Indian Institute of Technology Kanpur

Computer Centre

Minutes of the CCCC Meeting held on January 20, 2012, at 5 P.M. in CC Conference Room

Members present: Piyush Kurur, Bharat Lohani, Raj Pala, K.S. Singh, Brajesh Pande, Navpreet Singh, Aftab Alam, Gopesh Tiwari, Amalendu Chandra

1. Minutes of the previous meeting of CCCC held on November 16, 2011, were confirmed.

2. Announcements:

Head, CC, informed the Committee of the following recent developments:

(i) DD has approved the proposal for LAN connectivity to Type I residences. Order for network items has been placed except the switches whose order is currently being processed by the Purchase Section. It is expected that the LAN connectivity to these residences will be operational in next 4 months or so.

(ii) Updates on Software purchase: All softwares that were discussed and approved in the last CCCC meeting were subsequently ordered by CC. Except BeCN, all other software, namely COMSOL, Mathematica and Abaqus, have been delivered. BeCN is expected to be delivered in a week.

(i) Details of CCCC meetings are now available in CC website in the Intranet.

3. Charges for using CC facilities for workshops/conferences/courses (other than regular courses of IITK)

Head, CC, first provided the following background information to the members:

CC facility is free to all Institute students and staff for their email, web and computing (shell). For other users, such as project employees, summer trainees etc, cc charges an amount. The issue of charges for usage of CC facilities was discussed in CCCC meeting on December 15, 2009, and the minutes are available on CC website. For Short term courses, conferences, it was decided that charges 'to be decided on a case to case basis'. However, operationally, it is better to have some CCCC guidelines on the matter regarding how much CC should be charging for such usage of CC facility.

Subsequently, long discussions took place on the matter to explore various options and finally, the members suggested the following:

(i) One e-mail account and reasonable web space will be given free for a conference/symposium/course provided the conference/symposium/course is an Institute approved event (here course means short courses or schools approved by QIP/CDTE, not IITK regular courses).

(ii) For web accounts of individual participants to enable them to use Internet during their visit to IITK, Rs. 50 per participant will be charged for a conference/symposium/course of duration less than 15 days. Case to case basis charge will be made for such events of duration more than 15 days.

(iii) If such an event also uses CC PC Lab facility, charges at the rate of Rs. 10 per hour per PC will have to be paid to CC. All these amounts will be directly deposited to CC DPA.

4. Security issues for CC accounts

Head CC made a presentation on some recent happenings related to ssh security of CC accounts. The presentation is included in the Annexure. In summary, unauthorized ssh security keys were found in several user accounts. Since it was not clear how these keys came into those accounts, CC found out the exact number of such compromised accounts using scripts and has also been monitoring the frequency of further changes on a daily basis. The details

of CC observations are available in the Annexure. The outcome of the findings was discussed and it was decided to (i) delete the old suspicious keys from authorized keys files, (ii) monitor any subsequent changes in the authorized keys regularly through scripts and (iii) eventually shift to more secure authentication systems like ldap to make such attacks more difficult. It was also noted that shifting to a new authentication system will require coordination among various IT activities of the Institute.

5. Direct access to Internet without proxy authentication for some specific mirror sites

The issue of providing direct access to some specific mirror sites on Internet without proxy authentication was discussed in great details. The following decisions were finally approved by the members. (i) It was agreed in principle to open mirror sites of http/ftp/rsync access to Linux/FreeBSD/OpenBSD and sites of similar flavor without proxy authentication. However, it was agreed to open about 2-3 such sites to begin with and review the matter again after a few months. (ii) Open access to journal sites and also to sites like google,gmail,yahoo etc will not be allowed. (iii) A new site will be added to the list of open access only after review by CCCC. (iv) A site can be deleted from the list of open access by the System Administrator at any hint of misuse without having to wait for CCCC approval.

6. Continuation of CC accounts of retired/resigned faculty & staff and their access to various Lists

This item was deferred to the next CCCC meeting.

7. Any other relevant item(s).

Head, CC, placed a proposal for purchase of a mesh generator software (Gambit) which was received from Prof. S. Mittal through email with cc to the respective CCCC member. It was noted that this software was earlier there in CC but it was discontinued after Ansys took over Fluent. Recently, this mesh

generator has again been made available in the market. The members present in the meeting approved the purchase of this software subject to the availability of funds.

The Meeting ended with thanks to the Chair.

Amalendu Chandra

(Head, CC)

Annexure

Security of CC Accounts

SSH Security Concerns

SSH

- Protocol for secure communication
- Replacement of telnet, rlogin, rexec etc
- Communications between machines are encrypted
- Telnet and other protocols have password and communication exchange in plain text.
- Usually would ask for a user password.

SSH-Authorized Keys

- When an authorized key is found in the <home directory>/.ssh/authorized-keys a user who has that home directory is allowed a password-less access from a machine whose authorized key is present in this file.
- Among several attacks possible one could be to add a spurious key in the this file

Recent Discovery

- Recently suspicious authorized keys were found in several user accounts. (Thanks P Kurur, E-mail to Head, CC dated)
- It is not clear how these keys came into the accounts in the first place.
- This attack could just be a harmless attempt at trying out some security exploit but malicious attempt cannot be completely ruled out.

Action taken at CC end so far

A meeting was held at CC amongst CC Engineers and P. Kurur from CSE. The suggestions were:

Find out the exact number of such compromised accounts using scripts similar to that used by Dr. Kurur for detecting the attack.

Monitor the frequency of further changes on a daily basis

Report the incident to CCCC/users

Delete suspicious keys

Move to more secure authentication mechanisms such as ldap, kerberos

Details of CC observations

- Total accounts with suspicious keys 2791 currently
- Number of files with dt. 2010: 2726
- Number of files with dt. 2011: 64
- Number of files with dt. 2012: 1
- Files with Date 2010-Feb-16: 2648
- Likely that this happened on 16-2-2010 and some files changed since then and hence the date changed

Possible Prevention Measures

- Stop ssh / password-less ssh (subject to discussion)
- Monitor authorized keys regularly through programs (being done already)
- Shift to more secure authentication like ldap, kerberos to make such attacks more difficult (Needs coordination among various IT activities)
- **It is proposed that the suspicious keys be deleted from authorized keys files**.