ISSN (Print) : 2320 – 9798
ISSN (Online): 2320 – 9801

International Journal of Innovative Research in Computer and Communication Engineering
Vol. 1, Issue 3, May 2013

An Overview and Security in Home Area Networks

Sheikh Raashid Javid [1], Sheikh Mohsin Pervez[2]

Assistant Professor, Dept. of CE/IT, RK University, Rajkot, India[1]

Research Scholar, Dept. of CS, Rayalaseema University, Kurnool, India[2]

ABSTRACT: This paper relates to an overview and a need to establish security of home area networks (HAN). With the widely growth of broadband technology, home area networks have become more venerable to network attacks as many of the non-computing savvy households pay less attention to secure their networks due to lack of technical knowledge. This paper begins with an overview of home area networks and various security measures to be taken to secure a home area network from being attacked by intruders**.**

Keywords: intruders, security, ISP, SOHO Router, HAN, dialup, broadband.

I. INTRODUCTION

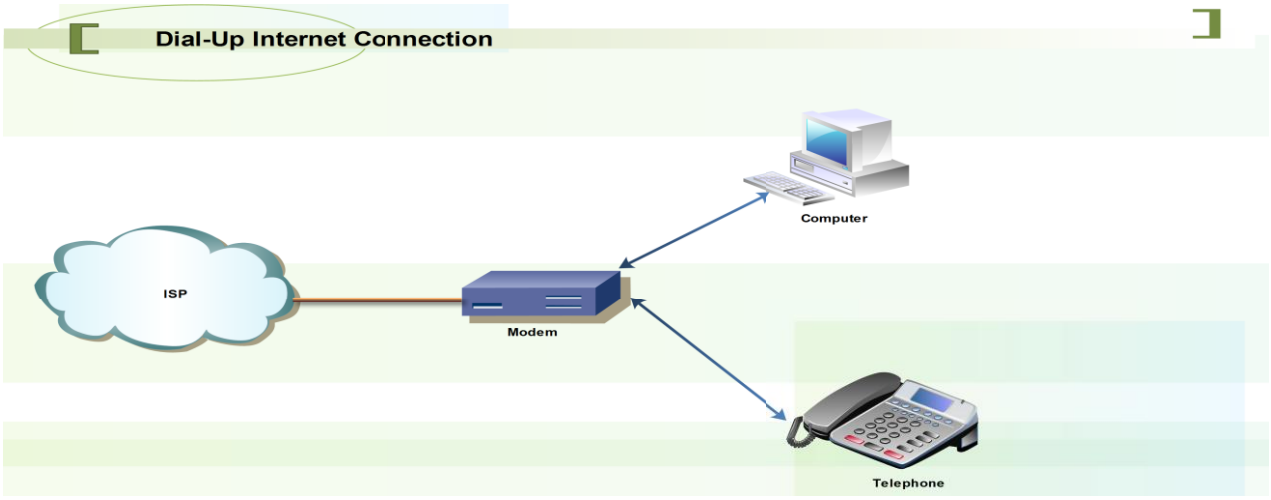
The simplest of home networks usually connects few networking devices so that resources can be shared between them using a single internet connection. The main objective of Home Area Networks (HANs) is that internet access can be provided to all IP enabled devices e.g. personal Computers, laptops, tablets, printers, scanners, play-stations etc. Resource sharing is another advantage of home networking, where various resources within a home such as videos, audios, files etc. can be shared among different users. With the concept of home networking, a computer with large storage can be used as a dedicated file server where files can be stored securely and accessed by the clients whenever needed. Another advantage of home networking is device sharing, where different devices like Printers, Scanners etc can be shared among different users, which is more economical. Also there is no need to purchase a public IP address for each device to go online but a user can purchase only one public IP address and assign this public IP address to a modem or a router depending on the type of an internet connection, while a modem or a router in turn assigns a private IP address to each device to access the internet using a concept of NAT (Network Address Translation).

This paper begins with an over view of home area network (HAN) in section 1, different types of internet connection in HAN are covered in section 2, section 3 discusses different devices used in home area networks, suggestions of HAN security are briefly covered in section 5 and section 6 concludes the advantage of taking security measures to secure a home networks from being attacked by intruders.

II. TYPES OF INTERNET CONNECTION

Home Networks can either use dialup or broadband internet connection to access the internet. The main difference between a dialup and a broadband internet connection is the manner in which a computer is connected to the Internet.

Dial-Up Internet Connection:



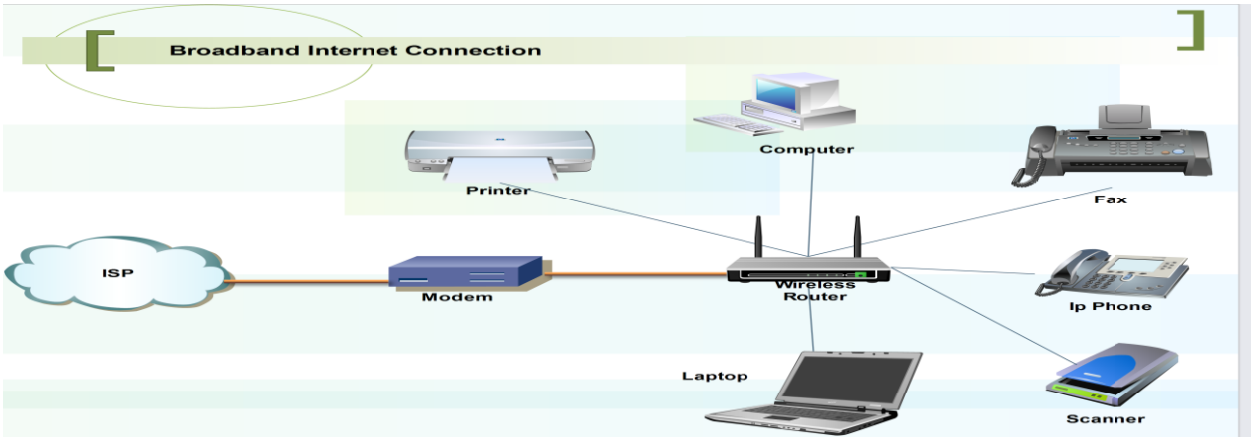
ISSN (Print) : 2320 – 9798
ISSN (Online): 2320 – 9801

International Journal of Innovative Research in Computer and Communication Engineering
Vol. 1, Issue 3, May 2013

In a dialup connection, a computer is connected to the internet through a telephone line. The modem dials an Internet Service Provider (ISP) and connects with a maximum speed of 56,000 bytes per second. Whenever a computer dials the ISP, it is assigned a different unique IP address after being authenticated. While using a dialup connection, we have to pay for a local call whenever we dial to connect to the internet. A phone line is engaged as long as we are using the internet, thus only a phone or the internet can work at any time and both can't work simultaneously. But with a broadband internet connection both the phone and the internet can work simultaneously also there are no dialup costs in a broadband internet connection. A dialup connection doesn't need a complex infrastructure; it just needs a computer, a telephone line and a modem. A modem can be external or it can installed inside a computer

Broadband Internet Connection:

The main advantage of a broadband internet connection is its very high speed, which is almost 10 to 20 times faster than the dialup internet connection and is useful to download large amount of data in less time. It is also more economical. Another important advantage of using the broadband internet connection is that there is instant internet access and there is no need to connect every time to go online.



Thus it's easy to access the information whenever needed and it's easy to check the mails and make phone calls instantly. The internet connection can be shared among multiple devices due to high speed of broadband internet connection. The speed of a broadband internet connection will be shared among all the devices, thus lesser the number of devices online, more the speed of the internet connection.

III. NETWORKING DEVICES IN HOME AREA NETWORKS

The main networking devices used in home networking to make an internet connection are.
Modem: A modem is a device which converts digital to analog signals and vice versa. Since a telephone line carries only analog signals but a computer works in a digital mode. Thus a modem converts analog signals of a telephone line into digital signals which can be read by the computer and also it converts the digital data of a computer into analog signals to be carried by a telephone line. Thus a modem acts as an interface between a computer and a telephone line.
Router: A router used in home area networks is known as SOHO (Small Office/Home Office) Router. It has many features which make it an ideal solution in home networking. Moreover if SOHO Router is configured properly during setup, it can secure a home network from being attacked by intruders to a large extent.

Features of a SOHO Router are

Switch: A SOHO Router has an inbuilt switch to connect various computers with an Ethernet cable. Thus there is no need to purchase a switch separately which is more economical.

Access Point: A SOHO Router works as an access point to connect wireless devices to the internet; it can also be used as a range extender to increase the size of a wireless network.

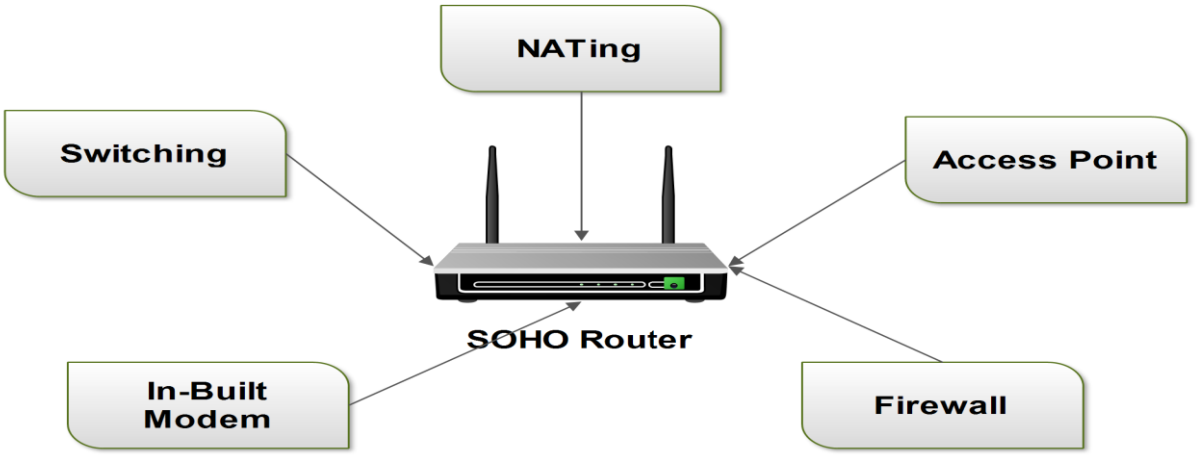
NAT: Since a SOHO Router assigns a private IP address to all the networking devices connected to it, but a private IP address is a non routable, and any device with a private IP address cant access the internet, thus the concept of NAT does the mapping of a private IP address with a public IP address which helps all networking devices connected to the Router to go online.

ISSN (Print) : 2320 – 9798
ISSN (Online): 2320 – 9801

International Journal of Innovative Research in Computer and Communication Engineering
Vol. 1, Issue 3, May 2013

Firewall: A SOHO Router has its own firewall software which prevents unauthorized access to the home network.

In-built Modem: Nowadays SOHO Routers have inbuilt modem to make the infrastructure very simple and to reduce the cost of purchasing a modem separately.



Features of a SOHO Router

.

IV. SECURITY IN HOME AREA NETWORKS

A SOHO Router is an important networking device in home networking, thus it needs to be made more secure to prevent un-authorized access to the home networks. Since a SOHO Router is pre-configured and ready to use, because a user may not know how to configure a SOHO Router or else he/she may not like to spend more time to configure a router. But the problem with default configuration is that it offers little security and may leave home networks vulnerable to attack. The wireless feature of a SOHO Router can be easily exploited by an intruder. Thus various security measures to prevent un-authorized access to home networks are.

Default Username/Password: Since a manufacturer of a Router sets up a default username and a password which are known to an attacker, thus the default user name should be changed and should be strong enough to prevent un-authorized access to home networks.

Default SSID: A SSID is a name of a network and it uniquely identifies a particular network, a wireless devices need to know the SSID of a wireless network to connect to that network. Manufacturers set a default SSID that identifies the device. Users also setup the SSID as the name of their company, thus an attacker can easily know about the business of that company and easily attack a company.

WPA2-AES Security: There are three types of security in a SOHO Router

1. Wired Equivalent Privacy (WEP)
2. WPA (Wi-Fi Protected Access)
3. WPA2 (Wi-Fi Protected Access 2)

It is always advisable to use WPA2 with AES, which is the most secure option, if WPA2 is not supported by a router then WPA is an alternative, but WEP is less secure option and should be avoided as far as possible.

Limit Network Coverage: It is always advisable to limit the broadcast coverage of a network to prevent the intruders from gaining accessing to a home network.

Power down the network when not in use: The wireless router should be turned off, when not in use to prevent the un-authorized and miss-use of a home network.

Disable Remote Management: This feature should be disabled in a router to prevent the intruders from accessing and changing the configuring of a router.

Update Firmware: The router firmware should be upgraded and updated in time to address most of the security vulnerabilities and loop holes in a router.

Limit DHCP reserved IP addresses: Since a router should assign a private IP address to a particular device to share the internet connection using a DHCP concept, thus the reserved IP address should be limited, so that a router can't

ISSN (Print) : 2320 – 9798
ISSN (Online): 2320 – 9801

International Journal of Innovative Research in Computer and Communication Engineering
Vol. 1, Issue 3, May 2013

assign an IP address to any device which is trying to get un-authorized access to a home network, the no of IP addresses reserved should be as many as the number of devices in need of internet access within a home network.

Universal plug and play (UPnP): This feature allows networking devices to discover and establish communication with each other on the network, this feature makes the initial network configuration easy but it should be disabled when not needed because a malware within a network could use UPnP to open a loop hole in a router firewall to let intruders in.

Turn-On Firewall: A router has an inbuilt firewall which should be activated and configured properly to allow authorized users to access a home network, It is advisable to create a black list for un-authorized websites, services etc. Also a firewall should be configured not to reply ping requests to prevent exposing a home network to intruders, thus firewall should be used to control both incoming and outgoing traffic.

Network Management Tool: An efficient network management tool can be used to monitor and manage a network and prevent intruders from having an un-authorized access to a network.

Some other security measures are

It is advisable to disable remote upgrade, un-necessary services and DMZ (Demilitarized zone) features in a Router.
Use anti-virus and anti-spyware programs.
The patching of OS should be done by downloading updates released by the manufacturer of the OS on time.
Change passwords frequently on all networking devices and make it strong enough so that it can't be easily guessed by an intruder.
The confidential files and folders should be encrypted to secure confidential data from being miss-used.
Enable MAC address filtering in a router so that an un-authorized client is not given a IP address to join a network.
Disable file sharing option in operating system to prevent un-authorized access of confidential

V. CONCLUSIONS

The findings of this study conclude that there are various security issues in home area networks (HAN). However most of the security issues can be addressed if HAN is configured properly at the time of setup. Since most of the home network users are either not much aware about the loop holes in home area networks or else they lack the knowledge of securing their home networks which results in the secure data being accessed and miss-used by the intruders, thus various security issues have been addressed in this paper and if these security measures are taken properly, then the home networks can be secured to prevent intruders from having un-authorized access to a home network.

ACKNOWLEDGMENT

We take this opportunity to express our deepest gratitude and appreciation to all those who have helped us directly or indirectly towards the successful completion of this paper.

REFERENCES

[1] Venkatesh, A. Kruse, E., & Shih C-F., An analysis of current developments and future trends, The Networked Home: Cognition Technology & Work, Springer London February 19, 2004.
[2] Rogers, L. R., Home Network Security, CERT® Coordination Centre, Software Engineering Institute, Carnegie Mellon University. USA. (http://www.cert.org/).
[3] Bischoff, G., Home Network Security. TELEPHONYonline.(http://www.centellium.com)
[4] Ciampa, M., Network Security Fundamentals, Thomson Course Technology, 2005, pp.1556-1561.
[5] Hira Sathu, Ranjana Shukla., Home Area Network: A Security Perspective, School of Computing and IT Unitech. New Zeland.
[6] Jay Beale, Caswell, Snort 2.1 Intrusion Detection, Syngress: May, 2004.
[7] Stuart McClure, Joel Scambray, George Kurtz, Hacking Exposed: Network Security Secrets & Solutions, McGraw-Hill Osborne Media:2003.
[8] Yong-Ming Haung, Ju Han Fu, Benjamin Tseng, Towards an online learning of "Network Security": A case Study, Department of Information Science, Hisng-Kuo University of Management, Taiwan.