all the corrupted system and also to organize the corrupted system in order to perform multiple attacks. In this paper we discuss about the management of the bots and also about the protocols which manage them . Some of the bots are refined and they will use a different approach like peer to peer connection because this approach avoids the necessary control for coordination.

As the home router and computers are easily to compromise they are usually targeted because a user is looking for a high speed connection they are easily exploited and are compromised. It is a fact that an average person do not know if the botnet is present or not in his system but a botnet can are also meant to fulfil various others goals such as measuring the wants of entity which are dominant. . Its is basically used for functions which are damaged or on the criminals. The task of botmaster is to manage all the corrupted system and also to organize the corrupted system in order to perform multiple attacks. In this paper we discuss about the management of the bots and also about the protocols which manage them.

E. Denial of Services (DoS)

The Denial of Service is an attack in which the attacker shutdowns are means to access our machine or services which is intended for us, it can be either a mail or web service or even a domain name system. In Dos the attacker uses the resources of the specific system by bandwidth resourcing and making the specific service unavailable to us. But because of bandwidth resourcing the attacker has to control a larger volume of processing power and bandwidth. Its the reason why this can be overcome by using Botnets which is even beneficial for the attacker.

F. Spamming

As we have already discussed what a Botnet is now we know that it offers large aggregate bandwidth to its master which is used for spamming.A bot is not only lethal for its sending of emails and post messaging purpose but can also slither into our mails to gather more email addresses . These emails are used by the attacker to add more mining functionality to its botnet. This mining functionality is an automated process which is used for finding the emails and using them for more spamming purpose that is how they get the information for spamming an email.

Type	Average Count of Botnets (in thousands)	Sending Capacity of Spam (in millions)
Srizbi	315	600
Bobax	185	90
Rustock	150	300
Cutwail	125	160
Storm	85	30
Grum	50	20
OneWord Sub	45	N
Ozdok	30	100
Nucrypt	20	50

G. Self Propagation

Ability to spread hostile code is most important feature that is provided by the bots. These features are used to infect the many devices as well as are used to update the bot. This can make various other devices to automatically join to make the botnet .The attacker can send the updates to all of its botnets to infect a large sum of device by finding a zero day attack. Now the botnet upon receiving the update can send the hostile code to the other botnet because of peer to peer connection . It is said that around 4000 to 9000 new botnets can be produced per day by using self propagation campaigns.

II. PROBLEM DEFINITION

The device which we currently use lacks the detection of malware. A a matter of fact most of the devices used do not even have the ability to add any kind of software in it(but some devices have the ability to RE-FLASH the device with a completely new image) . The router which we prefer do not have the ability to detect the malware(ie. Antivirus software) But as we know everyone still uses this system to stay online, more over the use of DSL is still widely used to get a router based connection. Moreover, the attack vector we have discussed earlier must be implemented not only to routers but to all the devices and they must share a common security standard. Even if we know that the correct configuration is vital for our security, sometimes the routers are configured. The basis protocol followed by ISP is that the router or the device should be ready to use when its delivered to the user . Average of the customers do not have the information to understand the complexity of the system they do not even have skills to configure the router and most of them also think that routers are a means to only connect to the internet and no security is needed for them. A research has shown that man of the users disable their security willingly to increase their speed of internet surfing. For peer to peer connection deactivating the firewall is commonly used. By doing so the only protection we have now within the device the router is connected to such as antivirus inside a system, its the only layer of protection a user has got now to protect the system from different kinds of threats. As such because of the ill implementation of the provider now the user does not know what a heavy price he has to pay for this kind of ignorance. Most of the vendors of the routers do not even any present the software update except for some of the open source routers like WRTG which provide the user with some updated security patches.

The codes are becoming more and more complex because of the increase in demand of software product which requires to add more features. That is why the software is becoming more complex and bigger. Every programmer knows as the complexity of the code increases so does the bugs and loop holes. So the main question arises “Is software security execution correlated to the complexity of the code?”. Many of the researchers are divided into two subjects for further study. Their is a definition given by such two researchers , Williams and Shin and they concluded that "the results of our study show weak evidence that software complexity is the enemy of software security". At the same time they even suggested that faulty code is less complex than a vulnerable code. Williams and Shin were also investigating the JavaScript engine of the Mozilla because while it focuses on the security the complexity of the code increases and when any vulnerable code is found the code present can become more and more complex..

As we have discussed earlier that its is not necessary for a router to be considered as a Pc in an local environment that is the reason why the software of the router is not updated as regularly and even we know that some of the router are never even updated. The only time it is ever updated is when be buy or receive it from the network provider. On top of that kernel of the Linux(propreietary software) is developed to support the services. Because of the limited time in development this software is usually full of bugs. In this security is not the primary issue and even some times the systems are not even designed very carefully. Various of the open source code are combined together into an image which is flashed on the devices. The various parts are made carefully but then even the design of the system is not made carefully which would eventually raise some issues.

III. METHODOLOGY

Our main goal is to provide solution to the problem to prevent the exploitation and security of the routers. For this issue to be solved the most basic need is the education of security issues. Every software has some issues in form of bugs either in programming or designing that is often used in the exploitation. This type of issues are even present on the new software even if advance security testing is applied to it.In most of the cases of information exploitation happens because of the carelessness of the user regarding their security of computers or devices. Many of the research shows that uses do not even change their default password or even when changed uses a password that is very easy to guess like BirthDate or PhoneNo.

Routers are a medium for a user to utilize the network for the personal use or for the organization. Some policies must be enforced by ISP’s that CPE which is provided to the user is secure by default and also keeping in mind that the average users cannot configure a device which makes it insecure. By this we can also say that the browser used by the user should not be trusted by a web application whose security implementation cannot be trusted.

SE Linux which stands for Security Enhanced Linux is an architecture design which is used to provides security to a large range for computing environment. Unix like operating system (Linux) are updated with patches of SE Linux. By using LSM a flexible MAC is provided.

For providing a better security against CSRF attacks, the HTML request of forms which are generated by the application should be verified by confirming if it is coming by the specified client or not. This technique can be established by using some of the tags or the hidden elements present in the form. The URL along with the Session Id can be used together to give a random token that can be used as a one time and on the proffering it can check that it is coming from the valid source. The value of the token can be calculated by the server before before submitting the request, if the token does not matches with the value then that form should be declared Invalid because of the security reasons .

The paper written by Mitchell, Brath and Jakson(Robust Defenses for CSRF) also explained that if we have to identify the origin of the request then the browser should send the Original Token along with the POST .They also suggested that it would be beneficial the use Original Token instead of the refered token to increase the privacy of the user. We know that the original token only contains the information required for the identification of the initaited request its does not contain any information of the URL but the refered token always includes such information.

For inspecting the users traffic ISP always raises some red flags. As the user can block a traffic which follows all the policies and safety issues along with the malicious traffic. The applications which do not provide an end to end encryption also raises the flag because the provider can store all the information of the user along with some personal emails and messages .The stored data can then be shared with a third party for various reasons.

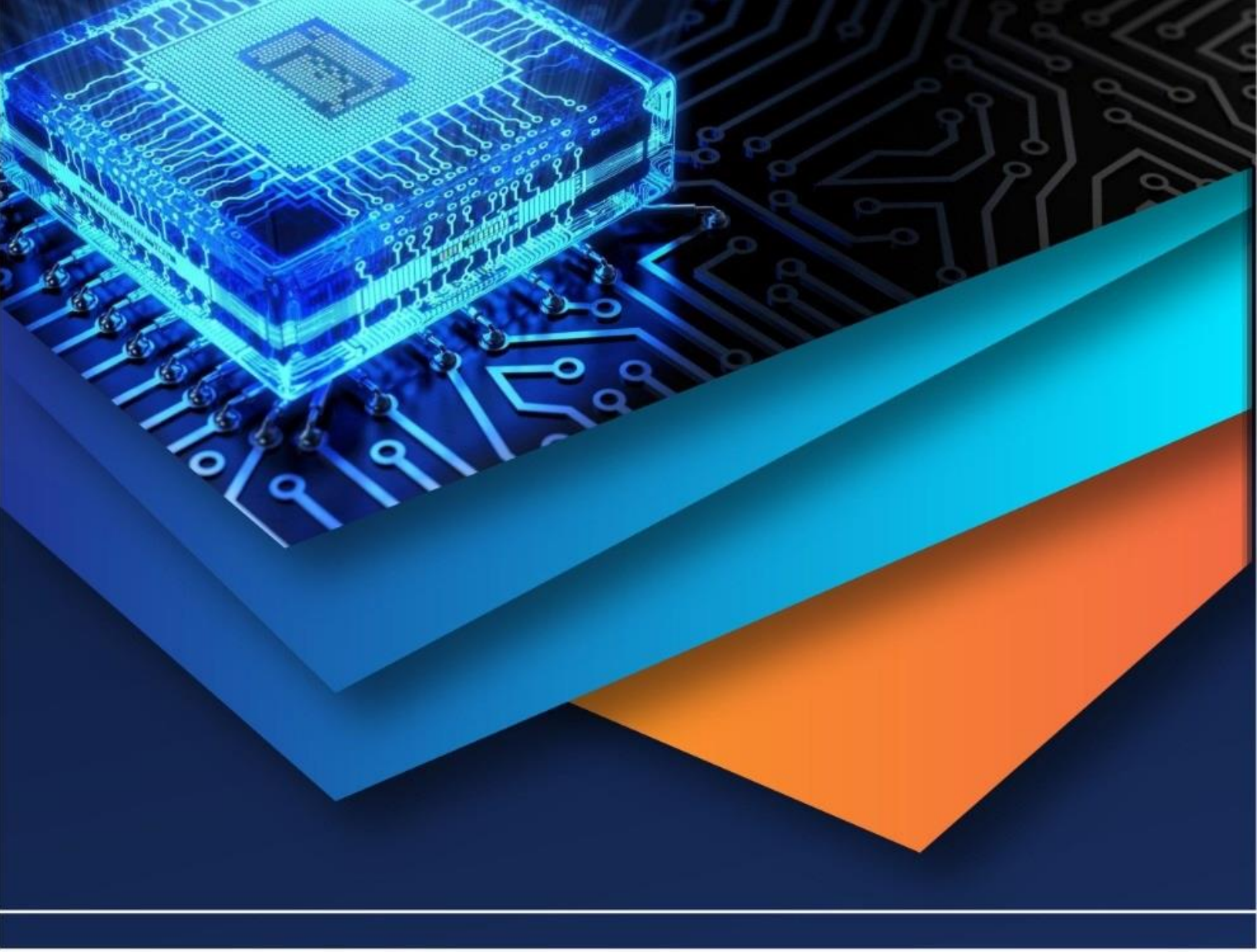
IV. CONCLUSION

Home Router security is an important factor of Network security .The base of this is the router which acts as a medium between a user and network and helps in establishing connection to the web. All the data from every environment goes through the router and then to its specific location. This device also perform NAT as well as behaves like a firewall to our environment.The variety of people connect to the web on the bases of quality and amount, the device which is used for a wide range of connection is the router. As the age of wired telephones are coming to an end and the increase of wireless internet connection raises some concerns in the security because as the wireless technology increases the issues with security also increases .

This paper is centered around the enhancement of the security of telephone circuit router and how doable it is, some of the security issues which an average user faces leading to the exploitation of the routers. If all the devices which are connected to the native network are also exploited , all these devices together can be used to create an advance botnet. The advance botnet have an advantage because the devices connected to this don not have a protection of a software and allows the attacker to take full control of the device by using the security flaws. As we know all the traffic is passed through the router and it can even monitor them which raises some security concerns like Identity theft that can gain any information regarding the user.

REFERENCE

[1] Terry Baume. Netcomm nb5 botnet, psyb0t 2.5l. Technical report, January 2009. http://www.adam.com.au/bogaurd/PSYB0T.pdf?info=EXLINK.
[2] Jesse Burns.Csrf - an introduction to a common web application weakness. *Information Security Partners, LLC*, 2007. https://www.isecpartners.com/files/CSRF_Paper.pdf.
[3] Gerald Combs. Wireshark website. Wireshark Website, February 2010. http://www.wireshark.org/.
[4] UPnP Forum. Upnp device architecture version 1.0. http://www.upnp.org/resources/specifications.asp. Gatespace. Gatespace cpe wan management



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY