I.3: Developments in Networking and Communication at RRCAT

A) Email service related developments and enhancements:

1) Design, development and deployment of setup for access of RRCAT emails over Internet

A secure webmail setup has been designed, developed and deployed in the Internet DeMilitarized Zone (DMZ) for secure access of RRCAT email service over Internet. Secure hyper text transfer protocol, Two Factor Authentication (2FA) and **C**ompletely **A**utomated **P**ublic **T**uring test to tell **C**omputers and **H**umans **A**part (CAPTCHA) techniques have been used for enhancing security of the conventional webmail setup. Conventional login name and password has been used as the first factor of authentication. One Time Password (OTP), prefixed with a code, has been used as the second factor of authentication. Figure I.3.1 illustrates the first page of the webmail setup.

Figure I.3.1: Login page of the secured "Email access over Internet" setup

Prior registration of the user is required for successful login. The user registration can be done from within RRCAT campus only.

Figure I.3.2: Authentication page for registration to secured "Email access over Internet" service

Required number of OTPs along with a OTP prefix code (to be memorized), can be generated by using the registration page as shown in figure I.3.3.

Figure I.3.3: Form for filling up user details and generating OTPs

Squirrelmail, the open source webmail package, has been modified to support OTP based authentication, as per our requirements. Figure I.3.4 illustrates a snapshot of the failed login page, generated due to wrong OTP entry by the user. As can be clearly seen, the page displays the current OTP index value that the user is expected to use.

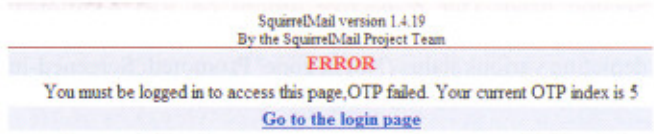

Figure I.3.4: Login error page with current OTP index value

Currently, the system has been released for limited users.

2) Design, development and deployment of Email Account Life Cycle management System (EALMS)

The design, development and deployment of **Email Account Life Cycle Management System (EALMS)** was completed. The system allows the email administrator to i) automate the entire process of email account life cycle management, from its creation to deletion and ii) to enforce email account management policies. The system has been developed, to create email accounts in three steps, namely, Request, Approval and Creation. Every step can only be performed after proper authorization. The ***"Request Module"*** allows the necessary email account request details, to be entered. This is primarily meant for initial level data entry. The ***"Approve Module"*** allows the email account moderator to approve the request generated using the "Request Module", after examining details of the 'to be created account'. The module has provisions to change the group and account validity parameters. The ***"Create Module"*** allows the email account administrators to create the approved account The account creation form is auto filled with the approved data. The ***"Delete Module"***, allows archiving of the directory of the "to be deleted account", before actual deletion. The status,

validity and the password expiration time values are changed automatically to mark the account as 'deleted'. The ***"Reporting Module"*** allows generation of reports in Portable Document Format (PDF) format, based on various search filters. Figure I.3.5, illustrates snapshot of the report module and figure I.3.6 illustrates a sample report generated using the EALMS.

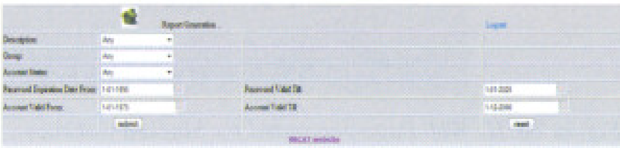

Figure I.3.5: Search filters of the report module

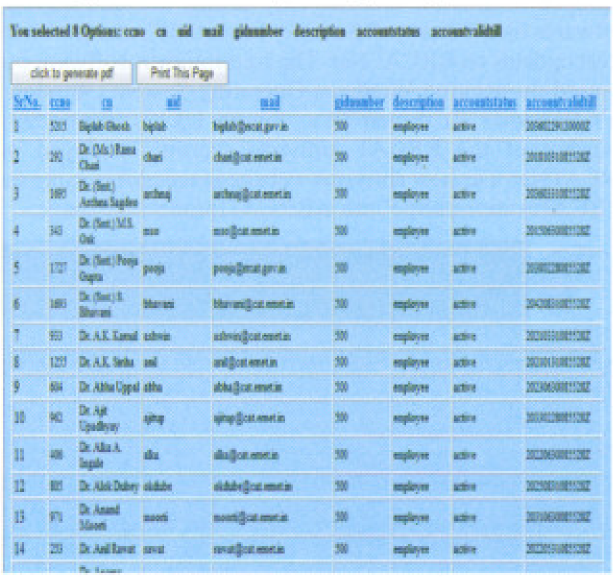

Figure I.3.6: Sample report generated using EALMS

B) Internet Proxy service related enhancements and developments:

1) Design, development and deployment of software for detection and blocking of malware infected PCs on RRCATNet

Software has been developed and deployed for detecting and blocking PCs generating unwarranted internet traffic on RRCATNet. Malware infected PCs have been found to access proxy servers quiet often and generate lot of logs, thereby reducing server performance by engaging the server processor in i/o wait states. The developed software, continuously monitors the proxy server log files for PCs generating excessive "TCP_DENIED" logs and blocks them. The software automatically blocks the malware infected PC from accessing the proxy server temporarily, by changing the routing table of the server. This reduces the load on proxy servers. The list of all such blocked systems is displayed on a web page, accessible to the proxy administrator, as illustrated in Figure I.3.7.

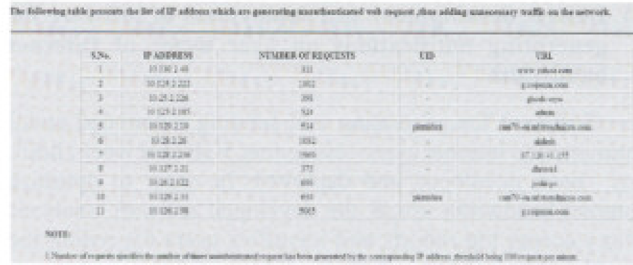

Figure I.3.7: List of PCs, blocked for Internet access, at some point in time, because of malware infection

The software also provides blocked users the option to unblock their PC, using a browser. The user is expected to ensure that the malware responsible for the blocking of PC, has been removed. To help user in finding the malware application in their PC, necessary help and free software are also provided in the URL accessible using the link "Internet Access Status" on RRCATInfonet. Figure I.3.8, illustrates a snapshot of the "Internet Access Status Page" in case of the blocked PC.

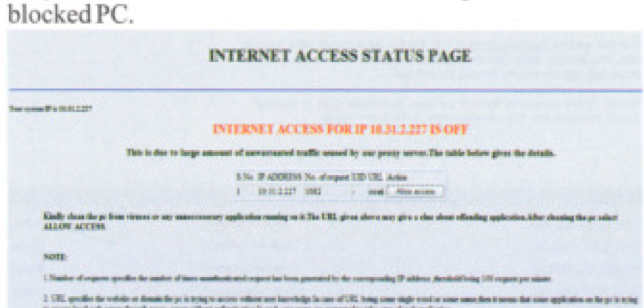

Figure I.3.8: Internet Access Status page as visible on the PC, blocked for presence of malware

The software also gives administrator an option for removing blocked PCs from the block list, either individually or in groups. Figure I.3.9 illustrates a snapshot of the administrator level blocked PC removal screen.

Figure I.3.9: Administrator level blocked PC removal screen

With the deployment of this software, the size of proxy server log files, have got reduced by a factor of 10 and there has been a remarkable improvement in the performance of the proxy servers.

2) Design, development and deployment of software for generating notifications on over usage of Internet bandwidth

Software for generating and sending automated email intimation to Internet users - exceeding 5GB (per week) limit, has been developed and deployed. In order to optimize Internet bandwidth usage, the developed software analyzes proxy access log reports and identifies users exceeding the weekly usage limit of 5GB. It generates emails with attachment of logs of Internet usage and intimates such users and their Head of Division/Independent Sections (HoD/IS). A sample email generated by the software for a user is as shown in figure I.3.10.

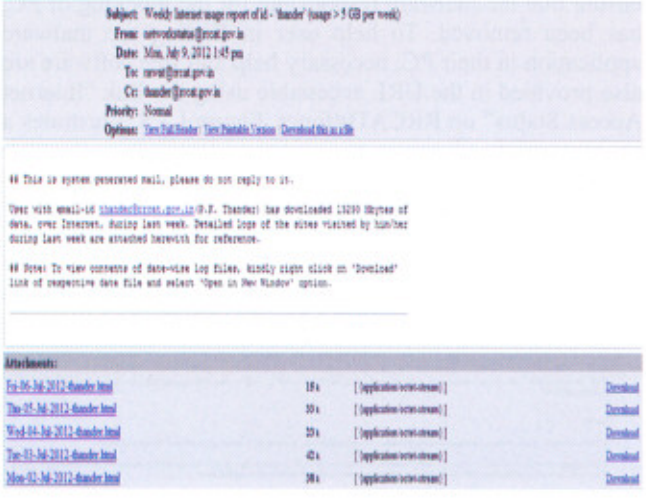

Figure I.3.10: Email of Internet Usage of a user

C) Centralized Antivirus setup related developments and management:

The mail gateways, the proxy server and the mail server on RRCATNet have been upgraded with the latest version of clamav (ver. 0-97.4-1) antivirus software, for improving the effectiveness of the antivirus setup.

The Internet proxy server setup at RRCAT provides high speed, authenticated and reliable Internet proxy services to the users at RRCAT. These proxy servers are upgraded with inline filtering of viruses, using the "havp" (ver. 0.92) and "clamav" (ver. 0-97.4) virus filtering softwares. The proxy servers are also upgraded to support domain and Uniform Resource Locator (URL) based blocking of Internet sites, as per the standard block lists, available in squidGuard (ver. 1.4) addon of SQUID proxy server. Hashed, world-wide database of blocked sites for filtering porn, sports, social networking and share marketing sites, have been integrated into squid servers to optimize Internet proxy server performance. Figure I.3.11 illustrates a snapshot of the 'Access Denied' page, generated for requests made for blocked sites/domains.

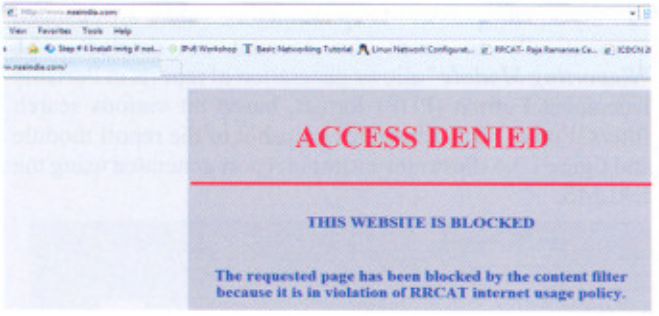

Figure I.3.11: Web Page generated for blocked websites

New antivirus website has been developed and deployed to provide users an easy access to free Antivirus softwares like "Microsoft Security Essentials", along with its latest updates on RRCATNet. The free antivirus software can be used on licensed Windows Operating System (Windows XP/ Windows 7) driven PCs. Figure I.3.12, illustrates a snapshot of the RRCAT antivirus website deployed on RRCATNet. The new antivirus website is accessible using the "RRCAT Antivirus Site" tab in RRCATInfonet homepage.

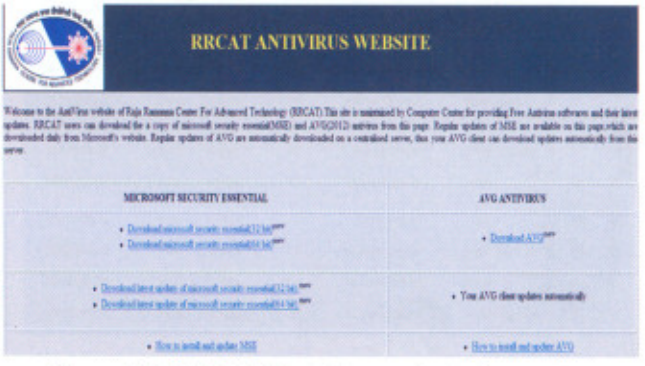

Figure I.3.12: RRCAT antivirus website home page

D) RRCATNet Planning, Expansion and Upgradation:.

16 port Local Area Network (LAN) in LCW extension building, 16 port LAN in CME Lab building, 12 port LAN in LWC building, 48 port LAN in Training School Hostel, 16-port LAN in New-CAP building has been commissioned and integrated to RRCATNet. Old-CAP building network has been provided a link from New-CAP building network using a 100 Mbps copper link. A new network rack has been installed in New Cryogenics building. Another rack has been installed in SCLS building with 44 ports terminated at rack end.

Augmentation of campus wide LAN with 40 ports in B-Block, 11 ports in ADL, 16 ports in A Block and A Block extension, 04 ports in Indus-1, 08 ports in MDL building, 16 ports in Photo Cathode building and 04 ports in Stores was completed. New 48 port switches were installed in ADL, B-Block, Indus-2-A and Indus-2-B building racks. Faulty Switches were replaced in AECS-old, CME, Guard house, A-block, C-Block and C1-Block buildings.

E) Expansion of communication network:

60 number of new telephone connections were provided at various locations in RRCAT campus including SCRF, LCW extension and New Cryogenics Building. Approximately 28 telephone connections were shifted to other location as per user requirement. New 4029 model digital phone equipments were provided to officers with SOH designation.

Reported by:
S. S. Tomar (tomar@rrcat.gov.in) and Anil Rawat

I.4: Developments in Library & Information Resources at RRCAT

A) Implementation of RFID Based Self Issue and Return System (LSmart-RFID) and Web-Centric Library Management Software (LibSys-7) in RRCAT Library

Library has installed Radio Frequency IDentification (RFID) technology based system for issue, return of books (LSmart-RFID) and book stock inventory. The library management software (LibSys-4) is also upgraded to web-centric library automation software (LibSys-7) for improved management of the library functions. This article briefly describes various components of this new setup, implementation approach, new facilities to users and the unique features of the new technology deployed in RRCAT Library.

RFID tags and stickers with RRCAT logo are pasted (affixed) in each book. RRCAT library currently has about 15000 books. Details of the book are encoded on the RFID tags and this encoded information also includes a 'Theft Bit'. An automatic self check-in/check-out system (RFID Kiosk) has been installed near the circulation counter to facilitate self issue and return of books by the users themselves. One Staff Station is also installed to issue and return books by the library staff members.

RFID Security Gate has been installed near the entrance gate of the library which makes buzzing sound if any book passes through the gate without proper issue (theft bit on). Thermal printers are inbuilt in the self check-in & check-out kiosk and staff station, to print check-in and check-out slips. RFID card readers connected to the kiosk and staff stations are interfaced with the Employee ID Cards, so that users can use their already issued employee cards to check-out and check-in library books.

Automatic generation of e-mail has been interfaced, so that system generated e-mails are sent to users email account on issue and return of books. A hand held Wi-Fi based shelf management system has been installed for stock checking and re-shelving. This facility can also be used to locate specific book on the shelf.

Components of the RFID system:

The system consists of various components: it mainly includes RFID tags (affixed in books), RFID Kiosk, Staff Station, RFID Security Gate, Server/Docking Station, Application Software, and Wi-Fi inventory reader. The system enables automatic identification and uses wireless technology. It uses radio waves to identify the items. A tag has a microchip and an antenna, in the microchip information about a book is stored. The RFID reader has an antenna, transmitter, receiver and decoder that communicate with tag and receives the data, whenever the tag comes in the field of the reader. The application software integrates the reader hardware with the existing library automation software. The software to interface with library management software is installed on the Server/Docking Station and it also acts as a communication gateway.

Self Check-in / Check-out Kiosk

RFID system facilitates the self check-in and check-out service of the library books. Every book (including books in Hindi Library) of library is affixed with RIFD tag. Users who want to borrow a book can themselves get the book issued using the facility at the RFID Kiosk (Figure I.4.1) installed near the Circulation Counter. It is an interactive station/kiosk with touch screen. User has to put his/her Identity Card on card reader and book(s) to be issued on RFID reader provided in the kiosk. It reads information pertaining to library member and books and check out is done in a few seconds by choosing appropriate option given on touch screen. Similarly user who wishes to return the books has to simply drop the book through RFID reader in the kiosk and the system automatically records return of book. There is option to have a transactions receipt in printed form and system also sends confirmations by email.

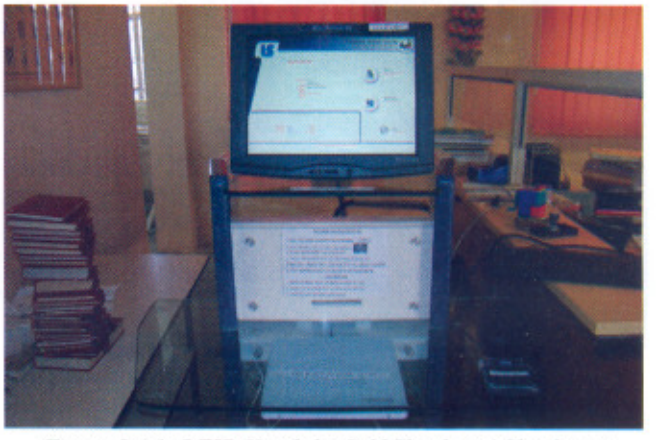

Figure I.4.1: RFID Kiosk for Self Check-in / Check-out