Minutes of CCCC Meeting held on December 16, 2010

Members present: Animesh Das, A. Pal, H. Wanare, M. Ranganathan, R. Sanakaramakrishnan, Y.N. Singh, Sanjay Gupta, K.S. Singh, Brajesh Pande, Gopesh Tiwari, Navpreet Singh, Aftab Alam, Saikat Hira, A. Chandra

1. The minutes of the previous CCCC meeting held on April 23, 2010, were confirmed.
2. Head CC made the following announcements: (i) The installation work of the new HPC cluster is almost completed and the system is being tested at present. The cluster is likely to be released to HPC users in next two weeks. (ii) The new 4x300 KVA UPS is also undergoing its installation and is likely to be operational in two weeks. The new cluster will be fully powered on only after the new UPS is in operation. (iii) CC has procured four GPU servers. These machines are being tested at the moment. (iv) The new Mail Storage is also in its final stage of installation and it is hoped that users will be migrated to this new storage by end of this month. (v) CC has ordered a number of HPC application softwares from DST HPC project. These are parallel softwares (like parallel Matlab, parallel NAG, Accelrys, Fluent, Gaussian Linda etc) meant to be run on the new HPC cluster. Further details of these softwares are available with CC.
3. Subsequently, the agenda item on Internet Gateway Security was taken up for discussions. The members were presented a document on the current set-up of Internet Gateway Security at IITK and proposed upgradation (See the Appendix). Head CC briefed the members about the issued being faced currently with the current system and the ground work that CC has done to explore technology options to upgrade the current set-up. The proposed gateway security solution from Cisco is considered to be the best product available in the market. The matter was discussed at length. On queries from some of the members, the technical issues of

authentication failure beyond five simultaneous users, SSL certification issues, inadequacy of log entries, no automatic switching between primary and secondary internet lines in the present set-up were clarified and possible solutions as included in the proposed upgradation were discussed. The members noted that the key advantages of the new set-up are: The solution can handle upto 2 Gbps of incoming and outgoing traffic, automatic shift to the backup link in case the primary link fails, inbuilt reputation filter, correlation engine to monitor logs and generate security alerts, no restriction on simultaneous authentications, strengthening of overall gateway security of IITK network. On another query on the commercial aspects of the proposed solution, the members were informed that the new solution from Cisco is expected to cost around Rs. two crores. The members opined that the Internet Gateway Security is a critically important issue and all possible measures must be taken to tighten it proactively. The members unanimously approved the proposed upgradation and asked CC to take the proposal forward toward its implementation.

4. Next, the issue of internet bandwidth was discussed. The current 1 Gbps 1:4) primary internet link is expiring on March 31, 2011, hence the process of purchase of the primary link for 2011-12 needs to start soon. The members expressed satisfaction with the current bandwidth, hence it was decided that no change in the bandwidth of the primary link will be considered for 2011-12. The members also felt that if the NKN link is stabilized and journal access is made available through this link, the current back-up link of 100 Mbps may not be required. Since the current back-up link will expire only in August 2011, it was decided to check the status of NKN link in summer 2011 before a call on the back-up link is taken regarding its renewal for 2011-12.
5. Under any other items, the members were informed of the present status of the ongoing work on LAN connections in residences. The members were informed that the Fiber cable laying has been completed. The

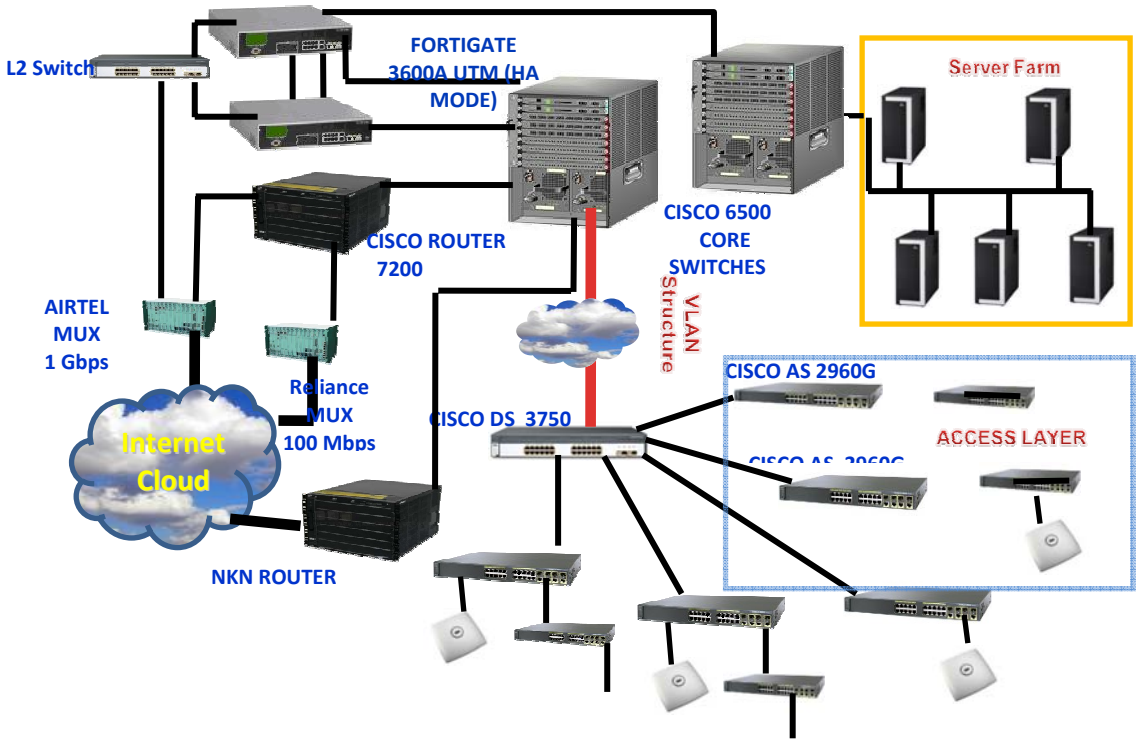
Network Pillars are being finished and they will be ready soon. CC will start providing the network connectivity by 15th January, 2011. First the Type 3 houses will be covered and then Type4, 5 and 6 houses will be connected. The work is expected to complete by March end.

A. Chandra
Head, CC

Appendix

Internet Gateway Security at IITK: Present Set-up and Proposed Upgradation

CC has been reviewing its cyber security aspects to prevent misuse of its facilities. In this context, CC Head had constituted a committee to review the existing cyber security aspects and make recommendations to improve them. The recommendations are included in the Annexure 1. Among other things, a key recommendation was that the Internet Gateway Security should be enhanced to reduce the threat of hacking attack from the Internet and misuse of facilities from the inside. It may be noted that CC has also been asked by Board to review and tighten its cyber security measures. Subsequently, CC initiated the measures to be taken to enhance its Internet Gateway Security aspects. The current Internet Gateway connectivity is as follows:



The issues being faced currently are:

- Latency: The current setup was designed for an average incoming and outgoing traffic of 200 – 300 Mbps. Currently the outgoing traffic reaches upto 600 Mbps and the incoming traffic reaches upto 400 Mbps. Whenever the traffic becomes high, increased latency (slowness) in Internet access is observed.

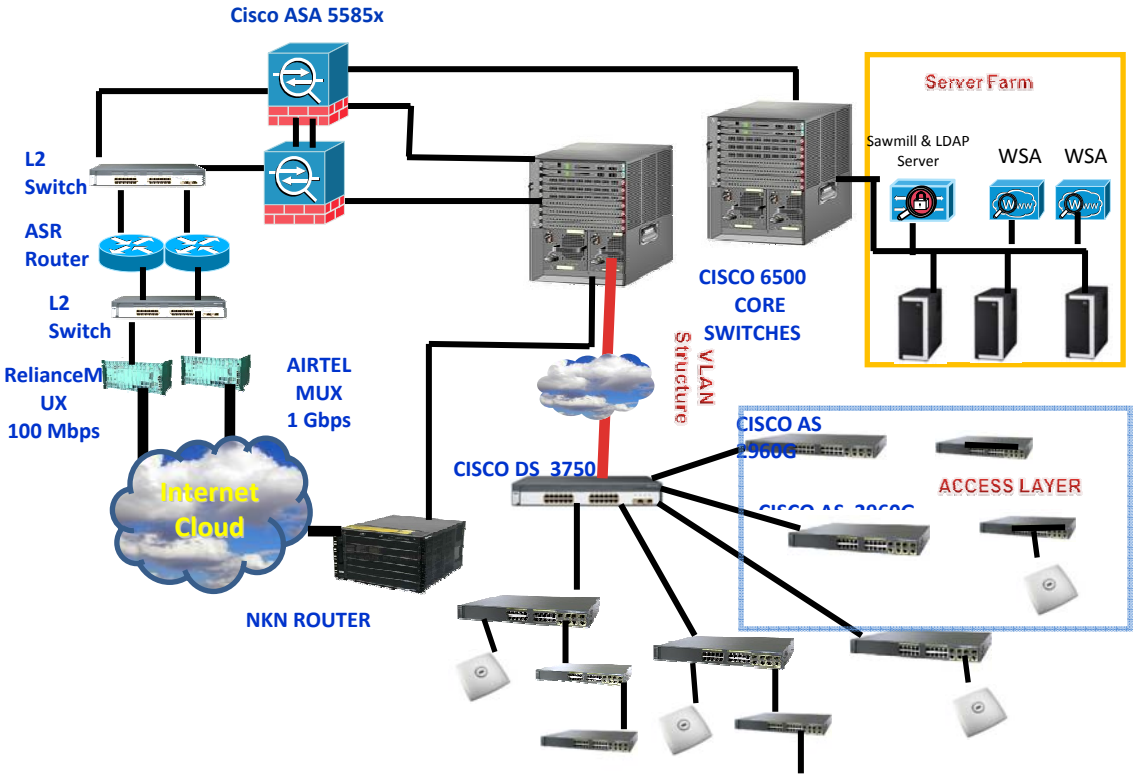
- Authentication Failure: The current Fortigate UTM allows upto 5 simultaneous authentication requests for direct Internet access. This is not adequate and needs upgradation.

- Correlation of Logs: There is no provision to correlate the logs to identify the security threats and attacks on the network. In case there is a misuse of any facility (inappropriate access of Internet or generating inappropriate facebook/orkut profile or sending inappropriate mail), it is very difficult to trace the culprit.

- Zero Day Attacks: There is no protection against zero day attacks. This problem is maximum for phishing and password collecting sites. Our users fall pray to such sites and it results in the users' machine getting compromised and at times generating large volume of spam mails from compromised machines.

- Automatic switch-over to Backup Link: In case the primary 1 Gbps link fails, the traffic, especially the mail traffic, does not automatically shift to the backup 100 Mbps link.

CC has done the necessary groundwork to explore technology options to upgrade its setup. Currently the Fortigate UTM appliance is being used for Internet Gateway security while all other networking products are from Cisco. Other international universities like MIT, Harvard etc. are using Cisco gateway security solution. Cisco gateway security solution is also considered to be the best product available in the market. In view of this, Cisco was invited for a presentation and discussion on a possible solution. Cisco made a presentation on October 05th, 2010 at CC during which a solution was proposed by Cisco. Based on the feedback and suggestions from the members present, the design was further modified and presented to all the members again by Cisco on October 13th, 2010. The revised proposed setup is:



The Fortigate 3600A appliances will be replaced by the following appliances:

1. ASR Routers: 2 Nos. of ASR Routers will provide Internet Leased Line connectivity for Primary and Backup links. They will work in automatic failover mode. They will also provide SSL VPN facility.

2. Cisco ASA Firewall and IPS: 2 Nos. of Cisco ASA Firewalls and Intrusion Preventions appliances will work in load balancing and failover mode and protect the network from any attack from the outside and also filter any malicious traffic being generated by internal machines.

3. Cisco WSA: 2 Nos. of Cisco Web Security Appliances will work in load balancing mode and will provide web filtering and proxy services.

4. Sawmill and LDAP Server: The LDAP server will be used for user authentication.

5. Cisco CSM: The Cisco Security Manager will provide event logging and reporting.

The advantages of the proposed setup are:

- The solution can handle upto 2 Gbps of incoming and outgoing traffic. So the solution is scalable to support two 1 Gbps or one 2.5 Gbps Internet leased line.

- The traffic will automatically shift to the backup link in case the primary link fails.

- The solution has inbuilt reputation filter which will automatically block newly released phishing and password collecting sites and protect the network from zero day attacks.

- The security manager will provide the correlation engine to monitor the logs and generate security vulnerability alerts.

- There is no restriction on simultaneous authentication requests being generated from any user machine.

- The solution will strengthen the overall gateway security for IITK Network.

The proposed upgradation proposal is to be placed before CCCC at its next meeting for discussions and necessary action.

Annexure 1

Minutes of the Meeting to Review the Cyber Security in Computer Centre held on May 17, 2010

In view of recent security breaches and misuse of Institute facility, the Board had asked CC to review its Cyber Security and take adequate measures to ensure that the Cyber Security is made robust to prevent any misuse of the Institute facility in future. In view of this, the following committee was constituted to review the CC Cyber Security and make recommendations regarding what measures should be taken to make the system robust:

1. Prof. Rajat Moona, Department of Computer Science and Engineering (Chairman)
2. Mr. Brajesh Pandey, Computer Centre (Member)
3. Mr. Gopesh Tiwari, Computer Centre (Member)
4. Mr. Navpreet Singh, Computer Centre (Convener)

The committee members met on May 17, 2010 and discussed all the existing issues and threats and suggested the following measures:

1. Block all the unused TCP/UDP ports for Internet Application Servers on the Internet Gateway Firewall. This will reduce the threat of hacking attack from the Internet.
2. Implement physical Access Control based in identity in all CC labs. In addition, install CC Camera in all the labs. This will help in restricting only authorized users to use the lab, maintain a log of who accessed the lab facility and monitor the activities in the lab.
3. Implement DHCP based IP address allocation policy. A machine should be able to use the network only if it has been allocated IP address through DHCP (which may be bound to MAC address in case of servers and lab machines). This will avoid duplicate IP address and IP address clash.
4. Implement Network authentication for both wired and wireless network. Make provision for issuing temporary ids for visitors. This will allow only authorized users to use the IITK Network.
5. Implement Wireless Intrusion Detection and Prevention system. This will reduce the threat of security breach through the wireless network.
6. Implement more secure authentication than currently followed scheme. This will reduce the threat of password cracking and hacking.

7. Implement better security for system logs on the individual servers. This will help trace the attack.

The committee recommended that the above mentioned measures should be explored from the point of implementation aspects and accordingly appropriate action should be taken to strengthen the Cyber Security in CC.

(Rajat Moona) (Brajesh Pandey) (Gopesh Tiwari) (Navpreet Singh)