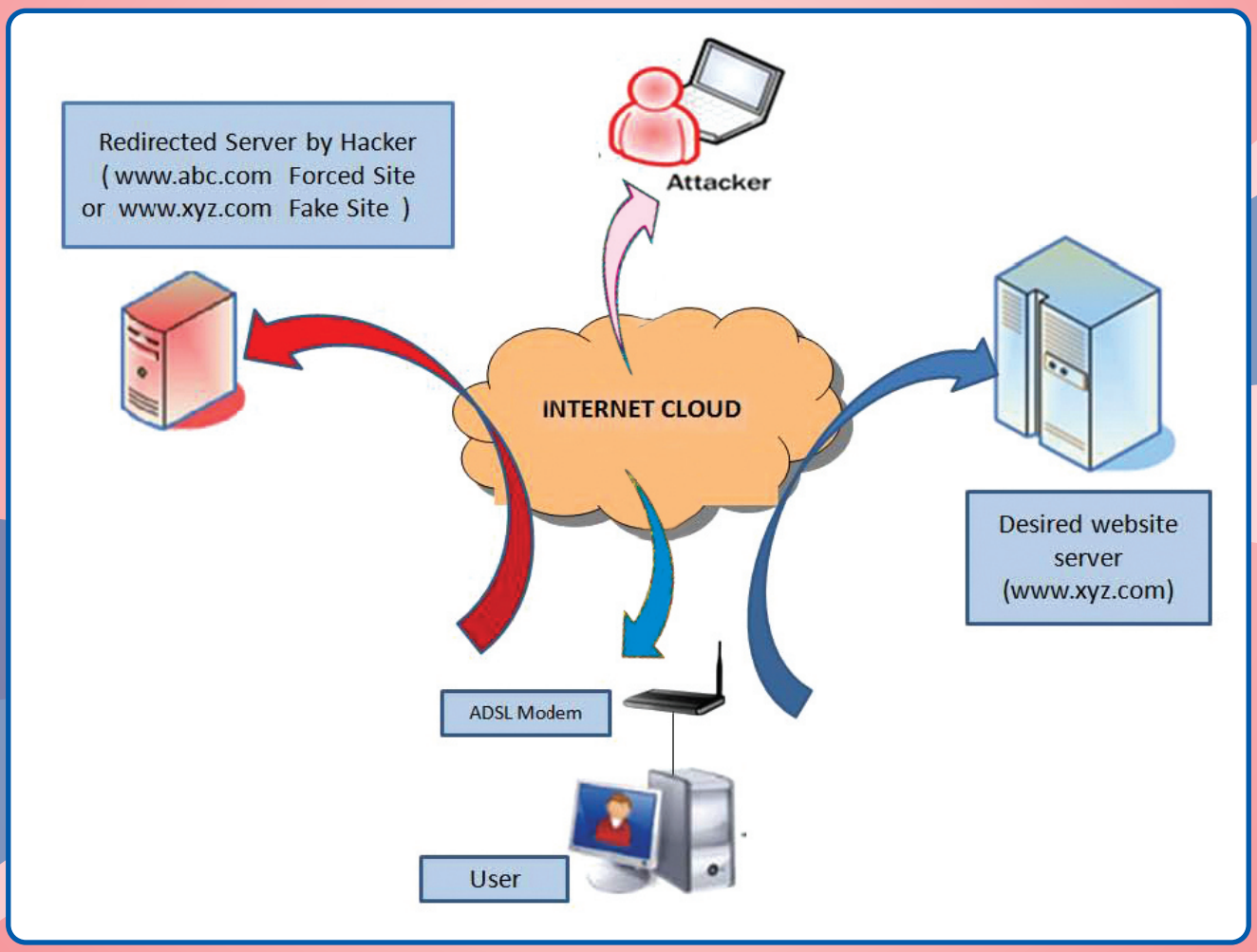
ISO 9001 : 2008

TEC

टी ई सी संचारिका
NEWSLETTER

VOL 18 | AUG 2014 | ISSUE 3

CYBER SECURITY : VULNERABILITY OF INTERNET USERS



(Typical Compromised ADSL based internet Connectivity)

ISO 9001: 2008
TELECOMMUNICATION ENGINEERING CENTRE

IN THIS ISSUE

1.0 Introduction:

Internet has emerged as the most useful technology of the modern times which has made our daily life increasingly dependent on the services which it offers, be it communications like email, face book, twitter etc or banking, online purchasing/ selling or e-governance or e-education. This dependency on internet has also seen spurt of cyber attacks on individuals and institutions.

If our internet connection is not secured properly, we are vulnerable to others eavesdropping to access our personal/ confidential information or to hijack internet connection or computer for their own purposes.

The computers which are always connected become more vulnerable to such attacks.

There are various ways of compromising security of internet connection. Readers might be aware about the Botnet discussed in last edition of TEC Newsletter on Cyber Security. This issue focuses on certain other threats and provide safety precautions for internet users.

2.0 Vulnerability check of internet connection on ADSL modem

With an Internet connection that's "always on" when we want to surf the Web, there is always a chance for hackers from around the world who sweep through thousands of random IP addresses exploit the weakness in the security.

At the end of Mar, 2014, there were around 18 Million Wireline Broadband subscribers in the country. All these subscribers use ADSL routers/modems to connect to the Internet. However, most of them are unaware of the fact that ADSL modem/router has a serious vulnerability which can easily be exploited by anyone with a basic knowledge of computer.

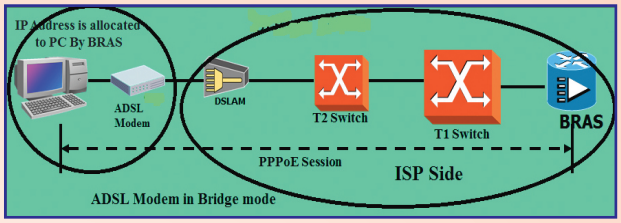
2.1 Configuration of ADSL modem

The ADSL modem can be configured for one of the following modes

1. PPPoA 2. PPPoE 3. MER
4. IPoA 5. Bridge

The most popular modes are PPPoE mode and Bridge mode.

(a) In Bridge mode, the PC interacts with the ISP & gets the public IP address, ADSL modem remains transparent. (figure1)



(Figure1)

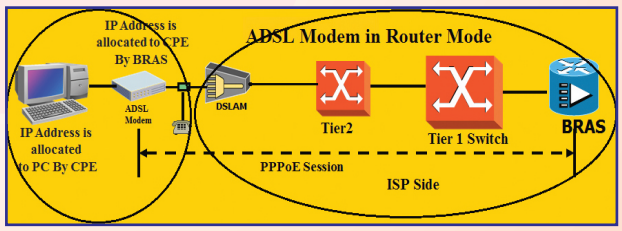
(b) In PPPoE (Point to Point Protocol over Ethernet) mode ,

I. ADSL modem interacts with ISP/network and gets the public address.

II. ADSL modem acts as a DHCP (Dynamic Host Configuration Protocol) server and provides private IP address to the connected PCs. The private IP address pool used is 192.168.1.0 with subnet mask 255.255.255.0.

III. ADSL modem acts as a NAT (Network address translation) device, providing a suitable port to the requesting PC from the LAN

IV. The above procedure is followed irrespective of ADSL modem's Wi-Fi capability.



(Figure 2)

2.2 Scanning of IP Address of IP Address

Every ADSL modem comes with a username and password using which it is possible to gain access to the router settings and configure the device.

The vulnerability actually lies in the **Default username and password** that comes with the factory settings. Usually the ADSL modem comes preconfigured from the Internet Service Provider and the users do not bother to change the password later. This makes it possible for the attackers to

gain unauthorized access to the router and modify its settings using a common set of default usernames and passwords. One can find a large number of free software on internet, which can be used for scanning of IP addresses.

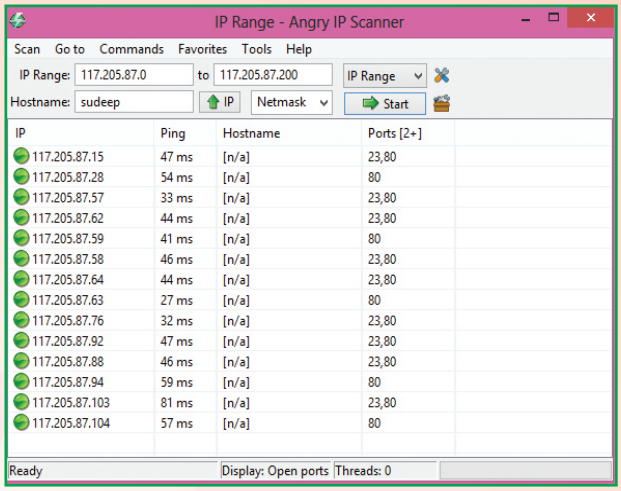
Some of the free downloadable software are listed below:

(a) Advanced IP Scanner
(b) Angry IP Scanner
(c) IP Tools
(d) Network Scanner

2.3 Verification of vulnerability of an ADSL router:

2.3.1. If a broadband user with ADSL connection wants to verify what has been said in para 2.2 above following procedure may be used.

1. There are a large number of sites which will display public IP address and user can note the public IP address.
2. In figure 3, for demonstration purpose, a screenshot of Angry IP Scanner software is shown. When user opens Angry IP Scanner , there is an option called **IP Range**, in which user can enter the range of IP addresses to be scanned.
3. If IP address is 117.192.195.101, user can set the range say 117.192.194.0 to 117.192.195.255 so that at least 200-300 IP addresses can be covered in this range.
4. After this, under the **'Tools'** menu, user can see the option of **'Preferences'** and select the tab **'Ports'.** Port number 20, 21, 23 and 80 are some of the ports which are normally open & one or all of them can be scanned. Here for verification purpose only one port i.e. 80 is selected. Under **"Port selection",** user may enter 80 (for scanning of port 80). Now user may switch to the **'Display'** tab, select **"Hosts with open ports only"** and click OK.
5. Now user may **"Start"** the IP scan. After few minutes, it will show a list of IPs with Port 80 open. Now copy any of the IP from the list, paste it in your browser's address bar and hit enter. A window will popup asking for username and password. Since most users do not change the passwords, it would most likely work with the default username and password.



(Figure 3)

6. Another method for getting into ADSL is through port 23(TELNET). For verifying the user should scan the IP addresses using the **Angry IP Scanner tool** for port 23 and 80. In the picture shown in figure 3, port 23 and port 80 have been scanned for IP address block 117.205.87.0 to 117.205.87.104. and the last column shows the ADSL modems which have port 23/80 or both open.
7. Now , using any of the IP address which has port 23 open, one can try remote login on ADSL modem using the TELNET command.
8. On TELNET, one can again try getting into ADSL modem using userid as **admin** and password as **admin.**

2.3.2 Thus anybody can gain access to ADSL modem irrespective of ISP and modify the configuration of ADSL Modem or implant a malware if default password has not been changed.

2.4 Precautions to be taken by users

1. Change the password of the ADSL modem.
2. Check the DNS entries in the Modem and confirm from the ISP that the IP address mentioned in the modem belongs to ISP.

3.0 Various internet threats and possible remedial actions.

Following are various threats posed to the internet users and their possible remedial actions.

3.1 Fake antivirus messages

There may be many malicious program which show the "antivirus warning". This fake scan will always finds tons of "viruses".

If user clicks on the provided link then it will take user to a professional-looking website, complete with glowing letters of recommendation. There may be fake advertising and they ask for credit card number and billing information, etc. Any innocent user who falls prey to this trap would lead into serious trouble by divulging their transaction information such as credit card / banking information to an unauthorised person.

Required Action: As soon as any fake antivirus warning message is noticed the computer should be shut down. If a user wants to save anything before power down he can do so. Boot up the computer system in Safe Mode, without internet connection and try to uninstall the newly installed software or restore system to a state previous to the exploitation by malicious program. If successful, test the computer in regular mode and make sure that now the fake antivirus warnings are not appearing. Then follow up with a complete antivirus scan.

3.2 Unwanted browser toolbars

This is probably the second most common sign of exploitation. New multiple toolbars may appear on the browser with the names that seem to be helpful; it's advisable to dump them unless these toolbars are from well-known /recognised sources.

Required Action: Most browsers allow the user to review installed and active toolbars. User can remove any of these, in case of doubt.

This can be removed by changing the setting of the browser. If the bogus toolbar still persists, go to the setting of browser and select the default settings. Even this doesn't work, follow the instructions listed in 3.1.

User can usually avoid malicious toolbars by making sure that all software in the PC/ laptop is original and fully updated.

3.3 Redirected Internet searches

Many hackers make their living by redirecting the user's browser somewhere else than the one user intends to surf. The hacker gets paid by getting the clicks to this diverted website, often the owner of these diverted sites doesn't know that the clicks to their site are from malicious redirection.

User can spot this type of malware by typing a few general words (for example, "puppy" or "goldfish") into Internet search engines and check whether the same website appears in the results or some other irrelevant sites appear repeatedly (almost) on every search. Unfortunately, today many redirected Internet searches are well hidden from the user through use of additional proxy servers and user do not receive any alert from these fake site and result are taken as a right search/query.

Required Action: Generally this malicious redirection problem can be solved by removing the bogus toolbars & browser, and also the action mentioned above in 3.2.

3.4 Frequent Random Pop-Ups

This is one of the most worrying problems when user gets random browser pop-ups, even from the website that does not normally generate them. This means that system is compromised. Sometimes a message may appear through that pop ups that one's system is hacked.

Many a times these pop ups, whether from legitimate or other websites, can bypass anti pop-up mechanism of the browser & appear on the user screen.

Required Action: Typically random pop-ups are generated by one of the three previous malicious mechanisms noted above in 3.1, 3.2 & 3.3. User needs to get rid of fake toolbars and browser if he wants to get rid of the pop-ups.

3.5 Fake emails from friend's email account

Lately, it has become very common to receive an email from known friend's/acquaintance's email id., but actually it is a malicious emails generated by hackers.

A decade ago email attached viruses were very common. These attached malware programs used to look into user's email address book and send malicious emails to each & every address from the address book.

But these days the hackers are sending fake emails to selected addresses of friends from address book, thus not giving any impression of system being hacked.

These days malware programs and hackers have another options, they often pull email addresses and contact lists from social media sites.

Required Action: If one gets information about emails being received by his acquaintances/ relatives from his email account, which he has not sent, then user should immediately notify to all concerned about his compromised account. This should be done to minimize the damage being done to others by this modus operandi. Subsequently, user must contact the online service of such compromised email account. Most online services do have facilities to tackle such maliciousness and can quickly get the account back under your control with a new password in a few minutes. Some services even have the whole process automated. A few services even have a "My friend's been hacked!" button that let your friend to start the process. This is helpful when your friend comes to know that your account has been compromised.

Subsequently user should immediately run a complete antivirus scan on his computer. He must also check for unwanted programs and toolbars installed in his system. Also follow the procedure mentioned above in 3.4.

3.6 Online Passwords Change Intimation

If a user receives a message about change in his password, which was not done by him, it is sufficient for believing that either his system is hacked or the online service is hacked. This particular scenario normally happen when the user has responded to an authentic-looking emails (Phishing) or other websites which might have prompted the user to change their password.

The hacker/attacker collects the information from user log and change the password & other information to make the recovery complicated and then uses one's account to steal valuable information about the user and/or his relatives/friends (while pretending to be the user).

Required Action: Genuine websites rarely send emails asking user to provide their logon information.

When in doubt, go to the website directly (don't use the links sent to you through email) and verify if the same information is being requested when user log on using the legitimate method.

User can also call the service via their phone line or through email to report them about the received phishing email or to confirm its validity.

3.7 Unexpected Software Install

Unwanted and unexpected installed software is also a major sign of likelihood that the system has been hacked. In the olden days, the malware (mainly the computer viruses), used to modify the other legitimate programme and hide themselves.

But now a days, these malware programmes like Trojans & worms, typically install themselves like legitimate programs, and by doing so they create a very thin line between authenticated programmes and thus can even escape from the courts of law.

Most of the times, these unwanted software get legally installed along with other downloads/ programmes, by making user to accept the agreed terms & conditions.

Required Action: Many programmes are available which will show the entire installed programme that automatically starts them when user PC is restarted. Most malware programme can be found here, which can be selectively disable programs and one can selectively disable them.

User must read the license agreements before downloading / installing programs which normally states that they will be installing one or more other programs also.

Here, user should unmark (deselect the right option) and disable other options, for which he is not sure. If user is not in a position or not able to take the decision about legitimacy of programme /software, then user must disable the unrecognized program and reboot the PC.

3.8 Money is missing from your bank account

Sometimes user gets a message on his mobile or an email from bank/financial institution about some transaction of money from his account, which was not done by him. In some cases, users may be lucky as financial institutions may agree to replace the stolen funds (especially if they can stop the transaction before the damage is truly done). However, there have been many such cases where the courts have ruled that it was the customer's responsibility to prevent from fake transaction done by hackers.

Required Action: For prevention of this type of problem, firstly user must avail the transaction alerts facility on each stage from financial institution that will alert him if something unusual is happening (like password change, access time, adding a new account as beneficiary etc).

Many financial institutions allow the user to set thresholds on transaction amounts, and if the threshold is exceeds or it goes to a foreign country, user will be informed. Unfortunately, many times the hacker/attacker reset the alerts or their contact information before they try to steal money. Therefore, user must ensure that whenever contact information or any alert information/ choice is modified, their financial institution must send an alert.

3.9. Most malicious hacking originates from one of three vectors:

Unpatched software, running Trojan horse programs, and responding to fake phishing emails.

Over and above everything stated here, self discipline, i.e. not to open unsolicited mail and not to open any link sent through unsolicited mails whatsoever be the type of allurement, is the best policy.

4.0 TEC Releases New Format for GR/IR/SR/SD

The format of content for documents issued by TEC including GR, IR, SR, SD and TSTP have recently been standardised to maintain uniformity across all Headquarter groups of TEC. The cover page of following documents has been given a new look with pattern in various shades of distinctive colour as below:

- Generic Requirements : Green
- Interface Requirements : Orange
- Service Requirements : Move
- Standard Requirements : Blue

(New Look of TEC Documents)

(Shri A K Mittal Sr DDG TEC and other DDsG of TEC on the occasion of release of documents)

Activities at NTIPRIT

1. In-service Courses for DOT Officers

i. Two day Seminar on Greening the Telecom for sustainable Development

ii. Three day course on Cyber Security

2. Induction courses for Officer Trainees

i. Training in Vigilance & Disciplinary Proceeding, PSTN Switching, Telecom Infrastructure, Optical Communications, Radio Communications, Satellite Communications, Hindi, Disaster Management, Ethical Issues in Public Administration, Data Communications conducted as a part of Induction programme for ITS 2012 batch.

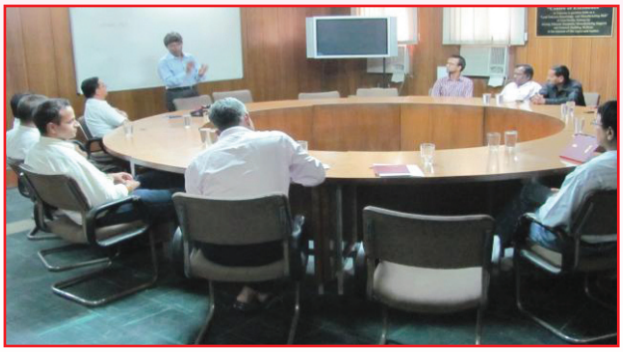
ii. Six week management, Acts & Laws training conducted for ITS-2010 batch at IIPA New Delhi

3. Trainings undergone by NTIPRIT Faculty

i. Two faculty members attended 'Design of Training' (DoT) course at Uttaranchal Academy of Administration (UAoA), Nainital from 16-06-2014 to 20-06-2014

ii. Three faculty members attended 'Direct Trainer Skills' (DTS) Course at Uttar Pradesh Academy of Administration, Lucknow from 23-06-14 to 27-06-14.

हिन्दी कार्यशाला : दूरसंचार अभियांत्रिकी केन्द्र में दिनांक 30.06.2014 को एक हिन्दी कार्यशाला का आयोजन किया गया। अतिथि वक्ता श्री अमित प्रकाश, उप निदेशक (रा.भा.) द्वारा खेर आयोग, राजभाषा अधिनियम-1963, राजभाषा नियम 1976, संसदीय समिति की पहली बैठक तथा इसकी अध्यक्षता किसने की एवं फाइलों पर नोटिंग करने आदि के बारे में बारीकी से बताया गया।



कार्यशाला में भाग लेते हुये अधिकारी एवं कर्मचारीगण

Approvals from APR 2014 to JUN 2014	
1	M/s Cisco Systems India (Pvt.) Ltd.,
1.1	Router ,CISCO ASR 1002-X
2	M/s NEC Infrontia Corporation
2.1	TDM-PABX,SV8300
2.2	TDM-PABX,SV8100
2.3	PABX,SV8500
3	M/s Hewlett Packard India (Sales) Pvt.Ltd.,
3.1	G - 3 FAX Machine, SNPRH-1203
3.2	G - 3 FAX Machine, BOISB-0906-00
4	M/s Huawei Telecommunications (I) Co.Pvt Ltd.
4.1	Transmission Equipment,OptiX OSN550
4.2	Transmission Equipment,OptiX OSN550
5	M/s Telecom Network Solution Pvt. Limited
5.1	40 M Tower for Cellular Systems,BSNL-T40-ANG-TNS-Y25
6	M/s Samsung Electronics Co.Ltd.
6.1	G - 3 FAX Machine, Xpress C460FW
6.2	Terminal for Connecting to PSTN,HS2032
6.3	Terminal for Connecting to PSTN,HS2016
6.4	Terminal for Connecting to PSTN,HS2064
6.5	G - 3 FAX Machine,C463B
7	M/s Centre for Development of Telematics,
7.1	G-PON,CDOT GPON
8	M/s Avaya India Pvt.Ltd.
8.1	PABX,IPO 500V2
8.2	PABX,Avaya Outbond contact Express
9	M/s Sunren Technical Solutions Pvt
9.1	G3 Fax Card,LEX-M03-001
9.2	Terminal for Connecting to PSTN,SL THS2128
9.3	Terminal for Connecting to PSTN,SL Team Connect CU1
10	M/s Nokia Siemens Networks Pvt. Ltd
10.1	Switching Node with Network-Network Interface at 2048 Kbits,DX200

Important Activities of TEC during APR 14 to JUN 2014

Sub DCC cum MF conducted on

- IR on LAN Switch, Firewall system
- IR on Data interface to G.703 converter
- IR on UTP to Optical converter
- IR on setup box,
- IR on IP based media gateway

White paper/study item issue

- Voice over LTE

Representation of TEC in training/ Seminar/ meetings

- 4th Annual LTE Summit 2014
- 8th international Conference on LTE
- M2M Communication
- Intelligent Transport System
- Next Generation Cyber Threat
- Greening the Telecom for Sustainable Development

ISO 9001:2008

Certifications
issued by TEC
Type Approval (TA)
Interface Approval (IA)
Certificate of Approval (CoA)

Visit

www.tec.gov.in

Regional TEC Contact :

Eastern Region	:	**033-23570008**
Western Region	:	**022-26610900**
Northern Region	:	**011-23329464**
Southern Region	:	**080-26642900**

Other Activity

- NWG meeting for ITU-T Study Group 5 & 17 held in TEC
- Testing of CDOT GPON for IPv6 Ready Logo
- IPv6 Ready Logo Examination of HP Laser Jet Series of Hewlett Packard

Approvals issued by TEC during the period from APR 2014 to JUN 2014

Interface Approvals..... 19
Type Approvals 2
Certificate of Approval.....0

टी ई सी संचारिका	:	दूरसंचार इंजीनियरी केंद्र
अगस्त 2014	:	खुर्शीद लाल भवन
भाग 18	:	जनपथ
अंग 3	:	नई दिल्ली 110001

Editor : Sunil Purohit, DDG (S) Phone : 23329354 Fax : 23318724 Email: ddgs.tec@gov.in